
Advance Unedited Version

Distr.: General
27 February 2019

Original: 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*

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.

* Submitted after the deadline in order to reflect the most recent information.

Contents

	<i>Page</i>
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:
 - (a) 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.
 - (b) 24 communications to Member States raising matters concerning the right to privacy, and 14 press releases and statements.¹
 - (c) Official country visits to the United Kingdom of Great Britain and Northern Ireland (June 2018) and Germany (November 2018).
 - (d) Given keynote and other papers (**Annex 1**).
 - (e) 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.
 - (f) 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.

¹ 18 letters and 6 press releases were jointly issued with other Special Rapporteurs.

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”.*²

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”³

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.”

² Sieghart P., *Privacy and Computers*, Latimer, London, 1976 p.24

³ Cannataci Joseph A., *Privacy & Data Protection Law*, Norwegian University Press, 1987, p60.

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 2017⁴ 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 Committee⁵.

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

⁴ (A/HRC/RES/34/7, par. 2, adopted by consensus on 23 March 2017, 34th Session of the Human Rights Council.

⁵ CCPR /C/USA/CO/4, para. 22.

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.⁶

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/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:

- (a) Recent regional initiatives such as the EU's General Data Protection Regulation⁷ (GDPR) (effective 25 May 2018) and the EU's Police Directive⁸ (effective 6 May 2018), while important, are insufficient for extending privacy

⁶ 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/>

⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (OJ L 119, 4.5.2016, p. 1)

⁸ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.

protection to the field of national security, including the oversight of intelligence activities undertaken for national security purposes.⁹

(b) The modernisation of Convention 108¹⁰, 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 ecosystem 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

⁹ 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.

¹⁰ The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108).

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.¹¹ 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.¹²

39. The United Kingdom’s Investigatory Powers Commissioner’s Office (IPCO) issued a statement¹³ 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 rejection¹⁴ 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.¹⁵

(a) 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.

¹¹ <https://english.ctivd.nl/documents/publications/2018/11/14/index>

¹² 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%20reportjnt%2024247%2026914

¹³ <https://www.ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx>

¹⁴ https://edpb.europa.eu/news/news_en

¹⁵ [https://hudoc.echr.coe.int/eng#{"itemid":\["001-186048"\]}](https://hudoc.echr.coe.int/eng#{)

(b) 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:

(a) 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;

(b) 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;

(c) 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*”¹⁶ in relation to any personal information exchanged between intelligence services and law enforcement agencies within a country, and across borders;

(a) 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.

(b) Whenever possible and appropriate, the independent oversight authorities of both the transmitting and the receiving States should have immediate and automated

¹⁶ 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.

access to the personal data exchanged between the intelligence services and/or law enforcement agencies of their respective States;

(c) 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;

(d) 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 2018¹⁷ 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 Council¹⁸ and the General Assembly¹⁹ 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.²⁰

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.²¹ 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.²² The Human Rights Council has adopted resolutions highlighting the interdependent and mutually reinforcing relationship between democracy and human rights.²³

54. The Special Rapporteur integrates a gender perspective throughout the mandate.²⁴ Following three successful ‘Privacy, Personality & Information Flows’ regional

¹⁷ <https://www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and>

¹⁸ HRC resolution 34/7

¹⁹ UNGA (2014). Right to privacy in the digital age, A/RES/71/199

²⁰ Communication No. 2172/2012 2 December 2011, 17 March 2017, CCPR/C/119/D/2172/2012, par. 7.2

²¹ 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).

²² 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/

²³ 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>

²⁴ <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

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,²⁵ and recognition of the interdependency between the right to privacy and democracy.²⁶

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.²⁷ 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 LGBTIQI.

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. Cybermisogyny²⁸ and general cyber-abuse of individuals of non-binary gender are enabled by new technologies²⁹ 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. LGBTIQI youth for example, use the internet more frequently to engage in social media and networking than non-LGBTIQI peers, and are more likely than non-LGBTIQI youth to be bullied or harassed online (42% vs. 15%).³⁰

61. Despite the benefits of digital technologies,³¹ those most at risk were seen as women, girls, children, LGBTIQI individuals and communities³² especially transgender individuals, activists, gay teachers, human rights defenders, sex workers, and women journalists.

²⁵ For example, APC Submission 2018.

²⁶ For example, Privacy Commissioner of Canada, Submission 2018

²⁷ Privacy Commissioner of Canada, 2018, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

²⁸ LEAF 2014, <http://www.westcoastleaf.org/our-publications/cybermisogyny/>

²⁹ 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>

³⁰ 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.

³¹ Name withheld Submission 2018 referencing Horres, V. “Online and Enabled: Ways the Internet Benefits and Empowers Women

³² 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

62. LGBTQI individuals can experience also specific, unique risks such as ‘outing’, and abuse directly related to their gender identity.³³
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.³⁴
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.³⁵
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.³⁶
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.³⁷
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.³⁸ 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.³⁹
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.⁴⁰
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.⁴¹
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.⁴² Technologically facilitated violence combines issues of gender inequality, sexualised violence, internet regulation, internet anonymity, and privacy.⁴³

van homoseksualiteit - COC Nederland, and the International Lesbian, Gay, Bisexual, Trans and Intersex Association ILGA Submission 2018.

³³ Gender Perspectives on Privacy in Eastern Partnership Countries and Russia by the Eastern European Coalition for LGBT+ Equality

³⁴ 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/>

³⁵ Op cit Kazakhstan Feminist Initiative et al Submission 2018.

³⁶ Ibid.

³⁷ Osgoode School of Law, confidential submission December 2018.

³⁸ Eastern European Coalition for LGBT+ Equality Submission, 2018.

³⁹ L. v Lithuania; A.P. (2008), Garçon and Nicot v France (2017)

⁴⁰ Joint submission of Kazakhstan Feminist Initiative et al, 2018.

⁴¹ <https://www.usatoday.com/story/news/nation/2018/08/28/intersex-surgeries-children-california-first-state-condemn/1126185002/>

⁴² Dejusticia Submission September 2018.

⁴³ *Report of the Special Rapporteur on violence against women, its causes and consequences on online*

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%).⁴⁴

74. Domestic violence increasingly involves using smart home devices directed at women and dependents⁴⁵ which enable new ways to infringe privacy, reduce autonomy and self-determination at home,⁴⁶ or in communications.⁴⁷ Sometimes legal protections are inadequate⁴⁸ or there is a lack of police enforcement of breaches.⁴⁹

75. Cybermisogyny has been manifested on digital platforms.⁵⁰ 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.⁵¹

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.⁵²

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.⁵³

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.⁵⁴

79. In a number of countries, gender bias is evident in the higher degree of surveillance of those who identify as members of the LGBTIQ groups.⁵⁵ State surveillance of the LGBTIQ community has been facilitated in some countries through legislation. An example given was the Anti-Cybercrime Law enacted in Egypt in 2018.⁵⁶

violence against women and girls from a human rights perspective, A/HRC/38/47. 2018

⁴⁴ RMIT University, *Not Just 'Revenge Pornography: Australians' Experience of Image-Based Abuse*, May 2017.

⁴⁵ '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>.

⁴⁶ 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

⁴⁷ Mason, C. and Magnet, S., *Surveillance Studies and Violence Against Women*, *Surveillance & Society* 10(2) 2012; APC p13

⁴⁸ 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>

⁴⁹ Hadeel Al-Alosi, *Cyber-Violence: Digital Abuse in the Context of Domestic Violence*, *UNSW Law Journal* 40(4) 2017.

⁵⁰ Op cit LEAF

⁵¹ Women's Institute of Mexico City; APC Submission 2018.

⁵² Irish Civil Liberties Council

⁵³ de Justicia Submission 2018

⁵⁴ Franks, M.A., *Democratic Surveillance*, *Harvard Journal of Law & Technology*, Volume 30, Number 2 Spring 2017

⁵⁵ APC Submission, 2018.

⁵⁶ Joint International Submission, 2018; <http://www.loc.gov/law/foreign-news/article/egypt-president-ratifies-anti-cybercrime-law/>

80. While State surveillance is generally presented as targeting males,⁵⁷ counter-terrorism measures have been said to disproportionately affect women and transgender asylum-seekers, refugees and immigrants.⁵⁸

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.⁵⁹

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.⁶⁰ Facebook has 60% of this ‘social log on’ market.⁶¹ 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.⁶²

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 LGBTIQI people is the non-consensual sharing of health data, particularly HIV status.⁶³ The Grindr app for example, was found to contain trackers and share personal information, including users’ HIV status, with various third parties.⁶⁴

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.⁶⁵

89. Violations of women’s right to privacy during childbirth can be a powerful disincentive to seeking care for subsequent deliveries.⁶⁶

90. Technologies such as Google’s Street View, can affect health service usage by women through concerns about being identified using certain health services.⁶⁷

⁵⁷ Privacy International 2017

⁵⁸ Scheinin, M. 2010

⁵⁹ Franks, M.A., *Democratic Surveillance*, *Harvard Journal of Law & Technology*, Volume 30, Number 2 Spring 2017; APC Submission, 2018.

⁶⁰ The Economist Essay, Christmas Edition, December 2018

⁶¹ Ibid.

⁶² 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.fefel.is/sites/default/files/2016/Lyon,_D._\(2003\)._Surveillance_and_social_sorting%26_computer_codes_and_mobile_bodies%20\(1\).pdf](http://www.fefel.is/sites/default/files/2016/Lyon,_D._(2003)._Surveillance_and_social_sorting%26_computer_codes_and_mobile_bodies%20(1).pdf).

⁶³ Op cit Kazakhstan Feminist Initiative “Feminita”, et al.

⁶⁴ APC Submission, 2018.

⁶⁵ Malta Times, Saturday April 7, 2018 ‘New Health care clinic for transgender people in pipeline’, p5.

⁶⁶ 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

⁶⁷ C. Wahlquist, Protect us from anti-abortion protesters, say women's clinics in WA, *The Guardian*

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).⁶⁸

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.⁶⁹

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.”⁷⁰

95. One submission reported positive action by the app Grindr to reduce misuse aimed at entrapment of gay men.⁷¹ 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.⁷²

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.⁷³

97. Experiences of privacy breaches are not homogeneous; infringements can result in increased domestic violence for women, and discrimination for LGBTQI people.⁷⁴

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.⁷⁵

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.

International Edition, 25 January, 2018.

⁶⁸ The Charter of Human Rights and Principles for the Internet, Internet Rights and Principles Dynamic Coalition UN, Internet Governance Forum, 2014; APC Submission, 2018.

⁶⁹ CPRC Submission citing ‘Money’ CNN News in March 2018.

⁷⁰ <https://decoders.amnesty.org/projects/troll-patrol/findings>

⁷¹ Op cit Kazakhstan Feminist Initiative “Feminita”, et all. Submission 2018.

⁷² Electronic Media cited in Dejusticia Submission, 2018

⁷³ 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/; Case submissions to TGEU; and European Union Agency for Fundamental Rights, Violence against Women: an EU-wide survey. Main Results. 2015.

⁷⁴ GLSEN (2013), *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* In Joint International Submission 2018.

⁷⁵ AWAVA Submission, 2018.

100. Good practices to address sexual orientation and gender identity privacy issues were seen to be encapsulated in the Yogyakarta Principles+10.⁷⁶

Conclusions

101. **The Universal Declaration of Human Rights calls on “every individual and every organ of society” to promote and respect human rights.⁷⁷ 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.⁷⁸**

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,⁷⁹ 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.

⁷⁶ 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/>

⁷⁷ Preamble, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

⁷⁸ <https://www.ohchr.org/en/issues/discrimination/pages/bornfreeequalbooklet.aspx>

⁷⁹ Australian Competition and Consumer Commission, ‘Preliminary Report of Inquiry into Digital Platforms’, 2018.

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 fundamentals 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."⁸⁰

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.

⁸⁰ Special Rapporteur on the right to privacy, 2018 Annual Report to the UN General Assembly, Recommendation at 117(k), p21, A/73/45712.

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**
 - II. The human right to privacy: a gender perspective – report on submissions received**
 - III. Privacy and health data – draft guidance opened for consultation**
 - IV. Privacy metrics – consultation draft**
 - V. Good practices on bulk powers**
-

Annex 1: SRP International Keynote and Other Papers

1. 'Legal Framework Around the Right to Privacy', United Nations Office of the High Commissioner on Human Rights Workshop, 19-20 February 2018
2. United Nations Consultation on Big Data – Open Data, Sydney Australia, 27-28 July 2018
3. 'Hysteria or Hazard? Big data and what the UN thinks about your privacy', Grand Challenges, University of New South Wales, Sydney, Australia, 24 July 2018
4. 'Plugging the Gaps on Privacy Protection in Cyberspace', Melbourne University, Australia, 31 July 2018
5. 'Big data, privacy & AI Who is responsible for decisions made by machines? What exactly does our right to privacy look like in this digital day and age?' La Trobe University, Australia, 31 July 2018
6. 'Why the EU General Data Protection Regulation is relevant to Australia, and the UN dimension', Edith Cowan University, Perth, Australia, 2 August 2018.
7. 'What Does the General Data Protection Regulation Mean for Australia', International Association of Privacy Practitioners (ANZ Chapter) Sydney, Australia, 23 July 2018
8. 'The International Privacy Scene & Australia', International Association of Privacy Practitioners (ANZ Chapter) Melbourne, Australia, 1 August 2018
9. Moderator, 'New and Emerging Issues Around the Right to Privacy', United Nations Office of the High Commissioner on Human Rights Workshop, 19-20 February 2018
10. Panel: 'The Invisible Revolution: utopia, dystopia and the many faces of tomorrow', Australian Human Rights Commission Conference 'Human Rights and the Digital Era', 24 July 2018
11. Commentator: Australian Human Rights Commission Conference 'Human Rights and the Digital Era', 25 July 2018
12. Moderator Panel 'New and Hindsight Perspectives', UN Consultation on Big Data – Open Data, Sydney Australia, 27-28 July 2018

Annex 2: The Human Right to Privacy: A Gender Perspective¹

‘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’ – A Report of Consultation by the SRP Thematic Taskforce ‘Privacy and Personality’.

1. The framework for examining the right to privacy from a gender perspective is found in Universal Declaration of Human Rights, Article 12; the International Covenant on Civil and Political Rights, Article 17; Resolutions of the United Nations’ General Assembly and Human Rights Council, and the international human rights legal framework.
2. The UN Human Rights Council² and the General Assembly³ have noted that “violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and persons in vulnerable situations, or marginalized groups”. They 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 effects for women, as well as children and persons in vulnerable situations or marginalized groups.”
3. In 1994, the United Nations Human Rights Committee in *Toonen v. Australia* determined that it is a violation of the right to privacy to criminalise consensual same-sex relations between adults. In 2017, the Committee reiterated that the right to privacy covers gender identity.⁴ The importance of the right to privacy is evidenced by its referencing in decisions which de-criminalise consensual relations between same sex couples.
4. In India in 2018, the Supreme Court struck down Section 377 of the Indian Penal Code, which punished same-sex relations with imprisonment, as discriminatory and unconstitutional.⁵ Over 70 countries however, still criminalise consensual same-sex relations thereby infringing the privacy rights of same sex couples.⁶
5. 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 goes to the innate dignity of the person, and it facilitates the enjoyment of other human rights.⁷ It is a right of all, not restricted to the public sphere, and is an issue about the common good as much as it is about individual rights.⁸
6. Privacy, as a necessary precondition for the protection of fundamental values including liberty, dignity, equality, and freedom from government intrusion, is also an essential ingredient for

¹ The term ‘gender’ is used here to recognise society’s attribution of roles to biological characteristics. The term is not a synonym for ‘women’ but inclusive of sexual orientation, gender identity, gender expression and sex characteristics.

² HRC resolution 34/7

³ UNGA (2014). Right to privacy in the digital age, A/RES/71/199 https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/199 United Nations High Commissioner for Human Rights (2014). The right to privacy in the digital age, A/HRC/27/37. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; United Nations High Commissioner for Human Rights (2018). The right to privacy in the digital age, A/HRC/39/29. www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/A_HRC_39_29_EN.docx; Human Rights Council (2015). The right to privacy in digital age, A/HRC/RES/28/16. p.4 (OP 4f) http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/28/16 Human Rights Council (2017). The right to privacy in the digital age, A/HRC/RES/34/7, p4. http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/34/

⁴ Communication No. 2172/2012 2 December 2011, views 17 March 2017, CCPR/C119/D/2172/2012.

⁵ https://www.sci.gov.in/supremecourt/2016/14961/14961_2016_Judgement_06-Sep-2018.pdf

⁶ Hon. Sayed Naveed Qamar, MP, New Legislation introduces Transgender Rights in Pakistan, *The Parliamentarian*, 2018, Issue three, p211.

⁷ 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; Human Rights Council resolution 20/8).

⁸ Solove, D The Digital Person, 2004, p186

democratic societies and requiring strong protections.⁹ The Human Rights Council has adopted resolutions highlighting the interdependent and mutually reinforcing relationship between democracy and human rights.¹⁰

7. Living a life of dignity is essential for a human being to fulfil the liberties and freedoms that are the cornerstone of democracies. Privacy is a form of dignity.
8. Privacy is a form of freedom built into social structures, and privacy advocacy is part of the broader political struggle for equality, citizenship rights and democracy. The human right to privacy is a limit on the exercise of power whether of States or non-State actors. By enabling personal choice, association and expression, and by protecting civil and socio-economic freedoms and equality, privacy can help secure the legitimate political rights of individuals to participate in democracies fully and without hindrance.¹¹
9. Understanding this human right from a gender perspective raises a spectrum of issues¹² requiring examination of lived experiences of privacy in its many forms - positive and negative, over physical, psychological, sexual, patrimonial and moral dimensions, both online and offline. The privacy experiences of all individuals arising from their gender, sexual orientation, sex characteristics and gender identity, are pertinent.
10. Relevantly, the Yogyakarta Principles, a set of international principles relating human rights to sexual orientation and gender identity, were supplemented in 2017 for information and communication technologies, and Additional State Obligations including Principle 6 for Privacy.¹³
11. The mandate of the Special Rapporteur on the right to privacy (SRP) entails the integration of a gender perspective throughout its work.¹⁴ In promoting a better understanding of privacy in the digital age and the gender experience of privacy, the SRP has convened 'Privacy, Personality and Information Flows' regional consultations. The first (Western countries) in July 2016 in New York; the second (Middle East and Northern Africa) in Tunisia in May 2017, the third (Asia) in September 2017 in Hong Kong, and the fourth (Latin America) is planned for May 2019.
12. Further work has been undertaken via an online consultation seeking advice on:¹⁵
 - a) Gender issues arising in the digital era in the Thematic Action Streams (Privacy and Personality; Security and Surveillance; Big Data and Open Data; Health Data, and the Use of Personal Data by Corporations)? What challenges need to be addressed and what positives can be promoted more widely?
 - b) Has the digital era produced new or significantly different gender based experiences of privacy? If so, what are these?
 - c) What are the gendered impacts of privacy invasions on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics, arising from the loss of the right to privacy, for example but not limited to, health issues, discrimination in employment or other areas?
 - d) What are good practices in law and service delivery models that address gender based differences in the enjoyment of the right to privacy?

⁹ OPC Submission to Innovation, Science and Economic Development Canada for 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/

¹⁰ Eg 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>

¹¹ Lever, A., Privacy Rights and Democracy: A Contradiction in Terms? Contemporary Political Theory 5. 2006, 142-162

¹² Franklin, M., Submission 2018

¹³ <https://yogyakartaprinciples.org/principles-en/yp10>

¹⁴ <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

¹⁵ <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>, April 2018.

13. Twenty submissions were received from individuals, civil society, academics and regulators.¹⁶ This report is a compilation of submissions received by the mandate 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 SRP Thematic Action Stream ‘Privacy and Personality’, nor those of the SRP, Professor Joseph A. Cannataci.

Submissions and Ancillary Research

14. The gender manifestations of ‘experienced privacy’ documented in submissions, are grouped under the most applicable Thematic Action Stream, though many issues are relevant to all. One such issue is the response of States to incursions into privacy based on gender and gender identity; described variously as supportive, as weak or even punitive towards individuals whose privacy has been infringed because of their gender or gender identity.
15. Submissions advocated an intersectional analysis of economic forces, class, religion, race with the gender continuum in order to identify areas of interest outside mainstream dominant issues, or groups,¹⁷ and recognition of the linkage between the right to privacy and democracy.¹⁸

A. Thematic Action Stream ‘Privacy and Personality’

16. The safe environment provided by privacy enables the person to develop without self-imposed limitations arising from concerns of being misunderstood or judged.¹⁹ Privacy also enables intimate relationships, and space to deliberate on moral and ethical choices enabling the full development of personhood and personality, including the exercise of personal responsibility. Personal development requires all dimensions of privacy, not just informational privacy.
17. Digital technologies were seen to have had enormous effect upon privacy through amplifying the experiences of the non-digital world. Cybermisogyny²⁰ and cyber-abuse of individuals of non-binary gender have been enabled by new technologies to challenge privacy and exert existing forms of aggression based on gender and gender identity²¹ with infinitely far greater reach, durability, and impact than previously.
18. Social patterns were seen also to be replicated with, for example, women already active in physical (offline) political and civic life, more likely to be connected, and three times more likely (controlling for education, age and income) to be exercising their right to freedom of expression online, or on important or controversial issues than other women.²²
19. The carryover into the online world of existing gender stereotypes, sex based characterisations and constrained roles was said to be illustrated by Virtual Personal Assistants (VPAs) such as Siri (Apple); Alexa (Amazon) and Cortana (Microsoft) amongst others.²³ These tools’ technological appropriation of female voices, female names and female characterisations are seen to reproduce discriminatory gender norms positioning women in inferior social positions: servile assistants with no right to say ‘no’, and moreover, ‘free of messy things like autonomy, emotion, and dignity’.²⁴ VPA use in homes and workplaces is increasing rapidly with the number of countries where Amazon’s Alexa, is available, doubling. More than 28,000 smart home devices now work

¹⁶ Joint submissions and three confidential submissions were received.

¹⁷ APC Submission 2018; Op cit Franklin.

¹⁸ For example, Privacy Commissioner of Canada, Submission 2018

¹⁹ Ibid

²⁰ LEAF 2014, <http://www.westcoastleaf.org/our-publications/cybermisogyny/>

²¹ Eastern European Coalition for LGBT+ Equality’s submission, ‘Gender Perspectives on Privacy in Eastern Partnership Countries and Russia’, 2018.

²² <http://webfoundation.org/docs/2015/10/QROinfographic.png>

²³ Loideain, N.N. and Adams, R. Submission, 2018; <https://medium.com/pcmag-access/the-real-reason-voice-assistants-are-female-and-why-it-matters-e99c67b93bde>

²⁴ Cross, K., ‘When Robots are an Instrument of Male Desire’ (2016): <<https://medium.com/the-establishment/when-robots-are-an-instrument-of-male-desire-ad1567575a3d>, cited in Loideain, N.N. and Adams, R. ‘From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of EU Data Protection Law’

with Alexa, six times as many as at the beginning of 2018, and 100 plus distinct products have Alexa.²⁵

20. The contribution of privacy to ‘personality’ was described in submissions in terms of how digital technologies are used by individuals, as well as State and non-State actors, according to gender or gender identity.²⁶
21. The starting point is that access to digital technologies varies by gender.²⁷

Digital Gender Divide

22. Not everyone has equal opportunity to benefit from the internet’s potential for economic, social, cultural, civic, and political advancement.²⁸ In two out of every three countries worldwide, there are more men using the internet than women. In Africa, this gender gap has increased since 2013.²⁹ Not surprisingly, the ability to protect privacy online differs across men and women because of the disparity in digital skills and confidence. Young women in the Philippines for example, are reported as saying that only when they became more experienced users, did they realise the risks to privacy arising from social media.³⁰
23. For others, such as LGBTQI individuals the ‘digital divide’ can take the form of inability to access online content due to mandated internet filtering.³¹
24. The ability to access the internet fully contributes to differences in the development of ‘personality’ in the digital era. Only 21% of women on average, used the internet to look for information on their legal rights and women are half as likely as men to speak out online, and a third less likely to use the internet to look for work (controlling for age and education).³²

Digital technology - social media, apps and smart devices

25. Submissions recognised the benefits of smart devices, apps, search engines and social media platforms to women and LGBTQI individuals, but also their capacity to infringe users’ privacy. Submissions indicated that those most at risk were women, young girls, children, LGBTQI individuals and communities especially transgender individuals, activists, gay teachers, Human Rights Defenders, sex workers, and high profile women/journalists.
26. Around the world, women have found a smartphone or safe, ‘respectable’ public access facilities can reduce cultural constraints and enable personal development through the privacy and autonomy provided.^{33 34}
27. Access to digital technologies however, was reported to threaten traditional patriarchal structures with resulting impacts upon the exercise of human rights.³⁵ In Northern India for example, the use of mobile phones and apps like WhatsApp and Facebook by women and girls, prompted village

²⁵ [https://www.wired.com/story/amazon-alexa-2018-machine-learning/?CNDID=55579454&CNDID=55579454&bxid=MzLzOTYzNTY0NzkwS0&hasha=927130c618501d6be2fbb6e421cf251&hashb=b500cbfde5454948121e66079daed34f611b0ccc&mbid=nl_122018_gadgetlab_list3_p1&utm_brand=wired&utm_mailing=Gadget%20Lab%20NL%20122018_Daily%20list%20\(1\)&utm_medium=email&utm_source=nl](https://www.wired.com/story/amazon-alexa-2018-machine-learning/?CNDID=55579454&CNDID=55579454&bxid=MzLzOTYzNTY0NzkwS0&hasha=927130c618501d6be2fbb6e421cf251&hashb=b500cbfde5454948121e66079daed34f611b0ccc&mbid=nl_122018_gadgetlab_list3_p1&utm_brand=wired&utm_mailing=Gadget%20Lab%20NL%20122018_Daily%20list%20(1)&utm_medium=email&utm_source=nl)

²⁶ “Online Reputation, What are they saying about me?”, Policy and Research Group, Privacy Commissioner of Canada, January 2016: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/

²⁷ UN Women Global Pulse references gaps in women’s access to ICTs and other technologies as 11.6% globally; 32.9% in Least Developed Countries.

²⁸ <https://www.technologyreview.com/the-download/608887/the-un-says-the-global-digital-divide-could-become-a-yawning-chasm/>

²⁹ AccessNow , The gender of surveillance: How the world can work together for a safer internet, 6 February, 2018, <https://www.accessnow.org/gender-surveillance-world-can-work-together-safer-internet/>, 31 October 2018 viewed

³⁰ http://webfoundation.org/docs/2015/10/womens-rights-online_Report.pdf

³¹ https://www.ohchr.org/Documents/Issues/Women/WRGS/GenderDigital/HRBDT_submission.pdf

³² Ranging from 52% Bogota, Colombia to 19% Lagos, Nigeria <http://webfoundation.org/docs/2015/10/WROinfographic.png>

³³ GSMA, Vital Wave Consulting and the Cherie Blair Foundation for Women, “Women & Mobile: A Global Opportunity” <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/GSMA_Women_and_Mobile-A_Global_Opportunity.pdf>

³⁴ Intel, “Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-Income Countries” 2012 <https://www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf>

³⁵ http://webfoundation.org/docs/2015/10/womens-rights-online_Report.pdf

leaders to ban their use. The connectivity and relative privacy the mobile phones provided, enabled women and girls to access information from external sources, develop relationships as they chose, make financial decisions, all of which increased personal development and the exercise of other human rights including freedom of expression.³⁶ Despite the Indian Supreme Court's criticism, the mobile phone bans are said to remain restricting enjoyment of human rights for these women/girls.³⁷ It is interesting to note that research indicates that in contrast to other countries, Indian men (34%) are much more likely than women (15%) to own smartphones – a gap of 19 percentage points. And reportedly, India's gender gap is growing: the gap in 2018 is 10 points wider than it was five years ago (then, 16% of men and 7% of women owned smartphones).³⁸

28. The internet was reported as the single most influential force on the lives of LGBTQI people facilitating private interactions with others, reducing social isolation and enabling personal development.³⁹ Reliance on the internet brings privacy risks which vary according to gender, for example, LGBTQI youth who use the internet more frequently to engage in social media and networking than non-LGBTQI peers, are more likely than non-LGBTQI youth to be bullied or harassed online (42% vs. 15%).^{40,41}
29. Fears around the dangers of the internet have seen protective strategies introduced to reduce these risks but potentially affecting personal development of some. The Children's Internet Protection Act in the USA, for example, aims to protect children from online dangers by requiring computers from K-12 and public libraries to have internet filters. Concerns have been raised however, about the filters reducing LGBTQI youth's access to information on gender identity.⁴²
30. In Canada, the eGirls Project investigated the relationship between gender, privacy and equality in online social networking of girls and young women. While social media enables social connections, it also amplifies societal norms. Rather than enabling the exploration of new forms of self and autonomy, social media maintained and augmented existing sex role stereotypes by reinforcing existing societal norms, intensifying commercial surveillance; and increasing surveillance by family members and peers.⁴³
31. Dating apps can provide private and uniquely empowering ways to communicate within a safe community.^{44,45} But fake accounts on LGBTQI dating apps and other social media platforms were reported as being used by State and non-State actors to lure gay men, expose them, entrap them, arrest or subject them to cruel and degrading treatment, or blackmail.⁴⁶ Countries where these practices were said to occur were Azerbaijan, the Russian Federation, and Belarus⁴⁷ and also the

³⁶ APC Submission 2018; Kovac, A. Reading Surveillance through a Gendered lens: Some Theory, February 2017.

<https://genderingsurveillance.internetdemocracy.in/theory/>

³⁷ Centre for Communication Governance, National Law University Delhi (CCG NLU) Submission 2018.

³⁸ Pew Research Center, 'Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally', 2018.

[http://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/?utm_source=Pew+Research+Center&utm_campaign=e8c3c7f83d-](http://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/?utm_source=Pew+Research+Center&utm_campaign=e8c3c7f83d-EMAIL_CAMPAIGN_2019_02_07_06_57&utm_medium=email&utm_term=0_3e953b9b70-e8c3c7f83d-400369205)

[EMAIL_CAMPAIGN_2019_02_07_06_57&utm_medium=email&utm_term=0_3e953b9b70-e8c3c7f83d-400369205](http://www.pewglobal.org/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/?utm_source=Pew+Research+Center&utm_campaign=e8c3c7f83d-EMAIL_CAMPAIGN_2019_02_07_06_57&utm_medium=email&utm_term=0_3e953b9b70-e8c3c7f83d-400369205)

³⁹ Joint submission of Kazakhstan Feminist Initiative "Feminita", ODR 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, 2018.

⁴⁰ 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.

⁴¹ The privacy of non-binary gender individuals can be repeatedly infringed in the physical world also in ordinary, everyday activities, for example, in the USA, a federal directive requiring public schools to let transgender students use bathrooms consistent with their gender identity was overturned⁴¹ giving rise to concerns of 'outings' breaching transgender students' privacy, and exposing them to risks of psychological and physical violence.

⁴² Holt OpCit; <http://www.onlinepolicy.org/media/schoolblocking030623.shtml>

⁴³ 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/>

⁴⁴ Name withheld Submission 2018 referencing Horres, V. "Online and Enabled: Ways the Internet Benefits and Empowers Women

⁴⁵ Horres, V. "Online and Enabled: Ways the Internet Benefits and Empowers Women

⁴⁶ Joint submission of Kazakhstan Feminist Initiative et al. 2018.

⁴⁷ <https://www.thedailybeast.com/the-hunted-gays-of-putins-russia-vicious-vigilantes-and-state-bigotry-close-up?ref=scroll>.

Ukraine and Moldova.⁴⁸ Access to justice and protection was stated to be limited as survivors feared further breaches of privacy and safety through reporting these crimes. It was said authorities in Egypt, Lebanon and Iraq used evidence of dating app use to prosecute or blackmail gay men.⁴⁹ In Iran, apps were reported to be used by non-State actors to obtain intimate images for extortion purposes.⁵⁰

32. It was reported the media, including new media, in for example, Uganda and Peru, publish the personal information of LGBTQI people, and of Human Rights Defenders, risking their safety.⁵¹
33. The internet not only creates contemporary stories but can carry forward in perpetuity those of the pre-digital era, and associated violations of privacy. Even if inaccurate, or private, or plain offensive, removing images and stories from public access can be difficult if not impossible. In a case involving a young girl submitted on a confidential basis, investigation of 'take down' options butted against constraints arising from other rights such as freedom of expression, public interest considerations, jurisdictional issues, corporate business models, professional interests versus professional ethics, and the passage of time – none of which worked in the best interest of the then child, and now, the grown woman.⁵²

Gender identity and its recognition

34. The recognition of gender identity, autonomy and bodily integrity and its expression, featured in a number of submissions. These expressed the view the digital era has seen an increase in transgender individuals disproportionately subject to breaches of their privacy and gender identity through inadequate privacy protections for legal gender recognition of name changes in identity documents.⁵³
35. The importance of privacy in identity recognition has been recognised by the European Court of Human Rights which has found States in violation of Article 8 of the European Convention on Human Rights for lacking legal gender recognition procedures that avoid violating the right to privacy of transgender people.⁵⁴
36. It was reported that the Ukraine and Russia have slightly easier procedures for identity change⁵⁵ but concerns were raised regarding the lack of automatic or swift update of name and gender marker across identity documents. Some countries, such as South Caucasus and the Republic of Moldova, are reportedly lacking an explicit law on gender identity, or clear parameters for changing the gender marker.⁵⁶
37. The online availability of public records, judicial notices and decisions concerning gender identity raised privacy concerns. Submissions raised the ability of Big Data and search engines to identify vulnerable individuals by increasing access to public records and registers once only held locally as hard copy.
38. Of particular concern were the records of legal gender recognition judicial procedures.⁵⁷ Countries mentioned in this regard were Russia, Chile and Peru. It was reported that search engines of judicial databases have enabled the access of highly specific and sensitive details of the sex

⁴⁸ Eastern European Coalition for LGBT+ Equality Submission, 2018.

⁴⁹ Joint submission of Kazakhstan Feminist Initiative et al; APC Submission 2018; <https://www.madamasr.com/en/2016/04/29/feature/politics/11-sentenced-to-3-12-years-in-prison-for-homosexuality/>

⁵⁰ Eastern European Coalition for LGBT+ Equality Submission, 2018.

⁵¹ Joint submission of Kazakhstan Feminist Initiative et al. 2018.

⁵² Osgoode School of Law, confidential submission December 2018.

⁵³ Eastern European Coalition for LGBT+ Equality Submission, 2018.

⁵⁴ L. v Lithuania; A.P. (2008), Garçon and Nicot v France (2017)

⁵⁵ Op cit Eastern Coalition, 2018.

⁵⁶ Two cases from Georgia at European Court of Human Rights <http://women.ge/en/news/newsfeed/195/To-the-Government-of-Georgia-and-To-UN-IE-on-protection-against-violence-and-discrimination-based-on-SOGI-Victor-Madrigal-Borloz>

⁵⁷ Joint submission of Kazakhstan Feminist Initiative et al. 2018.

characteristics of intersex children, addresses, details of genitalia and surgical procedures, amongst other information.⁵⁸

39. In Canada, online databases of legal decisions in Canada are not indexed by search engines, and thus do not come up in search results. “Globe24h” however, re-published online, Canadian court and tribunal decisions containing personal information and allowed indexing by search engines, and charged individuals a fee to have their personal information removed. Complaints to the Federal Privacy Commissioner against Globe24h had strongly gendered dimensions. Action taken to stop this practice was confirmed by the Federal Court of Canada.⁵⁹
40. For intersex individuals, privacy intrusions can commence literally from birth with intersex babies subjected to sex reassignment surgery and hormone treatment to assign them a certain sex. ‘Normalising’ surgery on intersex infants can impact a range of human rights, including the right to privacy as it extends to the right to personal autonomy/self-determination in relation to medical treatment. Infant surgery puts decision making in the hands of third parties and can have adverse impacts on personal development.⁶⁰
41. Countries were reported to be responding in a variety of ways. Colombia has limited the authority of parents of intersex children to authorise medically unnecessary genital plastic surgery due to concerns of the social and psychological impacts if the parents and physicians assign the wrong sex to a child. In August 2018, the Californian Legislature passed a resolution seeking the halt of non-consensual medical procedures that cosmetically “normalize” variations in intersex children’s sex characteristics.⁶¹
42. Privacy incursions arising from identity documents can mean ordinary everyday activities such as travel, banking, medical appointments impose frequently deeply embarrassing and distressing privacy infringements that limit the enjoyment of life and constrain personal development in ways not experienced by individuals of binary genders.

Technologically facilitated violence

43. Digital technology and smart devices (smartphones, iPads, security cameras, etc.) provide almost limitless ways to harass, control or monitor others.⁶² Technologically facilitated violence combines issues of gender inequality, sexualised violence, internet regulation, internet anonymity, privacy, copyright and ethics. The Special Rapporteur on Violence Against Women, in her 2018 report outlined the many forms of online gender-based violence violating women’s and girls’ rights to privacy.⁶³
44. Release of personal information on social networks can control, harass or blackmail others. Most widely known is the phenomenon of ‘revenge porn’ which involves sharing private sexual images and recordings of a person without consent, to cause harm. Generally seen as affecting women more than men, research in Australia has found that females and males 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%).⁶⁴
45. While technological forms of privacy incursions by strangers occurs online, domestic violence increasingly involves interconnected technologies.⁶⁵

⁵⁸ Ibid.

⁵⁹ <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-002/>

⁶⁰ Larson, S. Intersexuality and Gender Verification tests: The Need to Assure Human Rights and Privacy, *Pace International Law Review* 23(6) 2011.

⁶¹ <https://www.usatoday.com/story/news/nation/2018/08/28/intersex-surgeries-children-california-first-state-condemn/1126185002/>

⁶² De Justica Submission 2018.

⁶³ 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

⁶⁴ RMIT University, *Not Just ‘Revenge Pornography’: Australians’ Experience of Image-Based Abuse*, May 2017.

⁶⁵ UCL and Privacy International, ‘Gender and IoT’, <https://www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot>

46. Smart-home technologies in particular, facilitate cyber-domestic violence through new ways to harass, to monitor what people are doing at home,⁶⁶ or their communications.⁶⁷ Changing thermostat controls, monitoring via location data or sleep apps, camera surveillance, controlling the lights or music in the home, or ringing a doorbell remotely, are behaviours which intimidate and control. Abusers may have sole access to the device, making it difficult or impossible for the victim to change the settings. Sometimes legal protections such as ‘no contact’ type orders, do not address this abuse⁶⁸ and while family violence orders can include technology facilitated abuse, the lack of police enforcement of breaches can render inclusion of technological abuse, ineffective.⁶⁹ Typically directed at women and dependents,⁷⁰ these actions impede the enjoyment of privacy and personal development.
47. Online spaces are also public places where sexual harassment of women and girls is rife.⁷¹ The general online harassment of and encroachment on the privacy of women or ‘cybermisogyny’ proliferates on digital platforms.⁷² It was reported Twitter is the main platform for promoting hate campaigns against women and for dissemination of sexual content, while Facebook sees most attacks on women who defend their rights.⁷³
48. There is a growing body of international, regional and national research on digital abuse directed at women and some also examining this form of abuse against gender diverse individuals and communities. The role the right to privacy plays (or does not play) in this digital abuse however, is rarely subjected to close examination.
49. One study in Europe, by the Fundamental Rights Agency, found violence against women an extensive human rights abuse. The report did not examine the nature of the human rights abused however, but its survey of 42,000 women across 28 Member States of the EU helpfully documents the prevalence, types and consequences of gender violence, and the role played by new technologies in such abuse.⁷⁴
50. The body of research provides relevant and important contextual information as well as insights into how online abuse is manifested according to gender. In relation to the former issue, research from the United States of America for example, indicated differing gender perspectives on issues such as assistance and prevention by authorities, specifically:⁷⁵
- a) Women are more likely than men to say that law enforcement currently does not take online harassment incidents seriously enough (46% vs. 39%), to see online harassment as a major public issue problem (70% women vs. 54% men), and, 50% women say that offensive content online is too often excused as not being a big deal, whereas 64% of men say that many people take this type of content too seriously;
 - b) Women are much more likely than men to say people should be able to feel welcome and safe in online spaces (63% to 43%), whereas men are more likely to say it is important for people to be able to speak their minds freely online (56% to 36%); and

⁶⁶ 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

⁶⁷ SpyWare technologies allow abusers to know what victims have been searching, Mason, C. and Magnet, S., *Surveillance Studies and Violence Against Women*, *Surveillance & Society* 10(2) 2012; APC p13

⁶⁸ 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>

⁶⁹ Hadeel Al-Alosi, *Cyber-Violence: Digital Abuse in the Context of Domestic Violence*, *UNSW Law Journal* 40(4) 2017.

⁷⁰ ‘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>.

⁷¹ UK Parliament, House of Commons, Women and Equalities Committee, ‘Sexual harassment of women and girls in public places’, October 2018, para 108, <https://publications.parliament.uk/pa/cm201719/cmselect/cmwomeq/701/70111.htm>

⁷² LEAF op cit.

⁷³ APC Submission, 2018; Women’s Institute of Mexico City

⁷⁴ European Union Agency for Fundamental Rights, *Violence against Women: an EU-wide survey. Main Results*. 2015. <https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>

⁷⁵ Ibid

- c) Men are somewhat more likely than women to believe that improved policies and tools from online companies are the most effective approach to addressing online harassment (39% vs. 31%), while women are more likely to favour stronger laws (36% vs. 24%).
51. In terms of how online abuse is manifested according to gender, the same research indicated significant differences between females and males with 11% of women harassed because of their gender, compared with 5% of men.⁷⁶
52. Different organizations in Latin America have issued reports on gender and privacy in the digital age.⁷⁷ It was reported that despite the frequency of cyberbullying across Latin America, substantive studies have occurred only in Mexico, Brazil and Argentina.⁷⁸ In Mexico, 4.5 million children and adolescents aged 12 to 19 were reported to have been victims of cyberbullying⁷⁹ notably females.
53. In Brazil, 65% of complaints received by the NGO Safernet, on cyberbullying and offences related to women.⁸⁰ In Colombia, the Karisma Foundation undertook research on online violence against women journalists, finding online attacks are deeply personal in nature, demeaning and sexualised, and which can be seen to involve infringements of informational and physical privacy. Female Human Rights Defenders also are the targets of such attacks.⁸¹
54. A study of Canadian criminal law cases involving technology-facilitated voyeurism found a clear gender issue with the accused typically male, and the victims usually women and girls.⁸²
55. Women who have been trafficked also experience technology-facilitated privacy abuses by clients and traffickers, who are reported to use images and recordings to induct and retain women in the trade by threatening disclosure to children, family members, friends, teachers, employers, police, child protection services, Courts and taxation agencies.⁸³
56. Invasions of privacy and online violence are higher also for men who do not conform to conventional masculine norms or stereotypes and for people who identify as lesbian, gay, or bisexual. Race or ethnicity can also be a risk factor, for example black American internet users have a 7% higher risk factor compared to 3% of white users.⁸⁴
57. Digital abuse based on gender also affects the exercise of other rights with, for example, women reportedly also suffering online censorship and profiling in campaigns targeting activists and journalists.⁸⁵ Additionally, activists seeking rights equality for the LGBTQI community were said

⁷⁶ 44% of men and 37% of women reported facing some form of online harassment with men somewhat more likely than women to have been called offensive names (30% vs. 23%) or to receive physical threats (12% vs. 8%). Women, especially young women, receive sexualized forms of online abuse at much higher rates than men. Some 21% of women ages 18 to 29 have been sexually harassed online, more than double that of men in the same age group (9%). Further, 53% of young women say that someone has sent them explicit images they did not ask for (compared with 37% of young men). Pew Research, *Men, women experience and view online harassment differently*, 2017; http://www.pewresearch.org/fact-tank/2017/12/28/10-things-we-learned-about-gender-issues-in-the-u-s-in-2017/?utm_source=Pew+Research+Center&utm_campaign=56eb70a58b;EMAIL_CAMPAIGN_2017_12_26&utm_medium=email&utm_term=0_3e953b9b70-56eb70a58b-400369205

⁷⁷ De Justicia Submission September 2018. Eg. the joint report of Fundación Karisma (Colombia), Coding Rights (Brazil), Asociación por los Derechos Civiles (Argentina), Derechos Digitales (Chile), R3D (Mexico), Hiperderecho (Peru) and Internet Lab (Brazil); Coding Rights (Brazil).

⁷⁸ Report on the Situation in Latin America on Gender-Based Violence in Electronic Media

⁷⁹ National Women's Institute 2016.

