United Nations A/HRC/37/62

General Assembly

Distr.: General
25 October 2018

Original: English

**Human Rights Council**
**Thirty-seventh session**
26 February–23 March 2018
Agenda item 3
**Promotion and protection of all human rights, civil political, economic, social and cultural rights, including the right to development**

# Report of the Special Rapporteur on the right to privacy*, **

## Note by the Secretariat

In his report, prepared pursuant to Human Rights Council resolution 28/16, the Special Rapporteur on the right to privacy focuses on the work undertaken in the first three years of his mandate, with a particular focus on the work done on surveillance and privacy, and reflects on the role and mandates of special procedure mandate holders.

* The report was submitted late in order to reflect the most up-to-date information.
** The annex is reproduced as received, in the language of submission only.

GE.18-17811(E)
*1817811*

# Report of the Special Rapporteur on the right to privacy

## Contents

# I. Introduction

1. The mandate of the Special Rapporteur on the right to privacy commenced on 1 August 2015. Pursuant to Human Rights Council resolution 28/16, the Special Rapporteur reports annually to the Council and to the General Assembly.[1]

2. The present report is the Special Rapporteur's third report to the Council and thus the last one of the first and current mandate. It is therefore appropriate to use this opportunity to cast an eye back over the past three years, provide an overview of the activities and achievements, as well as elicit some of the lessons learned, and look at the mandate at present and in the future.

3. With this aim in mind, the present report is composed of four parts. Following the introduction, the Special Rapporteur's activities, achievements and future work are described for each of the eight areas of the mandate. In the third part of the report, the Special Rapporteur outlines the successful work undertaken on one of the mandate's key priorities: privacy protection, and government and other forms of surveillance. He describes a draft international legal instrument on surveillance, as well as a set of recommendations to be considered. In the fourth and final part of the report, the Special Rapporteur addresses the terms of the mandate and the clarifications and reinforcement required therein.

4. Since the commencement of the mandate, in addition to the right to privacy being enshrined and protected at the international[2] and regional[3] levels, and in other human rights instruments,[4] the importance of privacy has been reaffirmed by the Council, in particular in its resolution 34/7. In the resolution, the Council recognized that the right to privacy could enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noted with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association. This is consistent with the approach to personality taken by the Special Rapporteur in his 2016 report to the Council (A/HRC/31/64).

5. In his work, the Special Rapporteur is guided not only by the international legal framework on the right to privacy, but also by the resolutions regularly adopted on the topic by the Council, including the one mentioned above.

[1] See www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

[2] See: Universal Declaration of Human Rights, art. 12; International Covenant on Civil and Political Rights, art. 17; Convention on the Rights of the Child, art. 16; and International Convention on the Protection of All Migrant Workers and Members of Their Families, art. 14. See also www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

[3] See Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8; and American Convention on Human Rights, art. 11. See also www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

[4] For example, see: Cairo Declaration on Human Rights in Islam: art. 18; Arab Charter on Human Rights, arts. 16 and 21; Declaration of Principles on Freedom of Expression in Africa of the African Commission on Human and Peoples' Rights; African Charter on the Rights and Welfare of the Child, art. 10; Human Rights Declaration of the Association of Southeast Asian Nations, art. 21; Asia-Pacific Economic Cooperation Privacy Framework; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows; Council of Europe Committee of Ministers Recommendation No. R (99) 5 for the protection of privacy on the Internet; and Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

# II. Mandate of the Special Rapporteur

6. The activities carried out by the Special Rapporteur typically relate to more than one area of his mandate, so matters are reported under several mandate areas. The mandate appears in appendix 1, which is available online (see part V).

## A. Activities of the Special Rapporteur (2015–2017)

### 1. Gathering relevant information and study matters

7. The first paragraph of the mandate states that the Special Rapporteur will gather relevant information, study matters in relation to the right to privacy and make recommendations for its promotion and protection, including the challenges arising from new technologies.

8. To meet this first aim, the Special Rapporteur has established five thematic action streams. He has used official country visits, consultations, contacts with non-governmental organizations (NGOs), public privacy debates, international conferences and promotional events, such as the Asia Pacific Privacy Authorities' annual Privacy Awareness Week, and examined matters brought to his attention and allegation letters, among other means, to study the relevant matters.