⁸⁰ NGO Safernet, 2016

⁸¹ SR correspondence eg https://spcommreports.ohchr.org/TMResultsBase/DownloadPublicCommunicationFile?gId=24199;https://www.outrightinternational.org/sites/default/files/TransRpt_Colombia_En.pdf

⁸² Bailey, Jane and Mathen, Carissima, Technologically-Facilitated Violence Against Women and Girls: If Criminal Law Can Respond, Should It? (November 23, 2017). Ottawa Faculty of Law Working Paper No. 2017-44. Available at SSRN: <https://ssrn.com/abstract=3043506> or <http://dx.doi.org/10.2139/ssrn.3043506>

⁸³ Project Respect submission to Australian Senate Legal and Constitutional Affairs References Committee Inquiry into the 'Phenomenon colloquially referred to as 'revenge porn'
https://d3n8a8pro7vhm.cloudfront.net/projectrespect/pages/15/attachments/original/1453939756/Revenge_Porn_Submission.pdf?1453939756

⁸⁴ Irish Civil Liberties Council Submission 2018; ⁸⁴ Amnesty International 'Troll Patrol', 2018, <https://decoders.amnesty.org/projects/troll-patrol/findings>

⁸⁵ de Justicia op cit

to face significant threats online in response to their gender equality advocacy exercised via their rights to freedom of expression and political views.⁸⁶ The right to education is implicated in the reported release in China, of nude photos (required as part of collateral for student loans), of young female students, for financial gain by organised loan sharking criminal activity.⁸⁷

B. Thematic Action Stream ‘Security and Surveillance’

58. Submissions indicate gender experiences of surveillance can be broadly State-led; commercial; domestic or lateral, and even participatory in nature. The increasing interdependencies – economic and political⁸⁸ - between these forms of surveillance mean an individual can experience more than one form of surveillance.
59. Surveillance unless undertaken lawfully, proportionately and necessarily represents infringements of the human right to privacy. Factors such as race, class, and gender all help determine who is watched in society, and the right to privacy has been unequally distributed according to these factors.⁸⁹
60. While State powers of surveillance are extensive, they are inextricably tied to the private sector. The technology that makes mass surveillance possible was developed through collaboration between governments and private corporations, and the surveillance powers of the State are increasingly exercised through private technology.⁹⁰ Communication carriers, social media applications, and search engines function as huge information reservoirs for States who have recognised the value of information held by companies on service users and their contacts, and have sought access to it, including by legislative means.
61. Such surveillance is facilitated by the movement of major platform providers into the role of identity management via online identity authentication. Almost every website, app and service now require login details, and accept identity credentials as authentic following logon via Facebook or Google accounts.⁹¹ Facebook has 60% of this ‘social log on’ market and has become the de facto provider of identity validation in the non-Chinese parts of the internet.⁹² Identity validation provides access to vast amounts of information to compile profiles of individuals and groups in which gender would be a variable, enabling deep insights into the behaviours of individuals, families, groups and communities.
62. Surveillance technologies utilised by companies, such as GPS tracking, can facilitate abuse and enable the monitoring and targeting of communications to individuals and groups. Some submissions raised concerns about the use by States of this information to target individuals and groups according to their gender, pointing to the higher surveillance of those who identify as LGBTQI.⁹³
63. State surveillance of the LGBTQI community was seen to be facilitated in some countries, through legislation. For example, some fear the Anti-Cybercrime Law enacted in Egypt in mid-August 2018, to regulate internet activities, could be used to prosecute LGBTQI people and groups for social media content that “violates the family principles and values upheld by Egyptian society” (Article 25). Violations carry penalties of a minimum of six-months imprisonment and/or fines of EGP50,000–100,000.⁹⁴

⁸⁶ harassment (75%), intimidating online comments (63%) and blocked websites or filtering software preventing information access (54%).

⁸⁷ Pushkarna, N. and Ren, MM., Submission 2018 referencing Constable, P. (2016).

https://www.washingtonpost.com/news/worldviews/wp/2016/06/16/loan-sharks-in-china-offer-student-loans-for-nude-photos-giving-new-meaning-to-naked-greed/?noredirect=on&utm_term=.9f1be4224c01; <https://www.zerohedge.com/news/2018-12-14/chinese-millennials-secured-loans-nude-photos>; http://www.academia.edu/26833351/Extortion_Racketeering_in_the_EU_Vulnerability_Factors.

⁸⁸ Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.

⁸⁹ Franks, M.A., *Democratic Surveillance*, *Harvard Journal of Law & Technology*, Volume 30, Number 2 Spring 2017

⁹⁰ Ibid.

⁹¹ The Economist Essay, Christmas Edition, December 2018

⁹² Ibid.

⁹³ APC Submission, 2018.

⁹⁴ Joint International Submission, 2018; <http://www.loc.gov/law/foreign-news/article/egypt-president-ratifies-anti-cybercrime-law/>

64. State surveillance against the LGBTIQI community was reported in Azerbaijan and Belarus.⁹⁵ Action against reported breaches was said to rarely start or quickly closed.⁹⁶ The ‘Anti-propaganda Law’ in the Russian Federation was said to have made intrusions into private lives, a systematic occurrence⁹⁷ with the law being used by non-State actors to target LGBTIQI school teachers with 13 cases of wrongful dismissal documented.⁹⁸
65. While State surveillance is generally presented as targeting males,⁹⁹ counter-terrorism measures for instance, have been said to disproportionately affect women and transgender asylum-seekers, refugees and immigrants.¹⁰⁰
66. Females 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 to reproduction. The story of how Target identified a teenage girl as pregnant before her parents knew, is now almost part of folklore.¹⁰¹
67. Commercial use of personal data available to business has seen products developed that also maintain this flow of information via ‘participatory surveillance’¹⁰² or ‘self-surveillance’, marketed by gender groupings. Investors are reported to be concentrating money in ‘wellbeing’ apps such as those aimed at women’s reproductive functioning.¹⁰³ The data supplied by users is potentially available for monitoring purposes and/or on-sold without the individuals’ consent or knowledge, and fed into algorithmic models which in turn, determine marketing ‘itches’, depict societal norms and shape behaviours.¹⁰⁴
68. Women are subject to more lateral and domestic surveillance than men and this varies according to culture and religious backgrounds. While technology can extend women’s contacts and opportunities, technology provides enhanced opportunities for others to monitor their activities.¹⁰⁵
69. Surveillance experienced by some young women can involve State surveillance of their activism, raising amongst other matters, the question of expectations of privacy in public spheres.¹⁰⁶ In Ireland, the case of Dara Quigley was described as capturing the intersection of State authorised CCTV surveillance, image-based sexual abuse, gendered harassment, and existing legislation and law enforcement norms.¹⁰⁷
70. Much surveillance now relies upon vast quantities of data, Dataveillance¹⁰⁸ combines data and surveillance to describe systematic data-based surveillance practices that involve sorting and aggregating large quantities of data to monitor, track and regulate people and populations, and which can be effected according to gender/gender identity.

C. Thematic Action Stream ‘Big Data and Open Data’

⁹⁵ Eastern European Coalition for LGBT+ Equality Submission, 2018.

⁹⁶ Ibid.

⁹⁷ Ibid.

⁹⁸ Ibid.

⁹⁹ Privacy International 2017

¹⁰⁰ Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism Scheinin, M. to UNGA 64th Session, A/64/211, 3 August 2009.

¹⁰¹ BusinessInsider, February 2012, <https://www.businessinsider.com/the-incredible-story-of-how-target-exposed-a-teen-girls-pregnancy-2012-2>

¹⁰² Lupton, D., Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, 17 (4), pp. 440-453 http://www.canberra.edu.au/researchrepository/file/25d1310f-2c5d-4ca5-9e8e-c17f1a140cb1/1/full_text_postprint.pdf; <http://www.canberra.edu.au/researchrepository/items/25d1310f-2c5d-4ca5-9e8e-c17f1a140cb1/1/>

¹⁰³ The Guardian, Technology, Weigel, M., ‘Fitbit for your period? The Rise of Fertility Tracking’, 23 March 2016.

¹⁰⁴ Op cit. Lupton; ‘New App Changing the Way Women Relate to Reproductive Health’; APC Submission, 2018.

<https://www.womenshealth.northwestern.edu/blog/new-app-changing-way-women-relate-reproductive-health>; Diana-Ashley Krach, ‘Best apps for reproductive health now that we’re basically on our own’ 26 Jan 2017 <https://www.sheknows.com/health-and-wellness/articles/1131535/best-apps-for-reproductive-health/>

¹⁰⁵ Mason, C. and Magnet, S. *Surveillance Studies and Violence against Women, Surveillance and Society*, 10(2), pps105-118, 2012: 116 https://www.academia.edu/3561802/Surveillance_and_Violence_Against_Women

¹⁰⁶ APC Submission 2018.

¹⁰⁷ Irish Council for Civil Liberties Submission, 2018.

¹⁰⁸ Clarke, R., <http://www.rogerclarke.com/DV/CACM88.html>; APC Submission, 2018.

71. The SRP's reports and consultations have noted the differential effects of Big Data upon privacy according to gender and its interaction with other issues such as Indigenous Sovereignty Rights.¹⁰⁹
72. Almost all data in industrialised countries whether employment, financial, retail, lifestyle, socially related are recorded digitally, interconnected and networked. Many, if not most, companies using digital technology for service delivery, collect identifying information about individuals, their gender, their social networks, online (e.g. browser history, interests and preferences) and offline activities (e.g. purchases, location tracking, microphone recording on mobile devices). Companies also collect data externally compiled by other parties through public sources (e.g. public databases, data scraping), purchasing from third parties (e.g. data brokers), receiving consumer data through business partnerships, or swapping lists. In addition, data brokers amalgamate and on-sell information about consumers from other companies and data brokers.¹¹⁰
73. In 2018, UN Women in conjunction with Global Pulse reported Big Data could help close the gender gap for the 2030 Agenda for Sustainable Development while acknowledging the potential privacy risks from the use of data, even if de-identified.¹¹¹
74. Big data techniques can enable marketing at a micro-level, and technologies such as mobile geo-fencing, have the capacity to target people by gender. The use in the US by Anti-Choice groups of mobile geo-fencing technology to target anti-choice ads at women attending abortion clinics was raised as a non-consensual, predatory, unethical invasion of women's privacy against which legal protections appear absent.¹¹²
75. Data processing can affect structural and societal interests, particularly as data modelling such as predictive policing or social intervention, increasingly transcends the individual to focus on groups or communities. Societal biases relating to gender roles and identities can be embedded in such programs and systems via automated decision-making.¹¹³ Poor and working-class people are targeted by new tools of digital poverty management with automated eligibility systems within which women on welfare are one of the most privacy poor groups in society.^{114 115} Complex integrated databases collect their most personal information, predictive models and algorithms weigh them for risk and potential problems; vast complexes of social service, law enforcement, and neighbourhood surveillance make their every move visible for government, commercial, and public scrutiny.¹¹⁶
76. Sorting people into categories according to gender frequently in combination with other factors, and assigning values and risk ratings can have real consequences for opportunities in life, constraining personal development.¹¹⁷ The growth in the collection, storage and manipulation of data has increased the possibilities of privacy breaches. When these occur, even if they are not based on gender, breaches can have a more severe impact on women, and LGBTIQI people due to associated discrimination.
77. Data analytics resulting in inferences being drawn about individuals or groups according to gender and which lead to discrimination, are contrary to human rights law.

D. Thematic Action Stream 'Health Data'

78. An important issue for all is the protection of their health data.

¹⁰⁹ A/73/345712 <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

¹¹⁰ CPRC Submission 2018.

¹¹¹ UN Women Global Pulse 'Gender Equality and Big Data', 2018 at <https://www.unglobalpulse.org/sites/default/files/Gender-equality-and-big-data-en-2018.pdf>

¹¹² Coutts, S., *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, 2016 rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/

¹¹³ Bridges, K.M., *The Poverty of Privacy Rights*, Stanford University Press, 2017.

¹¹⁴ Ibid

¹¹⁵ The Guardian, Gomes, L.H., Parents Next: single mothers say they were forced to allow 'sensitive' data to be collected, 27 January 2019.

¹¹⁶ Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, Virginia Eubanks, St. Martin's Press 2018.

¹¹⁷ 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](http://www.felfel.is/sites/default/files/2016/Lyon,_D._(2003).Surveillance_and_social_sorting%26_computer_codes_and_mobile_bodies%20(1).pdf)

79. A particular concern for LGBTQI people is the non-consensual sharing of health data particularly HIV status.¹¹⁸ There have been grounds for these fears. The Grindr app for example, has been found to contain trackers and share personal information with various third parties, including users' HIV status.¹¹⁹
80. Studies have shown LGBTI individuals tend to have poorer access to health services than heterosexuals and that the intersection of multiple social identities reveal important gaps in health care experience.¹²⁰ Transgender inclusive healthcare can profoundly increase the quality of life for transgender people.¹²¹ Fears of humiliation or discrimination from loss of privacy however, can result in avoidance of health services or their restricted use affecting health outcomes.¹²² For transgender individuals, intake forms collecting legally identifying information such as name and gender marker, can present privacy incursions which do not arise for binary gender patients.¹²³ Privacy experiences in health care settings have been found to influence health service usage, and consequently possess public health impacts.
81. Violations of women's right to privacy during childbirth can be a powerful disincentive to seeking care for subsequent deliveries.¹²⁴ A review of 65 studies from 34 countries¹²⁵ found lack of informed consent for medical procedures; lack of physical privacy, and breach of confidentiality (for example, HIV status) in Kenya, South Africa and the United Kingdom made women avoid or fear facility-based delivery due to anxiety about HIV tests taken without consent or inadequate physical privacy. Muslim parents' views of maternity services have been found to be determined by their ability to retain their privacy in accordance with religious beliefs.¹²⁷
82. Technologies such as Google street view, can effect health service usage by women. It was reported for example, in Australia, that concerns about being identified resulted in women not using a women's health clinic after viewing online, protesters outside the facility.¹²⁸
83. Lastly, gender verification in sports was raised as invading women's physical and medical privacy more than that of male competitors.¹²⁹

E. Thematic Action Stream 'Use of Personal Data by Corporations'

84. There is growing recognition that the private sector has obligations under human rights law as in the UN "Protect, Respect and Remedy" Framework.¹³⁰
85. The concentration of digital communication in globally dominant, privately owned social media platforms with business models dependent upon advertising revenue, which are largely unregulated operations, has made privacy however defined, more difficult to guarantee.¹³¹ ¹³² ¹³³

¹¹⁸ Op cit Kazakhstan Feminist Initiative "Feminita", et al.

¹¹⁹ APC Submission, 2018.

¹²⁰ Hsieh, N. Ruther, M., 'Despite Increased Insurance Coverage, Nonwhite Sexual Minorities Still Experience Disparities In Access To Care', Health Affairs, Vol 36, No. 10, October, 2017.

¹²¹ Transgender Healthcare, Consultation Document, Office of the Deputy Prime Minister, Ministry for Health, April 2018. Malta.

¹²² NPR, Robert Wood Johnson, T.H. Chan School of Public Health 'Discrimination in America: Views and Experiences of LGBT Americans, November, 2017, p30.

¹²³ Malta Times, Saturday April 7, 2018 'New Health care clinic for transgender people in pipeline', p5.

¹²⁴ The Universal Rights of Childbearing Women Charter

¹²⁵ 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 . de Justica; APC

¹²⁶ 11 countries sub-Saharan Africa, 5 Asia, 2 Oceania, 4 Europe, 5 Middle East and North Africa, 2 North America, and 5 Latin America.

¹²⁷ The Maternity Alliance, *Experiences of Maternity Services: Muslim Women's Perspectives*, November 2004.

¹²⁸ C. Wahlquist, Protect us from anti-abortion protesters, say women's clinics in WA, The Guardian International Edition, 25 January, 2018.

¹²⁹ Larson, S., Intersexuality and Gender Verification tests: The Need to Assure Human Rights and Privacy, Pace International Law Review 23(6) 2011, in McKee, K. Submission 2018.

¹³⁰ The Charter of Human Rights and Principles for the Internet, Internet Rights and Principles Dynamic Coalition UN, Internet Governance Forum, 2014.

¹³¹ Australian Competition and Consumer Commission, 'Preliminary Report of Inquiry into Digital Platforms', 2018.

¹³² Zuboff, S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.

¹³³ UK Parliament, House of Commons Committee, Disinformation and 'fake news': Final Report, February 2019.

86. It is no surprise then, that research has found 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies.¹³⁴
87. This lack of control is exacerbated by the automated decision-making used by digital platforms and which can produce outcomes affecting genders differently. Legal action, still ongoing, was reported against Facebook for allegedly allowing landlords and brokers to exclude ads from being displayed based on the user's gender.¹³⁵
88. Concern was expressed at the increased number of social media pages and groups promoting violence against women, showing intimate images without consent, sexism, and harmful gender stereotypes. Concern was also expressed at the amount of community pressure it took to have these pages removed.¹³⁶ Although pages, such as those involving children, or hate speech have been taken down, for example by Facebook after official representations¹³⁷ or under Codes of Conduct.¹³⁸
89. It was reported that it is unknown how social media platforms make decisions following the receipt of complaints of online violence, and the types and number of cases reported by country, or the actions taken.
90. 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."¹³⁹
91. One submission reported positive action by the app Grindr to reduce mis-use aimed at entrapment of gay men,¹⁴⁰ 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. The general feeling of victims regarding companies' response to gender violence, was reported as one of abandonment.¹⁴¹
92. Reliance upon social media platforms to self-regulate is problematic. Some submissions noted that there has been no campaign by Internet platforms to prevent gender based infringements of privacy or gender-based violence regionally or globally; little proactive technological assistance, for example, through apps providing information of services, or, of using design choices, Terms of Service (ToS) and tools for reporting ToS violations.¹⁴²
93. Combined with the lack of State sanction, there is the sense that online gender-based privacy incursions are tolerated.¹⁴³ The loss of privacy leads many victims, frequently women, to silence or censor themselves affecting their enjoyment of other human rights such as freedom of expression, and of association.¹⁴⁴

https://publications.parliament.uk/pa/cm201719/cmselect/cmcomeds/1791/179103.htm#_idTextAnchor000

¹³⁴ Rainie, L. The state of privacy in post-Snowden America. Pew Research Centre. <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

¹³⁵ CPRC Submission citing 'Money' CNN News in March 2018.

¹³⁶ AWAVA Submission, 2018.

¹³⁷ http://www.huffingtonpost.com.au/2017/10/23/facebook-shuts-down-vile-rape-and-violence-group-linked-to-adf-troops_a_23253443/; <http://www.sbs.com.au/news/article/2017/10/24/facebook-closes-rape-meme-page-adf-troops-link> AWAV Submission, 2018; Zuckerberg, D. 2018.

¹³⁸ EU Code of Conduct, 'Countering illegal hate speech online', 4 February 2019 http://europa.eu/rapid/press-release_MEMO-19-806_en.htm

¹³⁹ Op cit Amnesty International 2018

¹⁴⁰ Op cit Kazakhstan Feminist Initiative "Feminista", et all. Submission 2018.

¹⁴¹ Electronic Media cited in De Justica Submission, 2018

¹⁴² Report on the Situation in Latin America on Gender-Based Violence Exercised by Electronic Media, in de Justica, Submission, 2018.

¹⁴³ Op cit de Justica

¹⁴⁴ Op cit Amnesty International 2018; APC Submission, 2018.

94. The difficulty of identifying hidden gender based losses of privacy and therefore of pinpointing the harms that follow privacy violations, has increased with the ever-growing ability to collect and process data using algorithms and AI, combined with the wider focus on large groups or society as a whole, rather than individuals.
95. The reported harms to individuals arising from gender based technological infringements of privacy include:
- a. Extension of patriarchal or abusive controls¹⁴⁵
 - b. Silencing of women's and girl's voices in public¹⁴⁶
 - c. Stigmatisation, humiliation and social isolation
 - d. Mental health issues and even suicide^{147 148}
 - e. Reputational impacts¹⁴⁹
 - f. Stalking, bullying and harassment, both online and offline
 - g. Economic harm through loss of professional reputation, reduction in job opportunities
 - h. Discrimination in employment, services received including possible loss of access to personal data if accounts are suspended or terminated
 - i. 'Outing' frequently introducing further privacy breaches and abuse, particularly for trans-women and trans-people of colour.¹⁵⁰
 - j. Physical danger, hate crime
 - k. Arrest, imprisonment, or execution in some jurisdictions
96. Experiences of privacy infringements are not homogeneous; incursions can have a greater impact on LGBTQI people due to associated discrimination, and resulting negative self-esteem and depression.¹⁵¹ Women report higher levels of emotional stress from their experiences of online violence.¹⁵² Transgender individuals can experience some specific, unique risks such as 'outing', and abuse directly arising from privacy infringements upon their gender identity.¹⁵³ For culturally and linguistically diverse women there is the added shame that may come from their cultural or religious community, or families back in their home countries experiencing violence, shame and other harmful reprisals which is particularly pertinent for trafficking victims.¹⁵⁴
97. Australian research on "revenge porn" revealed the damaging psychological toll on victims, with those threatened or experiencing "sextortion" and whose images had been distributed, the most severely affected by depression and/or anxiety.¹⁵⁵
98. Surveillance has serious, well-documented effects, ranging from loss of employment and educational opportunities, restrictions on the freedom to move, associate, or dress as one wishes, interference with parenting abilities, and loss of general confidence.¹⁵⁶
99. These harms raise questions about the societal effects of undermining human rights. Privacy harms to individuals which constrain their personal development affect society overall. In this

¹⁴⁵ APC Submission October 2018

¹⁴⁶ Op cit UK Parliament.

¹⁴⁷ Op cit Pushkarn and Ren.

¹⁴⁸ Op cit FRA.

¹⁴⁹ "Online Reputation, What are they saying about me?", a Discussion Paper Policy and Research Group, 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/.

¹⁵⁰ Case submissions to TGEU.

¹⁵¹ GLSEN (2013), *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet*. Jt Intl Submission -

¹⁵² Pew Research, Men, women experience and view online harassment differently, 2017; http://www.pewresearch.org/fact-tank/2017/12/28/10-things-we-learned-about-gender-issues-in-the-u-s-in-2017/?utm_source=Pew+Research+Center&utm_campaign=56eb70a58b;

EMAIL_CAMPAIGN_2017_12_26&utm_medium=email&utm_term=0_3e953b9b70-56eb70a58b-400369205

¹⁵³ Gender Perspectives on Privacy in Eastern Partnership Countries and Russia by the Eastern European Coalition for LGBT+ Equality

¹⁵⁴ Project Respect, 'Project Respect submission to the Senate Legal and Constitutional Affairs References Committee Inquiry into the 'Phenomenon colloquially referred to as 'revenge porn', which involves sharing private images and recordings of a person without their consent, with the intention to cause that person harm'. Australia, 2016.

¹⁵⁵ RMIT University, *Not Just 'Revenge Pornography: Australians' Experience of Image-Based Abuse*, May 2017.

¹⁵⁶ Franks, M.A., Democratic Surveillance, *Harvard Journal of Law & Technology*, Volume 30, Number 2 Spring 2017

way, privacy is an issue that concerns what type of society we want to construct for the future.¹⁵⁷ For example, the extreme forms of online abuse and the invasion of the personal and familial privacy inflicted upon high-profile women, discourage girls and women from participating in politics and adversely affecting gender representation in democratic institutions.¹⁵⁸

Addressing gender based differences in the enjoyment of the right to privacy

100. Submissions indicated good practices that protect privacy from a gender perspective range from legislative reform, legal decisions by Courts, community programs to educational resources. Some examples were provided of overarching frameworks such as the Inter-American Human Rights System's American Convention on Human Rights, with provisions protecting dignity, good name and equality, and the Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Convention of Belem do Pará) protecting the rights to integrity, security, equality and life of women, among others.
101. Submissions raised how legislation around the world, is determining experiences of privacy according to gender and gender identity.
102. In India, the Supreme Court in several judgments over the past 60 years has acknowledged the gendered aspects of privacy.¹⁵⁹ For instance, the Court has held that a mother's right to privacy cannot be violated by mandating the disclosure of the name and particulars of the biological father of her child for the child's passport. The right to privacy of victims of sexual assault was upheld when the Court condemned performing of Per Vaginal ("two finger" tests) on rape victims in order to verify if the victim was habituated to sexual intercourse. The Supreme Court has held also that the identity of the victims (typically women or young girls) of rape should not be disclosed in any manner, except with court authorisation.
103. Privacy, self-identity, autonomy and personal integrity were upheld by the Indian Supreme Court as rights guaranteed to members of the transgender community under Article 19(1)(a) of the Constitution of India that the State is bound to recognise and protect, in a petition filed by the National Legal Services Authority (NALSA). In 2017, the landmark judgment of the Court in *Puttaswamy v. Union of India* reaffirmed the right to privacy as a core value with Chandrachud J. recognising that sexual orientation is an essential component of the right to privacy.¹⁶⁰
104. In Canada, the Federal Office of the Privacy Commissioner has asked the Canadian Federal Court to clarify whether the *Personal Information Protection and Electronic Documents Act* s5(3) provides for a right to de-indexing on request in certain cases following a consultation addressing online reputation.¹⁶¹
105. Around the world, legislative responses to 'revenge porn' have been introduced, for example Malta in 2016.¹⁶² While seen as positive State responses, it was pointed out that such legislation does not guarantee the prevention of online image abuse against women in all situations involving the collection and distribution of images of genitalia. A submission from Australia illustrated this point¹⁶³ where it has been argued that a statutory cause of action for serious invasion of privacy, would be a better legislative response.¹⁶⁴ In other parts of the world, issues around ownership of an image have made prosecution of 'revenge porn' cases difficult.¹⁶⁵

¹⁵⁷ Solove, D.J., 'Conceptualizing Privacy', California Law Review, 90. Pps 1087-1155 in J.A. Cannataci. 'The Individual and Privacy Volume 1', Ashgate, 2015.

¹⁵⁸ AWAVA Submission, 2018.

¹⁵⁹ CCG NLU Submission 2018.

¹⁶⁰ Op cit CCGNLU.

¹⁶¹ Federal Office of the Privacy Commissioner Submission 2018, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/an_181010/.

¹⁶² <https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world>

¹⁶³ Confidential submission by complainant, under pseudonym, Australia.

¹⁶⁴ Australian Privacy Foundation <https://privacy.org.au>

¹⁶⁵ Farries, E and Sturm, T., Feminist legal geographies of intimate-image sexual abuse: Using copyright logic to combat the unauthorized distribution of celebrity intimate images in cyberspaces, Environment and Planning A: Economy and Space 0(0) 1–21, 2018.

106. The characteristics of privacy and gender respectful frameworks were described as including:
- a) evidence-based policy framework incorporating international, regional and national human rights frameworks, and addressing the structural factors that give rise to gender inequities in the enjoyment of the right to privacy^{166 167 168 169}
 - b) governance frameworks with tools such as impact assessments, that include gender impacts
 - c) promotion of encryption, pseudonymity and anonymity,^{170 171} and education to increase the technological and data safety capacities of vulnerable groups¹⁷²
 - d) utilisation of Civil Society Organisations' (CSOs) experience and community knowledge of gendered privacy by involving them in policy formulation, implementation and evaluation, and education initiatives.
107. Good practices specifically for sexual orientation and gender identity privacy issues were seen to be encapsulated in the Yogyakarta Principles+10 entailing:¹⁷³
- a) Adoption of all necessary legislative, administrative and other measures to guarantee the right to enjoy privacy, intimate decisions and human relations, including consensual sexual activity between persons over the age of consent, without arbitrary interference;
 - b) Repeal of all laws criminalising consensual sexual activity between people of the same sex over the age of consent, and ensuring the same age of consent applies to sexual activity between individuals of both same and different sexes;
 - c) Not criminalising sexual activity carried out consensually between people of the same sex over the age of consent;
 - d) Repeal of laws prohibiting or criminalising the expression of gender identity;
 - e) Release of all people detained under pretrial detention or on the basis of a criminal sentence, if their detention is related to consensual sexual activity between people over the age of consent, or to their gender identity;
 - f) Ensuring the right to decide, under ordinary conditions, the disclosing of information concerning sexual orientation or gender identity, and protect against arbitrary or unwanted disclosure or threatened disclosure of it.
108. Examples were provided of Court decisions in Colombia for example, where the Constitutional Court has played an important role in addressing the relationship between gender and privacy especially in cases of sexual and reproductive rights and of people with diverse sexual orientation and gender identity,¹⁷⁴ specifically:
- a. The right to an image constitutes an autonomous right protected by Article 14 of the Constitution. The dynamic aspects of the right to image, "constitute a form of self-determination of the subject and, therefore, are framed within the scope of protection provided by the fundamental right to the free development of the personality" (P.C. Article 16) (Sentence T-634/13).
 - b. Inability in judicial processes for sexual violence, to request certain evidence imposes re-victimization and the violation of their right to privacy. (Sentence T-453 of 2015)

¹⁶⁶ APC Submission 2018.

¹⁶⁷ De Justica Submission 2018.

¹⁶⁸ Op cit Loideain and Adams; <https://medium.com/pcmag-access/the-real-reason-voice-assistants-are-female-and-why-it-matters-e99c67b93bde>

¹⁶⁹ Op cit FRA, p53.

¹⁷⁰ UNESCO, Human rights and encryption, 2016; <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>

¹⁷¹ Special Rapporteur on the on the promotion and protection of the right to freedom of opinion and expression, David Kaye, May 2015. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement>

¹⁷² Dodge, A. R. Evolution of Technology Abuse. Presentation in Gender and Cyberspace Workshop at the Meridian 180 Global Summit, Chinese University Hong Kong, Hong Kong, June 2018.

¹⁷³ 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/>

¹⁷⁴ Op cit De Justica.

- c. A woman's decision to voluntarily terminate her pregnancy under the conditions of sentence C-355 of 2006, belongs to the private or intimate sphere, and is not a matter of public or general interest. (Judgment T-841 of 2011, among others)
 - d. Guardianship judges must reserve the identity of women and girls who apply for amparo their right to the IVE, regardless of whether the amparo is granted or denied. (Sentence T-841 of 2011, among others)
 - e. Health professionals and personnel who receive requests for voluntary termination of pregnancy must offer full guarantees of confidentiality and to respect women's right to privacy and dignity. (Sentence T-388 of 2009).
 - f. Proving a person's gender identity requires voluntary communication. (Sentence T-099 of 2015)
 - g. Authorities must take appropriate and necessary measures to guarantee the confidentiality and security of the personal data of same-sex couples and define the conditions for processing the database in which they are included. (Judgment T-444 of 2014).
 - h. Adoption of privacy protocols to protect intersex children that omit identifying details.¹⁷⁵
109. Examples provided of support programs, education and resources, included:
- a. training for front-line agencies on how abusive individuals misuse technology and how survivors can use technology safely and privately, and technical expertise provided to practitioners, policy makers, and technologists on technology-facilitated abuse issues impacting women, for example by Safety Net Australia.¹⁷⁶
 - b. collaborative projects such as Recharge Women's Technology Safety and SmartSafe, the expanded Recharge project with legal guides and referral information¹⁷⁷ for all states and territories, and online training programs (Australia).¹⁷⁸
 - c. preventative response model where healthy relationships have been mandated in health curriculum to teach respect, boundaries and appropriate expectations and behaviour (California, USA).
 - d. educational resources and training sessions for law enforcement and anti-violence workers, focusing on technology and the safety and privacy of women and children experiencing domestic violence and survivors of sexualized violence (*Safety Net Canada: Technology, Privacy, Safety and Violence Against Women, Youth and Children*).¹⁷⁹
 - e. practical and appropriate ways for service providers to collect information about sexual orientation, sex and gender, without breaching privacy, and increasing knowledge of the LGBTQI community (Australia).¹⁸⁰
 - f. chatroom for lesbian, gay, bi, trans(gender), hetero, questioning, pan, non-binary, queer, intersex or asexual young people under 18 years, developed by and for young LGBTQI people ('Jong & Out' project, COC Netherlands).¹⁸¹

¹⁷⁵ Constitutional Court of Colombia. Case [T-450A/13](#), [T-1025-02](#), [T-675-17](#).

¹⁷⁶ <https://wesnet.org.au/safetynet/>;

¹⁷⁷ <http://www.smartsafe.org.au/support-overview>

¹⁷⁸ <http://www.wlsnsw.org.au/recharge/>; <http://www.smartsafe.org.au/tech-safety-hub/resources/research>; <http://www.smartsafe.org.au/legal-guides>; <https://wesnet.org.au/safetynet/training/>

¹⁷⁹ "Safety Net Canada: Technology, Privacy, Safety and Violence Against Women, Youth and Children", Privacy Commissioner of Canada July, 2013 https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2012-2013/p_201213_04/

¹⁸⁰ A Guide to LGBTQI-inclusive data collection, 2017 The Canberra LGBTQI Community Consortium ACT, Australia.

¹⁸¹ Op cit Kazakhstan Feminist Initiative, 96.8% of users found the website safe and reliable, 91.4% would recommend the website to other young people.

- g. ‘European AI Alliance’ to assist in compiling ethical guidelines on AI development which will draw from the rights and principles of the EU Charter, including data protection.
- h. personal data of trans and intersex persons in court documentation: in Russia, several courts removed decisions revealing personal data of trans persons upon request.¹⁸²
- i. awareness raising among community members by providing practical booklets, seminars, trainings and media publications (Local defenders ‘Coming Out’ LGBT Group and ‘Stimul’ Initiative Group, Russia).¹⁸³

Conclusions

110. The Universal Declaration of Human Rights calls on “every individual and every organ of society” to promote and respect human rights.¹⁸⁴ States, companies, religious bodies, civil society, professional organisations all have important roles to play.
111. Protection for the privacy of individuals is a hallmark of States that value rights.¹⁸⁵ While privacy rights are not costless, or free of risks to governments, the challenges are outweighed by their contribution to democracy.¹⁸⁶
112. Individuals’ experience of digital technologies and privacy is influenced by their gender and gender identity, in combination with factors such as ethnicity, beliefs, culture, race, age, economic self-sufficiency, legal and political frameworks.¹⁸⁷
113. Privacy facilitates for all individuals, the full enjoyment of human rights, but is particularly important for women and children, individuals of diverse sexual orientations, gender identities, gender expressions and sex characteristics¹⁸⁸, who face inequality, discrimination or marginalisation due to gender, sexual orientation, gender identity or expression.
114. 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. Solutions focussing solely on individual victims are insufficient; inequalities in power, information, technology and economic standing need to be addressed at international, regional and domestic levels.
115. The virtual space is important for the construction of individual identity, but particularly so for members of the LGBTQI community. Identity is an integral part of personhood which is nurtured by the right to privacy. Formal recognition of identity is essential to effectively negotiating the modern world. As digital identity programs become mandatory in many parts of the world, the risks of discrimination on the grounds of sexual orientation, gender identity, gender expression and sex characteristics, are likely to increase.
116. While digital technologies enable users to participate in the public sphere, exercise human rights, find and create information, and engage with people and interests,¹⁸⁹ these benefits were

¹⁸² Joint International LGBTI Submission, 2018.

¹⁸³ Gender Perspectives on Privacy in Eastern Partnership Countries and Russia *Prepared by the Eastern European Coalition for LGBT+ Equality* 2018 e.g. <http://comingoutspb.com/news/kak-ne-stat-zhertvov-vymogatelstva-na-podstavnom-svidanii/>; <https://meduza.io/feature/2016/04/25/obschestvo-dobrota-novyve-ohotniki-na-geev>.

¹⁸⁴ Preamble, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

¹⁸⁵ Op cit Lever, A, referencing Westin, A.

¹⁸⁶ Op cit Lever, A.

¹⁸⁷ Privacy Commissioner of Canada, 2018, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

¹⁸⁸ <https://www.ohchr.org/en/issues/discrimination/pages/bornfreeequalbooklet.aspx>

¹⁸⁹ APC Submission 2018.

reported as differentially 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.

117. The use of the internet to target individuals according to gender generally involves infringing the right to privacy. Privacy harms extend beyond the individual to impact society as a whole. The loss of confidence of individuals to share ideas and to assemble undermines societies and democracy. Technological tools such as encryption, are critical to protect digital communications and thereby the enjoyment of human rights.
118. Protection of privacy can prevent discrimination. The role of States in preventing such discrimination includes actively protecting privacy in policy development, legislative reform, service provision, regulatory action, NGO and CSO support, and provision of education. These responses need to be based on the experiences of those affected and include females, males, transgender women and men, and people who are intersex, and others who identify as outside the gender binary and cis-normativity.
119. Protection of personal information online should be a priority with adoption of GDPR equivalent provisions (or better), in countries not party to the regulation.¹⁹⁰ Gender should be a key consideration for the development and enforcement of data protection frameworks.
120. Transparency and accountability is needed in how private companies are using personal data collected about users,¹⁹¹ and how they respond to reports of online harassment. Promoting greater gender diversity among those shaping online experiences is important for proactive steps to make products and platforms safer, more socially-responsible and accountable.
121. Even in a public or semi-public setting, individuals should be able to expect that certain aspects of their privacy will not be violated¹⁹² and to expect meaningful redress against, protection from, and consequences for, the perpetrator(s) of such privacy breaches.
122. **Further research is needed to understand better the interaction between privacy and gender** with specific research for example, on the experiences of all members of the LGBTQI community with regard to safety issues arising from app use.¹⁹³
123. The recommendations on privacy and gender have been made by the Special Rapporteur on Violence Against Women and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, amongst others, are supported.

Recommendations

United Nations bodies:

- (a) 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.

Member States to:

- (b) Adopt an intersectional approach which recognises the specific benefits, experiences and threats to privacy according to gender, and overarching privacy and human rights principles.

¹⁹⁰ C, submission 2018

¹⁹¹ Op cit Australian Competition and Consumer Commission.

¹⁹² Irish Civil Liberties Council Submission 2018, Office of the Privacy Commissioner of Canada Factum in the Jarvis SCC hearing, https://www.scc-csc.ca/WebDocuments-DocumentsWeb/37833/FM060_Intervener_Privacy-Commissioner-of-Canada.pdf.

¹⁹³ Clarke, R. Safeguards against Unpleasant Cyberspace Behaviour: Targets not Victims, and Self-Help before Criminalisation, Preliminary Draft 2 February 2016

- (c) 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 to ensure these do not discriminate on the basis of gender and adequately protect all, regardless of gender, gender identity and sex characteristics.
- (d) Adopt policies, legal and regulatory frameworks providing comprehensive protection for the use and development of secure digital communications, including by promoting strong encryption and anonymity-enhancing tools, products and services.
- (e) Promote meaningful internet access and bridge any digital gender divides through relevant mechanisms including building digital skills and appropriate online behaviour.
- (f) 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 of the victim.

In countering violence, States to:

- (g) Review and strengthen policies, legal and regulatory frameworks to address privacy violations leading to gender-based violence in digital contexts.
- (h) Increase primary prevention programs including education about gender; promoting and mainstreaming gender equality with guidelines for key aspects such as consent and inappropriate data practices; promote community awareness and support for victims, and challenge cultures of victim-blaming.
- (i) Reform criminal and civil laws to achieve consistent and uniform legislation to address cyberspace violence based on gender and gender identity, and provide civil regimes for redress that provide greater control to those concerned, and which adequately respond to technology-facilitated abuse, including use of online content to cause harm.
- (j) Explore third party liability options for platforms including social media networks, that permit the redistribution of private images and the continuation of harassment.
- (k) Ensure adequate consultation regarding legislation changes with victims and activists to ensure legislative changes meet the needs for justice.
- (l) Promote training for magistrates, lawyers, police, frontline workers and service providers on technology facilitated gender violence; review and improve existing investigation techniques and models with, for example, liaison-officers trained to investigate and respond to instances of assault using leading international practices, and provide technical support, counselling and advice services for victims.
- (m) Sustainably fund service providers for continuing service provision, training and resource development.
- (n) Privacy and data protection regulators, governments and other stakeholders to systematically consider the gender experience of privacy and how this defines necessary privacy protections, and to work with other authorities addressing human rights issues.

In responding to the identity issues raised, States to:

- (o) Implement Principle 6 of the Yogyakarta Principles+10 to protect the privacy of persons regardless of sexual orientation and gender identity.
- (p) Uphold the obligations to ensure that requirements for individuals to provide information on their sex or gender are relevant, reasonable and necessary as required by the law for a legitimate purpose in the circumstances where it is sought, and that such requirements respect all persons' right to self-determination of gender, and ensure that changes of the name or gender marker, as long as the latter exists, is not disclosed without the prior, free, and informed consent of the person concerned, unless ordered by a court.
- (q) Take all necessary legislative, administrative and other measures to fully respect and legally recognize each person's self-defined gender identity.
- (r) Develop, enact and implement a comprehensive legislative system for recognizing gender identity allowing transgender people to obtain legal recognition of their gender and to change their legal name and gender, including on official documents, through a quick, accessible and transparent procedure.

- (s) Provide guidance and training, particularly for front line service providers, on gender identity, on ending gender based discrimination and any other new measures taken allowing transgender people to obtain legal recognition of their gender.
- (t) design and implement a protocol for the definition of the military situation of trans people, in order for their gender identities to be recognised and for those who want to provide military service to be protected.

In relation to surveillance and gender, States to:

- (u) Enshrine the principles of gender-equality and non-discrimination in the design and implementation of all surveillance measures.
- (v) Undertake all appropriate measures to investigate, document and monitor the gendered impacts of surveillance infringements of privacy for women and lesbian, gay, bisexual, transgender and intersex individuals, including reporting to inter-governmental organisations.
- (w) Renounce the use of gender stereotypes for profiling, and promote human rights training to reduce the stigma, harassment and discrimination arising from profiling practices.
- (x) Implement policies and procedures that, amongst other human rights concerns, specifically address gendered and privacy implications of potentially sensitive CCTV footage, including relevant training of data controllers and those who can access the footage.
- (y) Implement data protection and security protocols to prevent the abuse, redistribution, or degrading treatment of captured images, including Privacy Impact and Risk Assessments and governance protocols with embargoes on face surveillance or other algorithmic analysis of captured surveillance without judicial permission and independent oversight.
- (z) Sanction egregious image-based sexual assault by law enforcement officials by both internal disciplinary and external disciplinary means. Create protocols for victim redress, and ongoing communication with victims' families.

In addressing gender privacy issues, Corporations to:

- (aa) Meet the 'UN Guiding Principles on Business and Human Rights' to respect the human rights of all persons effected by their practices by conducting due diligence including gender assessments, to prevent and human rights violations, mitigating adverse effects, and providing access to remedy for all who experience privacy violations.
- (bb) Enshrine the principles of gender-equality and non-discrimination in the design and implementation of all services including by renouncing the use of gender stereotypes for profiling, and promoting human rights training to reduce any stigma, harassment and discrimination arising from profiling practices.
- (cc) Take all necessary legal, administrative and other measures to fully respect and legally recognize each person's self-defined gender identity.
- (dd) Provide guidance and training, particularly for front line staff, on gender identity, and any other new measures taken allowing transgender people to obtain legal recognition of their gender, and end gender based discrimination within business operations.
- (ee) Engage more women and LGBTQI persons in the design, development and regulation of digital technologies to enable technical solutions to mitigate risks of mis-use of their technologies and to secure privacy and gender identities in digital contexts.
- (ff) Provide greater transparency of and access to data profiles, and monitor these for gender bias by, for example, algorithmic auditing.
- (gg) Implement a privacy by design/default approach using a gendered analysis, and embed users' meaningful consent into all aspects of the data life cycle use.
- (hh) Make it easier to report abuse (in local languages) and to respond to such reports in a timely manner.

- (ii) Limit data collection to restrict further data processing, prevent unnecessary access to and exploitation of data by utilising technological means and considering privacy in the design of systems.
- (jj) Resist requests for user data that do not comply with international human rights standards such as lawfulness, proportionality and necessity.

For the UNSRP to:

- (kk) Examine further the interactive dynamics between the right to privacy and gender experiences by engaging with the research, CSO/NGO and regulatory communities to explore the role infringements of the right to privacy play in gender based violence and discrimination, and how such infringements affect the enjoyment of other human rights.

Acknowledgements:

The submissions of individuals and organisations upon which this report is based, are gratefully acknowledged. The commitment of their authors is particularly recognised. The research support provided by Ms K. McKee, Mr S. McLaughlan and two others who wish to remain anonymous, also needs acknowledgement.

For Consultation

[Place], [Date]

[REFERENCE]

**DRAFT RECOMMENDATION ON THE PROTECTION AND USE OF HEALTH-RELATED
DATA**

Table of contents

Introduction	2
Chapter I. General provisions	3
Chapter II. The legal conditions for data processing of health-related data.....	6
Chapter III. The rights of the data subject.....	12
Chapter IV. Security and interoperability	15
Chapter V. Scientific research	16
Chapter VI. Mobile applications	18
Chapter VII. Transborder flows of health-related data	19
Chapter VIII. Electronic Health Records	19
Chapter IX. Health-Related Data, Genetic Data and Insurance	21
Chapter X. Health-related data and employers.....	24
Chapter XI. Indigenous Data Sovereignty and Health-related data	25
Chapter XII. Health-related data and Open Data.....	26
Chapter XIII. Health-related data and automated decision making	27
Chapter XIV. Mandatory Notification of Health-Related Data Breaches.....	27
Chapter XV. Right to Remedy for Health-Related Data Breaches.....	27
Chapter XVI. Protection of Reporters of Health-related Data Breaches	28
Chapter XVII. Liability	28
Chapter XVIII. AI, Algorithmic transparency and Big Data.....	29
Chapter XIX. Health-related Data in non-healthcare settings	29
Chapter XX. People Living with Disabilities and Health-related data.....	30
Chapter XXI. Gender and Health-related data.....	30
Chapter XXII. Intersectionality and Health-related data.....	30
References.....	30

Introduction

Recommendation on the protection and use of health-related data

This document was compiled by Sean McLaughlan in his capacity as Secretary to the Task Force on Privacy and the protection of health data (MediTAS) established by the United Nations Special Rapporteur on the Right to Privacy (SRP) Professor Joseph A. Cannataci. The document was prepared under the guidance of the SRP and the Chair person of MediTAS, Professor Nikolaus Forgo', with contributions from the members of the Task Force who, in February 2019 include Teki Akuetteh Falconer, Heidi Beate Bentzen, Elizabeth Coombs, Kenneth W. Goodman, Trix Mulder, Chris Puplick, William Smart, Sam Smith, Jane Kaye, Steve Steffensen, Thomas Trezise, Melania Tudorica and Helen Wallace.

This document is Version 0.1 and is work-in-progress. It is known to be incomplete in a number of areas and is not intended to be considered as a finished document. In particular, referencing and acknowledgment of sources used to develop ideas contained within the document is not yet complete, but will be documented. Reliance on work compiled and completed by others has assisted greatly in compiling this document for consultative purposes.

The document does not reflect necessarily the view of the Taskforce on Health Data, nor does it represent the view of any individual member or groups of members of that Taskforce. This very early version is being released for consultation in order to provide the opportunity for everybody to comment on the document and contribute to its development.

Chapter I. General provisions

1. Purpose

- 1.1 The purpose of this Recommendation is to provide guidance to the Member States for regulating health-related data in order to guarantee respect for the rights and fundamental freedoms of every person, particularly the right to privacy and to protection of personal data provided for in Article 12 of the Universal Declaration of Human Rights and related treaties or agreements.

2. Scope

- 2.1 This Recommendation is applicable to the data processing of health-related data in both the public and private sectors, not for profit entities, as well as charitable and non-government organisations. It applies to the collection, processing, analysis, exchange, transmission, and sharing of health-related data, including by means of digital technology. This Recommendation does not limit or otherwise affect any law that grants data subjects more, wider or better rights, protection, and/or remedies than this Recommendation.
- 2.2 The provisions of this Recommendation do not apply to health-related data processing performed by individuals in the context of purely personal or household activities. This Recommendation applies to individuals, government departments, agencies and authorities that may engage in personal activities in connection with their employment, service provision, volunteer work or under any contract where that individual deals with health-related data on their own behalf or as an agent for a third party.

3. Definitions

For the purposes of this Recommendation, the following definitions are used:

- “anonymisation” means a process applied to personal data so that the data subjects can no longer be identified either directly or indirectly, including with the use of, or linkage with, other data.
- “competent supervisory authority” means an independent public authority whose role, either solely or in conjunction with other purposes, is to oversee the implementation of, and compliance with, the terms of this recommendation.
- “controller” means the natural or legal person or persons, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to the processing of health-related data.
- “data processing” means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, preservation, adaptation or alteration, retrieval, access, consultation, use, disclosure, dissemination, making available, sharing, alignment or combination, restriction, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on personal data, and automatic processing of health-related data.
- “examination” includes any non-genetic or genetic test with diagnostic or predictive value. The results of an examination are of diagnostic value if they confirm or negate a

diagnosis of a disease in a person. The results of an examination are of predictive value, if they indicate a risk of the development of a disease in the future. The reliability of the results of examinations with predictive value is extremely variable from one to another. Examination also includes uses by law enforcement authorities (e.g. DNA screening for current or predictive investigations).

- "external data hosting" means the use of third-party data service providers irrespective of the platform used to securely and permanently store data in a digital form or forms.
- "genetic data" means all personal data relating to the genetic characteristics of an individual which have been either inherited or acquired during prenatal development, as they result from an analysis of a biological sample from the individual concerned, in particular chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.
- "genetic test" is defined in accordance with Article 2 of the Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes. The analysis undertaken in the context of genetic tests is carried out on chromosomes, DNA or RNA or any other element enabling equivalent information to be obtained.
- "health-care professionals" means all professionals recognised as such by law practising in the health, medical welfare or social welfare sector, bound by a confidentiality obligation and involved in providing health care.
- "health information system" means a system that provides the underpinnings for decision-making and has four key functions: data generation, compilation, analysis and synthesis, and communication and use. The health information system collects data from the health sector and other relevant sectors, analyses the data and ensures their overall quality, relevance and timeliness, and converts data into information for health-related decision-making¹.
- "health-related data" means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this individual's past, current and future health. Health-related data can be a basis for discrimination, and such discrimination may include "familial relationships" derived from health-related data.
- "health-related data breach" means the accidental, intentional or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, or prevention of lawful access to, or sale of, health-related data transmitted, stored or otherwise processed;
- "indigenous data" refers to data information or knowledge, in any format or medium, which is about, from or may affect indigenous peoples or people of first nations either collectively or individually and may include the language, culture, environments or resources of indigenous peoples.

¹ *Health Metrics Network Framework and Standards for Country Health Information Systems*, World Health Organization, January 2008.

- “indigenous data sovereignty” refers to the inherent rights and interests indigenous people have in relation to the creation, collection, access, analysis, interpretation, management, dissemination, re-use and control of data relating to indigenous peoples.
- “indigenous data governance” means the right of indigenous peoples to autonomously decide what, how and why indigenous data are collected, accessed and used. It ensures that data on or about indigenous peoples reflects the priorities, values, cultures, worldviews and diversity of indigenous peoples. This includes the principles, structures, accountability mechanisms, legal instruments and policies through which indigenous peoples exercise control over indigenous data.
- “insured person” refers to the individual whose risks are covered by a contract, whether in the process of being drawn up or already concluded.
- “insurer” refers to both insurance and re-insurance companies.
- “international organisation” means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
- “interoperability” means the ability of different information systems to communicate and exchange data.
- “mobile applications” means a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices that may be used for diagnostic, treatment or wellbeing purposes.
- “personal data” means any information relating to an identified or identifiable person (“data subject”).
- “processor” means a natural or legal person, public authority, agency or any other body which processes data on behalf of the controller.
- “profile” means a set of personal data characterising a category of individuals that is intended to be applied to an individual.
- “profiling” means an automatic data processing technique that consists of applying a profile to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.
- “pseudonymisation” means any processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organisational measures so that personal data cannot be attributed or attributable to an identified or identifiable individual. Pseudonymised data remain personal data.
- “recommendation” means this document.
- “reference framework” means a coordinated set of rules and/or processes updated and adapted to practice and applicable to health information systems, covering the areas of interoperability and security.

- “third party” means a natural or legal person, public authority, agency or body other than the data subject, insured person, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Chapter II. The legal conditions for data processing of health-related data

4. Principles concerning data processing of health-related data

- 4.1 Data processing of health-related data must comply with the following principles:
- a. Health-related data must be processed in a transparent, lawful and fair manner.
 - b. Health-related data must be collected for explicit, specific and legitimate purposes and must not be processed in a manner which is incompatible with the purposes for which it was originally collected.
 - c. Data processing of health-related data should be necessary and limited to the legitimate purpose pursued and must be carried out in accordance with paragraph 5 of this Recommendation.
 - d. Personal data must be collected from the data subject. Where the data subject is not in a position to provide the data and such data are necessary for the purposes of the data processing of health-related data, they may be collected from other sources in accordance with paragraph 5 of this Recommendation.
 - e. Health-related data must be adequate, relevant, accurate, up to date and limited to the purposes for which the data processing is to take place, and must be fit for those purposes or that purpose.
 - f. Processing of health-related data must take into consideration adequate security and organisational measures. Safeguards must be in place that guarantee respect for the rights of the individual or data subject and the security of the health-related data. Any other guarantees may be provided for by law that safeguard respect for rights and fundamental freedoms of data subjects and their health-related data.
 - g. Security measures must take into consideration the latest technological developments, the sensitive nature of health-related data and the assessment of potential risks. They must be established, implemented, documented, and regularly reviewed to prevent risks such as accidental or unauthorised access to, destruction, loss, use, unavailability, inaccessibility, modification, disclosure of health-related data or personal data, or any other health-related data breach.
 - h. The rights of the data subject whose health-related data are involved in any instance of data processing must be respected. This includes, but is not limited to, the rights of access to the data, information, rectification, objection, and deletion as provided for in paragraphs 11 and 12 of this Recommendation.
 - i. Data subjects have a right to data portability. This means that where the data subject has provided the health-related data and the data processing is based on

consent or on a contract to which the data subject is a party, the data subject shall have the right to request the transmission of their health-related data that are retained by an automated processing system and/or hard copy file or records to another entity chosen by the data subject.

- j. Data subjects have a right to informed consent prior to the processing or other use of their health-related data.
- 4.2 Personal data and health-related data protection principles must be considered by default (privacy by default) and incorporated into the design of information systems (privacy by design).
- 4.3 Compliance with all applicable principles for personal data and health-related data, including but not limited to those in this Recommendation, must be regularly reviewed. The controller must carry out, before commencing data processing and at regular intervals after the data processing, an assessment of the potential impact of the processing of data foreseen in terms of data protection, use of data and respect for privacy of the data subjects, including of the measures aimed at mitigating all risks.
- 4.4 Controllers and processors must take all appropriate measures to fulfil their obligations with regard to health-related data, including but not limited to those in this Recommendation, and must be able to demonstrate to a competent supervisory authority that all data processing of health-related data is being or has been undertaken in accordance with all applicable obligations.
- 4.5 Controllers and processors, including those who are not health-care professionals, must ensure that all data processing of health-related data is conducted in accordance with rules of confidentiality and security measures so that there is a level of protection equivalent to that imposed on health-care professionals.

5. Legitimate basis of data processing of health-related data

- 5.1 Data processing of health-related data is lawful if, and to the extent that, the data processing is carried out in accordance with the provisions of paragraph 4 of this Recommendation, there are legal safeguards, and the processing is necessary for:
 - a. direct benefits to the data subject such as medical diagnosis, care, treatment, and convalescence of the data subject;
 - b. preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of the social and medico-social sector, subject to the conditions provided for by law;
 - c. reasons of public health, for example protection against health hazards, communicable disease identification and containment, environmental hazards, humanitarian action or in order to attain a high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions provided for by law;
 - d. the purpose of safeguarding the vital interests of the data subject or of another individual where consent cannot be collected from the data subject, the other individual, or both;

- e. reasons relating to the obligations of controllers and to exercising the rights of the data subject regarding employment and social protection, in accordance with law or any lawful collective agreement;
 - f. the public interest in managing claims for social welfare and health insurance benefits and services, subject to the conditions provided for by law;
 - g. processing for archiving purposes in the public interest as defined in law, for scientific or historical research purposes assessed with reference to the role of the legal entity carrying out the activity, the role of the individual(s) carrying out the activity, quality standards including use of scientific methodology and scientific publication or statistical purposes subject to the conditions defined by law in order to guarantee protection of the data subject's fundamental rights and legitimate interests (see in particular the conditions applicable to the processing of health-related data for scientific research under Chapter V);
 - h. reasons essential to the recognition, exercise or defence of a legal claim in relation to the health-related data intended for data processing;
 - i. reasons essential to the identification of missing persons where there is no reason to believe that the individual said to be missing merely wishes to avoid contact and the circumstances of the person being missing raises concerns for his or her safety and well-being, on the basis of a law which provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject and their relatives; and
 - j. reasons of substantial public interest, on the basis of law, which shall be proportionate to the aim pursued, respect the right to privacy and data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
- 5.2 Health-related data may only be processed if the data subject has given her or his free, specific, informed and explicit consent to that data processing, except where law precludes a data subject from consenting to the data processing. Where the requirement for consent of the data subject is not precluded by law, the data subject must be informed at the time of being asked to consent of her or his right to withdraw consent to the data processing at any time and be notified that any such withdrawal of consent will not affect the lawfulness of any data processing already carried out on the basis of her or his consent prior to any withdrawal of consent. The data subject must also be provided with understandable, clear, comprehensive information relevant to making the decision to consent or not prior to making any decision to consent. It must be as easy for any data subject to withdraw consent as to give consent.
- 5.3 Data processing of health-related data may be undertaken by a data controller where the processing is necessary for the execution of a contract entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law that must include the obligation of secrecy. Any contract under this provision may not diminish or contravene the rights of the data subject under this Recommendation or any other law.
- 5.4 Data processing of health-related data manifestly made public by the data subject may be undertaken unless such processing would be inconsistent with the rights of the data subject under this Recommendation or otherwise safeguarded in law (such as for

insurance purposes). Information communicated by the data subject to her or his contacts on social media is not manifestly making data public.

6. Data concerning unborn children and minors

- 6.1 Health-related data and genetic data concerning unborn children, including but not limited to data resulting from a prenatal diagnosis, preimplantation diagnostics, or from the identification of the genetic characteristics of such children, must be protected to the same level as other health-related data.
- 6.2 Health-related data and genetic data concerning minors must be protected at least to the same level as other health-related data. Children have the same rights to privacy and data protection as adults. Wherever informed consent is the legal basis for the processing of personal data of a minor, the ability of the minor to fully understand consequences of processing must be taken into consideration. Therefore, where the child is below the age to understand the implications of processing, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. However, the consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child, provided that the services are offered by a health-care professional acting in the best interests of the child, in circumstances where the health of the child is otherwise at risk. Minors have a right to withdraw health related data from any health information system when they reach the age of legal majority.

7. Health-related genetic data

- 7.1 Data processing of genetic data may only be undertaken subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent expressed by the data subject in accordance with the provisions of paragraph 5.2, except where the law provides that a data subject cannot consent to any such processing of her or his genetic data.
- 7.2 Data processing of genetic data that is undertaken for preventative, diagnostic, or treatment purposes in relation to the data subject or a member of the biological family of the data subject or for scientific research may only be used for the particular purpose of the data processing or to enable persons concerned by the results of such processing of genetic data to take an informed decision without revealing to those persons concerned by the results the nature of their relationship to the data subject if that relationship is not already known to them. After such purposes have been achieved, the genetic data must be destroyed in the absence of the consent of the data subject to retaining and any subsequent use of the genetic data.
- 7.3 Data processing of genetic data for the purpose of a judicial procedure or investigation may be undertaken only when there are no alternative or less intrusive means to establish whether there is a genetic link for the production of evidence, to prevent a real and immediate danger or for the prosecution of a specific criminal offence, which must be subject to appropriate procedural safeguards. Such genetic data may not be used to determine other characteristics that may be linked genetically, nor may such genetic data or health-related data or personal data derived from that genetic data be retained beyond the necessary time period to complete the original purpose of the data processing of the genetic data. Universal genetic databases are prohibited. In the absence of consent from the data subject, genetic data to be used for the purpose of a

judicial procedure or investigation must be collected from the data subject and not from health-related data databases or biobanks that do not have a forensic purpose.

- 7.4 Processing of genetic data can be used for the purpose of identification of individuals in a humanitarian crisis, mass casualty event, or to assist in the identification of missing persons, and only where appropriate safeguards are provided for by law. Genetic health-related data held in biobanks and other health related data databases may be accessed for these purposes.
- 7.5 Existing predictive data resulting from genetic tests must not be processed for insurance (including life insurance) or law enforcement purposes, except where this is specifically provided for by law. In that case, their processing should only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.
- 7.6 The data subject is entitled to know any information relating to her or his genetic data subject to the provisions of paragraphs 11.5 and 12.7 that arise from data processing of genetic data. The data subject may have reasons for not wishing to know about certain health aspects arising from the data processing of genetic data. People must be informed, prior to any data processing, of the possibility of not being informed of the results, including of any incidental findings. The wish not to so be informed may, in exceptional circumstances, be restricted as foreseen by law, in cases such as where a doctor has a duty to provide care or where it is in the interests of public health. An individual's wish to be kept in ignorance of a diagnosis or prognosis should be respected, except where this constitutes a serious risk to the health of third parties. The information the data subject is entitled to know under this provision does not extend to unverified research results where, in an objective assessment, providing access may be misleading.
- 7.7 Genetic testing for health purposes should meet generally accepted criteria of scientific validity and clinical validity; a quality assurance programme should be implemented in each laboratory and laboratories should be subject to regular monitoring; persons providing genetic services should have appropriate qualifications to enable them to perform their role in accordance with professional obligations and standards; and the clinical utility of a genetic test shall be an essential criterion for deciding to offer this test to a person or a group of persons.

8. Sharing of health-related data for purposes of providing and administering health care

- 8.1 Where health-related data are disclosed by one health-care professional to another health-care professional and they are not connected to the same entity, for the purposes of providing and administering health care of an individual, the data subject shall be informed before the disclosure takes place, except where this proves to be impossible due to an emergency or in accordance with paragraph 11.4. Where the disclosure is based on the consent of the data subject, such consent may be withdrawn at any time in accordance with paragraph 5.2.
- 8.2 Health-related data can, unless other appropriate safeguards are provided for by law, only be communicated to an authorised recipient who is subject to the rules of confidentiality incumbent upon a health-care professional, or to equivalent rules of confidentiality.

8.3 The exchange and disclosure of data between health-care professionals must be limited to the information necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual. Health-care professionals should be able to disclose or receive health-related data necessary to care for the patient and undertake their duties according to prior authorisation. Appropriate measures must be taken to ensure the security of all data being exchanged or disclosed.

8.4 In the exchange and disclosure of health-related data, physical, technical or administrative security measures must be adopted to guarantee the confidentiality, integrity, authenticity, and availability of health-related data. In the event of the failure of these measures and a health-related data breach occurs, the parties to the breach must comply with the provisions of Chapter XV of this Recommendation.

9. Disclosure of health-related data for purposes other than providing and administering health care

9.1 Health-related data may be disclosed to recipients that are authorised and required by law to have access and possession of the health-related data for the purposes of data processing of that health-related data. Any such processing may only be authorised under appropriate and proportionate criteria defined by law, in light of the type of test used and the particular risk concerned.

9.2 Access to health-related or genetic data for the prevention or detection of a specific crime, or the conduct of a prosecution, must be subject to judicial oversight and specific approval by a court. Such access must only be provided where it is necessary and proportionate and where adequate safeguards exist in law to protect the rights and interests of the data subject.

9.3 Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

9.4 Insurance companies, employers and contractors cannot be regarded as recipients authorised to have access to health-related data of individuals unless law provides for this with appropriate safeguards and in accordance with paragraph 5.

10. Storage of health-related data

10.1 Health-related data must not be stored for longer than is necessary for the purposes for which the health-related data was processed. Where data processing of health-related data is for archiving purposes that are in the public interest, for scientific or historical research purposes or for statistical purposes, there must be appropriate measures to safeguard the rights and fundamental freedoms of the data subject and to prevent discrimination amongst families, groups and populations. For these very specific purposes, health-related data may be retained beyond the period of the initial purpose of the data processing provided it is pseudonymised or anonymised as soon as reasonably practicable without materially affecting the research, archiving activity or the statistical study. In the case of archives of information held by the state, the state shall be responsible for ensuring necessary and proportionate protections of that

information to prevent health-related data breaches. Where anonymisation is not possible, the data must be destroyed.

- 10.2 Storage of health-related data in proprietary formats denying access by the data subject to the health-related data may constitute a restriction on the exercise of rights of data subjects and constitute a health-related data breach.

Chapter III. The rights of the data subject

11. Transparency of processing

- 11.1 The controller must take appropriate measures to inform the data subject of the processing of her or his health-related data. To ensure fair and transparent data processing of health-related data, the information provided to the data subject must include:

- a) the identity and contact details of the controller and any processors,
- b) the purpose for which the health-related data are to be processed, and the legal basis for the data processing of that health-related data,
- c) the length of time the health-related data will be stored for,
- d) the recipients or categories of recipients of the health-related data, and planned health-related data transfers to a country other than the country the health-related data is obtained in, or an international organisation (in this case data may only be transferred to an international organisation that accepts it must comply with the terms of this recommendation),
- e) the possibility, if applicable, of objecting to the processing of her or his health-related data, in the conditions prescribed in paragraph 12.2,
- f) the conditions and the means made available to her or him for exercising via the controller her or his rights of access, of rectification and to erasure of her or his health-related data,
- g) that data processing of her or his health-related data may subsequently occur if such data processing is for a compatible purpose or is for archiving purposes that are in the public interest, for scientific or historical research purposes or for statistical purposes, in accordance with appropriate safeguards provided for by law and in compliance with the conditions prescribed in paragraph 4.1.b,
- h) the existence of automated decisions, including profiling which is only permissible where prescribed by law and subject to appropriate safeguards, that may be made in respect of the health-related data,
- i) information required about the risks of the intended data processing and remedies available in the event of a health-related data breach,
- j) how the data subject may lodge a complaint about the data processing of their health-related data and to whom such a complaint is to be made in each jurisdiction the data processing may occur in,
- k) identity and contact details of data protection officers or data controllers from whom the data subject may seek further information in relation to the proposed data processing of health-related data,
- l) proposed jurisdictions the data processing of the health-related data may involve and the rights the data subject will have comparative to these rights.

- 11.2 This information specified in paragraph 11.1 must be provided prior to the data processing of the health-related data, namely data collection.

- 11.3 The information must be intelligible and easily accessible, in plain language and suited to the circumstances to enable a full understanding of the data processing of the health-related data by the data subject. Where the data subject is physically or legally incapable of receiving the information, or of making a decision based on the information, it must be provided to the person legally representing her or him or the person with authority to make these decisions for the data subject. If a legally incapacitated person is capable of understanding, he or she must also be informed before the data processing of the health-related data is conducted.
- 11.4 The controller is not required to provide the information in paragraph 11.1 where;
- (a) the data subject already has that information or
 - (b) health-related data is permitted not to be collected directly from the data subject or
 - (c) the data processing of that health-related data is expressly prescribed by law or
 - (d) it is impossible to contact the data subject.

In such cases the controller shall take appropriate measures to protect the data subject's rights.

Where the data processing of the health related data is for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, and the data subject cannot be found or is not reachable after reasonable efforts have been made, data processing of health related for these purposes may be undertaken provided that in these cases, the health-related data must be pseudonymised or anonymised before the data processing occurs, unless otherwise provided by law.

- 11.5 The controller is not required to inform the data subject where data processing of health-related data is provided for by a law that is both necessary to the purpose that it is intended to achieve and proportionate in the manner it seeks to achieve this purpose with regard to the rights and freedoms of the data subject. Such laws should nevertheless provide for general information to be accessible to all data subjects, including regarding the purpose and uses of the data, access to data by third parties, and data subjects' rights.

12. Access to, portability, rectification, erasure, and objection to the processing of health-related data

- 12.1 The data subject has the right to know whether data processing of health-related data that concern her or him is being conducted, and, if so, to obtain - without excessive delay or expense and in an intelligible form - communication of her or his health-related data and to have access on the same conditions to, at least, the following information:
- (a) the purpose or purposes of the data processing of the health-related data,
 - (b) the categories of health-related data concerned,
 - (c) the recipients or categories of the recipients of the health-related data and the envisaged data transfers to a third country or countries, or an international organisation or organisations,
 - (d) the period that the data-processing of the health-related data will take place,
 - (e) the reasoning underlying data processing of the health-related data where the results of such data processing are applied to her or him, including in the case of profiling, which is only permissible where prescribed by law and subject to appropriate safeguards.

- 12.2 The data subject has the right to erase any health-related data processed contrary to this Recommendation. The data subject is entitled to obtain rectification of health-related data concerning her or him that is inaccurate or misleading. The data subject has the right to object to the data processing of her or his health-related data on grounds relating to her or his personal situation. Where a controller is authorised by law to undertake data processing of health-related data notwithstanding the objection, the controller must notify the competent supervisory authority of the proposed data processing and the objection made by the data subject in a manner that will not identify the data subject (unless the data subject consents to being identified in this process). This information must be reported to the competent supervisory authority for the purposes of examining if systemic issues are arising and if unforeseen needs must be addressed.
- 12.3 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, she or he must be able to review that decision before a competent supervisory authority, and have access to a suitable remedy if a health-related data breach has occurred. If a health-related data breach has occurred the data controller or processor must undertake the steps provided for in this recommendation relating to breach notification and the data subject may access the remedy provisions of this recommendation or any others available to her or him in the relevant jurisdiction(s).
- 12.4 The data subject shall have the right not to be subject to a decision significantly affecting her or him based solely on an automated processing, including profiling, of her or his health-related data. Derogation from this prohibition is only allowed where the law provides that such a data processing of health-related data can be based on the consent of the data subject or that the processing is necessary for reasons of substantial public interest. Any such law must be proportionate to the aim pursued, respect the right to data protection and the right to privacy and provide for suitable and specific safeguards to protect the fundamental rights and freedoms of the data subject. Profiling for health purposes should meet generally accepted criteria of scientific validity, clinical validity and clinical utility and be subject to appropriate quality assurance programmes.
- 12.5 Data subjects may obtain from the controller, subject to conditions prescribed by law, where the data processing of health-related data is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of their health-related data with a view to transmitting that health-related data to another controller (data portability). The data subject may also require the controller to transmit the health-related data directly to a nominated controller without delay.
- 12.6 Health care professionals must put in place all necessary measures to ensure respect for the effective exercise of the rights of data subjects contained in this Recommendation as an element of their professional conduct and obligations.
- 12.7 The rights of the data subject may be subject to restrictions where such restrictions are provided for by law and that law constitutes both a necessary and proportionate measure in the interests of:
- (a) protecting State security, public safety, the economic interests of the State or the suppression of criminal offences;
 - (b) protecting the data subject or the rights and freedoms of others.

Provided that any such law must provide for appropriate safeguards ensuring respect for the data subject's rights.

Chapter IV. Security and interoperability

13. Security

- 13.1 Data processing of health-related data must be conducted securely. Security measures, which should consider human rights and fundamental freedoms, must be defined and implemented to ensure that all entities conducting data processing of health-related data observe the highest standards guaranteeing the lawfulness of any data processing, and security and confidentiality of any health-related data.
- 13.2 Data security provisions, provided for by law or other regulations, and which may be contained in reference frameworks, may require technical and organisational measures, that must be regularly reviewed, to protect health-related data from any health-related data breach. The law must make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.
- 13.3 System availability, meaning the proper functioning of systems containing health-related data, must be facilitated with measures that enable the health-related data to be made accessible in a secure way and with due regard for the level of permission of authorised persons. Such system availability is to be considered in the context or emergency situations to ensure system availability and integrity of health-related data, including access by the data subject.
- 13.4 Guaranteeing the integrity of any data processing of health-related data requires mechanisms to enable verification of the data processing actions carried out on the health-related data, such as any modification, deletion, copying, comparison, integration, communication and sharing of health-related data. It also requires the establishment of measures to monitor access to and use of the health-related data and the data themselves, ensuring that only authorised persons are able to access, use, and engage in data processing of the health-related data. Systems containing health-related data must be auditable, meaning that it must be possible to identify the user that undertook any specific action or data processing. No data processing by any person under the authority of the controller or the processor may be undertaken except on instructions from the controller, unless required by a necessary and proportionate law.
- 13.5 External data hosting of health-related data must ensure the security of the health-related data and comply with all principles of personal data protection and the right to privacy. Where external data hosting or any outsourcing of the storage and use of health-related data occurs, data subjects must be informed prior to the action being taken and given time to consider if they consent to their health-related data being dealt with in this way. In cases where they do not the health-related data should be dealt with in line with the provisions of this recommendation.
- 13.6 Professionals not directly involved in the individual's health care, including employees undergoing training, but by virtue of their assigned tasks enable the operation of information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to health-related data in an information system.

Such professionals must have full regard for the confidentiality of the information, any applicable professional secrecy and comply with all laws that guarantee the confidentiality and security of the health-related data as they will be liable, in conjunction with their employer or contracting party, for any consequential health-related data breach.

14. Interoperability

- 14.1 Interoperability must be carried out in full compliance with the principles provided for by this Recommendation, in particular the principles of lawfulness, necessity and proportionality and that data protection safeguards be put in place when using interoperable systems.
- 14.2 Reference frameworks, offering a technical framework that facilitates interoperability, must guarantee a high level of security. The implementation, compliance and use of such reference frameworks must be audited regularly.

Chapter V. Scientific research

15. Scientific research²

- 15.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards provided for by law, comply with the provisions of this Recommendation and with any other rights and fundamental freedoms of the data subject, and be carried out for a legitimate purpose. No individual may be required or compelled to participate in scientific research without their prior consent.
- 15.2 The need to perform data processing of health-related data for scientific research must be evaluated in light of the purposes of the scientific research, the risks to the data subject and, as concerns the processing of genetic data, the risk to the biological family that share some of that genetic data with the data subject. Any derogations from patients' rights for research may only be used when necessary and proportionate.
- 15.3 Processing of health-related data in a scientific research project may only be undertaken if the data subject has consented to it in accordance with the provisions of paragraph 5.2 of this Recommendation, except where provided for by law. Any such law providing for the processing of health-related data for scientific research without the data subject's consent must be necessary, proportionate and in accordance with a law that determines it to be in the public interest. Such a law must be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific safeguards to protect the rights and freedoms of the data subject. These safeguards should especially include the obligation to put in place technical and organisational measures to ensure the respect for the principle of data minimisation, purpose limitation and specification, deletion, destruction, pseudonymisation and anonymisation of data at the earliest opportunity.
- 15.4 The data subject must, in addition to what is required by Chapter III of this Recommendation (including but not limited to paragraph 11.1), be provided with prior,

² Considering orienting with World Medical Association *Declaration of Helsinki – Ethical Principles for Medical Research Involving Human Subjects 1964 and as amended and updated*.

transparent and comprehensible information that is as precise as possible with regard to:

- a) the nature of the envisaged scientific research, the possible choices that she or he may exercise as well as any relevant conditions governing the use of the health-related data, including recontact and feedback of results/findings;
 - b) the conditions applicable to the storage of the health-related data, including access and possible communication policies;
 - c) the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the scientific research and withdrawal of consent to take part on the scientific research in the same manner as paragraph 5.2 of this Recommendation at any time; and
 - d) the identity and location and purpose of any disclosure of health-related data to be made under paragraph 15.8 of this recommendation. The data subject must be informed specifically of her or his right to refuse to participate in the scientific research and withdrawal of consent to take part on the scientific research in the same manner as paragraph 5.2 of this Recommendation; and
 - e) the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, post-study provisions and any other relevant aspects of the study; and
 - f) the identities of any third parties who will be given access to the data, or who may lawfully seek access to the data for other purposes and how those purposes are limited; and
 - g) the publication that is proposed for the health-related data.
- 15.5 The controller should not be obliged to provide the information directly to each data subject if the conditions laid down in paragraph 11.5 are satisfied. However, when paragraph 11.5 applies, the information should nevertheless be made available to data subjects in a publicly-accessible way (for example, on a website).
- 15.6 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able to express consent for certain areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards. This provision does not in any way reduce the requirements of consent in paragraph 5.2 of this Recommendation as they apply to scientific research. Data subjects may also give prior consent to the future use of their health-related data for scientific research purposes after their death. In the absence of such consent, any health-related data retained must be anonymised after the death of the data subject.³
- 15.7 The conditions in which data processing of health-related data is conducted for scientific research must be assessed by the competent independent body (for example by an ethics committee) which includes lay members, prior to the commencement of the scientific research. This assessment must include consideration of the impact on data subjects in terms of privacy and other rights that may be affected. These assessments are to be reviewed periodically by the competent supervisory authority to ensure compliance with the terms of the approval, and the fact of the approval.
- 15.8 Health-care professionals entitled to carry out their own medical research and scientists in other disciplines may process health-related data as long as the data subject has

³ Consider provisions of the *Human Tissue Act 2004* (UK).

been informed of this possibility beforehand in compliance with paragraph 15.4 and has consented to it.

- 15.9 Other scientists holding health-related data will be liable for any health-related data breach in respect of the health-related data while it is in their possession or control. Complementary safeguards determined by law such as requiring explicit consent or the assessment of the competent body designated by law must be established before other scientists may acquire health-related data.
- 15.10 Where scientific research purposes allow, health-related data must be anonymised. Where research purposes do not allow anonymisation, pseudonymisation of the health-related data, with the intervention of a trusted third-party at the separation stage of the identification data, should be implemented to safeguard the rights and fundamental freedoms of the data subject. This must be done where the purposes of the scientific research can be fulfilled by further data processing of health-related data that does not permit or no longer permits the identification of data subjects.
- 15.11 Where a data subject withdraws consent for scientific research, her or his health-related data processed in the course of that research must be destroyed in compliance with the wishes of the data subject unless to do so would be contrary to law. If the destruction is contrary to law, the data subject must be informed of this and of the law requiring retention of the health-related data. Where manipulation of the data may be undertaken in a manner that does not compromise the scientific validity of the research but ensures the data subject cannot be identified even with the use of other data sets, this may be undertaken as an alternative to destruction and the data subject should be informed accordingly. Where the data subject continues to require destruction of her or his health-related data, this must be complied with.
- 15.12 Health-related data used for scientific research must not be published in a form that enables the data subject to be identified, except:
- a. where the data subject has consented to it and that consent has not been withdrawn, or
 - b. where law permits such publication on the condition that this is indispensable for the presentation of research findings on contemporary events and only to the extent that the interest in publishing the data overrides the interests and fundamental rights and freedoms of the data subject.

Where the consent of the data subject to publication of health-related data that identifies that subject is withdrawn, the data controller and or processors must destroy or take down the health-related data where practicable.

- 15.13 Provision(s) on transnational research to be drafted.

Chapter VI. Mobile applications

16. Mobile applications

- 16.1 Where the data collected by these applications, whether implanted on the individual or not, may reveal information on the physical or mental state of an individual in connexion with her or his health and well-being or concern any information regarding health care and medico-social provision, they constitute health-related data. In this connection they

enjoy the same legal protection and confidentiality applicable to other health-related data processing as provided by this Recommendation and, where applicable, supplemented by law.

- 16.2 Individuals using such mobile applications, as soon as they involve the data processing of their health-related data, enjoy the same rights as those provided for in Chapter III of this Recommendation. The individual must notably have obtained beforehand all necessary information on the nature and functioning of the system, as well as risks, such as health risks and security risks, in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor whose respective roles have to be determined in advance.
- 16.3 Any use of mobile applications must be accompanied by security measures that provide for the authentication of the person concerned, the encryption of the transmitted health-related data, and user or patient information standards on how the health-related data that is collected will be used.
- 16.4 Any external hosting of health-related data produced by mobile applications must comply with security rules providing for the confidentiality, integrity, access and restitution of the data upon request of the data subject.

Chapter VII. Transborder flows of health-related data

17. Protecting health-related data flows

- 17.1 Transborder data flows may only take place where an appropriate level of data protection is met by the recipient, or on the basis of the following provisions aimed at allowing a transfer to a recipient that does not ensure such an appropriate level of protection:
 - a. the data subject has given explicit, specific and free consent to the transfer, after being informed of risks arising in the absence of appropriate safeguards in a similar manner to paragraph 5.2; or
 - b. the specific interests of the data subject require it in the particular case; or
 - c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure; or
 - d. the transfer constitutes a necessary and proportionate measure for freedom of expression.

Chapter VIII. Electronic Health Records

18. Protecting health-related data in Electronic Health Records

- 18.1 All individuals have a right to privacy and the confidentiality and protection of their health-related data in electronic health record (EHR) systems, both institutional and cross-institutional, must be rigorously managed according to data protection, ethical, professional, legal and all other applicable requirements by all healthcare professionals and any person dealing with EHR systems.

- 18.2 No individual can be compelled to have an EHR against their will. Treatment of individuals cannot be withheld by virtue of the individual not having an EHR. No individual may be compelled to continue to have an EHR and where an individual provides notice that she or he no longer wishes to have an EHR, the health-related data in the EHR must be destroyed or rendered inaccessible to users of the EHR as soon as practicable after the instruction has been communicated. No health-related data in an EHR is to be destroyed where to do so would be in contravention of another law that is necessary and proportionate. These provisions are consistent with the right of the data subject to opt out at any time as required by this recommendation.
- 18.3 Data processing of health-related data in an EHR must be governed by an incremental system of “opt-in” requirements for the data subject to approve as they see fit having had the requirements consequences of any decision explained to them. Mandatory information regarding disclosure, ability to opt out and how health related data is handled must be provided to data subjects.
- 18.4 A data subject may elect to prevent disclosure of her or his health-related data in an EHR, documented by one health professional during treatment, to other healthcare professionals, if she or he chooses to do so. An EHR system must be auditable and include electronic protocol of who had access to data in an HER, duration of that access, logs of modification and protocols to ensure unauthorised access does not occur and that data subjects know who has had access to their health-related data.
- 18.5 Data processing of health-related data in an EHR may only be undertaken by healthcare professionals and authorised personnel of healthcare institutions who are involved in the data subject’s treatment. There must be a relationship of actual and current treatment between the data subject and the healthcare professional wanting access to health-related data in her or his EHR. Any other healthcare professional seeking access to health-related data of the data subject in an EHR must have the prior consent of the data subject. There must also be common standards for data accuracy and quality for all health-related data stored in an EHR.
- 18.6 Evidence of a patient’s consent to accessing her or his EHR data is necessary. Reliable instruments for such proof must be provided in any EHR system. Presentation of such proof must be electronically documented for auditing purposes. The same is true for evidence of a patient’s withdrawal of consent.
- 18.7 Where direct access by a data subject to her or his health-related data in an EHR is a feature of any EHR system, the operator of that EHR system must ensure that secure electronic identification and authentication is provided to prevent access by unauthorised persons, which is a health-related data breach.
- 18.8 The main purpose for data processing of health-related data in an EHR system is to achieve successful medical treatment of patients by using and having access to better health-related data to achieve that end. Data processing of health related data may be undertaken in relation to health-related data in an EHR where the data processing of health-related data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where the data processing of health-related data is undertaken by a health professional subject under law or rules to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

- 18.9 No person shall be induced to disclose or provide access to the health-related data in their EHR where such access or disclosure is not provided for or required.
- 18.10 Data processing of health-related data in EHR systems for the purposes of medical scientific research and statistical purposes is allowed where they are necessary for previously determined, specific purposes under special conditions and guarantee proportionality so as to protect the fundamental rights and the privacy of individuals and are provided for by an existing law. Health-related data from EHR systems may only be used for other purposes in anonymised form.
- 18.11 A data subject must have access to health-related data that relates to them that is in an EHR system. Access must be given without undue delay or expense. EHR systems may have many different data controllers, and where there is more than one controller, a single entity must be made responsible to data subjects for the proper handling of access and other requests about the EHR. Health-related data should not be stored in an EHR beyond the time required for the purposes for which it was collected.
- 18.12 Regular internal and external auditing of access protocols in any EHR must take place and be reported publicly. Entities that use EHR systems must have data protection officers to assist data subjects and health care professionals to meet their obligations in respect of the EHR.
- 18.13 No health insurance company may be granted access to the EHR of a data subject. Access to information that is required by law to be given to private insurance companies may be provided by the use standard protocols within EHR systems and transmitted electronically to the insurance company with the prior consent of the data subject if provided for by law.
- 18.14 Genetic data, including biological and test or tissue sample results, contained in an EHR cannot be provided to third parties except in compliance with a necessary and proportionate law.

Chapter IX. Health-Related Data, Genetic Data and Insurance

19. Health-related/Genetic data and insurance companies

- 19.1 Genetic data is the ultimate identifiable data. Genetic data and biological samples linked to an identifiable person may not be disclosed or made accessible to third parties, in particular, employers, insurance companies, educational institutions and the family of the individual, except where there is an important public interest reason in cases restrictively provided for by domestic law consistent with the international law of human rights or where the consent of the data subject has been obtained provided that such consent is in accordance with domestic law, the international law of human rights and paragraph 5.2 of this Recommendation. The privacy of a data subject participating in a study using human genetic data, human proteomic data or biological samples must be protected and the data must be treated as confidential.
- 19.2 Genetic data kept for statistical purposes must be rendered anonymous and retained in a form in which identification of the persons is no longer possible, including when used in conjunction with other available data sets.

- 19.3 Health-related data and genetic data obtained for scientific research purposes cannot be used for insurance related purposes in respect of the data subjects from which it was obtained, or the biological family members of those data subjects.
- 19.4 To draft a clause or clauses addressing employers who are self-insured and therefore acting as insurers. Also address degree to which employer can share information about a specific employee or general employee population with third party insurers for the purpose of risk and rate determination.
- 20. Insurers must justify data processing of health-related data including genetic data**
- 20.1 Health-related personal data may only be processed for insurance purposes subject to the following conditions;
- (a) the processing purpose has been specified and the relevance of the data has been duly justified and the person has been informed about the relevance to the risk and its justification. "Relevance" refers to the value of the information recognised as appropriate for assessing the state of health of an insured person and evaluating the risks relating to his or her future health. The results of an examination with predictive value do not per se fulfil the criterion of relevance, as the reliability of the results of examinations with a predictive value is extremely variable from one examination to another;
 - (b) the quality and validity of the proposed data processing of the health-related data are in accordance with generally accepted scientific and clinical standards;
 - (c) data resulting from a predictive examination have a high positive predictive value;
 - (d) processing is duly justified in accordance with the principle of proportionality in relation to the nature and importance of the risk in question; and
 - (e) The quality and validity of health-related personal data processed for insurance purposes should meet generally accepted scientific and clinical standards. Such data may include already existing health-related data resulting from examinations previously carried out as well as data resulting from examinations requested by insurers. In both cases, the examinations concerned must comply with generally accepted scientific and clinical criteria and be used in clinical practice. It is essential in this context that the interpretation of the data is of high quality.
- 20.2 Health-related data from family members of the insured person should not be processed for insurance purposes, unless specifically authorised by law. If so, the criteria laid down in paragraph 19.1 and the restriction laid down in paragraph 22.3 must be respected. The only permitted exceptions should be in cases where the information is relevant and where the family members concerned gave their consent prior to any such data processing.
- 20.3 The processing for insurance purposes of health-related data obtained in the public domain, such as on social media or internet fora, is not permitted to evaluate risks or calculate premiums.
- 20.4 The processing for insurance purposes of health-related personal data obtained in a research context involving the insured person is not permitted.
- 20.5 Questions posed by the insurer should be clear, intelligible, direct, objective and precise. Insurers must provide easy and free access to a contact person that has the

requisite competence and experience, to address any difficulties in understanding the documents relating to the collection of health-related data.

21. Insurers must not process health-related data without the consent of the insured person or data subject

21.1 Health-related data must not be processed for insurance purposes without the insured person's free, express and informed consent in accordance with paragraph 5.2.

21.2 Health-related data must be collected from the insured person by the insurer. The transmission of health-related data by a third party may only be made with the prior free, express, informed and explicit consent of the insured person.

22. Insurers must have adequate safeguards for the storage of health-related data.

22.1 Insurers may not store health-related data which is no longer necessary for the accomplishment of the purpose for which it was collected. Insurance companies may not store health-related data if an application for insurance has been rejected, or if the contract has expired and claims can no longer be made unless such storage is required by a law that is both necessary and proportionate.

22.2 Insurers must adopt internal regulations to protect the security and confidentiality of the insured person's health-related data. In particular, health-related data should be stored with limited access separately from other data, and health-related data kept for statistical purposes should be anonymised at the first opportunity.

22.3 Internal and external audit procedures should be put in place for adequate control of the processing of health-related personal data with regard to security and confidentiality.

23. Insurers must not require genetic tests for insurance purposes

23.1 Predictive genetic tests must not be carried out for insurance purposes.

23.2 Data processing of existing predictive data derived from genetic data tests may not be processed for insurance purposes unless specifically authorised by law. If such tests are authorised by law, the requisite data processing should only be allowed after independent assessment of conformity with the criteria laid down in paragraph 20.1 by type of test used and with regard to a particular risk to be insured.

23.3 Existing data from genetic tests of family members of the insured person may not be processed for insurance purposes and must be destroyed if comes within the purview of the insurer.

24. Insurers should take account of new scientific knowledge

24.1 Insurers must regularly update their actuarial bases in line with relevant, new scientific knowledge.

24.2 The insurer must provide relevant information and justification to any insured person regarding the calculation of the premium, any additional increase in premium or any total or partial exclusion from insurance that is based, in whole or in part, on health-related data.

25. States should ensure adequate mediation, consultation and monitoring

25.1 Mediation procedures must be established to ensure fair and objective settlement of individual disputes between insured persons and insurers. Insurers should inform all insured persons about the existence of these mediation procedures. Any such mediation procedures may not exclude any claimant from accessing legal remedies available to them.