#### Thematic action streams

9. The Special Rapporteur outlined his workplan in 2016 in his reports to the Council and to the General Assembly. He invited all stakeholders to engage in planned thematic reports and calls for consultations, all of which related to the five thematic action streams.

10. The five thematic action streams are: a better understanding of privacy; security and surveillance; big data and open data; health data; and the use of personal data by corporations. The thematic action streams all address the challenges to privacy in the digital era and are interconnected and sequenced to enable each task force to build on the work of the others. For example, the Task Force on Big Data and Open Data sets the scene for the thematic action streams on health data and on the use of personal data by corporations. Each task force is coordinated by a Chair who, on a voluntary basis, assists the Special Rapporteur by gathering research and information, identifying issues and consulting as widely as possible.

#### (a) Security and surveillance

11. To identify the best practices on safeguards regarding Internet surveillance, the Special Rapporteur created the International Intelligence Oversight Forum — an annual gathering of national agencies and parliamentary committees tasked with the oversight of national and foreign intelligence in their respective countries. The Forum serves as a platform to share information, exchange experiences and identify best practices at an international level.

12. The Forum has been an unqualified success. Membership of the organizing committee is refreshed regularly. In 2016, the Forum was held in Bucharest with the support of the Romanian Parliament's four oversight committees. It welcomed more than 60 delegates from 26 institutions in 20 countries. In 2017, it was held in the Belgian Parliament with the support of the data protection authorities of Belgium, Luxembourg and the Netherlands: 80 delegates from 30 countries participated. In 2018 it is scheduled to take place in autumn in Portugal. The oversight authorities of several countries are taking increasing ownership of the process and are working to identify issues and the responses thereto in intelligence oversight as a collective international concern, responding to a latent need that leads to the adoption of best practices that are important for the protection of privacy.

13. It is precisely the intersection of privacy and State security interests and surveillance in cyberspace that led to the creation of the Special Rapporteur's mandate in 2015 in the wake of the revelations by Edward Snowden, which have been ongoing since June 2013.

The Special Rapporteur shares the impressions of the Chair of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, who, in October 2017, noted, as regards a recommendation on raising awareness about the link between international peace and security, human rights and development as it applies to the information and communications technology (ICT) environment that, in sharing lessons and practices in countering the use of ICT for terrorist and other criminal purposes, including on cooperation among States and between States and the private sector, to prevent and counter the use of ICT for the purposes of recruitment and incitement to violence by terrorist and extremist groups, and for the financing, planning and preparation of their activities, and identifying where additional work might be needed, States should consider their commitment to and respect for and protection of human rights and fundamental freedoms. The Group of Governmental Experts offered various recommendations to support implementation of the voluntary, non-binding norms for responsible State behaviour presented in the 2015 report of the Group of Governmental Experts (A/70/174), inter alia, that States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights including the right to freedom of expression. The Group of Governmental Experts underscored that personal data held on, transmitted through or processed by ICT can have a profound impact on life and security. States should take appropriate steps to protect personal data, including its confidentiality, integrity, accessibility and authenticity, while respecting relevant international, legal human rights instruments.

14. Noting the failure of the Group of Governmental Experts to reach a consensus on a final report, the Special Rapporteur submits that the need is now greater than ever to achieve synergy among all actors at the international level whose mandates touch upon the use of information and communication technologies processing personal data.

15. The Special Rapporteur consistently maintains that cyberpeace depends on the willingness and ability of States to achieve synergy between security interests and privacy in cyberspace. In order to avoid cyberwar, measures to limit surveillance and other privacy-intrusive measures in cyberspace must also be contemplated. As part of an effort to explore the options for such measures, in synergy with the European Union-supported Managing Alternatives for Privacy, Property and Internet Governance project,[5] the Special Rapporteur has explored options for a draft legal instrument on surveillance and privacy to strengthen standards and create protection mechanisms to address the massive infringement of the right to privacy of individuals around the world.

16. The discussion and adoption within the United Nations of a legal instrument on surveillance and privacy could simultaneously achieve two main goals by providing States with:

(a) A set of principles and model provisions, to be integrated into national legislation, that embody and enforce the highest principles of international human rights law, especially the right to privacy, when it comes to surveillance;

(b) A number of options, based on international best practices, to balance the security interests and concerns about surveillance with the protection of the right to privacy.

[5] For the International Intelligence Oversight Forum, and for other events — for example, those on privacy, personality and flows of information — the Special Rapporteur receives logistical support from the University of Malta and the University of Groningen and through joint events with the European Union-supported Managing Alternatives for Privacy, Property and Internet Governance project. Since 2014, the Special Rapporteur has been the overall scientific coordinator of the Managing Alternatives project, which deals with Internet governance, privacy and intellectual property. Within this project, which formally ended in February 2018, the Special Rapporteur is also personally responsible for Internet governance and privacy therein, developed by the Institute for Legal Infomatics at Leibniz University Hannover, Germany.

17. An instrument of some form is necessary, whether as soft law in the form of a recommendation or even, and more appropriately, given current State practice, as hard law in the form of an international multilateral treaty. The Special Rapporteur's work to date has been very successful — particularly given the challenges involved — but it is not yet of such maturity that would allow the Special Rapporteur to assure the Human Rights Council that the instrument had the unanimous or even the majority support of States. Despite the pressing need for such a legal instrument, timing issues need to be accommodated.

### (b) Big data — open data

18. The Special Rapporteur's report on big data and open data was presented to the General Assembly in October 2017 as an introductory study identifying the key issues (A/72/540). The preliminary recommendations address:

(a) Governance, regulation, research and consultation with civil society organizations;

(b) Limits to using personal information based on international standards and principles, including an exempt category for personal information;

(c) Robust enforcement mechanisms;

(d) Requirements for a rigorous, public, scientific analysis of data privacy protection, including a privacy impact assessment;

(e) Active support by Governments and corporations of the creation and use of privacy-enhancing technologies.

19. Consultation is under way with a call for submissions by 28 April 2018, and a public consultation event scheduled for July 2018. Ongoing work will address:

(a) Principles for guidance and protection of privacy in the big data context;

(b) Consultation on the report and the privacy challenges of big data;

(c) Facilitation of research on de-identification;

(d) Responding to the failure of de-identification.

### (c) Health data

20. The Special Rapporteur's Task Force on Health Data is examining issues under the leadership of Dr. Steve Steffensen, Associate Professor, Dell Medical School, University of Texas, United States. A consultation event is planned for 2018, most likely in the United States.

21. All interested actors, States as well as other stakeholders, including NGOs, are invited to contribute to the development of guidelines on best practices.

### (d) Use of personal data by corporations

22. Some businesses, including the largest corporations, increasingly rely on the exploitation (collection, processing, repurposing and sale) of personal information, often without ensuring adequate transparency and the informed consent of the individuals concerned.[6] During his official visit to the United States in June 2017, the Special Rapporteur canvassed corporations about the way they reacted to requests from Governments regarding the personal data they held. The concerns of the Special Rapporteur regarding such requests led to the submission of an amicus curiae to the United States Supreme Court in December 2017.[7]

23. The Special Rapporteur also met with a number of United States corporations throughout 2017 on the use of personal data in their business models. This dialogue is

[6] See www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

[7] *United States of America v. Microsoft Corporation*, case No. 17-2, filed on 13 December 2017. See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf.

assisting the Task Force on Use of Personal Data by Corporations to commence its work formally in 2018.

### (e) Privacy and personality

24. The Human Rights Council's recognition of the right to privacy as an essential right for a democratic society[8] is explored by the Task Force on Privacy and Personality, chaired by Elizabeth Coombs (Australia), in consultations, received communications and in the examination of the existing literature. To promote a better understanding of privacy in the digital age, the Special Rapporteur has been convening regional consultation events on the theme of privacy, personality and information flows. The first (Western countries) was held in July 2016 in New York. The second (Middle East and North Africa) was held in Tunisia in May 2017, the third (Asia) took place in September 2017 in Hong Kong, China and the fourth (Latin America) is planned for May 2018.