25.2 Consultation between insurers, patient and consumer representatives, health professionals and the competent authorities should be promoted to ensure a well-balanced relationship between the parties and increase transparency to consumers.

25.3 Independent monitoring of practices in the insurance sector in order to evaluate compliance with the principles laid down in this recommendation must be established and monitored by a competent and independent regulator.

Chapter X. Health-related data and employers

26. Health-related data and employers

26.1 A controller of health-related data may include an employer⁴, and the obligations of controllers in this recommendation apply to employers that are controllers. Any health-related data breach for which an employer is liable as a controller will allow the employee or data subject affected by the breach access to remedies available in this Recommendation, and possibly elsewhere.

26.2 An employer may not seek health-related data from a job applicant until that person has been offered a job, except for one of the following purposes:

- (i) to enable the employer to make reasonable adjustments to the place of work to facilitate the employment of the individual;
- (ii) to establish whether the applicant can carry out a function that is intrinsic to the work concerned;
- (iii) to monitor diversity and facilitate the employment of disabled persons.

An employer may process relevant health-related data relating to employees (such as medical certificates and other medical data) provided that the health-related data is handled only by the medical service of the organisation. Human resources should only receive the administrative data necessary to process the sick leave (for example the number of days of sick leave) connected with any health-related data.

26.3 Employees must be informed by an employer about their rights and what the purposes are for the data processing of their health-related data. Such information must be specifically communicated to staff members when a new procedure is introduced and

⁴ Need to consider if this will apply to all employers, or if, say, SMEs may need to be excluded from some of the following provisions.

made permanently available for employees. This ensures that staff members have access to the information at all times.

- 26.4 Employees have the right to access their medical files and other health-related information to be able to verify whether it is accurate and to rectify any inaccurate or incomplete information. They must also be informed on how they may exercise their rights.
- 26.5 Employers must make sure that information relating to health of employees is not kept on their files for longer than necessary. Clear retention periods must be established. These can vary in accordance with the reason for processing the health data.
- 26.6 Due to its sensitivity, health-related data may only be processed by health-care professionals bound by the obligation of medical secrecy, or other professional bound by similar obligations of secrecy, such as lawyers and legal professional privilege. All human resources staff dealing with administrative or financial procedures in this respect should sign a specific confidentiality declaration and they should be reminded of their confidentiality obligations regularly. Furthermore, organisations should carry out a risk assessment and develop, where necessary, specific security measures on access control and management of all the information processed in the context of health data.

Chapter XI. Indigenous Data Sovereignty and Health-related data

27. Indigenous Data Sovereignty and Health-related data

- 27.1 Indigenous peoples have the right to:
 - (a) Exercise control of health-related data that relates to indigenous peoples. This includes the creation, collection, access, analysis, interpretation, management, security, dissemination, use, reuse infrastructure and all other data processing of health-related data relating to indigenous peoples.
 - (b) Access and be consulted on health-related data of indigenous peoples that is contextual and disaggregated (available and accessible at individual, community and first nations levels).
 - (c) Health-related data of indigenous peoples that is relevant and empowers sustainable self-determination and effective self-governance for indigenous peoples and first nations.
 - (d) Health-related data structures that are accountable to indigenous peoples and first nations.
 - (e) Health-related data that is protective and respects the individual and collective interests of indigenous peoples and first nations.
 - (f) Decide which sets of health-related data require active governance involving indigenous peoples.
 - (g) The right to not participate in any data processing of health-related data that is inconsistent with the principles asserted in this recommendation, and with the rights of indigenous peoples and first nations generally.

- (h) Exercise indigenous Data Governance and indigenous Data Sovereignty in respect of health-related data and the data processing of health-related data that relates to indigenous peoples.
 - (i) Decisions about the physical and virtual storage of health-related data relating to indigenous peoples shall enhance control for current and future generations of those indigenous peoples. Whenever possible, health-related data relating to indigenous peoples shall be stored in the country or countries where the indigenous people to whom the data relates consider their traditional land to be.
 - (j) The ability to disaggregate health-related data of indigenous peoples increases its relevance for the communities and other traditional groupings of indigenous peoples. Health-related data of indigenous peoples shall be collected and coded using categories that prioritise the needs and aspirations of indigenous peoples as determined by them.
 - (k) The collection, use and interpretation of data shall uphold the dignity of indigenous communities, groups and individuals. Data analysis that stigmatises or blames indigenous peoples can result in collective and individual harm and should be actively avoided.
- 27.2 Indigenous data governance enables indigenous peoples, representatives of indigenous Peoples and governing bodies of indigenous peoples to ensure that health-related data is accurately dealt with. Indigenous data governance provides indigenous peoples and first nations with the necessary tools to identify what works, what does not and why in respect of indigenous peoples. Effective indigenous data governance empowers indigenous peoples to make, or be more involved in making, decisions to support communities and first nations in the ways that meet development needs and aspirations of these communities. States must provide indigenous data governance to indigenous peoples within their territorial boundaries.

Chapter XII. Health-related data and Open Data

28. Health-related data and Open Data

- 28.1 As health-related data is sensitive data, and the consequences of disclosure of this sensitive data present greater risks to the individual in terms of discrimination and other consequences, no health-related data at the unit record or patient/person level may be released as Open Data, nor may pseudonymised data be released as Open Data, without the consent of each individual that may be affected. In the case of genetic data, an individual that may be affected includes a biological family member of the individual that proposes to disclose their genetic data.
- 28.2 Where information is released as Open Data and a consequential health-related data breach arises from that release, the party that processed the health-related data, and the party that released it as Open Data (where they are not the same) shall both be liable to data subjects harmed by such release.
- 28.3 Liability under this recommendation is in addition to any other liability for the harm caused that may exist under the relevant laws applying to the data subjects.

Chapter XIII. Health-related data and automated decision making

29. Health-related data and Automated Decision Making

- 29.1 The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, that relates to prognosis, diagnosis or treatment, or that similarly significantly affects her or him. The data subject shall also have the right to have the original decision made by automated processing to be reviewed and made again by a human. The data subject has a right to have any decision made in reliance or in part on their health-related data explained to them how any automated decision-making technology works, the factors that lead to the decision that has or will be made, and for necessary information to be provided that will justify any decision that has been or will be made.
- 29.2 Paragraph 29.1 shall not apply if the decision:
- (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) is authorised by a law to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) is based on the data subject's explicit consent and the data subject was advised prior to giving consent that the right to have a human review and remake the decision would be lost if consent was given.
- 29.3 In the cases referred to in points (a) and (c) of paragraph 29.2, the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least to secure that the data subject has the right to obtain human intervention in the data processing, to express her or his point of view and to contest any decision.

Chapter XIV. Mandatory Notification of Health-Related Data Breaches

30. Mandatory Data Breach Notification of Health-related data breaches

- 30.1 Controllers must report any health-related data breach to the competent supervisory authority, data protection authority, and affected individuals within 72 hours from becoming aware of a health data breach⁵.

Chapter XV. Right to Remedy for Health-Related Data Breaches

31. Right to Remedy for Health-related data breaches

- 31.1 Without prejudice to any available administrative or non-judicial remedy, a data subject has the right to an effective judicial remedy where he or she considers that her or his rights under this recommendation have been infringed as a result of the data processing of her or his health-related data in non-compliance with this recommendation, or they have suffered a health-related data breach.

⁵ The issue of a threshold requirement is being considered - eg the breach must be of a specific level of seriousness before reporting is required to avoid reports of technical health related data breaches.

- 31.2 Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a competent supervisory authority if the data subject considers that the processing of personal data relating to her or him infringes this recommendation, or they have suffered a health-related data breach.
- 31.3 Any person who has suffered material or non-material damage as a result of an infringement of this recommendation or health-related data breach shall have the right to receive compensation from the controller or processor for the damage suffered.
- 31.4 Any controller involved in processing shall be liable for the damage caused by processing which infringes this recommendation or otherwise results in a health-related data breach.
- 31.5 Additionally, disciplinary law applicable to the health care professionals and other persons undertaking data processing of health-related data in EHR systems must be implemented to counteract infringements of this recommendation.

Chapter XVI. Protection of Reporters of Health-related Data Breaches

32. Protection of reporters of Health-related Data Breaches

- 32.1 Any person that honestly believes, on reasonable grounds, that a controller or other person in possession of health-related data has engaged, is engaged or proposes to engage in activity that is likely to or will result in a health-data breach, is entitled to make a protected disclosure to the competent supervisory authority in connection with that information.
- 32.2 Any person that makes a protected disclosure concerning health-related data under paragraph 31.1 is entitled to protection whereby it is an offence to take reprisal action against the individual for having made the protected disclosure concerning health-related data breaches.
- 32.3 Where any protected disclosure concerns the conduct of the competent supervisory authority, provision must be made for the protected disclosure to be made to another government entity for investigation. Where no such provisions are made, the individual wishing to make the protected disclosure may do so publicly and may not be subject to reprisal action.
- 32.4 Where a protected disclosure is not accepted, either by the competent supervisory authority or as otherwise provided herein, the individual can elect to publish the claims they wish to make, however they will remain liable for the consequences, including under this recommendation.

Chapter XVII. Liability

33. Liability for Health-related data breaches

- 33.1 Where a health-related data breach under this recommendation has occurred, all parties to the transaction or event that gave rise to the breach are liable to the data subject jointly and severally for damages arising from the breach.
- 33.2 To be drafted. Liability for faulty algorithms.

Chapter XVIII. AI, Algorithmic transparency and Big Data

34. Algorithmic transparency and Monitoring Outcomes

- 34.1 To be drafted. Artificial Intelligence and health-related data
- 34.2 Check automated decision making, but is there enough in here about use of algorithms for purposes other than diagnosis?
- 34.3 To be drafted. Outcomes with outcomes monitoring and examination to identify and take action in respect of prejudice and discrimination arising from automated decisions.
- 34.4 To be drafted. Provisions on Big Data.
- 34.5 To be drafted. Lack of inclusion of minorities in health-related data sets and the effect of this on automated decisions.
- 34.6 To be drafted. Use of other data for health-related purposes without permission. For example, use of photographs taken of staff members and published on web sites to diagnose health conditions without permission.

Chapter XIX. Health-related Data in non-healthcare settings

35. Health-related data and law enforcement including forensic databases

- 35.1 To be drafted. Provisions on health-related data in a law enforcement context, including forensic databases, to be drafted. An area to examine specifically is the retention of health-related data beyond the purpose and the period of time for which it was collected.
- 35.2 To be drafted. Where data has been processed for a specific purpose without consent (for example, for the identification of a missing person, or during a criminal investigation), such data must not be used for scientific research except for the specific purpose of assessing the validity of the method used to achieve that purpose.

36. Health-related data and immigration

- 36.1 To be drafted. Access to health-related or genetic data for immigration purposes requires the free, specific, informed and explicit consent of the data subject and must be subject to adequate safeguards in law to protect the rights and interests of data subjects
- 36.2 To be drafted. Other provisions on health-related data and immigration to be drafted.

37. Health-related data and individuals in the care of the state

- 37.1 To be drafted. Provisions on health-related data in the context of individuals in prison, individuals living with mental health issues confined to institutions, and individuals in the care of the state, such as may be the case for orphans.

38. Health-related data and Marketing

38.1 To be drafted. Concerns the interaction of marketing data and health-related data, e.g., an individual's search history on a website and its correlation to their health-related data.

39. Health-related data and diminished capacity

39.1 To be drafted. Concerns issues raised by dementia or Alzheimer's and all ages in which the individual is mentally incapacitated. Are there any limits to health care proxy decisions and the degree to which advance directives include direction to HC data?

Chapter XX. People Living with Disabilities and Health-related data

40. People living with disabilities and Health-related data

40.1 To be drafted.

Chapter XXI. Gender and Health-related data

41. Gender and Health-related data

41.1 To be drafted.

Chapter XXII. Intersectionality and Health-related data

42. Intersectionality and Health-related data

42.1 To be drafted.

References

43. Bibliography

BBMRI-ERIC: Making New Treatments Possible. (2016). *New Recommendation on the processing of personal health-related data* | BBMRI-ERIC: Making New Treatments Possible. [online] Available at: <http://www.bbmri-eric.eu/news-events/new-recommendation-on/>.

Callens, S. (2010) "The EU legal framework on e-health," in Mossialos, E., Permanand, G., Baeten, R., and Hervey, T. K. (eds) *Health Systems Governance in Europe: The Role of European Union Law and Policy*. Cambridge: Cambridge University Press (Health Economics, Policy and Management), pp. 561–588. doi: 10.1017/CBO9780511750496.014.

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (2018). *Draft Recommendation on the Protection of Health-Related Data*. Strasbourg.

Council of Europe Committee of Ministers to the member States (2016). *Recommendation CM/Rec(2016)8 of the Committee of Ministers to the member States on the processing of*

personal health-related data for insurance purposes, including data resulting from genetic tests. [online] Strasbourg. Available at: <http://www.quotidianosanita.it/allegati/allegato2027308.pdf>.

Council of Europe (2014). *Opinion on The Draft Recommendation on The Use for Insurance Purposes of Personal Health-Related Information, In Particular Information of a Genetic and Predictive Nature*. [online] Strasbourg: Council of Europe. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016806b2c5f.

Council of Europe, Committee of Ministers (1997). *Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data*. Adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies.

Deguara, I. (2018). *Protecting Patients' Medical Records under the GDPR*. [online] Idpc.org.mt. Available at: <https://idpc.org.mt/en/articles/Pages/synapse-article.aspx>.

European Data Protection Supervisor - European Data Protection Supervisor. (n.d.). *Health data in the workplace - European Data Protection Supervisor - European Data Protection Supervisor*. [online] Available at: https://edps.europa.eu/data-protection/data-protection/reference-library/health-data-workplace_en. Includes source material.

European Patient Forum (2016). *The new EU Regulation on the protection of personal data: what does it mean for patients?* [online] Brussels: European Patient Forum. Available at: <http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf>.

Malafosse, J and DLA Piper France LLP legal consultancy (2015). *Introductory Report for Updating Recommendation R(97) 5 of the Council of Europe on the Protection of Medical Data*. [online] Strasbourg: Council of Europe. Available at: <https://rm.coe.int/introductory-report-for-updating-recommendation-r-97-5-of-the-council-/168073510c>.

Mantelero, A. (2017). *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. [online] Strasbourg: Council of Europe. Available at: <https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0>.

Maiam Nayri Wingara. (2018). *KEY PRINCIPLES — Maiam Nayri Wingara*. [online] Available at: <https://www.maiamnayriwingara.org/key-principles>.

Monteiro, R. (2014). *Medical Technologies and Data Protection Issues-Food for Thought*. [online] Strasbourg: Council of Europe. Available at: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806945a2>.

Te Mana Raraunga - Maori Data Sovereignty Network (2018). *Principles of Māori Data Sovereignty*. [online] Te Mana Raraunga - Maori Data Sovereignty Network. Available at: <https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5bda208b4ae237cd89ee16e9/1541021836126/TMR+Ma%CC%84ori+Data+Sovereignty+Principles+Oct+2018.pdf>.

Annex 4: Privacy Metrics - Consultation Draft

‘Metrics for Privacy - A Starting Point’,

Special Rapporteur on the right to privacy, Professor Joseph A. Cannataci.

Background:

This document is Version 0.1 (as at 13 February 2019). It is emphasised that this document is very much work-in-progress and is known to be incomplete. Starting from the Thematic Action Stream of Security and Surveillance, and using questions asked during 2017-2018 to national authorities, civil society and other stakeholders during country visits to USA, France, UK and Germany, a list of areas that may indicate the state of privacy within a country, has been compiled. There are additional questions included which extend beyond Security and Surveillance which will be updated when further comments are received about the mandate’s work on Big Data and Open Data, Health Data and Privacy and Gender.

Scoring systems/weighting are still subject to consideration as these are especially debatable.

This very early version of the document is being released for consultation as a ‘thought starter’ in order to provide the opportunity for comment and contribute to this work and its development.

Individuals, civil society and governments are invited to send their comments and suggestions by 30th June 2019.

Draft Questions:

1. Does your country’s constitution have a provision which specifically protects privacy or which has been interpreted to encompass a protection to privacy (+5)?
2. Does your country’s constitution extend privacy protections beyond the standards set in Art 12 UNDHR, Art 17 ICCPR, ECHR Art 8? (range of +1 to +5)
3. Does your country have a constitutional provision and/or constitutional jurisprudence which recognises the right to free development of personality (+5) and/or autonomy of thought and action of the individual (+5)?
4. Does your country have jurisprudence, especially from its highest court, which significantly reinforces the right to privacy? (e.g. right to personality, informational self-determination, digital privacy, requirement for judicial warrant to search cell-phone, requirement for judicial warrant to plant tracking device etc.), (range +5 to +20)
5. Does your country belong to a regional grouping wherein the citizens of your country can appeal to a regional court which has the power to over-ride decisions by your own country’s highest court thus adding a potential additional layer of safeguards for privacy protection (+10)
6. Does your country have, in addition to any possible constitutional and supra-national protection, one or more specific privacy laws of any sort? (+5)
7. Does your country’s privacy law meet Convention 108+ standards (+20)?
8. Does your country’s privacy law go beyond Convention 108+ standards to GDPR standards (+5)
9. Does your country have independent *ex ante* authorisation of surveillance? (+10)
10. Does your country have independent *ex post* inspection/oversight of surveillance? (+10 if fully independent of *ex ante* authorisation or +5 if part of *ex ante* authorisation authority)
11. Does your country have an independent *ex ante* and *ex post* surveillance authorisation which is on a full-time basis (+5) and which is properly resourced with adequate quantity (+5) and quality (+5) of human resources required to carry out the tasks it is expected to do?
12. Does your country allow politicians in power (the Executive branch of Government) to be involved in the decision-making authorising surveillance and, if yes, is their’s the only authorisation required (-30) or is it held in check by independent judicial review (+15)?

13. Does your country's independent oversight authority have technical systems in place such as a secure room with direct access to the IT systems of Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS) from which independent external oversight can be exercised at will without prior notice being given to the LEA or SIS concerned (+10)?
14. Does your country have Parliamentary (Legislative branch of government) oversight (+10) of any surveillance which is authorised by either the Executive branch and/or the Judicial Branch of Government and which has the power to change the behaviour of LEAs and/or SIS carrying out surveillance?
15. Does your country have independent Judicial (Judicial branch of Government) oversight (+10) of the activities of LEAs and/or SIS or are any of their activities precluded from judicial oversight by any law (-15)?
16. If your country's judges are involved in the oversight of surveillance, have they received specific training about surveillance and related law enforcement and intelligence activities? (+5)
17. If your country has mechanisms for the oversight of surveillance activities, irrespective of whether the surveillance is carried out by LEAs or SIS, do these independent oversight authorities have an exclusively advisory status (+5) or do they have the power *de jure* (+5) and/or *de facto* (+10) to impose changes and sanctions on the related activities of the LEAs or SIS?
18. Does your country share personal information and/or intelligence product with other countries and, if so, does it have adequate privacy safeguards in place for those occasions where such sharing of information/intelligence product occurs? (+5)
19. Does your country have technical capabilities for bulk powers (-55) and, if so, does it have a law granting a legal basis for bulk powers (+20) and detailed adequate safeguards for the use of bulk powers (range of +1 to +35)?
20. Does your country systematically monitor private communications within its borders (-55) and, if so, do such means of monitoring communications require their source code to be approved by a control authority which possesses the required technical and legal expertise and all of this within a range of detailed privacy safeguards (range of +1 to +55)?
21. Does your country have an agency devising and enforcing standards of encryption which may possibly enhance privacy? (+10)
22. Does your country require corporations to weaken encryption (-20) in communication technologies?
23. Does your country carry out intensive policing of the internet as used by your country's citizens and residents, monitoring chat rooms and/or private correspondence and/or public correspondence/expression by citizens for conformity with political ideology or religious faith? (range of -1 to -55)
24. Does your country permit the profiling of individuals using financial credit scoring or other means which are not strictly subject to rigorous data protection laws (range of -1 to -25) and/or maintain a social credit scoring system utilising Big Data analytics to aggregate data from various sources including financial information, on-line behaviour, etc. in order to create a profile of an individual? (range of -1 to -50),
25. Does your country permit unfettered export (-10) and import (-10) of surveillance technologies?
26. Does your country have laws negatively affecting the privacy of minorities such as sex workers (-10)?
27. Does your country have any other laws or policies not contemplated in the above questions which negatively impinge upon (range of -1 to -20)) or positively contribute to the protection of privacy (range of +1 to +20)?
28. Does your country have a police and/or intelligence service which systematically profiles and maintains surveillance on large segments of the population in a manner comparable to that of the STASI in the 1955-1990 GDR? If yes, then this is a "failing subject" (say. -1,000 – subtract one thousand marks) so please abolish that system and THEN start again at 1-27.

VOLUME 50

Upping the Ante on Bulk Surveillance

An International Compendium of Good Legal Safeguards and Oversight Innovations

By Thorsten Wetzling and Kilian Vieth

UPPING THE ANTE ON BULK SURVEILLANCE

**HEINRICH BÖLL STIFTUNG
PUBLICATION SERIES ON DEMOCRACY
VOLUME 50**

Upping the Ante on Bulk Surveillance

An International Compendium of Good Legal
Safeguards and Oversight Innovations

By Thorsten Wetzling and Kilian Vieth

Edited by the Heinrich Böll Foundation

The Authors

Thorsten Wetzling heads the SNV's research on surveillance and democratic governance. He directs the European Intelligence Oversight Network and is responsible for the EU Cyber Direct project's work relating to India. As an expert on intelligence and oversight, he was invited to testify before the European Parliament and the Bundestag on intelligence legislation. His work appeared in various media outlets. Recently, he became a member of the expert advisory board on Europe/Transatlantic of the Heinrich Boell Foundation in Berlin. Thorsten Wetzling holds a doctorate degree in political science from the Graduate Institute of International and Development Studies in Geneva.

Kilian Vieth manages SNV's work on government surveillance and intelligence oversight. He works on reform approaches for a more democratic and more efficient intelligence and surveillance policy in Germany and Europe. In 2018, Kilian Vieth was invited to testify before the parliament of Hesse on the regional surveillance legislation. Beyond that, his research interests include digital human rights, critical security studies, as well as political and social issues of algorithmic decision-making.

Partner Foundation

The **Stiftung Neue Verantwortung (SNV)** is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organisation adopted a concept of mixed funding sources that include foundations, public funds and businesses. Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organize conferences that address these issues and further subject areas. www.stiftung-nv.de



Published under the following Creative Commons License:

<http://creativecommons.org/licenses/by-nc-nd/3.0> . Attribution – You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work). Noncommercial – You may not use this work for commercial purposes. No derivatives – If you remix, transform, or build upon the material, you may not distribute the modified material.

Upping the Ante on Bulk Surveillance
An International Compendium of Good Legal Safeguards and Oversight Innovations
By Thorsten Wetzling and Kilian Vieth
Volume 50 of the Publication Series on Democracy
Edited by the Heinrich Böll Foundation

Design: feinkost Designnetzwerk, S. Langer (predesigned by blotto design)
Cover-Photo: «Data Security» Blogtrepreneur – flickr (CC BY 2.0)
Printing: ARNOLD group, Großbeeren
ISBN 978-3-86928-187-2

This publication can be ordered from: Heinrich-Böll-Stiftung, Schumannstr. 8, 10117 Berlin
T +49 30 28534-0 **F** +49 30 28534-109 **E** buchversand@boell.de **W** www.boell.de

CONTENTS

Foreword I	6
Foreword II	8
Abstract	10
I. Introduction	11
II. Methods	15
III. Best Practice Compendium	21
Phase 1: Strategic Planning	21
Phase 2: Application Process («Warrantry»)	31
Phase 3: Authorization / Approval	40
Phase 4: Collection & Filtering	48
Collection	49
Filtering	53
Phase 5: Data Processing	55
Data storage	55
Data maintenance	60
Data-sharing	62
Data deletion	65
Phase 6: Analysis	69
Phase 7: Review & Evaluation	72
Phase 8: Reporting	78
IV. Discussion	83
V. Conclusion	87
VI. Annex	89
List of Workshop Participants	89
List of Interviewed Experts	90
List of Good Practices	91
List of Abbreviations	99
Bibliography	101
List of reviewed Intelligence Legislation	107

FOREWORD

Modern democratic societies are increasingly being confronted with two difficult-to-reconcile demands of their citizens: protection against a growing number of new threats and the right to privacy. An open and vigilant democracy nevertheless can meet these requirements only in part. The difficulties have been illustrated through numerous examples involving intelligence services in recent years – ranging from the failure to prevent terrorism in the case of Anis Amri to the Edward Snowden revelations about mass surveillance by the National Security Agency.

The precarious balance between the need for security and the right to privacy will continue to characterize «risk societies» of the 21st century. The forces of globalization will furthermore push these difficult issues into new territory – be it through new threats from transnational terrorism, hybrid warfare, or novel technological monitoring capabilities such as digital face recognition. These developments call for a broad societal discussion about the appropriate risk management, which combines the effectiveness of security institutions with their democratic legitimacy.

Thorsten Wetzling, from the Stiftung Neue Verantwortung, already addressed these questions in a study for the Heinrich Böll Foundation in 2016: In our Democracy Series (Volume 43), he informed readers about the state of intelligence oversight in Germany and drew a sobering balance sheet.

With the present study, we want to broaden the discussion in two ways. We have asked the Stiftung Neue Verantwortung to look beyond the German example to the practices of intelligence oversight in a number of key countries in the transatlantic arena. At the same time, through this comparative study, we wanted to take a different approach when considering «effective oversight» and not only identify the deficits of intelligence oversight, but also highlight encouraging practices that have emerged in the respective survey countries in the wake of recently reported reforms.

Therefore, the study may well be understood as an invitation to the community of national regulatory authorities to look beyond national borders and be inspired by the best practices of their neighboring countries.

During the progressive integration of European foreign, security, and defense policies, and against the backdrop of increasing levels of cooperation between Western intelligence services, democratic oversight of these services must also be free from nation-centric views and strengthen the transatlantic exchange. This is especially true in a period of Western uncertainty and authoritarian temptations, especially within the transatlantic community. Robust oversight practices and good laws can serve as bulwarks against the erosion of fundamental rights should a government be infested with the illiberal virus that is currently rampant in Europe and America.

We hope that the present study will educate readers and fulfill both a political and social mission. At the political level, in a time of growing skepticism about the EU and NATO, we hope to promote the transatlantic dialogue on informational self-determination and, more generally, individual freedom and human rights. The study has identified encouraging examples of effective democratic intelligence oversight in many countries, examples that deserve further exploration. A liberal, value-based community relies on this exchange of «best democratic practices.»

At the societal level, we hope that questions about the suitable regulation of Western intelligence services will be given reification through this very detailed comparative study. The debate about intelligence has always suffered from a lack of professional analysis and an oversupply of empirically unverified hypotheses and conspiracy theories.

We owe it to our readers to provide them with the best possible guidance for a critical discussion on Western intelligence practices. Hopefully, they can use this study to further the debate on democratically legitimate and effective intelligence services.

Berlin, November 2018

Giorgio Franceschini
Heinrich Böll Foundation
Head of Foreign and Security Policy Division

FOREWORD

On September 13, 2018, the European Court of Human Rights ruled in the case of *Big Brother Watch and Others v. the United Kingdom*, examining the bulk interception of communications, intelligence-sharing, and the obtaining of communications data in light of the European Convention on Human Rights. The judgment marks the first occasion on which the Court has addressed compliance of intelligence-sharing with Article 8 of the Convention. Prior to this ruling, the Stiftung Neue Verantwortung worked hard to be able to provide you with this compendium concerning the bulk interception of foreign communications.

Addressing the complexities of bulk interception powers exercised by intelligence and security services is by no means an easy task. This is even less so where it concerns the ways in which such powers are organized and put into practice in different countries across the Western world. The Stiftung Neue Verantwortung has reached an impressive result. This compendium of good legal safeguards and oversight innovations thoroughly addresses the legal complexities of bulk interception powers. It pinpoints the need for adequate legal safeguards and the central role that oversight bodies need to play in making sure such safeguards are adhered to in practice. It provides us – the oversight bodies of both Germany and the Netherlands – with food for thought and brings us to the following mutual considerations.

Firstly, national legislation needs to provide oversight bodies with strong legal criteria to assess the use of bulk interception powers as well as with the adequate means and measures to conduct oversight. This is needed to enable oversight bodies to effectively oversee the complex processing of large volumes of data that comes with these powers. It is imperative that national legislators are aware of, and learn from, other national legal frameworks.

Next, oversight bodies need to critically reflect upon their own abilities and oversight practices in order to develop effective methods of oversight. We need to improve our technical expertise and oversight methods in order to adapt to an operational Intelligence reality characterized by technological developments and intensifying intelligence cooperation. By sharing with each other the ways in which we seek oversight innovation, we may learn from each other's efforts and best practices.

Last but not least, oversight bodies need to strengthen their cooperation in order to more effectively oversee the international exchange of data and developments toward more advanced intelligence cooperation, such as the joint processing of data and making joint intelligence products. There is an urgent need for oversight bodies to jointly search for ways to more effectively oversee such intelligence cooperation.

This compendium is an important tool for doing precisely these things. It provides us with an excellent overview of best practices in the areas of legal safeguards

and oversight developments. It gives us profound insights into the legal complexities of bulk interception and the choices that were made in structuring the national legal frameworks governing these processes. It helps us to understand the need for rigorous and effective oversight mechanisms and to identify where our own oversight practices might still fall short. Lastly, it provides us with a meaningful starting point to strengthen cooperation between oversight bodies and to find common ground in jointly overseeing intelligence cooperation.

We welcome you to carefully read through the compendium. It is an excellent read, and we invite you to take part in a still much needed international discussion.

Harm Brouwer

Chair of the Dutch Review Committee on the Intelligence and Security Services

Bertold Huber

Deputy Chair of the German G10 Commission

Abstract

Unprecedented public debates about intelligence governance following the revelations of Edward Snowden have not changed the fact that all major democracies allow their national intelligence services to intercept communications data in enormous quantities. Many people question the efficiency of bulk surveillance practices and their compatibility with fundamental rights. Others worry about its effect on the social fabric of democratic societies.

Yet, the fact is that most parliaments have expanded, rather than curtailed, surveillance powers in recent intelligence reforms. What is more, the European Court of Human Rights recently upheld the Swedish regime for bulk interception of foreign communications and called the practice a «valuable means» of counterterrorism in its Big Brother Watch decision of September 2018. Therefore, one can assume that the practice of bulk communications surveillance is here to stay. If that is the case, then it is high time to subject national legal frameworks and their corresponding oversight systems to a comparative review and to identify good practices. National courts and the European Court of Human Rights, alike, have frequently admonished national governments for flaws or shortcomings in the oversight regime. In the September 2018 decision, the European Court of Human Rights again demanded more rigorous and effective oversight mechanisms.

Yet, especially as surveillance technology is rapidly evolving, what exactly constitutes effective oversight of bulk collection in actual practice? A court will not design new rules or prescribe specific accountability mechanisms. This is the difficult and necessary work of democratic governance, and it needs to be done by the principled members of the different oversight bodies that understand the critical importance of their work.

This study presents individual examples of legal provisions and oversight practices that, by comparison, stand out as more balanced or more innovative responses to the many thorny challenges that ought to be met. The resulting compendium features a wide range of high-water marks from different national surveillance regimes. It shows that each nation – despite constitutional and political differences, and irrespective of individual reform trajectories – has a lot to learn from its international partners. These practices, we believe, should be widely promoted, for they increase the legitimacy and effectiveness of a controversial practice that is here to stay.

I. Introduction

All democracies rely on intelligence agencies to keep their open societies safe. They provide actionable intelligence to decision-makers on a wide range of security and foreign policy matters. Regardless of whether this concerns terrorism, arms proliferation, or organized crime,¹ this requires information beyond that which is publicly available. Intelligence services master a range of clandestine methods to acquire such information. Some methods – including the electronic surveillance of communications data – are difficult to reconcile with the fundamental principles of democratic governance, such as rule of law, transparency, and accountability. They may also infringe on fundamental human rights and civil liberties, such as the right to privacy as well as the rights to freedom of opinion, of expression, of association, and of assembly. In order to ensure public trust and the legitimacy of intelligence governance, democracies need to place all intelligence activities on a solid legal footing and subject them to rigorous and effective oversight.

This remains a formidable challenge.² Admittedly, the democratization of intelligence and the professionalization of oversight has made significant advances over the last few decades in many established democracies. Parliaments in Europe, North America, and Australasia, for example, frequently reformed national intelligence laws and extended the remit and the resources of independent oversight bodies over time. In addition, countries such as the United States have introduced transparency principles that commit the intelligence community to provide more information to the public than at any previous time in history.³ Still, as the failures of effective oversight of electronic surveillance prior to the revelations of Snowden have shown, democratic intelligence governance cannot be taken for granted. The stakes are high, and the temptations to abuse privileges such as government secrecy are omnipresent. The

-
- 1** Naturally, these are just a few common security threats that concern intelligence services the world over. Which particular threat or national interest a particular service is tasked to look into varies from service to service.
 - 2** Recent experiences and future challenges of democratic control of intelligence in different contexts are discussed, e.g., in Goldman and Rascoff (eds.), «Global Intelligence Oversight. Governing Security in the Twenty-First Century,» 2016; Leigh and Wegge (eds.), «Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World,» 2018; Anderson, «New Approaches to Intelligence Oversight in the U.K.,» January 2, 2018, <https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk>; Wetzling, «Options for More Effective Intelligence Oversight,» 2017, https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.
 - 3** U.S. Principles of Intelligence Transparency for the Intelligence Community, accessible via <https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic>.

legitimacy of intelligence action must constantly be earned – even in the presence of severe security threats. Effective governance and democratic control of intelligence is the result of a complex, multi-faceted effort that cannot be left to a small group of technocrats. Next to audits within the services, it requires rigorous executive control and parliamentary oversight. It also needs strong, independent, and tech-savvy judicial mechanisms to either authorize or approve and review individual intelligence measures. In addition, there ought to be independent public scrutiny over the process of intelligence legislation and the oversight practices. Together, these various layers of oversight and accountability mechanisms provide input legitimacy to intelligence governance. What is more, they also ensure that the output of intelligence policies and decisions are informed and effective (output legitimacy).

Intelligence governance is also very much a work in progress rather than a finished product. There ought to be regular updates to intelligence legislation and the oversight frameworks due to the pace of technological change. It brings new tools or entirely new practices to the field, some of which oversight bodies should also use in order not to lag behind and to become more efficient.⁴ Similarly, political pressure for stronger collective security or new revelations of intelligence malfeasance can prompt new reviews of the governance framework. What is more, and not just in the United Kingdom, it appears that «many of the daily activities of the security agencies are left unregulated by law. Key issues of targeting, processing, and liaison with other agencies at home and abroad are doubtless the subject of internal governance but little is disclosed to the public and even less is set in legal format.»⁵

Put simply, when democracies allow their intelligence services to deploy digital surveillance powers in the name of national security, they have to do this within the rubric of the rule of law and checks and balances. And while cultural, political, and constitutional differences among those nations render it futile to establish a one-size-fits-all intelligence governance blueprint, it is certainly worthwhile to study how common challenges are met across different systems and to identify and promote innovative solutions so that they may traverse national jurisdictions.

In this compendium, we focus on the bulk surveillance of foreign communications. By this, we mean the interception, collection, management, and transfer of enormous troves of communications data that is transmitted via different telecommunications

4 For a recent account of how artificial intelligence (AI) methods are used for the analysis of large datasets, see, e.g., Hoadley and Lucas, «Artificial Intelligence and National Security,» April 26, 2018, 9, <https://fas.org/sgp/crs/natsec/R45178.pdf>.

5 McKay and Walker, «Legal Regulation of Intelligence Services in the United Kingdom,» 2017, 1887. For a recent overview of unanswered questions when it comes to international intelligence sharing, see: International Network of Civil Liberties Organizations, «Unanswered Questions – International Intelligence Sharing,» June 2018, https://www.inclo.net/pdf/iisp/unanswered_questions.pdf. In Germany, for example, the acquisition and subsequent use of data that may have been collected by private companies or the military, and which may be used and modified by the intelligence services, remains to be placed on a more solid legal footing. See: Wetzling, «Germany's intelligence reform: More surveillance, modest restraints and inefficient controls,» 2017, 13–16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

networks (fixed telephone lines, mobile networks, the internet, and satellite networks). The foreign communications are intercepted as electronic signals, comprising various types of metadata as well as content. It is controversial because it is «non-targeted» or «unselected» or «general» – in other words, not directed at a particular individual.⁶ David Anderson, the former UK Reviewer of Terrorism Legislation, warned that the use of bulk powers may have serious adverse human rights implications: such powers «involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime [...] any abuse of those powers could thus have particularly wide ranging effects on the innocent [...] even the perception that abuse is possible, and that it could go undetected, can generate corrosive mistrust.»⁷

Bulk surveillance of (foreign)⁸ communication has been a standard intelligence practice for decades. Greater public interest in the wake of the Snowden revelations, and the fact that many countries lacked a robust legal framework for it, let alone effective oversight thereon, has led many parliaments to adopt new laws or to amend existing legislation since then. Now that a sweep of new laws, oversight institutions, and control practices are in place, and now that the European Court of Human Rights has decided – in July 2018 and in September 2018 – that the practice of bulk surveillance of foreign communications can be compatible with the European Convention on Human

6 Many countries, including Germany and the United States, apply different legal frameworks for the bulk surveillance of foreign traffic. Communications that have both their origin and destination outside the intercepting country are treated differently than communications where one end involves the territory of the intercepting agency. Others, such as the Netherlands, do not distinguish between foreign and domestic communication when it comes to bulk surveillance. Whether or not surveillance legislation can legally discriminate against non-nationals, and whether or not it is technologically possible to enforce different data protection regimes, is a matter of much contention. See, e.g., Swire, Woo, and Desai, «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft),» 2018, or Lubin, «We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,» 2017, <https://papers.ssrn.com/abstract=3008428>. Yet, there are also strong arguments against this practice, see, e.g., the recent challenge against the new German intelligence law or the expert testimony that elaborates on the technical shortcomings of the current data minimization practice in Germany: Rechthien, «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages,» September 2016, <https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf>.

7 Anderson, «Report of the Bulk Powers Review,» 2016, 9.6., https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc_100035016622.0x000001.

8 Some countries have detailed laws that regulate the bulk collection of domestic-foreign communications, but they may not have an explicit legal regime for foreign-foreign communications. Others do not distinguish between foreign and domestic communications at all in their respective intelligence legislation. Although we try to address the governance of bulk communications surveillance in general, at some points the specific reference to foreign communications becomes important for the application of legal safeguards and oversight practice. In such a case, a specific reference to the provision is made.

Rights,⁹ it is a good time to take the national governance regimes at face value. While pending litigation at both national and European courts may still prompt a re-design of some intelligence laws, the very practice of bulk surveillance of communication is unlikely to be abandoned. Quite the contrary, it is here to stay and will remain a key practice of modern intelligence.¹⁰

This makes it all the more important, then, to identify good solutions to the many thorny governance challenges that it entails. This is what we aim to provide with this publication. More specifically, the compendium identifies and contextualizes legal provisions and current oversight practices from different democracies on bulk foreign communications surveillance that – by comparison – stand out for either their compatibility with democratic governance, the rule of law, or the protection of human rights. They are also seen as good practices when they embody an innovative attempt to improve the effectiveness of oversight.

We believe that all countries stand to benefit from a thorough discussion on the growing acquis of good practices regarding the governance and oversight of bulk surveillance of (foreign) communications. Despite the relevant and legitimate criticisms that can be directed at recent intelligence reforms,¹¹ most of them also brought about individual changes that embody significant improvements in governance. When taken together, these promising practices paint a unique picture, which, in turn, can help identify opportunities for progress in national frameworks. Obviously, it takes knowledge to develop a reform agenda and political will to overcome national shortcomings. Yet, if other countries successfully demonstrate that the sky did not fall when they implemented more ambitious solutions to particular governance challenges, then this can be used as a powerful argument to persuade others to follow suit.

9 European Court of Human Rights, «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08),» 2018, <http://www.statewatch.org/news/2018/jun/echr-sweden-judgment-bulk-interception-communications-FULL.pdf>.

10 The advancement of encrypted communication does, however, put additional weight on techniques such as computer network exploitation and the exploitation of software vulnerabilities.

11 Lubin, «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights,» August 2, 2018, <https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/>.

II. Methods

When democracies allow their intelligence services to conduct large-scale electronic surveillance of foreign communications data, they must do so within the limits of the law. They must also ensure that this practice is subject to effective and independent oversight. Yet, what does that mean in practice, and how can one best distinguish between good and poor legal safeguards and efficient and inefficient oversight dynamics?

To find out, we studied a wide range of different public resources, such as commentary on intelligence laws, oversight body reports, strategic litigation materials, as well as commentary on intelligence policy.¹² We developed our own analysis scheme (see below) and conducted a series of interviews with a range of different experts (legal scholars, computer scientists, public servants and oversight professionals, industry representatives, etc.) to obtain further information on current practices. Once we had

12 For some recent accounts of new intelligence legislation and the reform of oversight mechanisms concerning Canada, France, Germany, the United Kingdom, the United States, as well as some comparative reviews, see: Forcese, «Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18,» 2018; Parsons, Gill, Israel, Robinson, Deibert, «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).» The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2017, <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>; Chopin, «Intelligence Reform and the Transformation of the State: The End of a French Exception,» 2017, <https://doi.org/10.1080/01402390.2017.1326100>; Ohm, «The Argument against Technology-Neutral Surveillance Laws,» 2010, [https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=](https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=;); Tréguer, «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France,» October 2016; Schaller, «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden,» 2018; Wetzling, «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls,» 2017, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf; Anderson, «A Question of Trust: Report of the Investigatory Powers Review,» 2015, <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>; McKay, Blackstone's Guide to the Investigatory Powers Act 2016, 2018; Smith, «A Trim for Bulk Powers?,» September 7, 2016, <https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html>; Donohue, «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law,» 2017, <https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law>; Wizner, «What Changed after Snowden? A U.S. Perspective,» 2017; European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services – Volume I: Member States' Legal Frameworks,» October 22, 2015, <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>; European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update,» 2017, <http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega>.

collected enough information, we wrote a draft compendium and organized two expert workshops – one with oversight body representatives in May 2018, and one with European and North American civil society experts in June 2018 – to further test and refine our findings.¹³

Based on this work, we can now present this compendium of *good practices on bulk surveillance of (foreign) communications* from different national intelligence laws and oversight systems across Europe, North America, and Australasia. The compendium is by no means meant to be exhaustive, and we invite your comments and additional suggestions. If a particular example is taken from one country, this does not exclude the possibility that the same, or similar, rule or practice exists in another jurisdiction.

We consider a practice to be good when, by comparison, it provides an improved safeguard against potential violations of rights, or because it stands out in the way that it solves a common governance challenge, or because it may make innovative use of technology for the benefit of greater oversight effectiveness.

Although our method may allow us to identify international high-water marks regarding the governance and control of bulk surveillance of communication, we do not hold enough information to rate the overall quality of individual surveillance laws or national oversight frameworks. Too many individual factors contribute to this, and we cannot reflect on all of them here.¹⁴ Moreover, there are limits to what a comparative study of this kind may reveal. Every country has its unique social, legal, and political setup that influences the governance and reform of intelligence. As we do not account for these differences here, we cannot credibly make declarations on the overall governance framework in which these good practices are embedded. This also means that the amount of citations that a national law or oversight regime receives in this compendium cannot be construed as a suitable indicator for the overall quality of the bulk surveillance regime in each country.

Our focal points are the legal frameworks and oversight regimes regarding non-targeted signals intelligence (SIGINT), with a special emphasis on foreign communications data.¹⁵ This provides intelligence services «mass access [...] to data from a population not itself suspected of threat-related activity.»¹⁶ Unsurprisingly, then, non-targeted (or «bulk») SIGINT capabilities are often considered to be the crown jewels of a national intelligence community. It is a technically sophisticated and highly complex intelligence-gathering discipline that involves a lot of international cooperation and grew in the shadows of many democracies for quite some time. The National Security Agency (NSA) of the United States famously proclaimed that, due to the shift

13 See Annex for a list of workshop participants and interviewees.

14 For an overview of those factors, see, e.g.: Richardson and Gilmour, *Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis*, 2016; Zegart, «The Domestic Politics of Irrational Intelligence Oversight,» 2011; Wetzling (ed.), *Same Myth, Different Celebration? Intelligence Accountability in Germany and the United Kingdom*, 2010.

15 Communications data, for the purpose of this report, refers to both content of communications (e.g., the text of an email) and information about communications, also known as metadata (e.g., the email addresses of sender and recipient).