25. In addition, the Special Rapporteur has also worked on:

(a) Examination of landmark decisions, such as the Supreme Court of India in 2017 in the case of *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*. In the judgment, the Supreme Court stated that: "Privacy is the ultimate expression of the sanctity of the individual. It is a constitutional value which straddles across the spectrum of fundamental rights and protects for the individual a zone of choice and self-determination";[9]

(b) Reporting the effects upon individuals and their personal development of a deprivation of the right to privacy;

(c) Examining cyberviolence, with an emphasis on a gender-based analysis and vulnerable sections of the community;[10]

(d) Exploring the importance of privacy to the full development of the individual and to the societies in which they live and contribute.

### Official country visits

26. The dates and timing of official country visits are negotiated with the relevant member States. Countries are selected largely on the basis of privacy-related developments.

27. Requests for official country visits in the period from 2016 to 2018 are as follows:

| *Country* | *Request date* |
|---|---|
| China | 31 March 2016 |
| Republic of Korea | 31 March 2016 |
| South Africa | 31 March 2016 |
| United States of America | 20 September 2016 |
| Germany | 21 October 2016 |
| India | 21 October 2016 |
| United Kingdom | 21 October 2016 |
| France | 29 November 2016 |
| Argentina | 20 December 2017 |
| Uruguay | 8 January 2018 |

[8] Human Rights Council resolution 34/7.

[9] See http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf.

[10] Hadeel al-Alosi, "Cyber-violence: digital abuse in the context of domestic violence", University of New South Wales Law Journal, vol. 40 (4), pp. 1573–1603.

28. Delays in conducting country visits are generally the result of late responses or non-responses by Governments to requests to visit or circumstances that render it inappropriate for the Special Rapporteur to visit at a previously planned time. Visits form an integral part of the Special Rapporteur's role in monitoring the right to privacy. Meeting schedules accordingly involve:

(a) Official authorities, such as the intelligence services, law enforcement and regulators/oversight authorities, and the ministers responsible for such authorities;

(b) Representatives of civil society and other stakeholders, including activists, journalists, academics and others.

29. Meeting agendas generally comprise:

(a) Constitutional, legal and institutional frameworks;

(b) Big data, surveillance, threats to privacy, the Special Rapporteur's five thematic action streams, as well as assessments of intelligence oversight mechanisms;

(c) Concerns shared with the Special Rapporteur by experts and civil society organizations.

**Non-official country visits**

30. The Special Rapporteur visits countries for other purposes, such as international conferences, and gathers information that can be used in his thematic action streams. For example, in the five months prior to the report to the General Assembly in 2016, the Special Rapporteur participated in multiple activities in 11 countries as diverse and as geographically distant as Australia, Austria, Denmark, France, Germany, Italy, Latvia, the Netherlands, New Zealand, Switzerland and the United States. These engagements identified areas important to the promotion of privacy, such as the protection of the privacy of children, the structural and organizational arrangements for privacy and data regulators, among others.

**Consultations**

31. The Special Rapporteur has engaged with civil society, Governments, law enforcement, intelligence services, data protection authorities, intelligence oversight authorities, academics, corporations and other stakeholders in Africa, America (North, Central and South), Asia, Australasia and Europe. In 2016 and 2017 alone, 26 activities took the Special Rapporteur to over 30 different cities, some in Asia, North Africa and Central America, with a quarter in the United States and over a half in Europe.

**Drafting recommendations for the promotion and protection of the right to privacy, including the challenges arising from new technologies**

32. The information gathered by the Special Rapporteur in the activities outlined above helps him to formulate recommendations for his reports to the Human Rights Council and to the General Assembly.

**Achievements**

33. The thematic reports submitted to date are as follows:

- First approaches to a more privacy-friendly oversight of government surveillance, Human Rights Council, March 2017 (A/HRC/34/60);
- Security and surveillance, Human Rights Council, March 2017 (A/HRC/31/64);
- Interim report of the Task Force of Big data and Open Data, General Assembly, October 2017 (A/72/540);
- Some preliminary options within Internet governance for an international legal instrument on government surveillance, Human Rights Council, March 2018 (see present report and appendix 7 thereof available online).

### Ongoing progress in thematic action streams

34. The Special Rapporteur has developed guidance on big data, which he presented to the General Assembly in October 2017 and which is currently under consultation; and a draft international legal instrument on surveillance and privacy that addresses the issues identified.

35. The Special Rapporteur has held consultation events, such as the 2017 Conference on Privacy, Personality and Flows of Information: Asian Perspectives for Privacy as a Global Human Right.

36. The Task Force on Health Data has commenced its work under the guidance of the Special Rapporteur.

37. The Special Rapporteur gathered support for the Task Force on Use of Personal Data by Corporations and submitted the associated amicus curiae brief to the United States Supreme Court on the Microsoft case.

### Official country visits

38. The Special Rapporteur has conducted two official country visits, to the United States (June 2017)[11] and France (November 2017).[12] The reports will be presented to the Human Rights Council in March 2019 in order to allow additional time for follow-up exchanges with the Governments concerned.

### Consultations

39. Consultations have produced greater awareness of privacy issues across different jurisdictions, differing levels and different sections of the community, which have included events organized by the Irish Council for Civil Liberties, the Japan Civil Liberties Union, the Japan Federation of Bar Associations and the Northern Ireland Human Rights Commission, and multiple activities at the Internet Governance Forum and RightsCon, among others.

### Future activities and opportunities

40. If the mandate of the Special Rapporteur is renewed by the Human Rights Council, he plans to present the following reports:

(a) To the Human Rights Council

(i) “Lessons learned for improved safeguards and remedies in effective oversight of government surveillance”, March 2019;

(ii) “Proportionality, necessity and law in government surveillance, law enforcement and transboundary flows of personal data: the effectiveness and improvement of existing legal safeguards and remedies”, March 2020;

(iii) “Progress, regress and other dimensions of the effective oversight of government surveillance”, March 2021.

(b) To the General Assembly

(i) “Improving safeguards and remedies for privacy and health data”, October 2018;

(ii) “Profits and privacy: the monetization of personal data as a business model and the responsibilities of corporations”, October 2019;

[11] See end-of-mission statement: www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

[12] See preliminary findings: www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F.

(iii) "Privacy, personality and flows of information: a first global overview of the universal right to privacy from the perspectives of time, place and space", October 2020;

(iv) "The transboundary flow of personal data between corporations, law enforcement and surveillance", October 2021.

41. The Special Rapporteur may also report, time and resources allowing, on other issues related to the right to privacy: big data and open data; health data; the corporate use of personal information; the privacy of children and young persons; strategies to address privacy challenges inherent in surveillance activities; a gender-based approach to the right to privacy; responses to privacy breaches, such as big data de-identification failures; complaints received by the Special Rapporteur; official country visits; matters under discussion with States (public domain letters); and privacy issues in the digital age.

42. The Special Rapporteur's next planned official visits are the United Kingdom of Great Britain and Northern Ireland (June 2018) and Germany (autumn 2018).

43. The Special Rapporteur will continue consulting with State institutions, individuals and organizations on the right to privacy. Major events in 2018 include the Conference on Managing Alternatives for Privacy, Property and Internet Governance held on 19 and 20 January in Rome, the Latin American privacy, personality and flows of information event planned to be held in May and the Task Force on Health Data consultation and the consultation on big data and open data to be held in Australia in July.

## 2. Seeking, receiving and responding to information

### Consultations

44. The Special Rapporteur exchanged information with the officials, ministries and institutions of various Governments (at national and subnational levels); data protection and privacy commissioners; the Chair of the European Union's Article 29 Working Party;[13] the Chair of the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; standards-setting organizations, such as the International Telecommunication Union and the Institute of Electrical and Electronics Engineers; civil society organizations; permanent missions to the United Nations Office and other international organizations in Geneva; other special procedure mandate holders; officials of the Office of the United Nations High Commissioner for Human Rights (OHCHR); and researchers, academics and professional bodies. He has delivered keynote speeches and participated extensively in conferences and civil society meetings.