16 Forcese, 2018, 3.

toward digitized means of communication, we were now living in «the golden age of SIGINT.»¹⁷ This said, bulk surveillance of foreign communications is but one practice in a much larger universe of intelligence-gathering disciplines.¹⁸ Targeted surveillance and active computer network operations (i.e., getting access to datasets via hacking computer networks, etc.) are two other prominent examples. Communications data can, of course, also be collected in bulk through hacking operations.¹⁹ Due to our own resources, and for the sake of reducing complexity, we decided to focus only on bulk collection of foreign communications here.

What are the relevant aspects that one needs to consider when it comes to creating a legal basis for – and the democratic control of – bulk surveillance? According to what standards and criteria can we assess the quality of either a legal provision or an oversight practice? Clearly, this, too, needs further unpacking. The following graph breaks down the most relevant governance aspects for bulk surveillance of foreign communications into eight phases.

Whether it is the initial strategic planning, the application processes, or the authorization/approval processes that are required prior to the execution of bulk powers, one can depict in legislation and actual oversight practices a range of relevant standards that democracies ought to meet. The same holds true, of course, for the implementation of bulk powers in practice: This, too, involves many processes and constitutional obligations that become more readily apparent when the entire cycle is depicted in its different stages. Our multi-stage model is based, in essence, on the more common intelligence cycle that has traditionally been used to explain the different stages required to produce actionable intelligence.

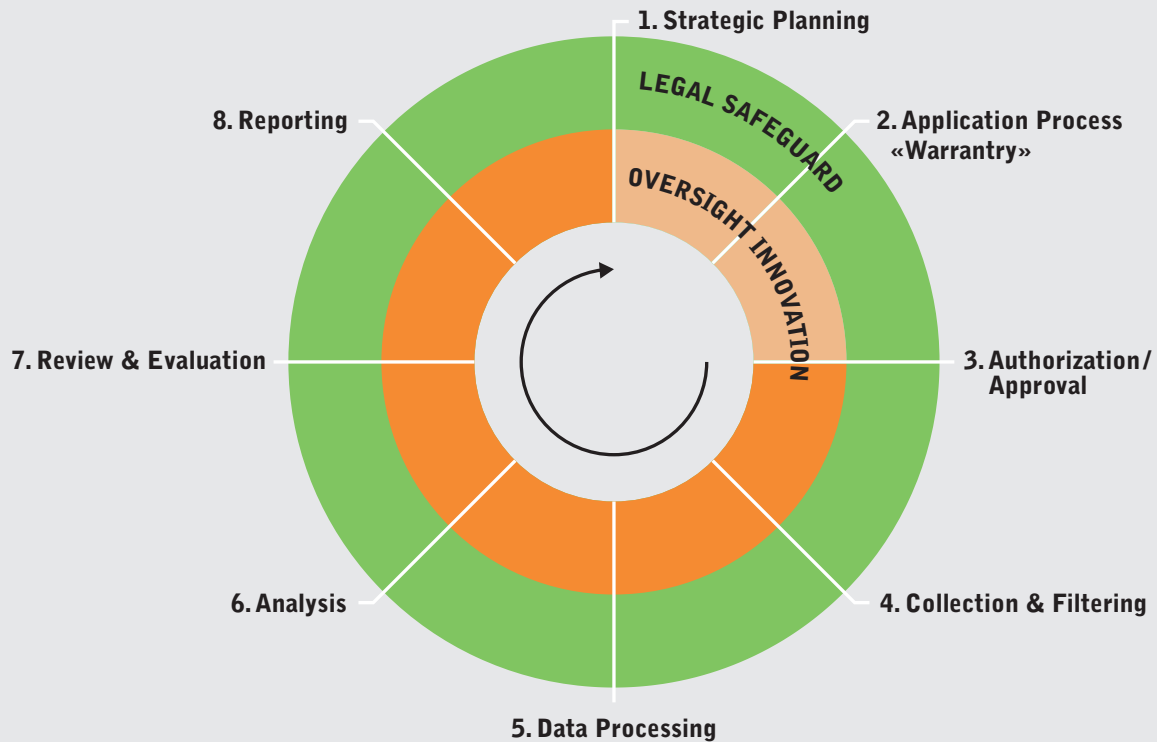
This compendium devotes a chapter to each of the eight phases shown in figure 1. They begin with a brief account of the typical activities in that stage before elaborating on the relevant governance aspects. Next, and to the extent possible, we present and discuss exemplary legal safeguards and examples of concrete oversight practices from different systems. We decided to include both legal safeguards and oversight

17 National Security Agency/ Central Intelligence Agency, «(U) SIGINT Strategy,» 2012, 2, <https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf>.

18 Targeted surveillance or active computer network operations (i.e., getting access to datasets via hacking or disrupting computer networks, etc.) are just two prominent examples of other intelligence-gathering techniques. They are, of course, also very important, and they, too, must be subject to rigorous oversight. Due to our own resources, but also for the sake of reducing complexity, we focus only on the bulk collection of foreign communications here. Bulk collection is usually conducted by intercepting large amounts of data from fiber optic cables and radio and satellite links, but data can also be collected in bulk through hacking operations, which can be more effective in order to access data in a non-encrypted form, as opposed to data from transit links, which are usually encrypted nowadays.

19 Given that more and more people encrypt their communications, this is becoming increasingly more effective, as it allows intelligence services access data prior to their encryption. Hence, bulk equipment interference, as it is called in the United Kingdom, must also be placed on a robust legal footing and is subject to rigorous oversight. For a recent discussion on this, see: Nyst, «Regulation of Big Data Surveillance by Police and Intelligence Agencies,» 2018, <https://ling-2s14id7e20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf>.

Figure 1: Bulk surveillance governance analysis scheme

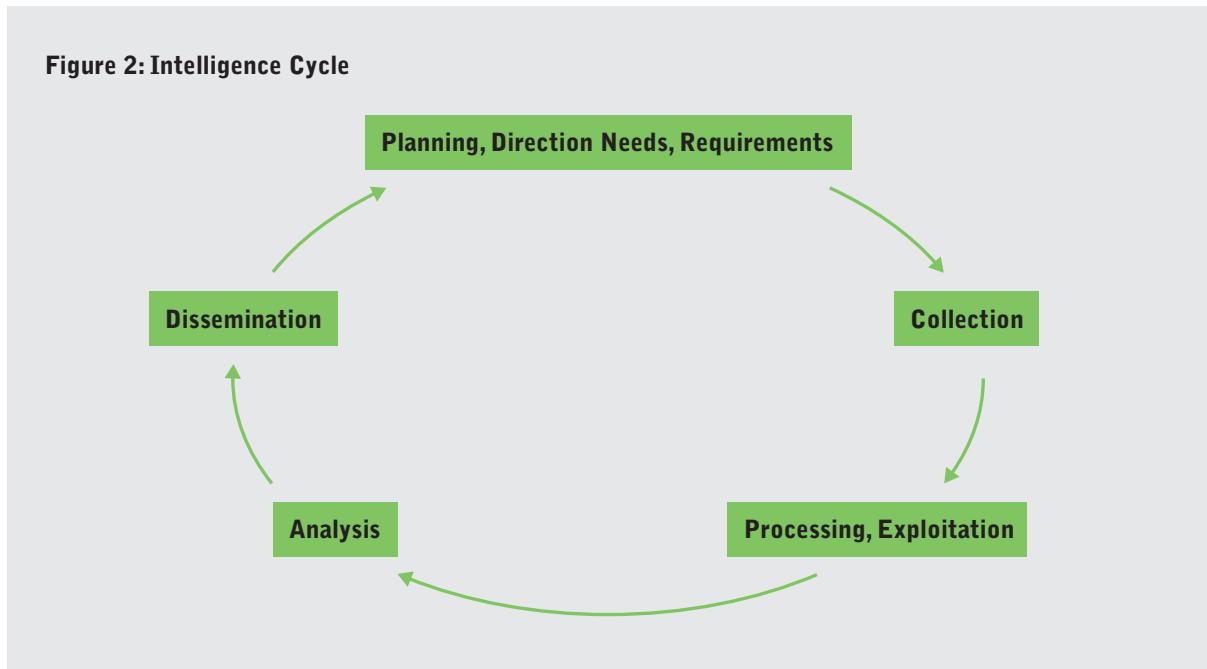


practices, because they are each extremely important and mutually constitutive. Comprehensive intelligence legislation is a necessary but not sufficient condition for the effective democratic control of bulk surveillance. While not everything can be legislated,²⁰ one can draw, for example, on the quality of law or the strict necessity test developed by the European Court of Human Rights for some orientation on standards that modern intelligence laws ought to meet.²¹ Whether or not these standards are then observed in actual practice is another story. This needs to be independently and effectively reviewed. What matters here are the actual dynamics of judicial oversight as well as its resources, legal mandate, and technological tools.

²⁰ For reasons of source protection, e.g., national intelligence laws may not provide detailed accounts of individual tools that are to be used in the field. Others suggest that, due to the pace of technological change, it is better to adopt tech-neutral rather than tech-specific surveillance laws. Others disagree. See: Ohm, 2010.

²¹ As concerns the former, see, e.g., Malgieri and De Hert, «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards «Good Enough» Oversight, Preferably but Not Necessarily by Judges,» 2017, <https://papers.ssrn.com/abstract=2948270>. As concerns the latter, see: Murray, Fussey, and Sunkin, «Response to Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers,» 2018, points 3–14, <https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf>.

Figure 2: Intelligence Cycle



For this compendium, we looked at countries with recent reforms and at places where we had access to language support and local resources. More specifically, we drew only on intelligence legislation and oversight practices from the following countries: Australia, Belgium, Canada, Denmark, France, Germany, New Zealand, Norway, Sweden, Switzerland, The Netherlands, United Kingdom, United States.

The different good practice examples in this compendium pertain to different governance dimensions, e.g. trimming the surveillance mandate, more transparency or better access to information to name just a few. For better orientation, each text boxes includes an icon. This will be further explained in the chapter IV (Discussion).

There are a number of other important caveats that readers should bear in mind before consulting our findings. First, there are many fine distinctions between targeted and non-targeted surveillance practices and the protections that are given to national and non-national data in national intelligence laws. When we run the risk of comparing things that are fundamentally different, we account for those important differences and make a case for why, as an exception, we are still drawing on a targeted surveillance regime in order to bring attention to an existing practice that, we think, should be given further consideration in bulk regimes. For example, it makes good sense to borrow from regimes on «targeted surveillance,» such as the US Section 702 program, which is meant to target only the internet and telephone communications of people

outside the United States to gather foreign intelligence information.²² We believe that some safeguards or oversight practices that currently apply only to targeted regimes are equally suitable for bulk collection because they, too, involve big data challenges. When we borrow from targeted collection programs, we make this explicit with the help of orange text boxes.²³

In addition, there are important differences in the intelligence laws of countries such as the United States and Germany that further distinguish in law and oversight between international communications (e.g., where either the communication originates or ends within the territorial jurisdiction of that nation) and foreign communications (e.g., where a communication may be transiting national territory, but where neither its origin or destination are on national territory). Other countries, such as the Netherlands, do not adhere to such distinctions in their respective intelligence legislation. This, too, is borne in mind and contextualized when necessary.

Second, while helpful to identify and discuss key governance challenges, we acknowledge that our multi-stage model is too linear, in the sense that an intelligence service often combines the data collected from different gathering techniques. For example, bulk surveillance data may trigger further bulk equipment interferences, and data from bulk equipment interference may be fused with the data from bulk surveillance at different stages in the «collection.» Our model does not look into the triangulation of different digital powers of modern intelligence services.

Third, some safeguards or oversight practices that we discuss in this compendium may be relevant – or even more important – in other phases of the cycle, too. Whenever we think this is the case, we cross-reference to that phase in the discussion.

22 More specifically, «the U.S. government may only designate foreigners located outside of the United States as «targets» for surveillance under Section 702. However, this is not to say that this practice has no impact on Americans. Section 702 currently has more than 100,000 designated targets, and it is not just limited to terrorists or «bad guys,» but rather any foreigner whose communications might relate to the conduct of US foreign affairs, such as diplomats and officials from friendly nations, or even individuals who protest outside a US embassy, support a global human rights group, or blog about international relations. The implications of this are profound: Section 702 can monitor innocent foreigners, and in the process may sweep up the communications of the average Americans they are talking to. Laperruque, «After «Foreign Surveillance» Law, Congress Must Demand Answers from Intelligence Community,» *The Hill*, January 2018, <https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answersfrom>. See also: Human Rights Watch, «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act,» September 14, 2017, <https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance>.

23 For example, we know that the US Foreign Intelligence Surveillance Court (FISC) has no role at all in overseeing bulk collection now that the Section 215 bulk collection program was ended in the USA Freedom Act. Therefore, when we single out a practice that involves the US FISC, we are mentioning a practice that relates to a targeted collection effort. While the law makes a very clear distinction between bulk and targeted surveillance, we propose here that these lines are not that clear in actual intelligence practice and that the debate on the governance of bulk surveillance should borrow good practices from neighboring regimes when possible.

III. Best Practice Compendium

Phase 1: Strategic Planning

Every government's resources are limited, and legal rules may prevent the collection of data regarding certain aspects of life. Human rights obligations or constitutional provisions prohibit or limit the collection of data in certain situations, for example when the privacy of the home is concerned.²⁴

Intelligence services may also not be able to effectively process too much information, and therefore need to focus their activities.²⁵ Such factors require that governments set political and strategic priorities and determine the specific assignments of their intelligence community. The first phase of the SIGINT process thus involves the identification and formulation of certain intelligence needs. Ideally, strategic planning will also draw on insights from previous assessments of collected intelligence and their value after analysis.

Relevant aspects

A clear and specific legal mandate is the precondition for the transparency and accountability of foreign intelligence gathering. The mandate should describe specific legal grounds, against which the permissibility and proportionality of a particular measure can be assessed. It should also stipulate what data sources or types of communications may and may not be included in SIGINT collection.

According to jurisprudence by the European Court of Human Rights and the Court of Justice of the European Union, bulk surveillance is only permissible when it is strictly necessary to protect the democratic institutions of society.²⁶ This indicates that intelligence services of signatory countries of the European Convention of Human Rights and the European Union Charter of Fundamental Rights may only engage in bulk collection techniques in relation to clearly confined categories of serious threats

24 In Germany, for instance, the privacy of the home is protected by Article 13 of the Grundgesetz (Basic Law).

25 There is evidence suggesting that an overflow of data might cause intelligence failures: Gallagher, «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure,» June 7, 2016, <https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/>.

26 This was established both by the European Court of Human Rights (ECtHR) and the Court of Justice of European Union (CJEU). See, e.g.: ECtHR and Council of Europe judgment in *Klass and Others v. Germany*, Application No. 5029/71, September 6, 1978, para. 42; ECtHR judgment in *Szabo and Vissy v. Hungary*, Application No. 37138/14, January 12, 2016, para. 73; CJEU judgment in *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v. Watson and others*, Cases C-203/15, C-698/15, December 21, 2016, paras. 108, 110, 116.

to a democratic society. These categories ought to go beyond a general understanding of what constitutes a serious threat.²⁷

The actors involved in setting intelligence priorities play a significant role here. There may be both external planning and tasking by government officials or ministers outside the service, and internal planning and tasking by the services. External planning and tasking traditionally focus more on a strategic/political level, whereas internal planning typically includes a stipulation of data sources or types of communications.

Who can influence and challenge the tasking process? Does an evaluation of previous intelligence cycles feed into the planning of future intelligence collection? If so, how? When it comes to the formulation of concrete intelligence needs, does the process allow those with adversarial positions to challenge what may be taken for granted? Matters concerning cooperation with foreign intelligence agencies must also be addressed at this stage: Will the need for cooperation with foreign services be weighed against other factors, such as human rights obligations and other national security interests? If so, how?

Good practice in legal safeguards

Ending discrimination based on citizenship

The majority of foreign intelligence laws are structured along a basic separation between «domestic» and «foreign» data. Domestic communication – defined either according to citizenship or based on territoriality – typically enjoys greater protection in most countries than what is seen as «foreign» or «overseas» communications. Though, as many authors have rightly pointed out, this distinction is problematic, both from a legal and from a technological perspective: As regards the latter, in a global digitized environment, it is very difficult to distinguish accurately between national and non-national data. Unless the filter programs work with 100 percent precision, incidental collection of domestic data appears inevitable. No foreign intelligence service can know in advance whether national data will be swept up in its bulk collection activities.

There is comprehensive evidence that suggests that no filter system can sufficiently sort out domestic communications from an internet data stream.²⁸ Even communications that are sent and received within the same country can be routed via third countries. The technical features of packet-based transmissions of communications on the internet make it practically impossible to clearly encircle a complex data category such as «German citizen.» Even if filters were to attain approximately 99 percent accuracy, in the sphere of bulk collection, where millions of communications

²⁷ Murray, Fussey, and Sunkin, 2018, 3, point 9, <https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf>.

²⁸ For a recent discussion on the accuracy of data minimization programs, see: Rechthien, 2016, and Dreo Rodosek, «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode,» 2016, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisierung_rodosek.pdf.

are intercepted indiscriminately, such a small percentage of wrongly categorized communications data amounts to large-scale infringements of the right to privacy of thousands of people. Consequently, poorly documented and designed filter systems do not assuage concerns about the chilling effects and the possible rights violations. What is more, separating populations may conflict with the principle of non-discrimination, as laid down in some national constitutions, EU law, as well as in international human rights law.²⁹ In addition, although international law may not explicitly prohibit suspicionless bulk surveillance, it does not endorse it either. Democracies such as Germany also have an obligation to interpret its national laws with a view to their compatibility with international law. This includes the right to privacy under Article 17 of the International Covenant on Political and Social Rights (ICCPR), which, many people argue, cannot be construed as a club good.³⁰



**The Netherlands:
No discrimination between foreign and domestic data in
intelligence collection**

The Dutch intelligence law does not differentiate between national and foreign communications, thereby granting the same privacy protections to all. Given the unresolved technical challenge to accurately distinguish between national and non-national communications data, let alone the constitutional and human rights challenges to such an approach, this appears to be the most consistent and rights-based solution to the problem.

Avoiding discrimination based on citizenship in national intelligence laws does entail the risk, however, that a lower standard of privacy protections will be adopted for both citizens and non-citizens alike. This is simply because equalizing safeguards on a lower level appears to be easier and would allow for broader data collection than if the bar were raised for all. Ideally, national intelligence laws will aim for the highest possible protection for all communications data collection, regardless of the citizenship of the population under surveillance.

The German intelligence law did not do away with discrimination based on nationality in foreign intelligence collection. However, German legislators created

²⁹ E.g., Schaller, 2018, 944.

³⁰ Yet, there may, of course, be variations in the way in which this right may be enforced domestically. For example, a Colombian citizen may not have the same expectations of being notified that his or her communications data was intercepted by the German foreign intelligence service. More information on the topic of citizenship in national surveillance legislation can be found in: Swire, Woo, and Desai, «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft),» 2018 (arguing for nationality as a key factor in surveillance laws) and the case against the German federal intelligence law recently brought to the German Constitutional Court (in German, see: https://freiheitsrechte.org/home/wpcontent/uploads/2018/01/GFF_Verfassungsbeschwerde_BNDG_anonym.pdf).

higher privacy protection standards for European Union data, as compared to the foreign intelligence collection rules regarding non-European Union data. The BND Act (Section 6 (3) in conjunction with Section 9 (2) and (5)) establishes that the use of selectors which target public bodies of EU member states or EU institutions is restricted to 12 warranted cases and requires orders that mention the individual search terms. The use of selectors that target EU citizens is restricted to 21 warranted cases.³¹ This demonstrates the willingness to grant higher levels of privacy protections, at least for European neighbors.

Legitimate criticism has been raised against the compromise made in German law, because it does not fulfill the standard of non-discrimination and ignores the issues of technical feasibility, as described above. Though, taking the realities of modern surveillance practices into account,³² introducing additional safeguards for certain foreign populations softens the traditional dichotomy of «us» versus «them»; and by blurring this line, it can be seen as a pragmatic step forward.

Clear rules for setting intelligence priorities



United States: Additional efforts to restrict the use of bulk powers

Presidential Policy Directive 28 (PPD 28) requires the US government to prioritize targeted collection over bulk collection, if targeted surveillance will achieve the desired results. Section 1 states that «[s]ignals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the United States shall consider the availability of other information, including from diplomatic and public sources. Such appropriate and feasible alternatives to signals intelligence should be prioritized.»

Notice that PPD 28 is only an executive decree and not enshrined in statute. A US president can, therefore, change it unilaterally. In the absence of change, however, PPD 28 is binding on the executive branch. As such, these basic principles can limit the use of bulk powers. The Dutch government also proposed a policy rule that special powers have to be applied in as targeted a manner as possible.³³ Arguably, the services are already bound by the general principle of proportionality, but introducing such a requirement in the intelligence law adds an accountability dimension and reinforces

³¹ For a more detailed analysis of the four different standards, see: Wetzling, «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform,» June 23, 2017, <https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform>.

³² Lubin, 2017.

³³ Article 29, Dutch Act on the Intelligence and Security Services 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017), <http://wetten.overheid.nl/BWBR0039896/2018-05-01>.

the need to deploy bulk collection methods only when less intrusive means are not able to achieve a given objective.³⁴ The new Dutch authorization body, TIB (Review Board for the Use of Powers), is requested to include the as-focused-as-possible principle in its regularity review, and the Dutch review body, CTIVD (Oversight Committee for the Intelligence and Security Services), is tasked to report on this.



**Germany:
Transparency on actors involved in formulating the National Intelligence Priority Framework**

Section 6 (1, number 3) of the German BND Act accounts for the actors that can formulate needs for the future tasking of the foreign intelligence service's signals intelligence. According to this, the Federal Chancellery determines the National Intelligence Priority Framework (Auftragsprofil BND) in consultation with the foreign office, the home office, as well as the ministries for defense, economy, and international cooperation.



**United States:
Annual review of any intelligence priorities by heads of departments**

Section 3 of PPD 28 requires all competent department heads to «review any priorities or requirements identified by their departments or agencies and advise the Director of National Intelligence [DNI] whether each should be maintained.»

Such a requirement for periodic review constitutes an important measure to ensure the timeliness and relevance of intelligence priorities. It also creates public accountability dimensions for key stakeholders in the intelligence policy-making process. The annual review is conducted within the executive branch only; no input from actors outside the corridors of power must be taken into account. Similarly, albeit not in statute, the Intelligence Community Directive 204 states how the National Intelligence Priorities Framework is established in the United States.³⁵

34 The «as targeted as possible» criterion is part of an adopted parliamentary motion and the policy rules issued in April 2017. It is also included in a draft legislative proposal changing the ISS Act 2017. For more information, see: Houwing, «The Wiv 2017. A Critical Contemplation of the Act in an International Context,» 2018, 17, https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.

35 US National Intelligence Priorities Framework, ICD 204, see: <https://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf>.



The Netherlands: Adequacy review of foreign cooperation partners

In order to assess which countries the services can share information with, weighting notes are drawn up on cooperation partners. These notes must be kept up to date and provide information on the basis of five criteria provided in law:

- the «democratic embedding» of the intelligence and security services in the country concerned;
- the respect for human rights in the country concerned;
- the professionalism and reliability of the service concerned;
- the legal powers and capabilities of the service in the country concerned;
- the level of data protection maintained by the service concerned.³⁶

Planning intelligence needs involves laying sound legal groundwork for intelligence cooperation. Based on the five criteria listed above, Dutch intelligence services have to submit a weighting note for each foreign partner service they cooperate with. The weighting process requires several compulsory risk assessments on the basis of such notes.³⁷ In addition, the pertinent policy rules from April 2018 state that unevaluated data from bulk cable interceptions may not be exchanged without the existence of a weighting note that covers this type of exchange.³⁸ Put differently, in the absence of a weighting note for such a case, no sharing of unevaluated data can be authorized by the responsible minister. The Dutch oversight body CTIVD can review the notes and

³⁶ Eijkman, Eijk, and Schaik, «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?», 2018, 31; see also: Dutch Act on the Intelligence and Security Services 2017, Articles 88–90.

³⁷ In these weighting notes, the government assesses how far cooperation with a foreign service may go. If there are developments in the country of the foreign service that give rise to a revision of the cooperation, the weighting note will be revised. The Dutch government does not exclude cooperation in advance with countries that do not meet the criteria, even if there are limited democratic safeguards and a poor human rights situation. In that case, the government speaks of a «risk service.» In case of cooperation with a «risk security service,» additional permission from the competent minister is required. The weighting of cooperation with these countries and these types of risk services must always be submitted to the minister. More background on Dutch Weighting notes: Dutch Review Committee on the Intelligence and Security Service (CTIVD), «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD,» 2016, <https://english.ctivd.nl/documents/review-reports/2016/12/22/index48>.

³⁸ However, when it comes to sharing unevaluated data that stems from other special powers (such as targeted interception or computer network exploitation), this rule does not apply. This data can be exchanged without the existence of a weighting on the basis of Article 64 ISS Act 2017, provided there is an urgent and important reason for this.

report to parliament whether it found them to be correct and adequate (see oversight practices section below). This is an innovative way to assess which countries intelligence can be shared with. Supposedly, other intelligence agencies weigh similar factors and make their decisions accordingly, but when writing this into the intelligence legislation, it underlines the importance of appropriate weighting, and it allows oversight bodies to review the process.



**Germany:
Written agreements on the aims, the nature, and
the duration of international cooperation must be
approved by the Chancellery**

Aiming for greater accountability for international intelligence cooperation, Germany has introduced new criteria for adopting bilateral agreements between intelligence services.

According to Section 13 of the BND Act, all cooperation agreements involving bulk SIGINT on foreign-foreign communications between Germany and EU, NATO, and European Economic Area countries require a prior written memorandum of understanding (MoU)³⁹ and approval from the Chancellery.⁴⁰ A list of broad permissible goals for such cooperations is included in Section 13 (4) of the law.⁴¹ The executive is required to inform the parliamentary intelligence oversight body about all such agreements. This also includes an appropriations clause that the data may only be used for the purpose it was collected, and that the use of the data must respect fundamental rule of law principles. Agreements also require a consultation among the foreign cooperation partners to comply with a data deletion request by the German Federal Intelligence Service (BND). In the end, though, due to the lack of an international arrangement, German intelligence officials cannot verify the accuracy of the assurances they may get from their cooperation partners in this regard.

Explicit mention of objectives that may not be advanced through bulk collection
Many recent reforms of SIGINT legislation have shied away from setting effective limits to bulk collection. That the United States has ended «about collection» and rolled back the bulk collection of telephone records under Section 215 of the Patriot Act in

³⁹ One SIGINT MoU that was made public as part of the Snowden revelations is the US-Israel MoU. It is available at: https://upload.wikimedia.org/wikipedia/commons/4/41/Israel_Memorandum_of_Understanding_SIGINT.pdf.

⁴⁰ Agreements with foreign partners further afield require the approval of the Head of the Chancellery.

⁴¹ Wetzling, «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls,» 2017, 13-16, https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

2015 is a notable exception to that rule. It proves that liberal democracies can do away with excessive collection practices. Some less prominent examples of new intelligence laws that have further restricted or trimmed the permissible use of bulk powers include the following:



**Germany:
Prohibition of economic espionage**

Section 6 (5) of the BND Act prohibits the use of foreign-foreign strategic surveillance to obtain economic advantages («*Wirtschaftsspionage*»).⁴²



**United States:
Prohibition of discrimination against protected classes
through bulk collection**

«In no event may signals intelligence collected in bulk be used for the purpose of suppressing or burdening criticism or dissent; disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion; affording a competitive advantage to U.S. companies and U.S. business sectors commercially; or achieving any purpose other than those identified in this section» (Section 2 PPD 28).



**United States:
Criminal liability for willful real-time surveillance conducted
for an unlawful purpose**

The criminal wiretapping statute contains a prohibition to engage in real-time surveillance (18 U.S. Code 2511 (1)). The provision bans certain wiretapping activity, and then creates exceptions to that general prohibition. Section 2511(4) exempts from this criminal statute lawful intelligence surveillance activity. But intelligence officials who conduct unlawful wiretapping are committing a crime.

⁴² It is important to note that this provision, in general, does not preclude the German intelligence services from targeting private organizations, such as corporations. The provision has been criticized as blurry and «poorly crafted» for the lack of proper legal definition of the term «economic espionage»: Graulich, «Reform des Gesetzes über den Nachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und internationale Datenkooperation,» 2017, 46, <https://kripoz.de/wp-content/uploads/2017/01/graulich-reform-des-gesetzes-ueber-den-bundesnachrichtendienst.pdf>.

Criminalizing certain forms of intelligence surveillance deters the misuse of surveillance powers. The penalty for intentional violations against the prohibition of real-time surveillance in the US wiretapping act may range up to five years imprisonment (18 U.S. Code 2511(4)). Such criminal liabilities are rarely found in the realm of bulk surveillance, but they could be an effective means to enforce compliance with regulations.

Good practices in oversight

Setting strategic goals and formulating operational priorities is a core competence of the executive. Consequently, we found only very limited involvement of oversight bodies in the tasking and planning phases. Privacy International also found recently that no intelligence oversight body currently possesses the power to authorize decisions to share intelligence.⁴³ Clearly, this invokes not just legal and operational questions but also political ones. Can a government sufficiently trust a foreign service to engage in new cooperations? Interestingly, some oversight bodies have recently taken an interest in reviewing the tasking of and cooperation between intelligence services, as the following examples illustrate.

Oversight involvement in tasking



United Kingdom: Parliamentary committee must be informed regularly about operational purposes

Section 142 of the Investigatory Powers Act details the procedure for specifying operational purposes for bulk interception. Any operational purposes must be approved by the Secretary of State (142 (6)) and must go beyond what is already prescribed in law (142 (7)). Every three months, «the Secretary of State must give a copy of the list of operational purposes to the Intelligence and Security Committee of Parliament» (142 (8)). «The Prime Minister must review the list of operational purposes at least once a year» (142 (10)).

Keeping oversight bodies regularly informed about operational purposes in actual practice helps them to identify shifting priorities and assess their compatibility with the legal framework. Thus, having a legal statute that prescribes detailed purposes or uses for bulk powers is one thing. Better still is to add actual reports on how priorities have been set in practice.

⁴³ Privacy International, «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards,» 2018, <https://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global>.



**Canada:
Full access to documentation of cooperation
agreements**

The Commissioner of the Communications Security Establishment (CSE) can access all relevant information about the intelligence-sharing activities of the CSE. The CSE Commissioner has all the powers of a Commissioner under Part II of the Inquiries Act, including the power of subpoena, which gives CSE Commissioner and staff unfettered access to all CSE facilities, documents and personnel.⁴⁴



**The Netherlands:
The CTIVD can review the weighting notes**

The Dutch Review Committee, the CTIVD, has the power to review the weighting notes on international cooperation partners and the subsequent international cooperation, as such. The CTIVD also has to be informed of any exchange of unevaluated data.⁴⁵



**Germany:
Parliamentary oversight committee must be informed
about all MoUs**

Section 13 (5) of the BND Act requires the government to inform the parliamentary intelligence oversight body, the Parliamentary Control Panel (PKGr), about all the MoUs signed concerning bulk SIGINT cooperation with foreign partners. This does not include ad hoc SIGINT cooperation on foreign intelligence collection.

⁴⁴ Should Bill C-59 pass, the creation of a single agency to review national security activities across government departments and agencies should resolve the single focus on the CSE in this regard; see also Privacy International, 2018, 67.

⁴⁵ The obligation to inform was broadened by policy rules. The law itself stipulates that the CTIVD has to be informed of unevaluated data from bulk SIGINT interception.

The three practices above are attempts to tackle the «accountability deficit»⁴⁶ of international intelligence cooperation. Unrestricted access to all cooperation agreements is a crucial step for oversight bodies to gain a better understanding of the scope and nature of intelligence-sharing. In a 2016 report, the CTIVD publicly criticized some of the services conclusions: «In one case, the foreign service does not meet the criteria of democratic anchorage, professionalism and reliability and reciprocity. Nevertheless, the MIVD [Military Intelligence and Security Service] determined that all forms of cooperation are permitted. [...] The CTIVD is of the opinion that the contents of the weighting note cannot support this conclusion. The MIVD does not indicate which compelling reasons are regarded by the service as a basis for being able to go so far in the cooperation, despite the failure to meet certain cooperation criteria.»⁴⁷ This example shows that the CTIVD may even publicly disagree with the services' weighting conclusions.

Summary of findings and reform agenda

The practices discussed in this phase comprise fundamental aspects (such as the Dutch practice to do away with the discrimination based on citizenship in bulk surveillance) to smaller, more incremental steps toward improved accountability (such as the introduction of concrete ministerial responsibilities for the steering of bulk surveillance processes).

It is noteworthy how international cooperation plays a significant role in this phase. Especially in the SIGINT world, where burden-sharing among foreign partners is a fundamental feature, weighting notes and improved access of oversight to international intelligence-sharing agreements are laudable practices. Ideally, they should be linked to mandatory and regular reevaluation by oversight bodies. The explicit mention in legislation of objectives that may not be advanced through bulk collection is another crucial dimension in shaping better governance.

Phase 2: Application Process («Warrantry»)

With a warrant, the intelligence service (or, as the case may be, the ministry performing executive control over a particular intelligence service) submits an application for authorization to collect data in bulk. Warrants need to describe and delimit bulk SIGINT measures based on specific criteria regarding both the form and content of the warrant that are set out in law. Warrants are a core element of accountability in intelligence governance, although they have to provide detail and particularity in order to constitute an effective safeguard against overly intrusive surveillance authorities.⁴⁸

⁴⁶ Bos-Ollermann, «Mass Surveillance and Oversight», 2017, 152.

⁴⁷ CTIVD, 2016, 32.

⁴⁸ Donohue interviewed by Farrell, «America's Founders Hated General Warrants. So Why Has the Government Resurrected Them?», June 14, 2016, https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/?noredirect=on&utm_term=.2f3ee3b71c69.

In the SIGINT world, warrants might therefore be tied to classes of individuals or activities rather than specific persons. We are aware that some jurisdictions apply much stricter limits to the legal concept of a warrant. In the United States and Canada, for instance, warrants always refer to targeted surveillance operations that involve a judge, who has to authorize them. A range of countries in Europe only apply the concept of warrants to criminal investigations and not to intelligence collection. In this conventional understanding, «bulk powers are irreconcilable with the requirements of classic warrants. There is no specificity. By definition, bulk powers are not targeted; they are indiscriminate.»⁴⁹ Under the United Kingdom's Investigatory Powers Act, on the other hand, the term «warrant» is used for different types of applications for bulk interception or acquisition of data. This, then, implies a class-based warrant system, in which large categories of data can be collected.

Although terminology is tricky and warrants for untargeted collection or bulk surveillance are not a feature of some legal systems, they are included here as a useful comparative category. Warrants can be a powerful tool to specify the minimization rules, the authorization requirements, and the purpose limitations of a measure. The more specificity a bulk warrant can provide, the better its protective function. Warrants may also be used to exclude certain data categories from collection and limit the use of the data collected.

It is important to note that many such limits and conditions could appear in a law governing intelligence surveillance. The major advantage of warrants, though, is the active involvement of an independent judicial authorization body *before* the collection begins (see phase 3), which allows for case-by-case controls. Ideally, a clear legal mandate is combined with obligatory, independent, ex-ante controls of all applications for bulk data collection.

Warrants also often define the duration of an operation for a specific collection method. This, in turn, triggers a mandatory reassessment of the measure, and potentially the subsequent reapplication and reauthorization. Setting an expiration date is, hence, an accountability mechanism as well as a regular efficacy test that helps to ensure the efficient allocation of resources by the agencies.

Naturally, the more targeted an envisaged surveillance operation, the more specific the warrant can be formulated. Given the focus of this study, that is, safeguards and oversight innovation regarding non-targeted communications surveillance, we mostly reviewed types of «bulk» warrants. This said, interesting features in targeted surveillance warrants might be discussed when applicable to the sphere of untargeted collection.

49 Forcese, 2018, 3.

Relevant aspects

It is common for various intelligence laws to include a list of criteria that each application for a SIGINT measure needs to address.⁵⁰ Ideally, these include the:

- purpose(s) of the requested activity;
- alternative means available;
- private companies that may be compelled to cooperate;
- service or services that will be instructed to perform the activity;
- time frame for assessment and authorization of the warrant, including for emergency situations;
- geographical zones or organizations or groups of people that a particular measure is directed at;
- technical device or facility to be tapped;
- exploratory monitoring or preliminary aptitude tests that have been conducted in preparation;
- type(s) of data to be retrieved;
- search terms or selectors used (i.e., a range of IP addresses);
- types of data use and forms of data exploitation to be performed on the data;
- duration of the warrant and rules for renewal;
- additional background materials to be submitted with the warrant.

Dimensions of SIGINT warrants

The following table provides examples of different types of warrants that exist in different jurisdictions. It is by no means a comprehensive list. It demonstrates, however, the diversity of different uses and applications for SIGINT warrants. The types of bulk warrants are illustrated with reference to only one legal regime, but similar provisions may exist in other intelligence laws as well. In general, the different warrants identified illustrate two things: First, warrants may be required for different collection *methods*, that is, detailing the techniques that can be used to obtain communications data. Second, many intelligence laws now require separate warrants for different *stages* of the SIGINT process. For example, the Dutch have now adopted a three-stage process that requires warrants for 1) the collection and filtering (Article 48), 2) the pre-treatment of the unevaluated data (Article 49),⁵¹ and 3) the selection of content for operational use

50 For example, a coalition of civil society, industry, and international experts has formulated a list of 13 principles to meet the human rights obligations in relation to communications surveillance: Necessary and Proportionate Coalition, «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance,» May 2014, <http://necessaryandproportionate.org/principles>.

51 The pre-treatment phase (Article 49 of the Dutch intelligence Act) exists to then either improve the collection (Article 49 (1)) or to improve the selection (Article 49 (2)).

and automated data analyses (Article 50).⁵² Moreover, warrants are used to regulate the retention of data, the sharing of data, and even the use of data for experiments and training. Although a specific bulk warrant must be viewed within the broader legal framework in the respective country, the table shows that various legislators have found versatile applications for bulk warrants. This, too, helps to hold the executive accountable for specific intelligence activities.

Table 1: SIGINT warrants

Type of warrant	Example provision
Bulk interception	United Kingdom: «Bulk Interception Warrants» (Section 136 (1) IP Act)
Bulk acquisition	United Kingdom: «Bulk Acquisition Warrants» (Section 158 (5) IP Act)
Bulk personal datasets	United Kingdom: «Bulk Personal Datasets Warrants» (Section 199 (1) IP Act)
Data examination	France: «Data Exploitation Warrant» (Article L. 854-2.-III. of Law No. 2015-1556) ⁵³
Retention	United Kingdom: «Retention notice» that orders an operator to retain communications data (Section 87 (1) IP Act)
Metadata analysis	France: The prime minister has the power to authorize, on request, the «Exploitation of non-individualized connection data.» ⁵⁴ (Article L. 854-2.-II. of Law No. 2015-1556)
Operational support	The Netherlands: The Dutch services need to obtain operational support permission, in case no formal cooperation agreement exists, as if they were applying the powers themselves. «Granted permission then makes exercise of the special powers abroad as covered by Dutch law.» ⁵⁵ (Article 90 Intelligence and Security Services Act 2017) ⁵⁶

52 Dutch Act on the Intelligence and Security Services 2017; see also: Eijkman, Eijk, and Schaik, 2018, 22.

53 In French original «exploitation de communications [...] interceptée.» A similar type of examination warrant is, e.g., required in UK law: «An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised by a warrant under this Part» (Section 200 (2) United Kingdom, Investigatory Powers Act 2016). In other cases, the conduct authorized by a bulk warrant includes safeguards on selection for examination and disclosure.

54 In French original «l'exploitation non individualisée des données de connexion interceptée.»

55 Ibid.

56 A similar type of warrant is also foreseen in New Zealand's intelligence law: «An intelligence and security agency may not, without an authorisation, request a government of, or an entity in, another jurisdiction to carry out an activity that would be an unlawful activity if it were carried out by the intelligence and security agency.» (Intelligence and Security Act 2017 (2017/10) Section 49 1A).

Type of warrant	Example provision
Testing	New Zealand: «A testing warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to test, maintain, or develop the capability of the agency in relation to the performance of its statutory functions.» (Intelligence and Security Act 2017 (2017/10) Section 91A)
Training	New Zealand: «A training warrant authorises an intelligence and security agency to carry out an otherwise unlawful activity that is necessary to train employees in relation to the performance of the agency's statutory functions.» (Intelligence and Security Act 2017 (2017/10) Section 91B)

Doubts have been raised, though, about whether having warrants for separate stages of the intelligence process is feasible in practice. Problems might occur if the warranted phases outlined in law do not correspond to the actual consecutive steps that have to be taken. In the Dutch case, experts claim that the three steps that must be authorized are closely interrelated and run in parallel.⁵⁷ This, they argue, could mean that different warrants for separate stages of the process would, in practice, not be authorized one after the other, but in fact all at once, thereby potentially undermining the purpose of this separation.

Good practice in legal safeguards

Naturally, the level of granularity in the criteria for bulk warrants differs from country to country. Several examples stand out for their attention to important details.

Legal specifications of SIGINT warrants



France: Restriction on the number of agencies allowed to use the data

According to the French foreign intelligence law, only the services named in the warrant are allowed to process the collected data. This specification is a protection against subsequent interagency data-sharing. Furthermore, the provision determines that the purpose stated in the warrant may not be changed, and the data may not be used for other purposes.⁵⁸

⁵⁷ See Electrospace.net. «Collection of Domestic Phone Records under the USA Freedom Act,» July 14, 2018, <https://electrospace.blogspot.com/2018/07/collection-of-domestic-phone-records.html>; CTIVD opinion: «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX,» August 26, 2015, <https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel>.

⁵⁸ Article L. 854-6. of French Law No. 2015-1556 on international surveillance.

This rule limits unforeseen spillovers of collected data from one intelligence service to another. Other agencies that may develop an interest in the collected data are prevented from performing unwarranted «searches on top of searches»⁵⁹ with such a requirement.



**France:
Type of automated processing accounted for in warrants**

Warrants for foreign-foreign intelligence must include the type of automated processing that can be implemented, specifying its purpose.⁶⁰

Stating exactly how a bulk dataset is processed and exploited may enable reviewers to better assess the privacy intrusions that are generated by the respective operation. The level of privacy intrusions and the effects on other fundamental rights may differ based on what kind of examination is performed, and for what aim. In France, however, such applications for the exploitation of bulk metadata are authorized by the French prime minister and not independently reviewed by an oversight body.



**Canada:
Specific requirements to make the «intelligence case»
in a bulk SIGINT application**

The proposed CSE Act (Section 35 (2) (b) as foreseen in Bill C-59)⁶¹ requires the Canadian foreign intelligence service (CSE) to *independently demonstrate* in their application why the information to be acquired in bulk (in Canadian terms: unselected information) «could not reasonably be acquired by other means» – that is, to demonstrate why less intrusive collection methods are insufficient.

Codifying such a specification in law (as opposed to an executive decree) is *prima facie* a much stronger safeguard, because governments cannot change it at will.⁶²

⁵⁹ Renan, «The Fourth Amendment as Administrative Governance,» May 2016, 1068, http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/06/68_Renan_-_68_Stan._L._Rev._1039.pdf.

⁶⁰ Article L. 854-2.-II. of French Law No. 2015-1556 on international surveillance.

⁶¹ All provisions referring to the Canadian Bill C-59, deal with the draft law as it exists at the time of writing: after first reading in the House of Commons, online: <http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading>.

⁶² By comparison, the German BND Act (§6 (7)) merely states that a secret service regulation will determine the specifics of the authorization process. In the United Kingdom, IPCO has recently published an advisory note (01/2018) on how it wants to review warrants, which is discussed in the section on oversight.

Naturally, lawmakers are not immune to adopting underwhelming provisions, which, once adopted, are also harder to change. Another advantage with codified provisions is that the public can have more trust in the rigorousness of the proportionality check, and the authorization body has a firm right to a more detailed explanation by the services. In Switzerland, similarly, the law explicitly demands that warrants for bulk surveillance must contain an explanation of necessity.⁶³



**Germany:
Listing of search terms in untargeted communications
data surveillance warrants⁶⁴**

Warrants covering foreign-foreign strategic surveillance relating to EU institutions and public bodies of EU member states must specify the search terms to be used (Section 9 (2) German BND Act).

Having to specify search terms in advance is an incentive for analysts to narrow down what is relevant and to use more restrictive terms. This helps to limit the number of persons affected by the collection and avoids the risk of having to obtain a new warrant because a use of broad terms returned too many records to be useful for analysis. What is more, subsequent judicial reviews of the SIGINT practice are far more meaningful with actual knowledge of the search terms used.