45. The Special Rapporteur held particularly productive engagements with data protection and privacy commissioners, who form a core constituent group in his mandate. At the International Conference of Data Protection and Privacy Commissioners in 2015, the Special Rapporteur sought their feedback on his 10-point plan. At the Conference in 2016, the Special Rapporteur reported progress on that plan and at the Conference in 2017 in Hong Kong, China, he spoke and participated in parallel events and held his third "privacy, personality and flows of information" event to complement the Conference.

### Correspondence

46. The Special Rapporteur receives correspondence from various sources. However, only the correspondence received through the official registry of OHCHR is registered and counted, making it difficult to report the total number of communications received. Nevertheless, since the commencement of the mandate, the OHCHR has registered the following correspondence on behalf of the Special Rapporteur.

[13] Data Protection Working Party established by article 29 of Directive 95/46/EC.

47. Registered correspondence 2015–2017:[14]

| *2015* | *2016* | *2017* | *Total* |
|---|---|---|---|
| Not available | 3 | 47 | 50 |

48. A disaggregation of the letters received by country or issue is not available, but in 2017 most of the correspondence was received from permanent missions, NGOs and international organizations.[15] These figures do not take into account the hundreds, possibly thousands, of other messages received at the Special Rapporteur's official email address (srprivacy@ohchr.org).

**Achievements**

49. In October 2015, the International Conference of Data Protection and Privacy Commissioners adopted a resolution on cooperation with the Special Rapporteur.[16]

50. The Special Rapporteur issued joint communications with other mandate holders on the situations in Egypt, Haiti, Honduras, Mexico and Spain.

51. The Special Rapporteur identified and responded to emerging matters and the allegations of privacy breaches, and potential technology-based incursions into privacy, such as facial recognition software.

**Future activities and opportunities**

52. The Special Rapporteur will continue his activities, emphasizing engagement with all stakeholders (particularly security and surveillance issues, including cybersecurity for information systems), the drafting of guidance material and recommendations on emerging issues with the input of civil society organizations and other stakeholders, technical assistance on the growing and diverse risks to the right to privacy in the digital age and the collaboration with other special procedure mandate holders on the protection of human rights.

## 3. Identifying obstacles, promoting principles and submitting recommendations

**Obstacles to privacy**

53. One of the Special Rapporteur's most important initiatives is in the field of security and surveillance, as is befitting of the core issue that led to the creation of the Special Rapporteur's mandate by the Human Rights Council. Obstacles to protecting the right to privacy under surveillance include the current lack or inadequacy of detailed rules, practical procedures and appropriate oversight mechanisms to ensure an independent, reliable and efficient control of surveillance, both nationally and globally. An overview of the gaps that have been identified in privacy protection may be found in the annex.

54. As regards big data, information no longer needs to be "personal" to identify an individual.[17] Technological capacities and data analytics only require information that "leads to" an individual and their connections to pose a threat to privacy.

55. The thematic action streams identify contemporary obstacles to protecting and promoting the right to privacy, such as technology-based incursions in the health sphere; the smartphone in the witness box; cyber-based violence; differential vulnerability across

[14] Excludes emails sent to srprivacy@ohchr.org.

[15] Advice from OHCHR, 19 December 2017.

[16] See https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

[17] Graham Greenleaf, "Data protection: a necessary part of India's fundamental inalienable right of privacy — submission on the White Paper of the Committee of Experts on a Data Protection Framework for India", University of New South Wales Law Research Paper No. 6, January 2018. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810.

communities; embedded gender and other biases in algorithms; government access to private sector data; and facial recognition and other technological tools.

**Responding to obstacles — promoting privacy**

56. As regards the theme of surveillance, the Special Rapporteur has embarked upon a strategy to build a consensus around the means to strengthen the international legal framework and create adequate oversight mechanisms for surveillance globally.

57. The Special Rapporteur has issued formal communications in response to topical privacy issues, official country visits and matters requiring a joint response with other mandate holders (see appendix 3).

**Promotion of principles and best practices**

58. The Special Rapporteur has provided inputs, among others, to public consultations on draft legislation by the Governments of India and the United Kingdom and the Parliament of Australia.[18] The Special Rapporteur also submitted letters expressing his concern, some of which remain confidential[19] and some of which are in the public domain, such as those written to the Governments of Japan and Mexico.

**Proposals and recommendations to the Human Rights Council**

59. The Special Rapporteur's recommendations on big data and open data are contained in appendix 4 to the present report.

60. The preliminary recommendations of the Special Rapporteur following his official visit to the United States cover surveillance for national security purposes (membership of the Privacy and Civil Liberties Oversight Board and section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008); smart surveillance in urban environments and surveillance carried out for law enforcement purposes; situations covered under Executive Order 12333; personal data held by corporations; extending the protection provided by the Health Insurance Portability and Accountability Act of 1996 to all health data; identity management of sex workers; the simplification of privacy; and fostering privacy-positive initiatives at State level. As regards surveillance, the Special Rapporteur recommended the cessation of any discrimination between United States citizens and residents and those who were neither citizens of nor resident in the country, when it comes to privacy safeguards and remedies, and action by Congress to introduce new legislation that treated mass surveillance as disproportionate and unnecessary in a democratic society.

61. The Special Rapporteur has also made other recommendations concerning security and surveillance in his annual reports to the Human Rights Council.

**Achievements**

62. The Special Rapporteur has reported emerging obstacles in his annual reports to the General Assembly and to the Human Rights Council (between 2015 and 2017) and in communications concerning violations of the right to privacy by member States.

63. The Special Rapporteur has responded to these obstacles by engaging in advocacy with Governments in order to address initiatives and programmes that could violate the right to privacy; the creation of task forces on the thematic action streams; the promotion of "privacy by design" among technology companies; the development of a draft legal instrument on Government-led surveillance (see part II); public consultations; participation in international events; and the publication of papers.

64. The Special Rapporteur has submitted the following proposals and recommendations, some of which have been outlined above: a 10-point action plan, 2015;

[18] Submission to the Parliament of Australia, Parliamentary Joint Committee on Intelligence and Security, inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, 24 January 2018.

[19] Confidential, pending expiration of a 60-day-response deadline.

the priorities of the mandate (thematic action streams), 2016; and the preliminary recommendations in his end-of-mission statement on his official visit to the United States, 2017, and those on Government-led surveillance (A/HRC/34/60) and Big Data and Open Data, 2017 (A/72/540).

**Future activities and opportunities**

65. The Special Rapporteur will present his final report on his official visit to the United States in March 2019, focusing on existing oversight mechanisms in situations in which Executive Order 12333 applies. The report on his official visit to France is due in March 2019.

66. The report of the Special Rapporteur on privacy and health data will be presented to the General Assembly in October 2018.

67. Following international consultations in mid-2018, the final proposals and recommendations of the Special Rapporteur on big data and open data will be released.

## 4. Contributing to international events to promote a systematic and coherent approach to the right to privacy

**Activities**

68. The Special Rapporteur has spoken at many events, including as a keynote speaker, thereby reaching key stakeholders and generating wide media coverage.

69. An ongoing strategic contribution of the mandate holder is his cooperation with the International Conference of Data Protection and Privacy Commissioners. On 19 and 20 February 2018, the Special Rapporteur presented and moderated a session for OHCHR at the expert workshop on the right to privacy in the digital age. A report on this workshop will be submitted to the Human Rights Council at its thirty-ninth session (in accordance with its resolution 34/7).

70. The Special Rapporteur is implementing his 10-point action plan, which was presented to the Human Rights Council in March 2016 and which comprises (see A/HRC/31/64, paras. 45–55):

(a) Research and consultations on protecting the right to privacy in the digital age, highlighting the need to increase the protection of the right to privacy of children and young persons, and privacy and gender issues;

(b) Awareness-raising efforts, such as the Asia Pacific Privacy Authorities' Privacy Awareness Week, and other events for community members, regulators and public and private sector organizations;

(c) Structured dialogue about privacy in security and surveillance, including NGOs, data protection and privacy commissioners, law enforcement agencies and security and intelligence services as interlocutors;