**The Netherlands:
Predefining specific fiber optic cables to be intercepted**

The explanatory memorandum of the Dutch government noted that warrants should typically specify what (fiber) cables are to be intercepted.⁶⁵

Stipulating the concrete technical infrastructure that is to be intercepted can be an important restriction. In the United States, orders issued for intelligence surveillance

⁶³ Article 40 (1b) of Swiss Federal Intelligence Service Act (Nachrichtendienstgesetz, «Genehmigungsverfahren für Kabelaufklärung»).

⁶⁴ A similar obligation to list «categories» of search terms in the Swiss Federal Intelligence Service Act (Article 40 c Nachrichtendienstgesetz, «Genehmigungsverfahren für Kabelaufklärung»)

⁶⁵ Annex to the letter of the Minister of Interior regarding the Dutch intelligence law (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Bijlage bij brief Wiv 2017 en regeerakkoord), 2017, 3, https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZ-K+over+Wiv+2017+en+regeerakkoord.pdf.

under the Foreign Intelligence Surveillance Act (FISA) must specify the device, account, or «facility» (50 U.S. Code 1805(a)) for which surveillance is to be applied. Naming a specific cable could qualify as a «facility» in that sense.⁶⁶ This can be an important aspect for assessing the proportionality of the operation in question, because fewer people might be affected if a specific access point for intercepting a certain communication stream is assigned.



**Germany:
Direct ministerial responsibility for the activation of certain
search terms**

Section 9 (2) of the BND Act provides direct ministerial responsibility for applications involving search terms that target EU institutions or bodies of EU member states. The law requires the Federal Chancellery to be informed about SIGINT warrants and the search terms listed therein. This strengthens ministerial accountability, also retroactively, for malfeasance in steering foreign communications collection.

Selected examples of bulk warrant durations

The following table offers examples for the duration of warrants for foreign communications data collection in selected countries. In principle, the duration of a warrant should be determined with a view to the essential criteria for issuing the bulk warrant, for example the operational purpose for collecting the data in bulk. A shorter duration is called for if the relevant conditions underlying this operational purpose are likely to change within a short time period. If the conditions are stable over longer time periods, a longer warrant duration could become necessary. Introducing such normative guidelines for determining the duration of warrants could provide even greater flexibility for issuing warrants and lead to durations being determined by what is factually needed.

⁶⁶ Kris and Wilson, «National Security Investigations & Prosecutions 2d,» 2012, 572f.

Table 2: Bulk warrant durations

Country	Duration time	Provision
France	12 months, renewable for 12 months	Article L. 854-2.-II. of Law No. 2015-1556 on international surveillance
Germany	9 months, renewable for 9 months 3 months, renewable for 3 months	Section 9 (3) BND Act Section 10 (5) G10 Act
The Netherlands	3 months, renewable for 3 months ⁶⁷	Section 29 Intelligence and Security Services Act 2017
United Kingdom	6 months, renewable for 6 months	Section 143 (1)(a) IP Act
Switzerland	6 months, renewable for max. 3 months at a time	Section 41 (3) ND Act

Good practice in oversight

Given that the drafting of applications for surveillance operations is typically a matter for the executive branch, our comparative review of oversight practices revealed no commendable or instructional examples that are relevant to this phase in the SIGINT governance process.

Summary of main findings and reform agenda

Warrants can open the door for detailed scrutiny of the tasking process. They allow reviewers to assess the legality and proportionality of communications data interception prior to their implementation. In some countries, the intelligence community cannot put its envisaged bulk surveillance measures into practice without judicial oversight. Unlike parliamentary oversight, which is often ex post in nature, this is a powerful means by which to rein in the executive.⁶⁸ Detailed warrants enable oversight bodies to better conduct meaningful proportionality tests and encourage agencies to be specific and efficient in their surveillance applications.

The various forms of bulk warrants that now exist in many countries highlight the potential for even broader applications of this accountability mechanism in the field of foreign communications surveillance. There is a need to think more creatively about further relevant criteria and additional aspects that add more precision to bulk warrants. For example, lawmakers could ask the executive to specify the actual use of

⁶⁷ Notice, however, the three-month period mentioned in Article 29 of the Dutch Intelligence Act is a standard authorization period for special powers. Deviations can be found in Article 48 (collection, 1 year), Article 49 (search, 1 year), Article 50 (automated data analyses, 1 year).

⁶⁸ Of course, there may be emergency situations where the intelligence community can be allowed to implement bulk surveillance measures without independent scrutiny. Yet, by default, it is preferable to have warrants by design; that applies when bulk warrants are warrants that are systematically checked by courts or review bodies before the measures are put into action.

minimization procedures and how the intelligence services intend to honor data-use limitations. If readers know of other safeguards in national intelligence laws regarding additional information that is required for warrants, we invite your comments. The same goes for the lack of best practice examples in the area of oversight innovation.

Phase 3: Authorization/Approval

After a warrant has been issued, the requested bulk SIGINT measure must be authorized or – as the case may be in different jurisdictions – approved by a review body that assesses the necessity and proportionality. Differences exist across nations as regards the moment when the independent judicial review process comes into play. In some countries, the competent minister or other members of the executive authorize warrants. In the United Kingdom, for example, the *authorization* of warrants is the privilege of the executive. Ministerial authorization, then, has to be *approved* by independent Judicial Commissioners. By contrast, in the German legal framework, warrants are *authorized* by bodies such as the G10 Commission or the Independent Committee.

The independent ex-ante authorization/approval of data collection is a crucial safeguard against the misuse and abuse of bulk surveillance powers.⁶⁹ The legitimacy of surveillance practice depends on the control of executive conduct from the outside. Enacting the control mechanism *prior* to implementation is crucial, because this can both deter and prevent certain actions from being taken. Independent authorization/approval also contains an important learning element, because the competent bodies can improve their controls, draw lessons from past mistakes, and then declare more assertively that certain measures are not required, or that no sufficient proof was presented.

Across many democracies, a dual system of authorization/approval has emerged that combines a judicial and an executive control function. A judicial oversight body – ideally a court – is best suited to administer a competent legal review of a bulk surveillance application. But, as several discussions with intelligence oversight practitioners have shown, the involvement of the political leadership level, for example the responsible minister or secretary of state, may also present a relevant safeguard, especially in the realm of foreign intelligence. The acceptance of a surveillance operation may go beyond legal criteria of necessity and proportionality and move into the political domain. Including political considerations, such as possible damage to diplomatic

⁶⁹ «In *Popescu v. Romania*, the Court considered that the Romanian authority which ordered the surveillance (the prosecutor) was not independent from the executive. It stated that the authorising body must be independent and that there should either be judicial control or independent control over the issuing body's activity. Similarly, in the *Iordachi and Association for European Integration and Human Rights and Ekimdzhev* cases the Court stressed that independent controls should exist at both the authorisation stage and the follow-up stage. The Court has a preference for judicial authorisation, even if, in *Kennedy v. the United Kingdom*, it accepted the British system of ministerial authorisation.» See: Venice Commission, «Report on the Democratic Oversight of Signals Intelligence Agencies,» 2015, para 106, [http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)011-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e).

relations with a foreign country, may add an important perspective to the authorization process.

Relevant aspects

The complexity and confidentiality of the subject matter require that the authorization body must be sufficiently qualified (e.g., a specialized court for SIGINT operations) and has to have the necessary powers and resources to conduct the authorization (e.g., access to all relevant information).⁷⁰ A fundamental requirement for an authorization/approval body is its independence. Further relevant aspects include:

- Who is involved in the authorization process?
 - How is the independence of the authorization/approval ensured? For example, unified, fully resourced authorization bodies with full access rights are far better equipped to conduct comprehensive reviews.
- When does the review take place? Prior to, or after the implementation of bulk surveillance measures?
- How does the authorization take place?
 - Are all warrants independently authorized, or does the law account for exceptions? For example, are there any exceptions for emergency procedures? If so, are they designed so that they do not unduly open up loopholes for unauthorized operations?
 - What assessment criteria are being used?
 - How explicit are the oversight bodies as regards its use of criteria to assess the legality, necessity, and proportionality in concrete practice?
 - How much time does the oversight body have to assess a warrant?
- Does the law foresee an appeal procedure?
 - Are the authorization decisions legally binding?
 - Is technical and adversarial advice incorporated into the authorization process? If so, how?

70 «The Court [...] found that ... in principle [it is] desirable to entrust supervisory control to a judge. ... Supervision by non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control.» See: ECtHR judgment in *Roman Zakharov v. Russia*, Application no. 47143/06, para. 275, <http://hudoc.echr.coe.int/eng?i=001-159324>.

- Do the warrants also account for metadata and «secondary data»⁷¹?
- Does the authorization take other (ongoing) surveillance measures into account when assessing a new warrant?⁷²
- How is the authorization decision documented? Are there publicly available statistics on the number of rejections and total number of applications reviewed?

Good practice in legal safeguards

Margin of discretion for authorization bodies



Canada: Option to approve a warrant with conditions

Bill C-59 envisages a rule (Part 2, Intelligence Commissioner Act, Section 21 (2 b)) that allows the Intelligence Commissioner to approve, reject, or *approve with conditions* the retention of foreign datasets. These conditions may refer to «the querying or exploitation of the foreign dataset or the retention or destruction of the dataset or of a portion of it,» and the intelligence commissioner has to «provide reasons for doing so, if he or she is satisfied that those conclusions are reasonable once the conditions are attached.»

Should Bill C-59 pass, the option to authorize with conditions will apply across the board for all intel authorizations (beyond the CSE, which is the Canadian foreign intelligence agency). In principle, this can provide oversight bodies with greater control over the implementation of surveillance measures. This could mean, for example,

⁷¹ «Secondary data» is a term that is often used in UK intelligence legislation. According to Graham Smith, it is «perhaps the most important category of data within the IP Act. It is, roughly speaking, metadata acquired under a targeted, thematic or bulk interception warrant. As such it is not subject to all the usage restrictions that apply to intercepted content. In particular, unlike for content, there is no requirement to obtain a targeted examination warrant in order to select metadata for examination by use of a selector (such as an e-mail address) referable to someone known to be in the British Islands. The broader the scope of secondary data, therefore, the more data can be accessed without a targeted examination warrant and the more of what would normally be regarded as content will be included.» Source: Smith, «Illuminating the Investigatory Powers Act,» February 22, 2018, <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html>.

⁷² The concept of «Überwachungsgesamtrechnung» was developed by the German Federal Constitutional Court (Judgement BVerfG, of 12. April 2005 - 2 BvR 581/01). The concept departs from the premise that the authorizing body rarely, if ever, considers the entirety of other existing measures when deciding to approve a particular application. The court therefore proposed that, in order to assess the overall infringement of fundamental rights of a citizen, all ongoing surveillance measures must be taken into account when authorizing additional data collection.

setting a specific number of days before data has to be deleted, or defining specific kinds of information that must be destroyed before analysis.

Public reporting on individual authorization decisions



The Netherlands: Mandatory public report by authorization body

The Dutch TIB commission is legally required to publish a public annual report.⁷³



United States: Option to request publication of a Foreign Intelligence Surveillance Court decision or opinion

«The Judge who authored an order, opinion, or other decision may sua sponte or on motion by a party request that it be published. Upon such request, the Presiding Judge, after consulting with other Judges of the Court, may direct that an order, opinion or other decision be published.»⁷⁴

As mentioned earlier, we purposely borrow some ideas from targeted collection systems when we believe that some of the specific practices or provisions can also be applied to non-targeted collection systems. In this case, publishing court decisions opens up room for debate and better public scrutiny of surveillance practice and legal interpretations of surveillance law.



United States: Required declassification review for new legal interpretations

Section 602 (a) of the USA Freedom Act outlines a declassification requirement. «[T]he Director of National Intelligence, in consultation with the Attorney General, shall conduct a declassification review of each decision, order, or opinion

⁷³ Eijkman, Eijk, and Schaik, 2018, 41.

⁷⁴ United States Foreign Intelligence Surveillance Court (FISC), «Rules of Procedure,» November 1, 2010, rule 62, <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.

issued by the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review (as defined in Section 601(e)) that includes a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term «specific selection term,» and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion.»⁷⁵

To satisfy the needs for the protection of sources and methods, documents may also be made publicly available in redacted form.

Adversarial proceedings provide additional input legitimacy to the authorization/ approval decision process



**United States:
Option to request external legal opinion in authorization
procedures**

The FISC can «appoint an individual to serve as amicus curiae to assist in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law.»⁷⁶ Hence, the Court has the option to engage in an adversarial proceeding when determining the legality/necessity of foreign intelligence warrants. The law explicitly requires the appointed «friend of the court» to provide «legal arguments that advance the protection of individual privacy and civil liberties.»⁷⁷

The authorization of a surveillance operation becomes more robust if adversarial counsel is made available to the authorizing (or approving) body at the decision-making point in time. Hearing only one side of the argument invites regulatory capture. Therefore, the FISC maintains a pool of designated legal counsels, from which the Court may appoint an individual amicus curiae for a specific case. Requesting external expertise from such amici offers a fresh view on a significant or new legal matter and helps to avoid tunnel vision while enhancing the input legitimacy of the process. In Sweden, similarly, «in all proceedings before the Swedish Foreign Intelligence Court [*Försvarsunderrättelsedomstolen*], a privacy representative [*Integritesskyddsombut*]

⁷⁵ Section 602 of the USA Freedom Act, <https://www.congress.gov/bill/114th-congress/house-bill/2048/text>.

⁷⁶ 50 U.S. Code §1803 (i)(2)(A); Cook, «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty,» 2017, 543, <http://digitalcommons.wcl.american.edu/cgi/view-content.cgi?article=1960&context=aulr>.

⁷⁷ 50 U.S. Code § 1803(i)(4)(A).

must be present, unless this would delay and compromise the operation.»⁷⁸ This representative is appointed by the government.

The mere indication that the FISC intends to appoint an amicus curiae has already proven to have had a deterrence effect on the executive branch. According to the FISA Annual Report 2017,⁷⁹ no amicus was appointed during that year. Yet, the Court considered appointing a person three times, but in all three cases, the government ultimately did not proceed with the proposed application or modified the final application «such that they did not present a novel or significant question of law, thereby obviating a requirement for consideration as to the appropriateness of appointment of amicus.»⁸⁰ This said, the opinions presented by an amicus curiae need not be «adversarial.» They may also bolster the government's argument, for example with technical aspects, as opposed to by default taking the opposite position from that of the government.⁸¹

Defining maximum permissible number of certain surveillance instruments



France: Quotas for specific data collection methods

The French intelligence law sets quantitative limits for the use of specific intelligence techniques in order to end dispensable authorized warrants before approving new ones. The number of simultaneous authorizations of specific operations is limited to a fixed amount set by the prime minister at the recommendation of the French oversight body the National Commission of Control of the Intelligence Techniques (CNCTR).⁸²

The French have adopted fixed quotas for certain collection methods in their governance scheme for targeted surveillance methods. The underlying logic – namely to force agencies to use or abandon existing authorized warrants instead of simply applying for new authorizations – seems to be an adequate tool to limit the use of specific

⁷⁸ Lubin, 2018.

⁷⁹ Administrative Office of the United States Courts, «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017,» April 25, 2018, http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.

⁸⁰ Ibid., 4.

⁸¹ Next to legal amici, there should also be technical amici that serve the court with expertise on technological questions. Thus far, no technical amici have been designated, let alone appointed contribute to a proceeding.

⁸² Commission nationale de contrôle des techniques de renseignement (CNCTR), «Deuxième Rapport d'activité 2017,» 2018, 37ff., https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.

instruments. Potentially, quotas may also spur annual public debates about the set numbers. Naturally, the effectiveness of this approach hinges both on the process and the actual quotas used. Ideally, the quota-setting should be based on a transparent and verifiable process that outlines the specific need for a surveillance allowance.

The quota system applies to three types of data collection: first, to the interception of electronic communications,⁸³ with a quota of 3,040 in 2017; second, to the use of international mobile subscriber identity (IMSI) catchers, with a total quota of 60; and third, to the real-time collection of connection data, with a quota of 500.⁸⁴ The different relevant ministerial departments are assigned a subset of the overall quota (e.g., sub-quotas for interior, customs, defense, and other ministries) and checked on a daily basis by the GIC.⁸⁵

Good practice in oversight

Explicit standards for proportionality assessments when approving bulk SIGINT warrants in actual practice

Explaining exactly how the necessity and proportionality test of a bulk collection warrant is conducted is crucial information for rating the thoroughness and legitimacy of the process. The United Kingdom's Investigatory Powers Commissioner's Office (IPCO) has published an Advisory Notice that provides advice and information to public authorities and to the general public as to the general approach that Judicial Commissioners will adopt under the IP Act when deciding whether to approve decisions to issue warrants.



United Kingdom: IPCO Advisory Notice 01/2018

The Judicial Commissioners, who are in charge of approving bulk SIGINT warrants, must have regard for whether what is sought to be achieved by the warrant, authorization, or notice could reasonably be achieved by other, less intrusive means. In exercising that statutory responsibility, the Judicial Commissioners must, in particular, take into regard:

⁸³ Article L. 852-1 of French Interior Security Act.

⁸⁴ CNCTR, 2018, 37ff.

⁸⁵ In France, the interception of communications data is managed by a specialized body called Groupement interministeriel de control (GIC). The GIC centralizes the referral of authorized data collection to the respective providers that hold the data. This body works under the purview of the prime minister and is also charged with controlling compliance with the quotas.

- whether the level of protection to be applied in relation to any obtaining of information by virtue of the warrant, authorization, or notice is higher because of the particular sensitivity of that information;
- the public interest in the integrity and security of telecommunication systems and postal services;
- any other aspects of the public interest in the protection of privacy;
- additional safeguards for matters such as legal professional privilege (e.g., all for professional legal advisers) and journalistic material;
- the tests of necessity and proportionality, as applicable under the Human Rights Act 1998 and under European Union law, to the extent that this applies to the powers/activities for which approval is sought.⁸⁶

This Advisory Notice is not binding and can theoretically change at any point in time. Therefore, it only represents the opinion of the current Judicial Commissioners, because there is also no obligation to inform the public whether the guidelines were revised. The gold standard for providing transparency remains setting out such procedural rules in law. Some critics have pointed out that the Advisory Notice has failed to emphasize «the importance of a current and relevant intelligence case justifying the decision to issue warrants,»⁸⁷ particularly in national security cases, where the Advisory Notice leans toward a wider margin of judgment.



**United Kingdom:
Open oversight – civil society dialogue on proportionality standards for the review of bulk powers**

Following the publication of the Advisory Notice in January 2018, IPCO proceeded to enrich these principles in May 2018 with the help of a public invitation for input on issues relevant to the proportionality of bulk powers. IPCO asked NGOs and others to provide assistance in identifying the broad range of factors that the Judicial Commissioners should have in mind when evaluating the proportionality of bulk warrants:

⁸⁶ IPCO, «Advisory Notice 1/2018. Approval of Warrants, Authorisations and Notices by Judicial Commissioners,» 2018, 4, <https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf>.

⁸⁷ The Chambers of Simon McKay, «Judicial Approval of Warrants, Authorisations and Notices under the Investigatory Powers Act 2016: A Review of the Investigatory Powers Commissioner’s Office First Advisory Note,» 2018, <https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/>.

- What factors should the Judicial Commissioners take into account when considering whether the conduct proposed in a bulk warrant is proportionate?
- Is there any particular approach that the Commissioners should adopt when evaluating those factors, some of which may be competing?⁸⁸

Summary of main findings and reform agenda

Independent authorization becomes an even more powerful democratic safeguard if the procedure is fully transparent and when the review officials are endowed with a robust mandate and enough discretion to authorize or approve warrants with conditions. Ideally, the legal framework stipulates a mandatory declassification review that aims to publish as much information as possible, for example about critical legal interpretations.

Adversarial proceedings are an essential feature of potent independent approval/authorization. Equally, explicit standards for proportionality assessments for authorizing or approving bulk SIGINT warrants in actual practice, such as IPCO's Advisory Notice combined with its subsequent outreach to civil society and other experts, are promising examples of good practice. If readers know about other specific standards that are being used by other oversight bodies when it comes to availing themselves of adversarial counsel or assessing the proportionality of SIGINT measures, kindly let us know. The same holds true for information on how oversight can or should verify whether a particular measure is likely to yield timely and relevant information.

Further oversight body involvement should now be considered when it comes to the authorization to share intelligence.

Phase 4: Collection & Filtering

Once a warrant has been authorized or approved, an intelligence agency can proceed with the implementation of a particular surveillance measure. For this, it intercepts the relevant signals, for example by tapping an internet service provider's (ISP) fiber optic backbone cable or diverting data at an internet exchange point. Afterwards, the collected data has to be filtered for two reasons: First, because of the huge volumes passing through, which would be far too much to be stored long-term, gratuitous data that is extremely unlikely to yield any intelligence value is filtered out (e.g., all data from public video feeds); second, the collected data stream has to be filtered so as to abide by legal requirements. Certain data – for example domestic communications or the communications involving lawyers, priests, or other professions relying on

⁸⁸ IPCO, «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers,» May 23, 2018, https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf; the submissions can be found here: <https://www.ipco.org.uk/Default.aspx?mid=4.13>.

the confidentiality of correspondence – may be offered higher levels of protection in national surveillance laws.⁸⁹

Collection

Relevant aspects

At the collection point, it is critical to clearly define who is in charge of extracting the data and where and how the extraction devices may be installed. Is the collection administered by the intelligence service, or do private entities (e.g., ISPs) do this on behalf of the intelligence services? This distinction is relevant, as provider intermediation can be an important safeguard against over-collection. In principle, intelligence agencies should not have direct access to the facilities of telecommunications providers. Cases have surfaced, though, in which internet companies agreed to search the data they administer on behalf of an agency. Yahoo, for example, secretly scanned all email accounts for information provided by US intelligence agencies.⁹⁰ A legal framework, therefore, has to define how (private) intermediaries may be compelled to cooperate and what means are available for operators to challenge particular measures.

Good practice in legal safeguards

Intermediary for centralized data collection



France: Specialized executive body serves as data collection center

In the French intelligence community, most data collection from third parties, such as internet service providers or communication service providers such as Google and Facebook, is handled by the GIC. This body is technically not part of the intelligence community. Rather, it serves as a centralized hub that manages all data interception/acquisition under the purview of the prime minister.⁹¹

⁸⁹ As established earlier, it is not always technically possible to filter out the communications of protected categories such as certain professions. Individuals or groups concerned could submit their phone numbers to intelligence and law enforcement agencies, but for internet communications, clear-cut filtering is much more complicated.

⁹⁰ Menn, «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources,» October 5, 2016, <https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT>.

⁹¹ Government of France, «Groupement Interministériel de Contrôle (GIC),» <http://www.gouvernement.fr/groupement-interministeriel-de-controle-gic>; «Le Groupement interministériel de contrôle va beaucoup donner,» <http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html>.

It is preferable for an intermediary body such as the GIC to be responsible for the first filter/selection process, as fewer agents will have access to the collected data. A similar specialized data collection center exists in Switzerland.⁹² Consolidating all cable-tapping and data acquisition in the hands of one body may also be done for reasons of cost efficiency: Instead of having technical experts spread across the intelligence community, bundling expertise and competencies in one body may allow for the better use of the staff and resources available. Plus, it simplifies the accountability process.

Centralizing the management of data access on behalf of the agencies can also serve to facilitate holistic oversight of all the data collected. The GIC only grants analysts access to data that they need for a given assignment. This gatekeeping function may help to maintain secrecy. That said, centralizing data storage also entails the risk of creating a single point of failure for data security (e.g., hacking attacks, etc.). However, the French oversight body CNCTR describes the data intermediary as an effective safeguard, because the GIC – and not the intelligence services themselves – implement and manage the data collection.⁹³



United States: Options for providers to object to government requests for data

A private intermediary that receives an interception order under the FISA regime, such as an ISP or an internet exchange point, may challenge such an order in the FISC.⁹⁴

One well-documented, albeit unsuccessful, objection to a government request was a 2007 Yahoo case. The service provider challenged the constitutionality of an order to hand over user information under the Protect America Act. After losing the initial challenge before the FISC, «the provider appealed the decision to the Foreign Intelligence Surveillance Court of Review.»⁹⁵

⁹² The implementing data interception service is called «Zentrum für elektronische Operationen» (ZEO). See: Führungsunterstützungsbasis FUB, «ZEO (Elektronische Operationen),» <https://www.vtg.admin.ch/de/organisation/fub.html>.

⁹³ CNCTR, 2018, 16.

⁹⁴ One such proceeding is published (in redacted form) here: <https://www.aclu.org/2014-fisc-opinion-internet-service-providers-challenge-section-702-surveillance>.

⁹⁵ Electronic Frontier Foundation, «Yahoo's Challenge to the Protect America Act in the Foreign Intelligence Court of Review,» October 22, 2013, <https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review>; other, more recent provider challenges include: Conger, «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying,» June 14, 2017, <https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752>.



United States: ISPs responsible for installing splitters and selector lists

Under Section 702, private internet service providers – and not the agencies – are in charge of implementing the authorized upstream collection systems. «The government identifies or <tasks> certain <selectors,> such as telephone numbers or email addresses, that are associated with targeted persons, and it sends these selectors to electronic communications service providers to begin acquisition.»⁹⁶ Then, «the provider is compelled to give the communications sent to or from that selector to the government.»⁹⁷ If the agencies were in charge of the selector activation, this could lead to additional collection.⁹⁸

Relying on a private intermediary to install and maintain the interception devices constitutes a safeguard, because the agencies cannot single-handedly reuse or misuse the devices for other aims. Intermediaries that are compelled to cooperate have an incentive to closely measure each government request against the relevant legal requirements. Internet companies have reputational costs associated with enabling far-ranging access to their customers' data and, therefore, may only allow what is strictly necessary. This additional layer of scrutiny is missing when countries give their intelligence agencies direct access to systems or communication infrastructure, with no provider serving as an intermediary.⁹⁹

Good practice in oversight

Technical oversight interfaces for direct database access

A number of European countries (see table 3) have installed interfaces that give oversight bodies direct access to collected data. Such direct access could be an important innovation for oversight, but it also entails risks that have to be addressed.

⁹⁶ Privacy and Civil Liberties Oversight Board (PCLOB), «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act,» July 2, 2014, 7, <https://www.pclob.gov/library/702-Report.pdf>.

⁹⁷ Ibid.

⁹⁸ The public also gain some insights in the cooperation between agencies and ISPs based on an email sent from Deutsche Telekom to the BND that was published here: <https://de-de.facebook.com/peterpilz/photos/902029969840817>.

⁹⁹ E.g., a number of EU countries (Sweden, Hungary, Romania, Estonia, Latvia, Lithuania) have direct access, and Finland is now considering direct access legislation. For more information on this, see the forthcoming paper by the Center for Democracy and Technology on the subject.

Table 3: Technical oversight interfaces

Country	Access characterization
France	«The CNCTR enjoys permanent, complete and direct access to the implementation reports and registries of surveillance techniques, to the collected intelligence, as well as to the transcriptions and extractions carried out by the intelligence services.» ¹⁰⁰ This is based on the oversight body's direct technical interface with the GIC.
The Netherlands	«To conduct their assessment, the oversight department of the CTIVD has direct (digital) access to classified information kept by the AIVD [General Intelligence and Security Service] and MIVD.» ¹⁰¹
Norway	«The Committee can carry out most of its inspections without assistance directly in the services' electronic systems.» ¹⁰²
Switzerland	AB-ND [independent supervisory authority on intelligence activities] has direct online access to the data stored by the Federal Intelligence Service (NDB), including specially protected personal data. This remote access is not permanent, but granted on a case by case basis for a specific investigation of the oversight body on a specific database. ¹⁰³

The advantage of direct access to databases is that the oversight body can conduct random checks, unannounced inspections, and potentially also automated controls on the data handling by the intelligence agencies. This has the potential to level the playing field between the controller and the controlled. Traditionally, oversight bodies depend, to a large extent, on the information provided by the intelligence services. If overseers gain direct access, the incentive to comply increases, because intelligence officials cannot know whether an incident will be reviewed or not. Technical interfaces might also empower review bodies to monitor statistical anomalies in the databases. This opens a new field of (automated) oversight applications that will support overseers in effectively diverting their limited resources for in-depth compliance auditing. Such an approach – using analytical techniques to identify potential non-compliance – amounts to «predictive oversight» and is already being practiced by institutions entrusted with financial audits in the banking sector.

Granting direct, unfettered access for oversight bodies to the intelligence databases may, however, turn them into attractive targets for foreign espionage and hacking

100 Article L. 854-9 of Law No. 2015-1556; see also: European Union Agency for Fundamental Rights, «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU - Volume II: Field Perspectives and Legal Update,» 2017, 79, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf; see also: French Interior Security Act, Article L. 833-2.

101 Eijkman, Eijk, and Schaik, 2018, 38.

102 Norwegian Parliamentary Oversight Committee (EOS Committee), «Annual Report 2017 - Document 7:1 (2017-2018),» February 22, 2018, 10, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

103 Article 78 (4-5) of Swiss Federal Intelligence Service Act (Nachrichtendienstgesetz, «Aufgaben, Informationsrechte und Empfehlungen der Aufsichtsbehörde»).

attacks. It is important, therefore, to only grant such access to properly trained oversight personnel and to provide the highest level of cybersecurity to oversight bodies.

Making sense of raw intelligence data and log files is hard. It is not enough for oversight bodies to merely have access. The information advantage that direct access may bring comes from data analytics. In other words, oversight bodies need to engage with the data that they now have access to. In order to learn how much more rigorous their controlling could become, overseers may want to learn from financial audit bodies and will need special training. They may also want to commission the design and implementation of control algorithms.

Filtering

Once data has been acquired by means of untargeted electronic surveillance, it may be subject to additional filtering, depending on the national surveillance regulations.

Relevant aspects

The specifics of the data minimization and filtering processes should be subject to critical review, for they may reveal the extent to which intelligence agencies abide by constitutional and human rights standards. For example, some intelligence laws grant enhanced privacy protection to professions that depend on the confidentiality of information. This may pertain to communications involving priests, lawyers, journalists, and physicians. Whether and how data minimization and filter tools are capable of accommodating such communications in practice should be of interest to oversight bodies. This may also extend to the review of protected health data and DNA-related information.

In addition, there are technical questions that come to mind, as they, too, reveal interesting information about the independence of oversight bodies and the extent to which data minimization is an actual priority (or not) within the intelligence community. For instance, how is «surplus information» treated in the collection and filtering process? When data minimization systems, such as the Massive Volume Reduction (VRE) systems of the United Kingdom's Government Communications Headquarters (GCHQ), are being used, are they subject to independent oversight? More specifically, are the technical equipment and filter programs regularly subject to independent verification, or do the oversight bodies merely rely on the assurances of the intelligence agencies that the data minimization and filtering processes are fit for purpose?

Good practice in legal safeguards

Deletion of material that has been filtered out



The Netherlands:
All raw data (including content and metadata) that gets filtered out will be impossible to retrieve by the intelligence services

While content and metadata may be stored for up to three years (by default one year; two possible extensions of one year each) in the Netherlands, data must immediately and irretrievably be destroyed as soon as it is filtered out, or otherwise determined not to be relevant for any other intelligence investigation.¹⁰⁴

The services have an obligation to assess the relevance of the data collected (see data maintenance section below).

Good practice in oversight

Review of compliance audits



United States:
The FISC reviews compliance audits performed by the intelligence community

Modern intelligence agencies should have dedicated staff for internal compliance auditing. Allowing an independent body such as the FISC to review internal audits strengthens the impact of these controls. However, the FISC relies only on the intelligence community to present audit data and does not engage in its own compliance investigations. Ideally, an oversight body would also conduct its own random sample test in order to verify the thoroughness and completeness of these compliance audits.

¹⁰⁴ Dutch Act on the Intelligence and Security Services 2017, Article 48 (5). See also: Annex to the letter of the Minister of Interior regarding the Dutch intelligence law, 2017, 3.

Summary of main findings and reform agenda

A noteworthy practice is the increasing availability of technical oversight interfaces in various European countries. We also discuss the involvement of private parties (e.g., providers) and public intermediaries (such as the GIC in France) that may facilitate and centralize the collection of data. Whether the centralization of the data management and the live access to intelligence databases can be turned into an added value for oversight and democratic governance remains an open question, however. There is a need for further research as regards the effective use of such tools for different control functions.

Telecommunications providers are a central stakeholder group in the field of surveillance and, hence, must have a strong voice. Providing the possibility to substantially challenge surveillance orders is an important practice in this regard.

The independent verification of data minimization techniques deserves greater attention from oversight bodies. They ought to look into the technical implementation of the filtering process and the independent auditing of filter effectiveness. Similarly, the deletion of data is an ongoing oversight challenge that many review bodies are gradually waking up to. Here, we find that mutual learning from regular exchanges with other oversight bodies in other countries and the promotion of systematic dialogues with external experts ought to be intensified.

Phase 5: Data Processing

Once data has been collected and filtered, it must be stored, tagged, and later removed or destroyed. This phase of the SIGINT process is particularly relevant for oversight and the services because lawful and efficient data management is the basis for relevant data analysis. For the sake of clarity, this phase is divided into four subcategories reflecting the different facets of data processing: storage, maintenance, sharing, and deletion.

Data storage

Relevant aspects

Due to different retention periods, it may become necessary to keep separate databases, for example for encrypted data, metadata, and content data, or in order to distinguish data pools according to their legal basis or warranted purposes. It can therefore be relevant whether there are isolated data storage locations. Increasingly, bulk surveillance governance relies on the verifiable technical or institutional separation between the authority to intercept and the authority to analyze the data. In order to honor data protection obligations, a surveillance law should further restrict the extent to which databases may be linked or accumulated.

Transnational threats prompt closer trans-border cooperation among intelligence services, not least for neighboring countries. Intelligence data – both unevaluated and evaluated – is therefore not just shared bilaterally, but also stored in joint intelligence

databases for different threats and purposes. When we speak of *joint databases*, we refer to a multilateral exchange of data that can be hosted either on national territory or abroad. Typically, joint databases are run multilaterally, with all participating services adding and accessing data.

The European Counter Terrorism Group (CTG), for example, runs a database that facilitates the multilateral exchange of evaluated data on individuals who have traveled to and returned from certain conflict areas.¹⁰⁵ This database became operational in July 2016, is administered on servers in the Netherlands, and makes information available in (near) real-time to the 30 participating services of the CTG. Interestingly, unevaluated data may also be exchanged within the CTG, albeit not via the database. It may be jointly stored and processed within standard SIGINT cooperations.¹⁰⁶

The CTIVD’s report concludes that safeguards for the protection of fundamental rights are currently not being sufficiently addressed and recommends setting up additional safeguards and multilateral controls.

Data storage periods for «foreign» data

The table below shows exemplary data storage periods in three countries for foreign intelligence collection. Not listed are the various options for extension of storage periods, which are also provided for in the respective laws.

Table 4: Data storage periods

Country	Storage periods	Provision
Germany	Metadata: 6 months Content data: 10 years (exceptional extension possible)	Section 6 (6) BND Act Section 20 (1–2) BND Act Section 12 (3) BVerfSch Act
France	Metadata: 6 years (from their collection) Content data: 12 months from the date of first data exploitation Unevaluated content data may be stored for 4 years from the date of collection Encrypted data: 8 years	Article L. 854-5. of Law No. 2015-1556 on international surveillance

¹⁰⁵ CTIVD, «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD,» 2018, 10, <https://english.ctivd.nl/documents/review-reports/2018/04/24/index>. See also: van Eijk and Ryngaert, «Expert Opinion – Legal Basis for Multilateral Exchange of Information,» Appendix IV of CTIVD rapport no. 56 to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD, 2017, <https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv>.

¹⁰⁶ CTIVD, 2018, 9.

Country	Storage periods	Provision
The Netherlands	<p>Content and metadata after filter process: 3 years, starting after decryption</p> <p>Encrypted data: 3 years with <i>unlimited</i> extension possibilities for further three years</p>	Article 48 (5–6) of the Dutch Intelligence and Security Services Act 2017

Good practice in legal safeguards

Protecting all data categories



The Netherlands: No distinction between metadata and content data in data retention

Metadata alone – that is, information about calls and emails, for example – can reveal just as much, or even more, about a person or group as content. It is in no way less sensitive or worthy of protection than communications content.¹⁰⁷ On a technical level, the line between content and metadata can also be blurry and create legal uncertainties.¹⁰⁸

Whereas content can be relatively easily encrypted by users, metadata such as call records and information about sender and recipient of a message is technically much harder to conceal. Due to the large quantities of data in SIGINT, the bulk of all data processing done by signals intelligence agencies concerns metadata. Consequently, many legal safeguards that only concern content fall short of effectively protecting the right to privacy. Doing away with the content vs. metadata divide in legislation therefore appears to be a laudable step toward better privacy protections.

¹⁰⁷ Carey, «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information,» May 16, 2016, <https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/>, and Bradford Franklin, «Carpenter and the End of Bulk Surveillance of Americans,» July 25, 2018, <https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans>.

¹⁰⁸ Bellovin, Blaze, Landau, and Pell, «It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law,» 2016, <https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf>.



**Germany:
Obligation to keep a file classification scheme**

The BND has to keep a separate file arrangement memo for each joint database that it is responsible for (Section 28 BND Act). Therein, it must inform about the title of the database; its purpose; the conditions for retention, transfer, and use; the originator and access; the mandatory review and protocol periods; and the legal basis for creating the file. It must also provide an explicit account of foreign public authorities that are entitled to upload or download data from the database. The Chancellery needs to approve each file arrangement memo, and the German data protection authority (DPA) is to be consulted prior to the implementation.

A restriction to this rule is that the law explicitly states that the review mandate of the German DPA covers only the creation of the joint database and the data transfer from the BND to the joint database.

If a joint database with a foreign service is run by a foreign intelligence service abroad, the Chancellery needs to approve the BND's contribution to such a database, too (Section 30 BND Act). Moreover, the BND may only submit personal data to such joint databases if it is allowed to hold such data in its own databases. This is of relevance because the local DPA or review body may need to know to what extent the submissions of data from the national service to a joint database that is administered abroad are identical with the data the national service keeps in its files.¹⁰⁹



**Germany:
Appropriations clause for joint databases**

For German services to contribute to joint databases (irrespective as to whether such a database is hosted at home or abroad), there needs to be a written MoU that covers the purpose of the database and also includes an appropriations clause. The latter requires all signatories to attest that the data cannot be used for purposes other than the ones for which they have been originally collected (Section 26 (4) BND Act).

¹⁰⁹ Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041),» September 21, 2016, <https://www.bundestag.de/blob/459634/a09df397dff6584a83a43a334f3936a3/18-4-660-data.pdf>.



**United States:
Equalized SIGINT retention rules for US persons and non-US persons**

Section 4 (a) of PPD 28 states that «[p]ersonal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of Executive Order 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons.» The general storage period is five years, with the possibility of the DNI extending that period.

Good practice in oversight



**The Netherlands:
Oversight 3.0 project on future challenges run by oversight body**

The CTIVD has set up a multi-year research project to better understand and address the technical challenges of intelligence oversight in the digital age.¹¹⁰ These include new data acquisition techniques, the effective deletion of irrelevant or outdated data, and automated data analyses. By actively investing time and money in the exploration of new options for the oversight of digital intelligence methods, and by including scientists and other independent experts in the process, the CTIVD is laying important groundwork for the future development of oversight.



**Germany:
Joint inspections of judicial oversight body and DPA¹¹¹**

In many countries, separate bodies take on different oversight functions in the SIGINT cycle. In the Netherlands, for example, there is the TIB, the CTIVD, and the parliamentary oversight committee. In Germany, bulk SIGINT is reviewed

¹¹⁰ CTIVD, «Start project Toezicht 3.0.» April 25, 2017, <https://www.ctivd.nl/actueel/nieuws/2017/04/25/index-2>.

¹¹¹ BfDI, «26. Tätigkeitsbericht 2015–2016,» 2017, 134, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=7.

by the G10 Commission and the Independent Committee. Both the federal DPA and the parliamentary oversight body also have roles to play in the democratic control of bulk surveillance.

A higher number of review bodies may mean a higher risk that important information may fall between the cracks or is not sufficiently contextualized when reviewed. Against this backdrop, the German DPA and members of the G10 Commission have begun to perform joint inspections.

Data maintenance

This comprises all practices that concern the labeling and registration of intelligence databases. Data upkeep is not only required by data protection regulations but also serves a practical end: It ensures that the services keep only relevant and accurate data.

Relevant aspects

How is bulk data tagged? And what authority do DPAs have to investigate the sound implementation of databases? For auditing purposes, data must be traceable throughout the entire lifecycle. It is also important to anonymize data to the greatest extent possible. The security and quality of the databases must be ensured to protect the sensitive information from being stolen or compromised.

Adequate data maintenance also builds on clear restrictions of data access. Is the access to the stored data regulated by law and restricted to specialized personnel only? Or is data access for operational teams limited by data exploitation warrants (see phase 2)?

Good practice in legal safeguards



The Netherlands: Duty of care as regards data processing, including the use of algorithms

The Dutch Intelligence Act imposes a general *duty of care* upon the heads of the security and intelligence services (Section 24). It includes adequate measures against data breaches and ensures the validity and integrity of processed data. The Dutch intelligence services are also obliged to «take sufficient measures

to safeguard the quality of data processing, including the algorithms and (behavioral) models used. By covering algorithms and models, the legislator intends to take a technology-neutral approach.»¹¹²

The law requires all data to be examined as soon as possible to determine whether it is relevant to the operation for which it was obtained (Article 48). Data that has been determined not to be relevant shall be immediately destroyed. After one year, all data that has not been examined for relevance must also be destroyed.

Taken together, these provisions create a legal umbrella that protects the privacy and the quality of the data. The CTIVD has the competence to monitor the measures taken to this effect and to control the design of the systems deployed to comply with these duties.



Germany: Mandatory tagging of all bulk SIGINT data

The BND Act requires the services to tag all data that is being collected (Section 10 (1)). This is an important precondition for meaningful data protection controls.

Good practice in oversight

Obligation to perform regular reviews of intelligence registration and data processing



France: Mandatory ex-ante opinion by oversight body on the data-tagging process

The interception and exploitation of communications data are subject to tagging mechanisms that allow for tracing the subsequent data handling. The CNCTR has to submit an ex-ante opinion to the prime minister.¹¹³ In the past, this included recommendations on metadata collection processes, retention periods,

¹¹² Eijkman, Eijk, und Schaik, 2018, 29.

¹¹³ See: Article L. 854-4. of French Law No. 2015-1556 on international surveillance.

storage conditions, and the creation of log files.¹¹⁴ Although these opinions are not binding, we find that such obligatory early involvement of the oversight body may encourage the services to address the needs of oversight while constructing the data-tagging process.

An obligation to regularly review all intelligence registrations (files, databases) would strengthen data maintenance. The Norwegian oversight body, the Parliamentary Intelligence Oversight Committee (EOS), made a proposal in that regard: «In the Committee's opinion, intelligence registrations should be reviewed periodically by the person or persons responsible for registering the information in order to ensure that the intelligence register contains up-to-date, correct, necessary and relevant information.»¹¹⁵ A member of the G10 Commission formulated a similar demand, calling for mandatory data protection reviews by the G10 Commission at least every two years.¹¹⁶

Data-sharing

Relevant aspects

Sharing data with foreign services entails a responsibility to assess and mitigate the risk of misuse of the shared data. Although SIGINT burden-sharing among partner services is a common practice, what rules and procedures are in place to evaluate partner services' data quality and data veracity? Oversight of – and accountability for – data-sharing agreements and joint databases must be ensured. Finally, in times of advanced joint intelligence databases, how do oversight bodies cooperate internationally to control the permissible use of international data pools?

Good practice in legal safeguards

Different logics for oversight body access to shared data

Our comparative review reveals that oversight bodies have found different responses to the originator control policy that, supposedly, governs much of the international intelligence cooperation. Accordingly, an intelligence service may neither share the information nor the source of information it has received from a partner service with third parties without the prior consent of the entity that provided the information in the first place.

¹¹⁴ See: CNCTR, 2018, 16.

¹¹⁵ EOS Committee, 2018, 19.

¹¹⁶ Huber, «Kontrolle der Nachrichtendienste des Bundes – Dargestellt am Beispiel der Tätigkeit der G10-Kommission,» 2017, 15, <https://beck-online.beck.de/Dokument?vpath=bibdata-%5Czeits%5CGSZ%5C2017%5Ccont%5CGSZ.2017.H01.gl2.htm>.

Table 5: Access to shared data

<p>Oversight body as «third party»</p> <p>General practice not to grant oversight body access to third-party data</p>	<p>Oversight body with more access to third-party data</p> <p>General permission with reservation to restrict access in exceptional circumstances</p>	<p>Oversight body with unrestricted access to third-party data</p> <p>Unrestricted access to intelligence stemming from third parties</p>
<p>Example country: Germany</p> <p>Information received from another intelligence service is, by default, not to be shared with the oversight body. However, the government is under an obligation to seek permission to do so from its cooperation partner.¹¹⁷</p>	<p>Example country: Norway</p> <p>In principle, the oversight body has access to all data the Norwegian intelligence service holds, including from third parties. Exceptions apply only to «particularly sensitive information.»¹¹⁸</p>	<p>Example countries: Denmark and the Netherlands</p> <p>Oversight bodies in these countries are not hindered by third-party restrictions and can see all the data that their intelligence service holds.</p>



**Norway:
By default, greater access to third-party information for oversight body**

The EOS Committee, as a clear rule, shall have access to all information in the Intelligence Service that the committee considers relevant for its control activities. Only exceptionally, the head of the intelligence service has the right and duty to refrain from giving the committee «particularly sensitive information» and, instead, refer to the ministry of defense for further assessment of whether access is to be granted.¹¹⁹

The exception of particularly sensitive information comprises:

- The identity of the human intelligence sources of the Norwegian Intelligence Service and its foreign partners;
- The identity of foreign partners» specially protected civil servants;
- Persons with roles in, and operational plans for, occupational preparedness;

¹¹⁷ Wissenschaftlicher Dienst des Bundestags, «Kontrolle von Nachrichtendiensten bei Zusammenarbeit mit anderen Nachrichtendiensten im Ausland,» March 2017, 6, <https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf>.

¹¹⁸ EOS Committee, «Dokument 16 (2015–2016). Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget),» February 29, 2016, 71 (point 19.5, own translation), <https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf>.

¹¹⁹ Ibid.

- Foreign partners› particularly sensitive intelligence operations abroad, which, if they were to be compromised,
 - could seriously damage the relationship with a foreign power due to the political risk involved in the operation, or
 - could lead to serious injury to, or loss of life of, personnel or third parties.¹²⁰

This does not limit the EOS Committee’s insight into information about, and from, Norwegian and foreign sources per se. As a general rule, the EOS Committee has access to intelligence services› and cooperation partners› foreign operations.

Compared to other countries, such as Germany, which apply a rather strict interpretation of the third-party rule vis-à-vis their oversight bodies, the Norwegian model of oversight access to shared data offers greater control options for review bodies. Yet, as the table above also shows, there are also countries such as the Netherlands and Denmark that allow their oversight bodies unrestricted access to intelligence stemming from third parties.¹²¹

Good practice in oversight



Germany: Random sample checks on automatic transfers of personal data to foreign intelligence services¹²²

Regarding the automatic transfer of personal data to foreign intelligence services, the Independent Committee is authorized to perform random checks to verify that no data that violates the ban on industrial espionage (Section 6 (5) BND Act) and no other data that may counter Germany’s national interest is shared (Section 15 (3) BND Act). Moreover, it can also perform random checks on the search terms that are being used for surveillance on data pertaining to EU member states or EU institutions (Section 9 (5) BND Act). Given the technical difficulties of fully ensuring that no national data is being shared (see phase 1), a review mandate for the oversight body to review such data transfers becomes even more important.

¹²⁰ EOS Committee, 2018, 54.

¹²¹ Information obtained at the European Intelligence Oversight Network workshop on May 14, 2018.

¹²² Section 15 (3) BND Act.

Data deletion

The proper deletion of data is an enormous challenge. Technically, it is not as easy as one may think to securely «get rid» of data. This is because «deleting» a file typically only marks the space it occupies as usable. Until the disk space is overwritten, the data is still there and can be retrieved. To ensure that the deleted data cannot be retrieved any longer, the physical records on a storage medium must be overwritten with other data several times (minimum of seven times as per the US Federal government's guidelines).¹²³ But simply overwriting the storage space on a physical medium with new data does not necessarily guarantee that none of the old data is gone for good. Although there are technical means to ensure that deleted data is actually unretrievable,¹²⁴ it seems necessary to develop more detailed standards for what constitutes the proper deletion of data. Errors in this process could result in millions of datasets being falsely stored for years.

Moreover, it is now also «more costly to delete data, than retain it.»¹²⁵ Therefore, legislators have found it difficult to insert the proper legal definitions or public standards for what «deletion» or «destruction» of data means into intelligence laws.¹²⁶ By extension, then, the deletion problem also becomes a veritable oversight challenge. This is because review bodies need accurate audit trails to be able to check services' compliance with data deletion requirements. This may include the automated destruction of data after legal retention periods have lapsed or if the relevant authorization for collecting data has ended.

There is also a need for better guidelines on what data should be deleted at what point in time. Storage periods (see part one of phase 5 above), for that matter, define maximum times for which data may be retained. With adequate normative criteria at hand, the services or the competent oversight bodies could, theoretically, also decide to apply a shorter storage period. For example, if a system flags data that has not been used for a certain time period, this should then prompt a check as to whether this specific dataset is still needed.

Relevant aspects

Intelligence law should outline specific and short retention periods, after which the data has to be permanently and unmistakably destroyed. There might be special requirements for the data deletion of large amounts of data. For example, the NSA's

123 Dorion, «Data Deletion or Data Destruction?,» July 2008, <https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction>.

124 For an encryption-based approach, see: Reardon, Ritzdorf, Basin, and Capkun, «Secure Data Deletion from Persistent Media,» 2013, <https://doi.org/10.1145/2508859.2516699>.

125 Organisation for Economic Co-Operation and Development, «The OECD Privacy Framework,» 2013, 100, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

126 We are grateful to Professor Nico van Eijk, who presented valuable information on the legal and technical challenges of data deletion during our workshop on May 14, 2018.

XKeyscore system may have a rolling buffer, so that new incoming data automatically overwrites the old data.

It is also relevant how data destruction is documented and controlled by the competent oversight body. For example, is stored data linked to specific warrants, and does it have traceable time stamps for full and proper deletion? Adequate records of the data destruction are also important for possible notification purposes.

How are storage and deletion implemented in practice? Should intelligence data be stored in «clouds»? Even in the sphere of national security, we witness close cooperation with commercial third parties, such as private cloud storage services.¹²⁷ How can it be ensured that such outsourcing – entailing the risk of shifting responsibility for a crucial phase of data processing to private companies – does not undermine democratic accountability and oversight?

Good practice in legal safeguards



**Germany:
Obligation to immediately delete data tied to rejected applications**

In case the Independent Committee rejects a bulk SIGINT application aimed at EU bodies or EU member state institutions, all data that has been acquired based on this application needs to be immediately destroyed (Section 10 (2) and (3) BND Act). The Act further includes the obligation to delete all data that may have been collected with the use of an unlawful search term.



**The Netherlands:
Obligation to destroy data from bulk collection that is deemed irrelevant**

The Dutch require that data from bulk collection has to be destroyed as soon as it has been determined to be irrelevant to an intelligence investigation.

¹²⁷ Konkel, «The Details About the CIA's Deal With Amazon,» July 17, 2014, <https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/>.



**France:
Obligation to record data deletions**

Section 854-6 of the French foreign intelligence law demands that «the destruction of collected intelligence, of <transcriptions> and <extractions> are carried out by individually designated and authorized agents and must be recorded.»¹²⁸



**Canada:
Obligation to delete health data in foreign datasets**

Section 11.1 (1 a) of Bill C-59 states that the services have the obligation «in respect of a Canadian dataset or a foreign dataset, to delete any information in respect of which there is a reasonable expectation of privacy that relates to the physical or mental health of an individual.»

Good practice in oversight



**Sweden:
Running statistical pattern analyses on the amount of deleted material**

The reviews of the Swedish oversight body, the State Inspection for Defense Intelligence Operations (SIUN), have to check how the rules concerning obligations to delete are applied. «A starting point for the review is statistical monitoring of the amount of destroyed material in order to respond to deviations.»¹²⁹

Reviewing all deleted material is not feasible. Using statistical anomalies as leads for further in-depth controls appears to be an effective way to allocate available oversight resources. To make patterns in the destruction of data visible, audit trails of data deletion have to be available over longer time periods. Such a deviation could, for example, be an unusual peak in deletion activities at a certain point or on a certain day.

¹²⁸ Article L. 854-6. of French Law No. 2015-1556 on international surveillance (own translation).

¹²⁹ Swedish State Inspection for Defense Intelligence Operations (SIUN), «Årsredovisning för 2017,» February 22, 2018, Section 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf.



Norway: Independent review of compliance with deletion obligations

The EOS Committee addressed the challenges relating to deletion in its latest annual report and demanded that the service must «shortly find a solution to prevent the processing of information when the basis for processing has ceased to exist.»¹³⁰

Summary of main findings and reform agenda

Bulk data processing presents several complex governance challenges that will occupy oversight bodies for years to come. To put it mildly, there is plenty of room for oversight innovation. This chapter has introduced a few laudable practices that have recently been initiated in this regard. Clearly, gaps remain in many countries when it comes to issues such as the rules and procedures for data destruction and data storage for foreign intelligence.

When drafting intelligence legislation, lawmakers may not have been sufficiently mindful of the role and depth of multilateral intelligence cooperation. Services exchange raw and evaluated data in enormous quantities with their foreign partners and jointly feed various databases. Legal frameworks should account for the joint responsibility that governments have for joint databases, even if they are not hosted on their territory. Furthermore, as acknowledged by the Dutch government, there is a pressing need to ensure effective oversight over joint databases, possibly in the form of multilateral oversight.

Many oversight bodies seem to agree that much more work needs to be done to independently verify that the services honor their obligations to delete data. Drafting standards for what constitutes proper deletion would be one important step in this direction. Equally interesting, we found, were the different standards that nations use as regards the originator control principle. Here, further research is necessary. What we found thus far seems to indicate that oversight bodies can successfully be exempt from the «third-party rule» without creating negative ramifications for the security – or the degree – of the intelligence shared.

¹³⁰ EOS Committee, 2018, 20.

Phase 6: Analysis

A wide range of data use is relevant for this phase. There are, of course, overlaps between data processing and data analysis. Whereas data processing refers to data registration and other formal or technical data management practices, in this phase data becomes information that is relevant for political decision-making. Different automated data analysis methods serve different purposes and are governed by their own specific rules. Bulk datasets are used both to «establish links between known subjects of interest» as well as to «search for traces of activity by individuals who may not yet be known but who surface in the course of an investigation, or to identify patterns of activity that might indicate a threat.»¹³¹ For example, contact chaining is one common method used for target discovery: «Starting from a seed selector (perhaps obtained from HUMINT), by looking at the people whom the seed communicates with, and the people they in turn communicate with (the 2-out neighbourhood from the seed), the analyst begins a painstaking process of assembling information about a terrorist cell or network.»¹³²

Automated pattern analysis and anomaly detection increasingly rely on artificial intelligence (AI) methods such as machine learning and predictive analytics. «AI is expected to be particularly useful in intelligence due to the large datasets available for analysis.»¹³³ The risks and benefits generally associated with AI also challenge existing oversight methods and push legislators as well as oversight practitioners to creatively engage with AI as a dual-use technology. In intelligence, AI «is intended to automate the work of human analysts who currently spend hours sifting through data for actionable information. It may free them to make more efficient and timely decisions based on the data.»¹³⁴ Conversely, malicious use of AI creates new security threats that have to be mitigated.¹³⁵

131 UK Home Office, *Interception of Communications. Draft Code of Practice*. December 2017, 52, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668941/Draft_code_-_Interception_of_Communications.pdf.

132 Government Communications Headquarters (GCHQ), «HIMR Data Mining Research Problem Book,» September 20, 2011, 12, <https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html>.

133 Hoadley and Lucas, 2018, 13.

134 The Central Intelligence Agency (CIA) has 137 projects in development that leverage AI in some capacity, e.g.: incorporating computer vision and machine learning algorithms into intelligence collection cells that would comb through footage and automatically identify hostile activity for targeting; image recognition or labeling to predict future events such as terrorist attacks or civil unrest based on wide-ranging analysis of open source information; developing algorithms to accomplish multilingual speech recognition and translation in noisy environments; geo-locating images with no associated metadata; fusing 2-D images to create 3-D models; and tools to infer a building's function based on pattern of life analysis. See Hoadley and Lucas, 2018, 9.

135 Brundage et al., «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration,» February 2018, <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>.

Relevant aspects

What types of data use are permissible in a given legal framework, and are there specific rules for different forms of data use? For example, procedures for each type of use, specifying the circumstances under which that specific use is permitted.

There should also be independent oversight (internal and external) over bulk data analysis techniques, including rules and safeguards as concerns the use of AI. How is the level of privacy intrusion of specific data-analysis tools measured? And what kind of material is fed into query-focused databases?

How is the convergence of different databases/ data sources regulated? For example, may bulk communications data be matched with other stored data (such as data gathered via sensors or in hacking operations) or publicly available data? If so, does such enrichment of material happen automatically?

Good practice in legal safeguards



The Netherlands: Human-in-the-loop safeguard for automated data analysis

«The services are prohibited from promoting or taking any action against a person solely based on the results of automated data analysis. For example, if a data analysis algorithm indicates that a certain person intends to commit a terrorist attack, an intelligence service cannot act based on the outcome of this algorithm alone.»¹³⁶

The Dutch law also clarifies what possible conduct may fall under «automated data analysis.» It includes comparing datasets with each other in an automated manner, and searching on the basis of profiles in order to find specific patterns.¹³⁷ Embedding a human in the loop does not necessarily prevent analysis failures,¹³⁸ but being obliged to present other forms of proof before taking action may help to mitigate errors and false inferences.

¹³⁶ Eijkman, Eijk, and Schaik, 2018, 19.

¹³⁷ Dutch Act on the Intelligence and Security Services 2017, Article 60 (2).

¹³⁸ Cranor, «A Framework for Reasoning About the Human in the Loop,» 2008, <http://dl.acm.org/citation.cfm?id=1387649.1387650>.



**The Netherlands:
Legally required specialized training for analysts**

The Dutch law codifies a separation of access to data, demanding that only teams consisting of specialized personnel may access and analyze warranted datasets.¹³⁹

Similarly, in the United Kingdom, adequate arrangements must be in place that limit the number of persons to whom certain materials can be disclosed and restrict the copying of a given dataset to the minimum number necessary.¹⁴⁰

Good practice in oversight



**United Kingdom:
Automated internal compliance systems for data
analysis**

«There are computerised systems for checking and searching for potentially non-compliant uses of GCHQ's systems and premises. For example, when an authorised person selects a particular communication for examination, this person must demonstrate that the selection is necessary and proportionate; this process is subject to internal audit.»¹⁴¹

139 Explanatory memorandum concerning the amendment to the Intelligence and Security Services Act (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten), 2016, 48f., <https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten>.

140 Section 150 (1) (a) and (2) United Kingdom, Investigatory Powers Act 2016.

141 European Union Agency for Fundamental Rights, 2017, 59; see also: UK Home Office, «Interception of Communications. Draft Code of Practice,» February 2017, 6.14.



France: Ex-ante review of AI experiments and data analysis techniques

The French prime minister authorizes automated data analysis based on certain parameters after the CNCTR submitted «a non-binding opinion on both the automatic processing and the parameters. The oversight body is kept informed about every modification during the operation and has permanent, complete and direct access to this processing and the intelligence gathered.»¹⁴²

If the services want to reauthorize the automated analysis, the renewal request provided to the prime minister should contain an assessment of the relevance of prior automated analysis and the number of targets obtained. When the French intelligence service planned to use «algorithms» to identify terrorist threats based on «connection data» in 2016, the CNCTR submitted two opinions to the prime minister concerning both the architecture of the algorithms and the meaning of the connection data.¹⁴³

Summary of findings and reform agenda

Intelligence oversight has struggled to effectively control «black boxes» for quite some time now. The increasing importance of AI is the most recent development in this regard, with potentially far-reaching implications for how intelligence analysis is conducted. Even if AI use in surveillance is only at an experimental stage, the risk of abuse and errors may already have real-life impacts. How can one ensure that accountability exists for the errors that such algorithms might make?

Oversight has to make sure it keeps abreast of such developments, with promising practices such as the Dutch «Oversight 3.0» project or the introduction of practice warrants in New Zealand currently leading the way. Additional resources and control instruments are definitely needed for oversight bodies to ensure accountability of such AI-driven surveillance operations.

Phase 7: Review & Evaluation

Compliance with legal safeguards must be ensured through comprehensive and regular judicial oversight. Examining the effectiveness of data collection measures is equally important. Overseers need to know about this to assess the political value, the cost efficiency, and the need for the reauthorization of warrants. Identifying suitable metrics and methods for this remains a considerable challenge. For example, if data

¹⁴² European Union Agency for Fundamental Rights, 2017, 97.

¹⁴³ European Union Agency for Fundamental Rights, 2017, 45; CNCTR, «Premier rapport d'activité 2015/2016,» 2016, 39f., <https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf>.

from a certain program or collection stream never feeds into the production of intelligence reports, does this mean that the particular data collection is superfluous and a strain on the limited resources of the intelligence community? Or, in contrast, would this be tantamount to someone cancelling a fire insurance policy simply because, thus far, his or her house has not caught fire?

Relevant aspects

The scope of the review mandate of the oversight body is a core factor. Effective review presupposes that there are no gaps in the control mandate. Control remits should be defined functionally, covering all aspects of intelligence collection, as recommended by the Council of Europe.¹⁴⁴

Does the competent oversight body have the sufficient resources (staff, time, money, technical expertise) to conduct meaningful reviews? Intelligence law should also define the role for oversight in assessing the political relevance of finished intelligence operations and assign the duty to the executive branch to demonstrate the efficiency of its bulk surveillance measures, despite the ubiquitous presence of open source information.

Good practice in legal safeguards

Expanding the scope of oversight



Canada:
Holistic review of SIGINT practices across different agencies¹⁴⁵

Security and intelligence services tend to pursue their investigations in close cooperation with other agencies of the national security sector (police, military, customs and border security agencies). If one oversight body were to only review the activities of one specific intelligence agency, reviews would be incomplete because they would miss the role and contributions of other agencies.¹⁴⁶

Against this backdrop, the National Security and Intelligence Review Agency (NSIRA) – the new oversight body foreseen in Bill C-59 – would be an integrated body with jurisdiction over activities carried out by the Canadian Security Intelligence Service

¹⁴⁴ Council of Europe, «Democratic and Effective Oversight of National Security Services,» May 2015, 11, <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb>.

¹⁴⁵ National Security and Intelligence Review Agency Act (NSIRA Act, in planning with Bill C-59), Section 8.

¹⁴⁶ Parsons et al., 2017, 35.

(CSIS), the CSE, as well as national security or intelligence activities of other departments to the extent that these relate to national security or intelligence.

The new British IPCO is responsible for overseeing the use of investigatory powers, not only by intelligence agencies, but also by law enforcement, prisons, local authorities, and other government agencies. Focusing review capacities in one review body in such a way is useful because the police, for example, increasingly uses electronic methods for investigatory purposes, which are less visible and controllable for an authorizing judge than classic law enforcement methods. The increased opacity requires additional technical expertise to review digital surveillance measures.

In the United States, the Privacy and Civil Liberties Oversight Board (PCLOB) has jurisdiction over all counterterrorism programs operated by any federal agency, even those outside of the intelligence community (e.g., the Department of Homeland Security). Although limited to counterterrorism, this extends the oversight remit across a broader spectrum of security agencies.

Regular renewal

Sunset clauses, which are a common feature in US law, for instance, are an effective tool to trigger regular evaluations and adaptations of intelligence laws. The durations of such mandatory reauthorizations may vary.



The Netherlands: Verification of effectiveness before renewal of authorization

An obligation to submit the necessary information in writing when applying to renew the authorization of a certain surveillance measure can be the foundation for any effectiveness assessment. For instance, the accurate tagging of information helps to identify the interception stream that was at the source of a given intelligence product.

The Dutch MIVD entertains a small «Devil's Advocate» office that provides a contrary view on (selected) intelligence reports and internal procedures.



Norway:
Criminal liability for non-compliance with oversight requests

Any acting or former Norwegian intelligence service official has a duty to answer questions and comply with all requests made by the oversight body (e.g., give evidence to the committee), regardless of the level of classification. «Willful or grossly negligent infringements» with this obligation «shall render a person liable to fines or imprisonment for a term not exceeding one year, unless stricter penal provisions apply.»¹⁴⁷

Good practice in oversight

Early and systematic oversight involvement



United States:
No claim to deliberative privilege vis-à-vis the PCLOB

The Privacy and Civil Liberties Oversight Board is an independent agency within the executive branch.¹⁴⁸ Because it works from within the executive branch, the PCLOB has full access to information, in particular to materials in a deliberative stage. The government cannot claim deliberative privilege, for example attorney-client privilege, in relation to the PCLOB. It also holds the highest level of security clearance. This unfettered access is an important precondition to challenge the arguments that the government puts forward.

The official report on Section 215¹⁴⁹ is an example of the PCLOB's ability to successfully question and contradict the government's reasoning and claim of the effectiveness of certain measures.

147 Norwegian Act relating to oversight of intelligence, surveillance and security services (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrollloven)), February 3, 1995, Section 21, <https://lovdata.no/dokument/NL/lov/1995-02-03-7>; English translation available in: EOS Committee, 2018, 60, https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.

148 Although the PCLOB lacks budgetary independence, i.e., it cannot argue publicly to receive more money for its activities, the independence of the mandate stems from being able to contradict the White House and its departments and adopting a dissenting point of view.

149 PCLOB, «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court,» January 23, 2014, https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.



New Zealand: Obligatory quarterly self-reporting of incidents to the Inspector General

Since 2016, all operational compliance incidents have to be registered and reported to the Inspectors General, and not just, as was the case previously, inadvertent interceptions. Such incidents include, for example: «Interception of incorrect numbers, lines, data sets or equipment (e.g. a staff member accidentally entering an incorrect telephone number); numbers intercepted correctly but subsequently abandoned by the target and/or adopted by a non-target; organisations assisting NZSIS [New Zealand Security Intelligence Service] not being given the correct or most up to date documentation relating to the particular warrant; failure to adhere to internal policy or procedures.»¹⁵⁰

International cooperation of oversight bodies



Europe: Joint review and mutual learning sessions

Over the last couple of years, cooperation between the intelligence oversight bodies of Belgium, the Netherlands, Switzerland, Norway, and Denmark has been established.¹⁵¹ The participating bodies decided to conduct «a similar review investigation in all participating countries into the international cooperation between the various intelligence services with regard to the fight against foreign terrorist fighters.»¹⁵²

150 Office of the Inspector General of Intelligence and Security Cheryl Gwyn, «Annual Report for the Year Ended 30 June 2017,» December 1, 2017, 31f., <http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf>.

151 The participating bodies are (thus far): The Belgian Standing Intelligence Agencies Review Committee (Comiteri), the Dutch Intelligence and Security Services Review Committee (CTIVD), the Swiss Strategic Intelligence Service Supervision and delegations from Sweden (Commission on Security and Integrity Protection), Norway (Parliamentary Oversight Committee), and Denmark (Intelligence Oversight Board); Belgian Standing Intelligence Agencies Review Committee (Comiteri), «Rapport d'activité 2015,» September 16, 2016, 80f., http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.

152 Comiteri, «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations,» 2018, 82f., <http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I-Activity-Report-2016.PDF>; EOS Committee, 2018, 12.

The goal is to investigate the topic from different perspectives, but based on a comparable approach. Such a focus allows for gaining a more complete picture of international intelligence cooperation efforts that would otherwise be much harder for one oversight body to investigate alone. It also allows for a more substantial dialogue on the role and reform of control instruments so as to better meet actual oversight challenges.



Five Eyes: Five Eyes Intelligence Oversight and Review Council (FIORC)

This council was created in September 2016 and is made up of members from Australia, Canada, New Zealand, the United Kingdom, and the United States.¹⁵³ This forum is supposed to foster closer linkages within the Five Eyes review and oversight community, allow for the exchange of views on subjects of mutual interest and concern, and provide room to compare oversight methodologies and explore areas where cooperation on reviews and the sharing of results is permitted and fruitful.¹⁵⁴

Oversight advisory teams

The CTIVD set up a «knowledge circle» in December 2014 that consists of subject matter experts and scientists and advises the oversight body on relevant developments. Some of these experts also consult the CTIVD regarding the selection of compliance investigations.¹⁵⁵ IPCO has created a technology advisory panel (TAP) of scientific

153 The participating oversight bodies are: the Office of the Inspector General of Intelligence and Security of Australia; the Office of the Communications Security Establishment Commissioner and the Security and Intelligence Review Committee of Canada; the Commissioner of Security Warrants and the Office of the Inspector General of Intelligence and Security of New Zealand; the Office of the Investigatory Powers Commissioner of the United Kingdom; and the Office of the Intelligence Community Inspector General of the United States; Office of the Inspector General National Security Agency, «Semiannual Report to Congress. 1 October 2017 to 31 March 2018,» 2018, https://www.dni.gov/files/documents/FOIA/OCT2017-MAR-2018_SAR_FINAL.PDF; and also Barker, Petrie, Dawson, Godec, Purser, and Porteous, «Oversight of Intelligence Agencies: A Comparison of the «Five Eyes» Nations,» 2017, 9, <http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf>.

154 The first FIORC conference – in which representatives of review bodies from all Five Eyes countries participated – took place in Ottawa, Canada, in October 2017, see: Security Intelligence Review Committee, «SIRC Annual Report 2017–2018: Building For Tomorrow: The Future Of Security Intelligence Accountability In Canada,» 2018, <http://www.sirc-csars.gc.ca/anrran/2017-2018/index-eng.html>.

155 CTIVD, «Kenniskring en tegenspraak CTIVD,» September 20, 2017, <https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak>.

experts led by the statistician Bernard Silverman.¹⁵⁶ The Inspector General of intelligence and security of New Zealand also appointed a two-person statutory advisory panel.¹⁵⁷

Summary of main findings and reform agenda

With a view to the highly integrated modern security operations involving many different agencies using similar tools, some lawmakers have rightly extended the remit of oversight bodies to agencies other than intelligence services. In so doing, these oversight bodies are becoming more visible, which, in turn, may help to attract technical expertise. Another good practice that we discussed is the increasing trend toward more regular, substantive exchanges among oversight bodies. In Europe, other countries, such as France and Germany, should consider joining existing platforms for oversight cooperation.

This chapter also discussed the need to further research the efficacy of bulk surveillance measures. Governments ought to demonstrate the continued added value of SIGINT operations at a time when their intelligence services can also resort to a trove of available open source information. However, are there better criteria and sources upon which governments' cases can be assessed?

Phase 8: Reporting

After a SIGINT collection cycle has been completed, both government and oversight bodies need to be transparent and provide adequate information about both the surveillance activities undertaken by the state and their specific oversight activities thereon. To enhance public trust, the intelligence services should proactively declassify key legal documents of public interest.¹⁵⁸ Such releases have, for example, allowed

156 IPCO, «A Message from the Commissioner By Sir Adrian Fulford,» May 17, 2018, <https://www.ipco.org.uk/Default.aspx?mid=16.1>; Investigatory Powers Commissioner's Office, Twitter Post, December 15, 2017, <https://twitter.com/IPCOOffice/status/941722822405013506>.

157 Inspector General of Intelligence and Security of New Zealand, «About: The Intelligence and Security Agencies,» <http://www.igis.govt.nz/about/>.

158 The US intelligence community, for example, has released official documentation of intelligence activities and procedures, such as declassified FISC opinions, quarterly reports, and semi-annual assessments. Many of these documents can be found at <http://www.icontherecord.tumblr.com>. A guide to released documents is available here: https://www.dni.gov/files/CLPT/documents/Guide_to_Posted_Documents.pdf. A searchable database of all documents is available at: <https://www.intel.gov/ic-on-the-record-database>.

the creation of rare public and quite comprehensive accounts of different types and patterns of compliance violations over the duration of the Section 702 program.¹⁵⁹

Although full transparency of oversight activities may not be possible due to secrecy requirements, the regular reporting by oversight bodies is a crucial means for public trust and accountability. For this, it ought to be as comprehensive and timely as possible.

Relevant aspects

What rules are in place regarding mandatory, periodical public reporting on surveillance measures and its democratic control? Information on oversight methods and capacities, especially with a view to bulk surveillance, should be provided to the greatest extent possible. Reports should draw a holistic picture of all intelligence activities. What contextual material and statistical information is provided to the public? What outreach activities are pursued, and how does the oversight body communicate with public?

Good practice in legal safeguards

Options for declassification

By default, all matters discussed by the German parliamentary oversight committee (PKGr) are classified. Yet, the committee can make certain procedures public if two-thirds of the members support this step. Then, individual members of the PKGr can publish a dissenting opinion («*Sondervotum*») of the specific case at hand.¹⁶⁰ This provision, which explicitly allows for deviations from the norm of classification and makes particular cases or activities public, can be a useful tool for oversight. In the United States, too, Executive Order 13526 on classified national security information explicitly provides for public interest declassification, stating that, «[i]n some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified.»¹⁶¹

159 Robyn Green has compiled highly informative documentation that informs the public about how unintentional violations may threaten the privacy of protected communications over a longer period of time «with significant and prolonged impact.» For a summary of compliance reports under Section 702 of FISA, see: Greene, «A History of FISA Section 702 Compliance Violations,» September 28, 2017, <https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/>.

160 Section 10 (2) German Parliamentary Control Panel Act (Parlamentarisches Kontrollgremiumgesetz), July 29, 2009.

161 U.S. Government Publishing Office, Executive Order 13526, 2009, Section 3.1(d), <https://www.gpo.gov/fdsys/pkg/CFR-2010-title3-vol1/pdf/CFR-2010-title3-vol1-eo13526.pdf>.

Obligation to inform about errors

The United Kingdom's IP Act introduced an obligation for IPCO to inform a person of any relevant error relating to that person when it is in the public interest for the person to be informed of the error (Section 231 (1) IP Act). This responsibility to report errors refers to specific persons, which suggests that mostly targeted surveillance practices are covered by this provision. But it would also be conceivable to inform people about errors that have occurred in bulk surveillance measures. The provision is significantly curtailed in its area of application. The IP Act also includes a provision stating that a breach of a person's rights under the Human Rights Act 1998 is not sufficient to justify the reporting of an error (Section 231 (3) IP Act). If human rights breaches are not enough to trigger reporting, then it remains to be seen what kind of errors will be reported.

Good practice in oversight

Advancing transparency on oversight methods



Norway: Reporting on non-conformities with selectors

The EOS has recently reported to the public that «non-conformity in the service's technical information collection that resulted in the unintentional collection of information from means of communication (hereinafter referred to as selectors) that were in reality Norwegian.»¹⁶²

Albeit without much further substantiation in the actual report, it is notable that an oversight body has publicly referred to such irregularities.



United States: PCLOB pushing for declassification

In the PCLOB's report on Section 702,¹⁶³ the oversight body was able to obtain the declassification of a large segment of information about the program.¹⁶⁴

¹⁶² EOS Committee, 2018, 43f.

¹⁶³ PCLOB, 2014.

¹⁶⁴ Federation of American Scientists, «Secrecy News 07/28/14,» July 28, 2014, <https://fas.org/sgp/news/secrecy/2014/07/072814.html>.

This was a new phenomenon, given that requests for declassification usually either come from above – the president – or from the public. This, though, was a case of a «lateral» request by an independent federal oversight entity.

Many oversight bodies have begun to build up significant resources for communicating with the public, for example via informative public websites and Twitter accounts. More important than this, however, are advanced transparency standards and accurate and timely oversight reports. In this regard, it is commendable that the oversight bodies of Belgium, Denmark, the Netherlands, and Norway publish their annual reports now also in English. In so doing, they provide a valuable resource for comparative work.

Institutional support for whistleblowers



United States: Expressed commitment to whistleblower protection

In July 2018, the NSA's Inspector General declassified a version of its semi-annual report, which contains its audits and investigations from October 2017 to March 2018, to Congress. The report states: «We recognize that agencies like the NSA are simply too big, and their operations too diverse, for an OIG [Office of the Inspector General] to know what is happening throughout the organization if people do not come forward when they see something they believe is wrong, and they cannot be expected to do that if they fear retaliation for doing so. The role of whistleblowers in furthering effective oversight is particularly important at an agency like the NSA, where so much of the work must be performed outside the public eye to be effective.»¹⁶⁵

At the same time the Inspector General announced the creation of a whistleblower protection page on the OIG's classified website and the establishment of a whistleblower coordinator position.¹⁶⁶

¹⁶⁵ Office of the Inspector General National Security Agency, 2018, iii.

¹⁶⁶ Clark, «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report,» July 27, 2018, <https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/>; further information about intelligence whistleblower protection in the United States is available at <https://fas.org/sgp/crs/intel/R43765.pdf>.

Summary of main findings and reform agenda

Intelligence governance will benefit from greater public knowledge of oversight activities as well as increased insights on how surveillance is conducted. Our comparative review of national oversight systems has shown that there is room for advanced transparency reporting. This includes both more information on the use of bulk powers in actual practice and the dynamics of oversight (e.g., how different control instruments have been used). Future comparative studies on reporting standards, for example on available statistics regarding the authorization process (i.e., total number of approved and rejected applications, number of authorizations with conditions, etc.) are in order. They may illustrate how oversight bodies can regain public trust. Systematic reporting on errors in bulk surveillance should also be explored.

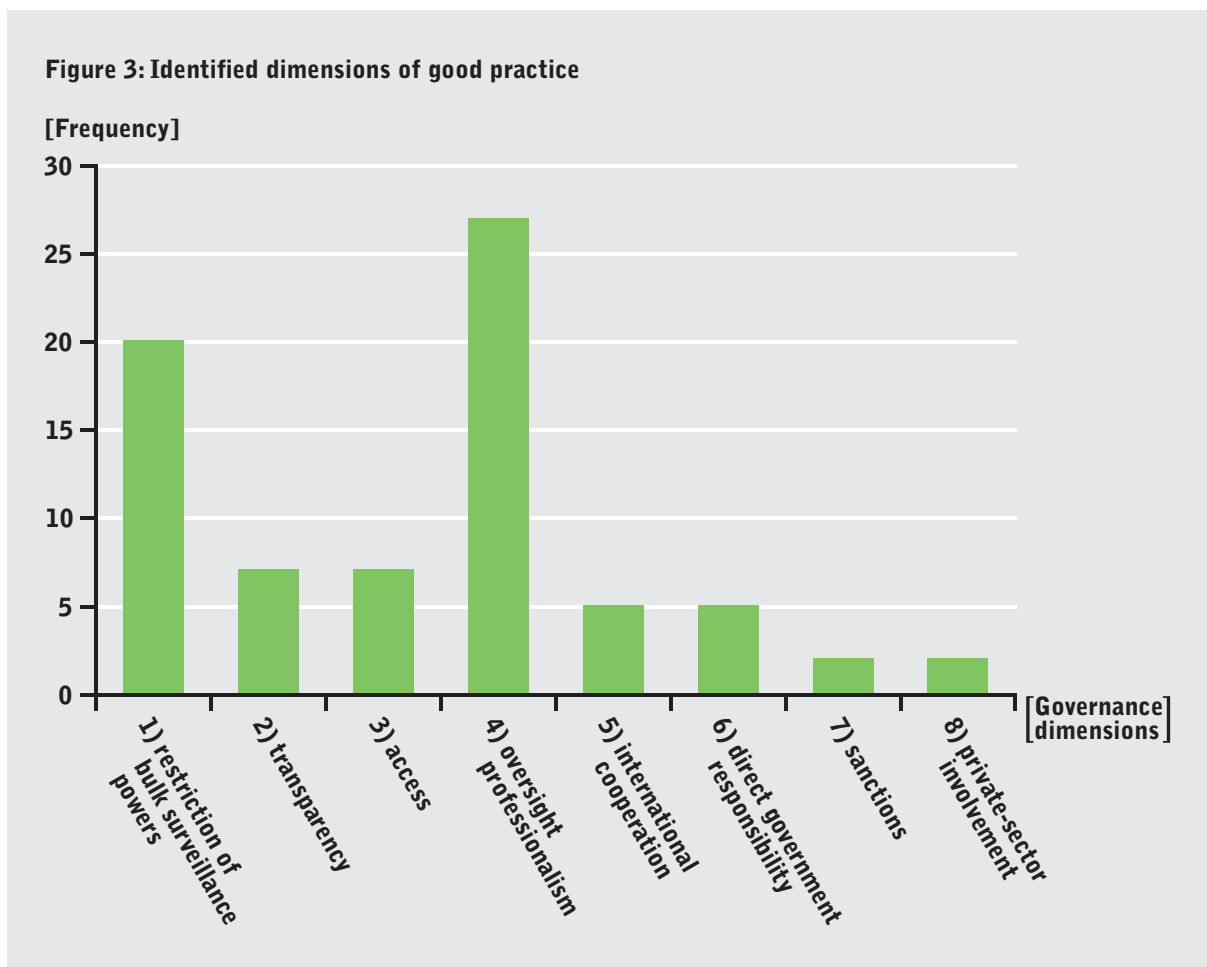
While effective whistleblower protections remain crucial, not least in SIGINT agencies, developing more structured accounts of both successes and failures could also support public trust in the services.

In targeted surveillance systems, persons whose private communications have been intercepted ought to be informed about this so as to provide them a chance for effective remedy. Although this may not be practicable in non-targeted foreign surveillance regimes, there might be options to introduce an obligation to inform EU citizens when their data is swept up in foreign communications data collection by a fellow European country.

IV. Discussion

Our review of legal safeguards and oversight innovations in different stages of the bulk surveillance governance process features 64 good practices. These range from ending discrimination based on citizenship to more specific authorization regimes and additional safeguards for international intelligence cooperation. Each pertains to different aspects of surveillance governance. More specifically, this includes:

- restriction of bulk surveillance powers
- transparency
- access
- oversight professionalism
- international cooperation
- direct government responsibility
- sanctions
- private-sector involvement



These categories are not mutually exclusive. For example, we believe that the requirement of an adequacy review of foreign cooperation partners pertains to both «international cooperation» and «oversight professionalism.» A full list of good practices and their assigned categories can be found in the Annex.

What can we learn from the dispersion of practices in the different categories? The table above shows that a majority of good practices can be tied to restrictions and the advancement of oversight professionalism. To us, this is a clear sign that lawmakers sought to overcome a lack of legitimacy in these two areas. Yet, our findings also illustrate that lawmakers tended to shy away from addressing other areas in their recent reforms – notably the direct government responsibility for the steering of surveillance measures. More concretely, we only identified five examples that pertain to this dimension. History is replete with examples in which the executive decided on the course of surveillance activities with hidden motives that may have led to malfeasances. It is important, therefore, that clear responsibilities for the important role of the executive are being established. Likewise, in the area of sanctions, which includes criminal liability for the abuse of surveillance powers, we identified only two examples. Further options to effectively sanction non-compliance on an organizational as well as individual level would strengthen the assertiveness of oversight bodies.

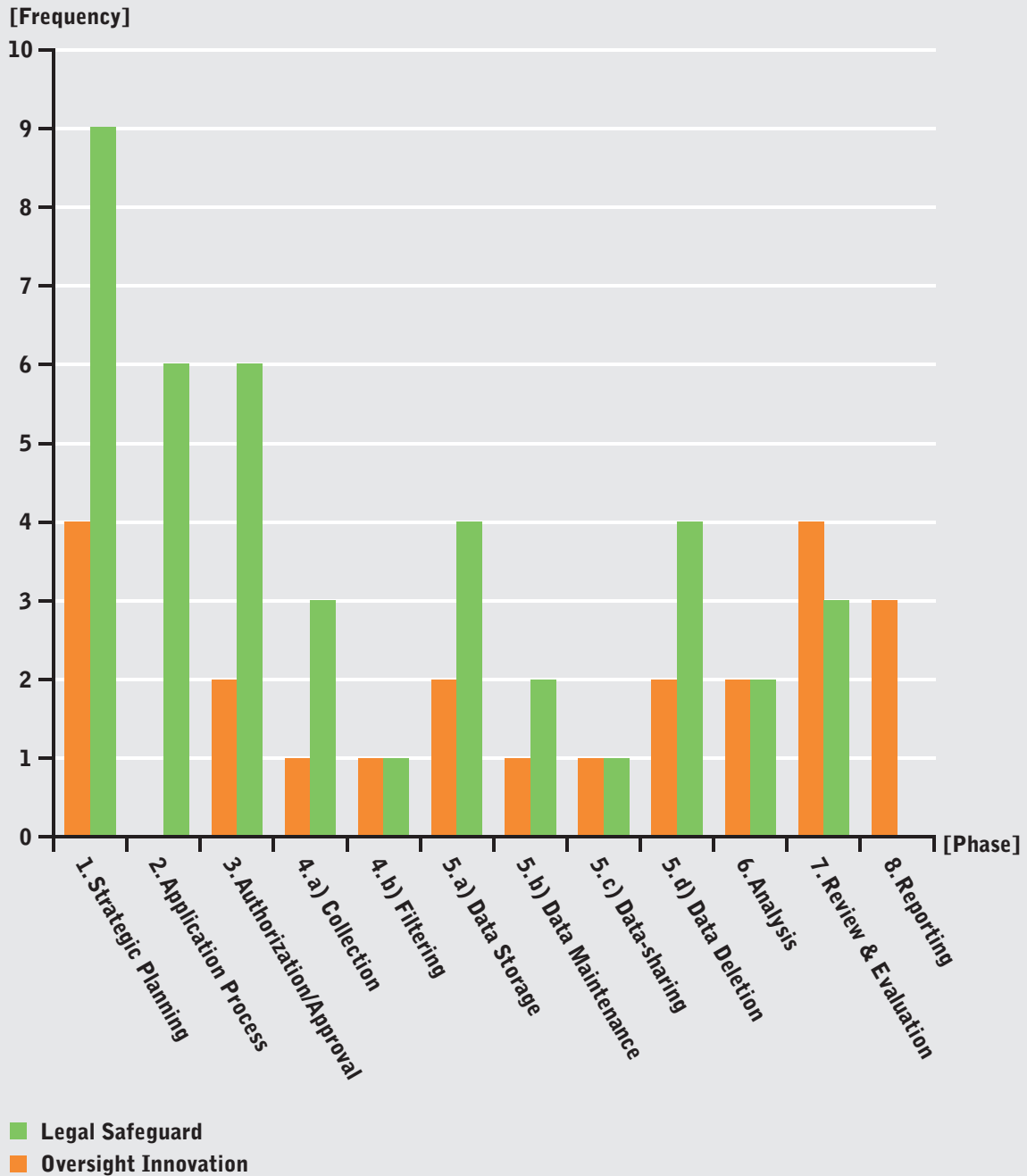
We identified seven laudable examples of advanced transparency reporting that we think merit further attention. For instance, declassifying new legal interpretations in authorization decisions is one such practice. However, here, too, there remains room for further improvements. Providing (better) statistics on the actual extent of surveillance measures (types of warrants granted, decisions on warrants and notifications, etc) and more detailed information on the auditing methods used should also figure into public reports. More transparency on the actual implementation of bulk surveillance measures will increase public trust.

Interestingly, very few reforms included rules that clearly define who is in charge of extracting the data and how providers can challenge government requests for access to data. Without private-sector involvement, most bulk collection activities would not be feasible. Provider intermediation can be an important safeguard against executive overreach, and therefore more systematic oversight-carrier dialogues should be established.

Looking at the distribution of good practice examples across the eight functional phases of our SIGINT governance analysis scheme (see figure 4), we can denote a general preference by lawmakers for legal safeguards as opposed to oversight innovation. Presumably, one reason for this could be that changes of actual oversight dynamics are labor-intensive and take time to implement. But they are equally important. Even the best laws can only go so far. Surveillance governance in democratic societies also requires the effective use of control instruments. It is in this area that oversight bodies need to work harder to keep up with technological change. Parliaments across the world are well-advised to invest not just in the latest surveillance technology but also in auditing tools for modern oversight bodies.

New tools such as technical interfaces for direct database access are major innovations in oversight practices. Unhindered and complete access to all relevant

Figure 4: Identified good practices per phase



intelligence information is extremely important for effective oversight. In this regard, though, most reform efforts remain underwhelming, especially in the area of intelligence cooperation. As multilateral cooperation among intelligence and security agencies is fast evolving, national oversight bodies need to catch up. Some oversight bodies have already begun to address this enormous task. In so doing, they will not only benefit from mutual learning. In the future, they may also find creative solutions to fix some of the current accountability deficits that international intelligence cooperation entails. As currently proposed by the Dutch CTIVD, one might also want to

start thinking creatively about the institutional design of multilateral oversight on the CTG database.

Some intelligence oversight bodies have now developed an independent voice that pushes back more often against regulatory capture and reaffirms their independence. Some have become increasingly mindful of the numerous risks that ever closer intelligence cooperation entails. They are now more influential than before due to public awareness and regulatory reform, and they tend to be better equipped to fulfill their critical democratic mission in the «golden age of surveillance.»

V. Conclusion

Reforms of bulk surveillance post-Snowden have been limited and underwhelming in the eyes of many observers. Yet, the debate about rights-based and democratically controlled surveillance governance is far from over. Although courts such as the European Court of Human Rights tend to grant a broad leeway to national governments to implement bulk surveillance, they also insist on adequate safeguards. What this means in practice, though, will not be decided by the courts. Rather, it involves the hard work of taking the lessons about ineffective oversight and applying better practices through the slow and steady channels of democratic institutions. This may not be the Snowden legacy that some expected. Yet, it is the difficult and necessary work of democratic governance.

We hope that this compendium can contribute to this effort, and we welcome feedback and any additional ideas on the good practices we selected. There are individual aspects in each intelligence reform that stand out by comparative review and merit further discussion. While better intelligence governance does not simply equal the sum of all best practices, we believe that adopting the presented legal safeguards and oversight practices in other countries will raise the bar for democratic standards in intelligence governance.

Good oversight is also good security. Citizens rightfully expect accountable, necessary, and effective modes of governing intelligence in the digital age. This must include legal safeguards and oversight practice, as both aspects play a crucial role in providing security for all. This is because effective oversight, in contrast, pushes governments to be as effective as possible in allocating their resources and selecting their targets. Implementing clear intelligence priorities (phase 1) and specific and robust authorizing mechanisms (phases 2 and 3 of our scheme) are key to accomplish that. Similarly, the collection, processing, and analysis (phases 4, 5 and 6, respectively) of communications are equally significant stages of the intelligence process. There are many potential forms of abuse that can be tied to these moments, which is why both intelligence legislation and oversight practice need to apply beyond the initial authorization moment. Moreover, with a view to institutional learning and public confidence in intelligence governance, the professional review and enhanced public reporting on modern bulk surveillance activities (phases 7 and 8) are fundamentally important. In the Appendix, we list 64 promising examples from all eight phases of the bulk surveillance process.

Naturally, the quest for better democratic control and governance of bulk surveillance is ongoing. Authorization bodies, courts, parliamentary committees, internal compliance departments, executive control and independent review agencies all play a vital role in maintaining and promoting public trust in intelligence activities. But the

burden to provide sufficient transparency and to demonstrate legal compliance rests also with the intelligence services themselves. As some examples in this compendium have shown, they can work harder in some countries than in others to release sufficient information for public scrutiny.

We hope that by presenting laudable aspects in either national intelligence laws or reformed oversight practices, we have contributed to the necessary debate on how to trim and effectively oversee bulk surveillance powers. Positive change, though, may not come from the identification of good practices alone. They need to be debated and become part of a broader national reform agenda. Yet, lawmakers who are now seriously discussing these practices with civil society organizations and the executive may eventually decide to adopt some of these good practices. We stand ready to offer our advice and encourage them to collectively up the ante for the protection and promotion of our security and our privacy.

VI. Annex

List of Workshop Participants

Many people offered their advice and expert knowledge to us. We received constructive feedback and additional information in a series of interviews and during two expert workshops in Berlin.

We are very grateful for the help we received and for the interest and time that a wide range of different stakeholders have invested in our project. The views and opinions expressed in this document are our own.

The following experts provided valuable input on earlier versions of this report during a workshop on June 14 and 15, 2018, in Berlin.

- Sharon Bradford Franklin, Director of Surveillance and Cybersecurity Policy, New America's Open Technology Institute
- Iain Cameron, Professor at Department of Law, Uppsala University and Swedish Member of the Venice Commission, Council of Europe
- Joan Feigenbaum, Grace Murray Hopper Professor of Computer Science, Yale University
- Giles Herdale, Policy Advisor and Co-chair, Independent Digital Ethics Panel for Policing
- Eric King, Visiting Lecturer at Queen Mary University of London
- Ronja Kniep, Research Fellow, Berlin Social Science Center (WZB)
- Klaus Landefeld, Director Infrastructure & Networks at eco - Association of the Internet Industry and Supervisory Board member of DE-CIX International
- Greg Nojeim, Senior Counsel and Director, Freedom, Security and Technology Project, Center for Democracy & Technology
- Jörg Pohle, PostDoc, Alexander von Humboldt Institute for Internet and Society (HIIG)
- Volker Roth, Professor of Computer Science, Freie Universität Berlin
- Graham Smith, Partner, Bird & Bird LLP
- Eric Töpfer, Senior Researcher, German Institute for Human Rights
- Nico van Eijk, Professor of Media and Telecommunications Law and Director of IViR, University of Amsterdam
- Njord Wegge, Senior Research Fellow, Norwegian Institute of International Affairs (NUPI)

The following oversight officials provided valuable input on an earlier version of this report during a workshop on May 14, 2018, in Berlin. Not all participants agreed to be named, hence this is not a comprehensive list of all workshop participants.










- Frank Brasz, Deputy General Secretary, CTIVD, the Netherlands
- Wouter de Ridder, Standing Intelligence Agencies Review Committee, Belgium
- Arild Færaas, EOS Committee's secretariat, Norway
- Emil Bock Greve, Intelligence Oversight Board, Denmark
- Bertold Huber, Deputy Chair, G10-Kommission, Germany
- Rune Odgaard Jensen, Intelligence Oversight Board, Denmark
- Jantine Kervel-de Goei, General Secretary, CTIVD, the Netherlands
- Charles Miller, Investigatory Powers Commissioner's Office, United Kingdom
- Dominic Volken, Deputy Head, Independent Oversight Authority for Intelligence Activities, Switzerland











List of Interviewed Experts












Not all interviewees agreed to be named. Please note, therefore, that this is not a comprehensive list of all interviews conducted.










- Marie-Laure Basilien-Gainche, Professor of Law, University Jean Moulin Lyon 3, Honorary member of the Institut Universitaire de France
- Susan Decker, Senior Research Advisor, Legal Counsel, Security Intelligence Review Committee, Canada
- Craig Forcece, Professor of Law, University of Ottawa
- Lex Gill, Research Fellow, Citizen Lab, University of Toronto
- Elspeth Guild, Professor of Law, Queen Mary University of London
- Lotte Houwing, File Coordinator, Public Interest Litigation Project
- Peter Koop, Electrospace.net
- Sébastien-Yves Laurent, Professor at the University of Bordeaux – Faculty of Law and Political Science
- Evan Light, Assistant Professor, Communications Program, Glendon College, York University
- Simon McKay, Barrister in Civil Liberties and Human Rights Law
- Brenda McPhail, Director, Privacy, Technology & Surveillance Project, Canadian Civil Liberties Association
- David Medine, Former chair of the US Privacy and Civil Liberties Oversight Board
- Mario Oetheimer, Head of Sector Information Society, Privacy and Data Protection, Freedoms and Justice Department, European Union Agency for Fundamental Rights
- Jonathan Obar, Assistant Professor, Department of Communication Studies, York University
- Félix Tréguer, Post-Doc Researcher, Sciences Po Paris









List of Good Practices












#	Example Practice	Phase	Dimension	Country*	Category
1	No discrimination between foreign and domestic data in intelligence collection	Strategic Planning	Legal Safe-guard	NL	Restriction 
2	Restricting the use of bulk powers: PPD 28 prioritizes targeted collection over bulk	Strategic Planning	Legal Safe-guard	USA	Restriction 
3	Transparency on actors involved in formulating the National Intelligence Priority Framework	Strategic Planning	Legal Safe-guard	D	Transparency 
4	Annual review of any intelligence priorities by heads of departments	Strategic Planning	Legal Safe-guard	USA	Government responsibility 
5	Adequacy Review of Foreign Cooperation Partners	Strategic Planning	Legal Safe-guard	NL	International cooperation  Professionalism 
6	Written agreements on the aims, the nature, and the duration of international cooperation must be approved by Chancellery	Strategic Planning	Legal Safe-guard	D	International cooperation  Government responsibility 
7	Prohibition of economic espionage	Strategic Planning	Legal Safe-guard	D	Restriction 










#	Example Practice	Phase	Dimension	Country*	Category
8	Prohibition of discrimination against protected classes through bulk collection	Strategic Planning	Legal Safe-guard	USA	Restriction 
9	Criminal liability for willful real-time surveillance conducted for an unlawful purpose	Strategic Planning	Legal Safe-guard	USA	Sanction 
10	Parliamentary committee must be informed regularly about operational purposes	Strategic Planning	Oversight	UK	Transparency 
11	Full access to documentation of cooperation agreements	Strategic Planning	Oversight	CA	International cooperation  Access 
12	CTIVD can review the weighting notes	Strategic Planning	Oversight	NL	International cooperation  Access 
13	Parliamentary oversight committee must be informed about all MoU	Strategic Planning	Oversight	D	International cooperation  Access 
14	Restriction on the number of agencies allowed to use the data	Warrantry	Legal Safegu-ards	F	Restriction 






#	Example Practice	Phase	Dimension	Country*	Category
15	Type of automated processing accounted for in warrants	Warrantry	Legal Safeguards	F	Professionalism 
16	Specific requirements to make the «intelligence case» in a bulk SIGINT application	Warrantry	Legal Safeguards	CA	Restriction  Professionalism 
17	Listing of search terms in untargeted communications data surveillance warrants	Warrantry	Legal Safeguards	D	Restriction  Professionalism 
18	Predefining specific fiber optic cables to be intercepted	Warrantry	Legal Safeguards	NL	Restriction 
19	Direct ministerial responsibility for the activation of certain search terms	Warrantry	Legal Safeguards	D	Government responsibility 
20	Option to approve a warrant with conditions	Authorization/ Approval	Legal Safeguards	CA	Professionalism 
21	Mandatory public report by authorization body	Authorization/ Approval	Legal Safeguards	NL	Transparency 
22	Option to request publication of a Foreign Intelligence Surveillance Court decision or opinion	Authorization/ Approval	Legal Safeguards	USA	Transparency 
23	Required declassification review for new legal interpretations	Authorization/ Approval	Legal Safeguards	USA	Transparency 

#	Example Practice	Phase	Dimension	Country*	Category
24	Option to request external legal opinion in authorization procedures	Authorization/ Approval	Legal Safeguards	USA	Professionalism 
25	Quotas for specific data collection methods	Authorization/ Approval	Legal Safeguards	F	Restriction 
26	IPCO Advisory Notice	Authorization/ Approval	Oversight	UK	Professionalism 
27	Open oversight – civil society dialogue on proportionality standards for the review of bulk powers	Authorization/ Approval	Oversight	UK	Professionalism 
28	Specialized executive body serves as data collection center	Collection	Legal Safeguards	F	Government responsibility 
29	Options for providers to object to government requests for data	Collection	Legal Safeguards	USA	Private sector involvement 
30	ISPs responsible for installing splitters and selector lists	Collection	Legal Safeguards	USA	Private sector involvement 
31	Installation of interfaces	Collection	Oversight	F NL NOR CH	Professionalism 
32	All raw data (including content and metadata) that gets filtered out will be impossible to retrieve by the intelligence services	Filtering	Legal Safeguards	NL	Restriction 

#	Example Practice	Phase	Dimension	Country*	Category
33	The FISC reviews compliance audits performed by the intelligence community	Filtering	Oversight	USA	Access 
34	No distinction between metadata and content	Data Storage	Legal Safeguards	NL	Restriction 
35	Obligation to keep a file classification scheme	Data Storage	Legal Safeguards	D	Professionalism 
36	Appropriations clause for joint databases	Data Storage	Legal Safeguards	D	Professionalism 
37	Equalized SIGINT retention rules for US persons and non-US persons	Data Storage	Legal Safeguards	USA	Restriction 
38	Oversight 3.0 project on future challenges run by oversight body	Data Storage	Oversight	NL	Professionalism 
39	Joint inspections of judicial oversight body and DPA	Data Storage	Oversight	D	Professionalism 
40	Duty of care and relevance as regards data processing, including the use of algorithms	Data Maintenance	Legal Safeguards	NL	Government responsibility 
41	Mandatory tagging of all bulk SIGINT data	Data Maintenance	Legal Safeguards	D	Restriction  Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
42	Mandatory ex-ante opinion by oversight body on the data-tagging process	Data Maintenance	Oversight	F	Restriction  Professionalism 
43	By default full access to all information for oversight body	Data-sharing	Legal Safeguards	NOR	Access 
44	Random sample checks on automatic transfers of personal data to foreign intelligence services	Data-sharing	Oversight	D	Professionalism 
45	Obligation to immediately delete data tied to rejected applications	Data Deletion	Legal Safeguard	D	Restriction 
46	Obligation to destroy data from bulk collection that is deemed irrelevant	Data Deletion	Legal Safeguard	NL	Restriction 
47	Obligation to record data deletions	Data Deletion	Legal Safeguard	F	Professionalism  Restriction 
48	Obligation to delete health data in foreign datasets	Data Deletion	Legal Safeguard	CA	Restriction 
49	Running statistical pattern analyses on the amount of deleted material	Data Deletion	Oversight	SWE	Professionalism 
50	Independent review of compliance with deletion obligations	Data Deletion	Oversight	NOR	Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
51	Human-in-the-loop safeguard for automated data analysis	Analysis	Legal Safeguards	NL	Professionalism 
52	Legally required specialized training for analysts	Analysis	Legal Safeguards	NL	Professionalism 
53	Automated internal compliance systems for data analysis	Analysis	Oversight	UK	Professionalism Restriction 
54	Ex-ante review of AI experiments and data analysis techniques	Analysis	Oversight	F	Professionalism 
55	Holistic review of SIGINT practices across different agencies	Review & Evaluation	Legal Safeguards	CA	Access Professionalism 
56	Verification of effectiveness before renewal of authorization	Review & Evaluation	Legal Safeguards	NL	Restriction 
57	Criminal liability for non-compliance with oversight requests	Review & Evaluation	Legal Safeguards	NOR	Sanction 
58	No claim to deliberative privilege vis-à-vis the PCLOB	Review & Evaluation	Oversight	USA	Access 
59	Obligatory quarterly self-reporting of incidents to the Inspector General	Review & Evaluation	Oversight	NZ	Professionalism 

#	Example Practice	Phase	Dimension	Country*	Category
60	Joint review and mutual learning sessions	Review & Evaluation	Oversight	BE NL CH NOR DK	Professionalism 
61	Five Eyes Intelligence Oversight and Review Council	Review & Evaluation	Oversight	AUS CA NZ UK USA	Professionalism 
62	Reporting on non-conformities with selectors	Reporting	Oversight	NOR	Transparency 
63	PCLOB pushing for declassification	Reporting	Oversight	USA	Transparency 
64	Expressed commitment to whistleblower protection	Reporting	Oversight	USA	Transparency 
<p>* BE = Belgium; CA = Canada; CH = Switzerland; D = Germany; DK = Denmark; F = France; NL = the Netherlands; NOR = Norway; NZ = New Zealand; SWE = Sweden; UK = United Kingdom; USA = United States</p>					

List of Abbreviations

Abbreviation	Name	English translation
AB-ND	Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten	Independent supervisory authority on intelligence activities (Switzerland)
AI	Artificial Intelligence	
AIVD	Algemene Inlichtingen en Veiligheidsdienst	General Intelligence and Security Service (the Netherlands)
BND	Bundesnachrichtendienst	Federal Intelligence Service (Germany)
BND Act	Gesetz über den Bundesnachrichtendienst	Act on the Federal Intelligence Service (Germany)
BVerfG	Bundesverfassungsgericht	The Federal Constitutional Court (Germany)
BVerfSch Act	Bundesverfassungsschutzgesetz	Act on the Federal Office for the Protection of the Constitution (Germany)
CJEU	Court of Justice of the European Union	
CNCTR	Commission nationale de contrôle des techniques de renseignement	National Commission of Control of the Intelligence Techniques (France)
COMINT	Communication Intelligence	
CSE	Communications Security Establishment (Canada)	
CSIS	Canadian Security Intelligence Service	
CTG	Counter Terrorism Group	
CTIVD	De Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten	Oversight Committee for the Intelligence and Security Services (the Netherlands)
DNI	Director of National intelligence (USA)	
DPA	Data Protection Authority	
ECtHR	European Court of Human Rights	
EOS	Stortingets kontrollutvalg for etterrettings-, overvåkings- og sikkerhetstjeneste	Parliamentary Intelligence Oversight Committee (Norway)
FIORC	Five Eyes Intelligence Oversight and Review Council	
FISA	Foreign Intelligence Surveillance Act (USA)	

Abbreviation	Name	English translation
FISC	United States Foreign Intelligence Surveillance Court (USA)	
G10 Act	Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz)	Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (Germany)
G10 Commission	G10-Kommission	Quasi-judicial authorization body of the German federal parliament (Germany)
GCHQ	Government Communications Headquarters (UK)	
GIC	Groupement interministériel de contrôle	Inter-ministerial control group under the purview of the prime minister (France)
HUMINT	Human Intelligence	
ISP	Internet Service Provider	
IP Act	Investigatory Power Act (UK)	
IPCO	Investigatory Powers Commissioner's Office (UK)	
MIVD	Militaire Inlichtingen- en Veiligheidsdienst	Military Intelligence and Security Service (The Netherlands)
MoU	Memorandum of Understanding	
ND Act	Nachrichtendienstgesetz	Federal Intelligence Service Act (Switzerland)
NDB	Nachrichtendienst des Bundes	Federal Intelligence Service (Switzerland)
NSA	National Security Agency (USA)	
NSIRA	National Security and Intelligence Review Agency (Canada)	
NZSIS	New Zealand Security Intelligence Service	
PCLOB	The Privacy and Civil Liberties Oversight Board (USA)	
PKGr	Parlamentarisches Kontrollgremium	Parliamentary Control Panel (Germany)
PPD 28	Presidential Policy Directive 28 on Signals Intelligence Activities (USA)	

Abbreviation	Name	English translation
SIGINT	Signals Intelligence	
SIUN	Statens inspektion för försvarsunderrättelseverksamheten	The State Inspection for Defense Intelligence Operations (Sweden)
TAP	Technology Advisory Panel (UK)	
TIB	Toetsingscommissie Inzet Bevoegdheden	Review Board for the Use of Powers (The Netherlands)

Bibliography

- Administrative Office of the United States Courts. 2018. «Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2017.» April 25, 2018. http://www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2017.pdf.
- Anderson, David. 2015. «A Question of Trust: Report of the Investigatory Powers Review.» London: Independent Reviewer. <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf>.
- . 2016. «Report of the Bulk Powers Review,» London: Independent Reviewer. <https://terrorismlegislationreviewer.independent.gov.uk/bulk-powers-review-report/>.
- . 2018. «New Approaches to Intelligence Oversight in the U.K.» *Lawfare*. January 2, 2018. <https://www.lawfareblog.com/new-approaches-intelligence-oversight-uk>.
- Barker, Cat, Claire Petrie, Joanna Dawson, Samantha Godec, Pleasance Purser, and Holly Porteous. 2017. «Oversight of Intelligence Agencies: A Comparison of the «Five Eyes» Nations.» Parliamentary Library, Research Paper Series 2017–18. Parliament of Australia. Department of Parliamentary Services. <http://apo.org.au/system/files/123831/apo-nid123831-515251.pdf>.
- Belgian Standing Intelligence Agencies Review Committee (Comiteri). 2016. «Rapport d'activité 2015.» http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2015.pdf.
- . 2018. «Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations.» Brussels. <http://www.comiteri.be/images/pdf/Jaarverslagen/Vast-Comit-I-Activity-Report-2016.PDF>.
- Bellovin, Steven M., Matt Blaze, Susan Landau, and Stephanie K. Pell. 2016. «It's Too Complicated: How the Internet Upends Katz, F, and Electronic Surveillance Law.» *Harvard Journal of Law & Technology* 30 (1). <https://jolt.law.harvard.edu/assets/articlePDFs/v30/30HarvJLTech1.pdf>.
- Bos-Ollermann, Hilde. 2017. «Mass Surveillance and Oversight.» In *Surveillance, Privacy and Trans-Atlantic Relations*, edited by David D. Cole, Federico Fabbrini, and Stephen J. Schulhofer. *Hart Studies in Security and Justice*, Volume 1. Oxford: Hart Publishing.
- Bradford Franklin, Sharon. 2018. «Carpenter and the End of Bulk Surveillance of Americans.» *Lawfare*. July 25, 2018. <https://www.lawfareblog.com/carpenter-and-end-bulk-surveillance-americans>.
- Brundage, Miles, Shahar Avin, Jack Clark, Helen Toner, Peter Eckersley, Ben Garfinkel, Allan Dafoe, et al. 2018. «The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Migration.» February 2018. <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>.
- Carey, Bjorn. 2016. «Stanford Computer Scientists Show Telephone Metadata Can Reveal Surprisingly Sensitive Personal Information». Stanford News (blog), 16 May 2016. <https://news.stanford.edu/2016/05/16/stanford-computer-scientists-show-telephone-metadata-can-reveal-surprisingly-sensitive-personal-information/>.

- Chopin, Olivier. 2017. «Intelligence Reform and the Transformation of the State: The End of a French Exception.» *Journal of Strategic Studies* 40 (4): 532–53. <https://doi.org/10.1080/01402390.2017.1326100>.
- Clark, Charles S. 2018. «NSA Watchdog Breaks Precedent By Releasing Semi-Annual Report.» *Government Executive*. July 27, 2018. <https://www.govexec.com/management/2018/07/nsa-watchdog-breaks-precedent-releasing-semi-annual-report/150105/>.
- Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD). 2015. «Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX.» August 26, 2015. <https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel>.
- . 2016. «Review Report on the Implementation of Cooperation Criteria by the AIVD and the MIVD.» CTIVD no. 48. <https://english.ctivd.nl/documents/review-reports/2016/12/22/index48>.
- . 2017. «Kenniskring en tegenspraak CTIVD – Over CTIVD.» September 20, 2017. <https://www.ctivd.nl/over-ctivd/kenniskring--en-tegenspraak>.
- . 2018. «Review Report: The Multilateral Exchange of Data on (Alleged) Jihadists by the AIVD.» CTIVD No. 56. <https://english.ctivd.nl/documents/review-reports/2018/04/24/index>.
- Commission nationale de contrôle des techniques de renseignement (CNCTR). 2016. «Premier rapport d'activité 2015/2016.» <https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf>.
- . 2018. «Deuxième Rapport d'activité 2017.» https://www.cnctr.fr/_downloads/NP_CNCTR_2018_rapport_annuel_2017.pdf.
- Conger, Kate. 2017. «An Unknown Tech Company Tried (and Failed) to Stop the NSA's Warrantless Spying.» *Gizmodo*. June 14, 2017. <https://gizmodo.com/an-unknown-tech-company-tried-and-failed-to-stop-the-1796111752>.
- Cook, Ben. 2017. «The New FISA Court Amicus Should Be Able to Ignore Its Congressionally Imposed Duty.» *American University Law Review* 66 (2, Article 5). <http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1960&context=aulr>.
- Council of Europe. 2015. «Democratic and Effective Oversight of National Security Services.» Strasbourg. <https://rm.coe.int/democratic-and-effective-oversight-of-national-security-services-issue/16806daadb>.
- Court of Justice of the European Union. 2016. «C-203/15 Tele2 Sverige AB v Post-Och Telestyrelsen and C-698/15 SSHD v Tom Watson & Others.» December 16, 2016. http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=186492&occ=first&dir=&cid=406338.
- Cranor, Lorrie Faith. 2008. «A Framework for Reasoning About the Human in the Loop.» In *Proceedings of the 1st Conference on Usability, Psychology, and Security*. UPSEC'08. Berkeley, CA: USENIX Association. <http://dl.acm.org/citation.cfm?id=1387649.1387650>.
- Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). 2016. «Stellungnahme zum Entwurf eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (BT-Drs. 18/9041).» Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. <https://www.bundestag.de/blob/459634/a09df397dff6584a83a43a334f3936a3/18-4-660-data.pdf>.
- . 2017. «26. Tätigkeitsbericht zum Datenschutz für die Jahre 2015 und 2016.» Bonn. https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/26TB_15_16.pdf?__blob=publicationFile&v=3.
- Donohue, Laura K. 2017. «The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law.» <https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law>.
- Dorion, Pierre. 2008. «Data Deletion or Data Destruction?» *SearchDataBackup*. July 2008. <https://searchdatabackup.techtarget.com/tip/Data-deletion-or-data-destruction>.
- Dreo Rodosek, Gabi. 2016. «Sachverständigengutachten. Beweisbeschluss SV-13, 1. Untersuchungsausschuss der 18. Wahlperiode,» September 30, 2016, https://cdn.netzpolitik.org/wp-upload/2016/10/gutachten_ip_lokalisierung_rodosek.pdf.

- German Federal Constitutional Court (BVerfG). 2005. «Leitsätze Zum Urteil Des Zweiten Senats Vom 12. April 2005 (2 BvR 581/01).» https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/2005/04/rs20050412_2bvr058101.pdf;jsessionid=969575C316AC611F8F71AAB2F6C75D6F.1_cid394?__blob=publicationFile&v=1.
- Eijk, Nico van, and Cedric Ryngaert. 2017. «Expert Opinion – Legal Basis for Multilateral Exchange of Information.» Appendix IV bij CTIVD rapport no. 56 to the review report on the multilateral exchange of data on (alleged) jihadists by the AIVD. Utrecht/Amsterdam. <https://english.ctivd.nl/documents/review-reports/2018/04/24/appendix-iv>.
- Eijkman, Quirine, Nico van Eijk, and Robert van Schaik. 2018. «Dutch National Security Reform Under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?» Institute for Information Law (IViR, University of Amsterdam). https://www.ivir.nl/publicaties/download/Wiv_2017.pdf.
- Electronic Frontier Foundation. 2013. «Yahoo’s Challenge to the Protect America Act in the Foreign Intelligence Court of Review.» October 22, 2013. <https://www.eff.org/cases/yahoos-challenge-protect-america-act-foreign-intelligence-court-review>.
- Electrospaces.net. 2018. «Collection of Domestic Phone Records under the USA Freedom Act.» July 14, 2018, <https://electrospaces.blogspot.com/2018/07/collection-of-domestic-phone-records.html>
- European Court of Human Rights. 2010. «Case of Kennedy v. The United Kingdom (Application No. 26839/05).» Strasbourg.
- . 2015. «Case of Roman Zakharov v. Russia (Application No. 47143/06).» Judgment. Strasbourg. [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-159324%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}).
- . 2016. «Case of Szabó and Vissy v. Hungary (Application No. 37138/14).» January 12, 2016. Strasbourg. <http://www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf>.
- . 2018a. «Case of Paul Popescu v. Romania (Application No. 64162/10).» Strasbourg. <https://www.juridice.ro/wp-content/uploads/2018/02/CASE-OF-PAUL-POPESCU-v.-ROMANIA.pdf>.
- . 2018b. «Case of Centrum För Rättvisa v. Sweden (Application No. 35252/08).» Strasbourg. <http://www.statewatch.org/news/2018/jun/echr-sweden-Judgment-bulk-interception-communications-FULL.pdf>.
- European Court of Human Rights, and Council of Europe. 1978. «Case of Klass and Others v. Germany (Application No. 5029/71).» Strasbourg. September 6, 1978. <https://stewartroom.co.uk/wp-content/uploads/2014/07/Cases-ECHR-Klass.pdf>.
- . 2009. «Case of Iordachi and Others v. Moldova (Application No. 25198/02).» Strasbourg. <https://rm.coe.int/168067d212>.
- European Union Agency for Fundamental Rights. 2015. «Surveillance by Intelligence Services – Volume I: Member States» Legal Frameworks.» October 22, 2015. <http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services>.
- . 2017. «Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU – Volume II: Field Perspectives and Legal Update.» October 18, 2017. <http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega>.
- Farrell, Henry. 2016. «America’s Founders Hated General Warrants. So Why Has the Government Resurrected Them?» *Washington Post*. June 14, 2016. <https://www.washingtonpost.com/news/monkey-cage/wp/2016/06/14/americas-founders-hated-general-warrants-so-why-has-the-government-resurrected-them/>.
- Federation of American Scientists, «Secrecy News 07/28/14,» July 28, 2014, <https://fas.org/sgp/news/secrecy/2014/07/072814.html>.
- Forcese, Craig. 2018. «Bill C-59 and the Judicialization of Intelligence Collection. Draft Working Paper 04-06-18.» *Ottawa Faculty of Law Working Paper No. 2018-13*, 13.
- Führungsunterstützungsbasis FUB. n.d. «Die Organisation Der FUB – ZEO (Elektronische Operationen).» <https://www.vtg.admin.ch/de/organisation/fub.html>.

- Gallagher, Ryan. 2016. «Facing Data Deluge, Secret U.K. Spying Report Warned of Intelligence Failure.» *The Intercept*. June 7, 2016. <https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/>.
- Goldman, Zachary K., and Samuel J. Rascoff (eds.). 2016. *Global Intelligence Oversight. Governing Security in the Twenty-First Century*. Oxford: Oxford University Press.
- Government Communications Headquarters (GCHQ). 2011. «HIMR Data Mining Research Problem Book.» September 20, 2011. <https://www.documentcloud.org/documents/2702948-Problem-Book-Redacted.html>.
- Government of France. n.d. «Groupement Interministériel de Contrôle (GIC).» *Gouvernement.fr*. <https://www.gouvernement.fr/groupement-interministeriel-de-controle-gic>.
- Graulich, Kurt. 2017. «Reform des Gesetzes über den Bundesnachrichtendienst Ausland-Ausland-Fernmeldeaufklärung und Internationale Datenkooperation.» *Kriminalpolitische Zeitschrift* 1: 43–52.
- Greene, Robin. 2017. «A History of FISA Section 702 Compliance Violations.» *New America*. September 28, 2017. <https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/>.
- Hoadley, Daniel S., and Nathan J. Lucas. 2018. «Artificial Intelligence and National Security.» Congressional Research Service. April 26, 2018. <https://fas.org/sgp/crs/natsec/R45178.pdf>.
- Houwing, Lotte. 2018. «The Wiv 2017. A Critical Contemplation of the Act in an International Context.» https://www.burojansen.nl/pdf/2018-LotteHouwing-WivCriticalContemplation_final.pdf.
- Huber, Bertold. 2017. «Kontrolle der Nachrichtendienste des Bundes – Dargestellt am Beispiel der Tätigkeit der G10-Kommission.» *Zeitschrift für das Gesamte Sicherheitsrecht*, no. 01. <https://beck-online.beck.de/Dokument?vpath=bibdata%5Czeits%5CGSZ%5C2017%5Ccont%5CGSZ.2017.H01.gl2.htm>.
- Human Rights Watch. 2017. «Q & A: US Warrantless Surveillance Under Section 702 of the Foreign Intelligence Surveillance Act.» *Human Rights Watch*. September 14, 2017. <https://www.hrw.org/news/2017/09/14/q-us-warrantless-surveillance-under-section-702-foreign-intelligence-surveillance>.
- Inspector General of Intelligence and Security of New Zealand. n.d. «About: The Intelligence and Security Agencies.» <http://www.igis.govt.nz/about/>.
- International Network of Civil Liberties Organizations. 2018. «Unanswered Questions – International Intelligence Sharing.» June. https://www.inclo.net/pdf/iisp/unanswered_questions.pdf.
- Investigatory Powers Commissioner’s Office. 2018a. «IPCO Advisory Notice: Approval of Warrants, Authorisations and Notices by Judicial Commissioners.» 01/2018. London. <https://www.ipco.org.uk/docs/20180403%20IPCO%20Guidance%20Note%202.pdf>.
- . 2018b. «A Message from the Commissioner by Sir Adrian Fulford.» *IPCO Blog*. May 17, 2018. <https://www.ipco.org.uk/Default.aspx?mid=16.1>.
- . 2018c. «IPC Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers.» May 23, 2018. https://www.ipco.org.uk/docs/IPC_Submissions_on_bulk_powers.pdf.
- Konkel, Frank. 2014. «The Details About the CIA’s Deal with Amazon.» *The Atlantic*, July 17, 2014, <https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/>.
- Kris, David S., and J. Douglas Wilson. 2012. *National Security Investigations & Prosecutions 2d*. National Security Investigations & Prosecutions 2d 1. West. <https://books.google.de/books?id=THYfMwEACAAJ>.
- Laperruque, Jake. 2018. «After «Foreign Surveillance» Law, Congress Must Demand Answers from Intelligence Community.» *The Hill*, January 2018. <https://thehill.com/opinion/cybersecurity/370271-after-foreign-surveillance-law-congress-must-demand-answers-from>.
- «Le Groupement interministériel de contrôle va beaucoup donner.» 2016. *Defense – La voix du nord*. February 1, 2016. <http://defense.blogs.lavoixdunord.fr/archive/2016/02/01/groupement-interministeriel-de-controle-14495.html>.
- Leigh, Ian, and Njord Wegge (eds.). 2018. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World*. 1 edition. Routledge.

- Lubin, Asaf. 2017. «'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance.» SSRN Scholarly Paper ID 3008428. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=3008428>.
- . 2018. «Legitimizing Foreign Mass Surveillance in the European Court of Human Rights.» *Just Security*. August 2, 2018. <https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/>.
- Malgieri, Gianclaudio, and Paul De Hert. 2017. «European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards 'Good Enough' Oversight, Preferably but Not Necessarily by Judges.» In *Cambridge Handbook of Surveillance Law, Forthcoming 2017*, edited by D. Gray and S. Henderson. Rochester, NY: Social Science Research Network. <https://papers.ssrn.com/abstract=2948270>.
- McKay, Simon. 2018. *Blackstone's Guide to the Investigatory Powers Act 2016*. Oxford, New York, NY: Oxford University Press.
- McKay, Simon, and Clive Walker. 2017. «Legal Regulation of Intelligence Services in the United Kingdom.» In *Handbuch des Rechts der Nachrichtendienste*. Stuttgart: Richard Boorberg.
- Menn, Joseph. 2016. «Exclusive: Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources.» *Reuters*, October 5, 2016. <https://www.reuters.com/article/us-yahoo-nsa-exclusive/yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN124IYT>.
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. 2016. «Memorie van Toelichting inzake wijziging Wet op de inlichtingen- en veiligheidsdiensten.» Kamerstuk. October 28, 2016. <https://www.rijksoverheid.nl/documenten/kamerstukken/2016/10/28/memorie-van-toelichting-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdiensten>.
- . 2017. «Bijlage bij brief Wiv 2017 en regeerakkoord,» 2017. https://www.aivd.nl/binaries/aivd_nl/documenten/kamerstukken/2017/12/15/kamerbrief-over-wiv-2017-en-het-regeerakkoord/20171215+Bijlage+bij+brief+minister+BZK+over+Wiv+2017+en+regeerakkoord.pdf.
- Murray, Daragh, Pete Fussey, and Maurice Sunkin. 2018. «Response to Invitation for Submissions on Issues Relevant to the Proportionality of Bulk Powers.» <https://www.ipco.org.uk/docs/Essex%20HRBDT%20Submission%20to%20IPCO%20Re%20Proportionality%20Consultation.pdf>.
- National Security Agency/ Central Intelligence Agency. 2012. «(U)SIGINT Strategy 2012-2016.» February 23, 2012. <https://edwardsnowden.com/wp-content/uploads/2013/11/2012-2016-sigint-strategy-23-feb-12.pdf>.
- Necessary and Proportionate Coalition. 2014. «Necessary & Proportionate. International Principles on the Application of Human Rights to Communications Surveillance.» May 2014. https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf.
- Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee). 2016. «Dokument 16 (2015–2016) Rapport til Stortinget fra Evalueringsutvalget for Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget).» February 29, 2016. Oslo. <https://www.stortinget.no/globalassets/pdf/dokumentserien/2015-2016/dok16-201516.pdf>.
- . «Annual Report 2017 – Document 7:1 (2017–2018).» Oslo. https://eos-utvalget.no/english_1/content/text_f3605847-bc4a-4c7c-8c17-ce1b1f95a293/1523360557009/_2017_eos_annual_report.pdf.
- Nyst, Carly. 2018. «Regulation of Big Data Surveillance by Police and Intelligence Agencies.» The Human Rights, Big Data and Technology Project, University of Essex. <https://ling2s14id7e-20wtc8xsceyr-wpengine.netdna-ssl.com/wp-content/uploads/2015/12/Regulation-of-Big-Data-Surveillance-by-Police-and-Intelligence-Agencies.pdf>.
- Office of the Inspector General National Security Agency. 2018. «Semiannual Report to Congress. 1 October 2017 to 31 March 2018.» <https://www.oversight.gov/report/nsa/semi-annual-report-congress-1-october-2017-31-march-2018>.
- Office of the Inspector General of Intelligence and Security Cheryl Gwyn. 2017. «Annual Report for the Year Ended 30 June 2017.» December 1, 2017. Wellington. <http://www.igis.govt.nz/assets/Annual-Reports/Annual-Report-2017.pdf>.

- Ohm, Paul. 2010. «The Argument against Technology-Neutral Surveillance Laws,» no. 88 Tex. L. Rev. 1685. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr88&div=60&id=&page=>.
- Organisation for Economic Co-Operation and Development. 2013. «The OECD Privacy Framework.» https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
- Parsons, Christopher, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert. 2017. «Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act Respecting National Security Matters), First Reading (December 18, 2017).» The Citizen Lab, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC). <https://citizenlab.ca/wp-content/uploads/2018/01/C-59-Analysis-1.0.pdf>.
- Perry, Rodney M. 2014. «Intelligence Whistleblower Protections: In Brief.» *Congressional Research Service*. October. <https://fas.org/sgp/crs/intel/R43765.pdf>.
- Privacy and Civil Liberties Oversight Board. 2014a. «Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court.» https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.
- . 2014b. «Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.» <https://www.pclob.gov/library/702-Report.pdf>.
- Privacy International. 2018. «Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards.» <http://privacyinternational.org/feature/1742/new-privacy-international-report-reveals-dangerous-lack-oversight-secret-global>.
- Reardon, Joel, Hubert Ritzdorf, David Basin, and Srdjan Capkun. 2013. «Secure Data Deletion from Persistent Media.» In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13*, 271–84. Berlin, Germany: ACM Press. <https://doi.org/10.1145/2508859.2516699>.
- Rechthien, Kay. 2016. «Sachverständigen-Gutachten gemäß Beweisbeschluss, 1. Untersuchungsausschuss (NSA-UA) der 18. Wahlperiode des Deutschen Bundestages,» September. <https://www.ccc.de/system/uploads/220/original/beweisbeschluss-nsaua-ccc.pdf>.
- Renan, Daphna. 2016. «The Fourth Amendment as Administrative Governance.» *Stanford Law Review*, no. 68 (May).
- Richardson, Sophie, and Nicholas Gilmour. 2016. *Intelligence and Security Oversight. An Annotated Bibliography and Comparative Analysis*. Palgrave Macmillan. <http://www.palgrave.com/de/book/9783319302515>.
- Schaller, Christian. 2018. «Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden.» *German Law Journal* 19 (4).
- Security Intelligence Review Committee. 2018. «SIRC Annual Report 2017–2018: Building for Tomorrow: The Future of Security Intelligence Accountability in Canada.» Ottawa. <http://www.sirc-scsars.gc.ca/anrran/2017-2018/index-eng.html>.
- Smith, Graham. 2016. «A Trim for Bulk Powers?» September 7, 2016. <https://www.cyberleagle.com/2016/09/a-trim-for-bulk-powers.html>.
- . 2018. «Illuminating the Investigatory Powers Act.» *Cyberleagle*. February 22, 2018. <https://www.cyberleagle.com/2018/02/illuminating-investigatory-powers-act.html>.
- Swedish State Inspection for Defense Intelligence Operations (SIUN). 2018. «Årsredovisning för 2017.» February 22, 2018. Stockholm. http://www.siun.se/dokument/Arsredovisning_2017.pdf.
- Swire, Peter, Jesse Woo, and Deven R. Desai. 2018. «The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance (Draft).»
- The Chambers of Simon McKay. 2018. «Judicial Approval of Warrants, Authorisations and Notices under the Investigatory Powers Act 2016: A Review of the Investigatory Powers Commissioner's Office First Advisory Note.» 2018. <https://simonmckay.co.uk/judicial-approval-of-warrants-authorisations-and-notices-under-the-investigatory-powers-act-2016-a-review-of-the-investigatory-powers-commissioners-office-first-advisory-note/>.
- Tréguer, Félix. 2016. «From Deep State Illegality to Law of the Land: The Case of Internet Surveillance in France,» October. <https://halshs.archives-ouvertes.fr/halshs-01306332v11/document>.

- UK Home Office. 2017. *Interception of Communications. Pursuant to Schedule 7 to the Investigatory Powers Act 2016. Draft Code of Practice*. December 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/593748/IP_Act_-_Draft_Interception_code_of_practice_Feb2017_FINAL_WEB.pdf.
- United States Foreign Intelligence Surveillance Court. 2010. «Rules of Procedure.» Washington, DC. <http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf>.
- Venice Commission. 2015. «Report on the Democratic Oversight of Signals Intelligence Agencies.» [http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD\(2015\)011-e](http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)011-e).
- Wetzling, Thorsten (ed.). 2010. *Same Myth, Different Celebration? Intelligence Accountability in Germany and the United Kingdom*. Geneva: Graduate Institute of International and Development Studies.
- . 2017a. «Options for More Effective Intelligence Oversight.» Discussion Paper. https://www.stiftung-nv.de/sites/default/files/options_for_more_effective_intelligence_oversight.pdf.
- . 2017b. «Germany's Intelligence Reform: More Surveillance, Modest Restraints and Inefficient Controls.» Policy Brief. Berlin: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.
- . 2017c. «New Rules for SIGINT Collection in Germany: A Look at the Recent Reform.» *Lawfare*. June 23, 2017. <https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform>.
- Wissenschaftlicher Dienst des Bundestags. 2017. «Kontrolle von Nachrichtendiensten Bei Zusammenarbeit Mit Anderen Nachrichtendiensten Im Ausland.» March 2017. WD 3-3000-072/17. Berlin: Deutscher Bundestag. <https://www.bundestag.de/blob/508038/5a79b26ee2205e08171ee396ef87ae45/wd-3-072-17-pdf-data.pdf>.
- Wizner, Ben. 2017. «What Changed after Snowden? A U.S. Perspective.» *International Journal of Communication* 11.
- Zegart, Amy. 2011. «The Domestic Politics of Irrational Intelligence Oversight.» *Political Science Quarterly* 126, no. 1: 1–25.

List of reviewed Intelligence Legislation

- Canada, Bill C-59 (proposed): An Act respecting national security matters (2017). 1st reading June 20, 2017.
- France, Interior Security Act (*Code de la sécurité intérieure*).
- France, Law No. 2015-1556 on international surveillance (*loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*), November 30, 2015.
- Germany, Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst*), December 20, 1990, as amended.
- Germany, Act on the Protection of the Federal Constitution (*Bundesverfassungsschutzgesetz*).
- Germany, G10 Act (*Artikel 10-Gesetz*), June 26, 2001.
- Germany, Parliamentary Control Panel Act (*Kontrollgremiumgesetz*), July 29, 2009.
- New Zealand, Intelligence and Security Act 2017.
- Norway, Act relating to the Oversight of Intelligence, Surveillance and Security Service No. 7 (*Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-kontrollloven)*) of February 3, 1995, amended in June 2017.
- Switzerland, Federal Intelligence Service Act (*Nachrichtendienstgesetz*), September 1, 2017.
- The Netherlands, Act on the Intelligence and Security Services 2017 (*Wet op de inlichtingen- en veiligheidsdiensten 2017*).
- United Kingdom, Human Rights Act, 1998.
- United Kingdom, Investigatory Powers Act 2016.
- United States of America, 50 U.S. Code §1805 – Issuance of Power.

United States of America, Executive Order 12333, December 4, 1981, amended 2003, 2004, and 2008.
United States of America, Foreign Intelligence Surveillance Act of 1978, amended 2008 and 2011.
United States of America, Foreign Intelligence Surveillance Court (FISC), Rules of Procedure, November 1, 2010.
United States of America, Presidential Policy Directive/ PPD 28 – Signals Intelligence Activities, January 17, 2014.
United State of America, Executive Order 13526, December 29, 2009.
United States of America, USA Freedom Act, Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, June 2, 2015.
United States of America, US Patriot Act, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, October 26, 2001.
United States of America, Wiretap Act, codified at 18 U.S. Code §§ 2510-2522.



DEMOCRACY
VOLUME 50

Upping the Ante on Bulk Surveillance An International Compendium of Good Legal Safeguards and Oversight Innovations

Robust surveillance legislation and effective intelligence oversight can serve as bulwarks against the erosion of fundamental rights in our democracies. Unfortunately, national governments regularly need to be admonished for flaws in their intelligence laws by national or regional courts. Rightly, courts demand more rigorous and effective oversight mechanisms. Yet, given the rapid evolution and the complexity of surveillance technology, what should effective oversight look like in actual practice? Courts will not design oversight institutions or prescribe specific accountability mechanisms. This is the important task of democratic governance that needs to be administered elsewhere.

This compendium by Thorsten Wetzling and Kilian Vieth invites regulatory authorities, oversight bodies and civil society to look beyond national borders and be inspired by the good practices that exist in other countries.

ISBN 978-3-86928-187-2