(d) Comprehensive approaches to legal, procedural and operational safeguards and remedies: for example, the draft legal instrument and the amicus curiae brief mentioned above;

(e) Technical safeguards discussed with the General Assembly in October 2017 and an ongoing engagement with the technical community to promote effective technical safeguards;

(f) Dialogue with the corporate sector, as outlined above;

(g) Promoting national and regional developments in privacy-protection mechanisms: the Special Rapporteur emphasizes the value at the global level of national

and regional developments in privacy-protection mechanisms.[20] The contact with privacy and data protection authorities worldwide facilitates this promotion;

(h) Cooperation with civil society. The Special Rapporteur met with 40 NGOs during his first six months in office and continues to engage with them through the work of the thematic task forces; meetings; and public events, such as those on privacy, personality and flows of information;

(i) Cyberspace, cyberprivacy, cyberespionage, cyberwar and cyberpeace: these issues regularly feature in the Special Rapporteur's reports as evidenced in the work of the thematic action stream on security and surveillance. Also of relevance is cyberviolence against the more vulnerable, including domestic violence enabled by digital devices, non-consensual distribution of intimate images and risks to the privacy of young children;

(j) Promoting the development of international law. In December 2017, the Special Rapporteur collaborated with the Harvard Law School's Cyberlaw Clinic to file an amicus curiae brief at the United States Supreme Court in respect of the Microsoft case, mentioned above, due to its potential impact upon international law (see appendix 6). On 24 August 2017, the Supreme Court of India handed down its decision in the important constitutional case of *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, ruling unanimously that privacy is a constitutionally protected right in India. This landmark case may lead to constitutional challenges to other Indian legislation[21] affecting gender matters, which the Special Rapporteur will monitor closely.

**Achievements**

71. The Special Rapporteur has delivered more than a hundred addresses since March 2015 to promote the protection of the right to privacy (see appendix 5); created a blog on privacy and personality (www.privacyandpersonality.org); submitted an amicus curiae brief to the United States Supreme Court; provided feedback to the consultation of the Government of the United Kingdom on the Investigatory Powers Act 2016 and proposed a response to the ruling of the Court of Justice of the European Union; provided submissions to the Australian Parliament's inquiry into the impact of information and communication technology advances on law enforcement agencies, and the inquiry on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017; provided input to the Government of India on the White Paper on a data protection framework; and collaborated with the Harvard Law School's Cyberlaw Clinic.

**Future activities and opportunities**

72. The Special Rapporteur will continue to contribute to and organize international events, such as the conferences on privacy and personality and flows of information, and examine landmark court decisions concerning privacy and personality, including gender issues.

## 5. Raising awareness on the right to privacy, including challenges and effective remedies

73. The Special Rapporteur has continued to raise awareness concerning the importance of promoting and protecting the right to privacy, with a view to particular challenges in the digital age, and the importance of providing individuals whose right to privacy has been violated with access to an effective remedy, consistent with international human rights obligations.

74. In mid-2016, the privacy of 1 in 10 citizens in one member State was put at risk when a database of supposedly de-identified health and pharmaceutical benefits usage data was publicly released. It was found possible to re-identify the practitioners and patients. The Special Rapporteur has written twice to the member State concerned. The

[20] For example, the Data Sharing (Government Sector) Act 2015 of New South Wales, Australia, which requires that data sharing be in compliance with the provisions of privacy legislation.

[21] See https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/.

correspondence remains confidential for 60 days. This matter is closely linked to the mandate's thematic action streams on big data and open data, and health data.

75. On 18 May 2017, the Special Rapporteur took the unusual step of publishing an open letter of allegation to the Government of Japan on the OHCHR website[22] and is now awaiting an invitation from the Government to engage in discussions regarding the standards of international human rights law.

76. On 19 July 2017, the Special Rapporteur issued, together with other special procedure mandate holders, a joint call on the Government of Mexico to carry out a transparent, independent and impartial investigation into allegations of monitoring and illegal surveillance against human rights defenders, social activists and journalists.[23]

77. The Special Rapporteur wrote to a member State concerning the lack of remedies available for an individual who had experienced a gross invasion of her privacy. The correspondence is published in the special procedures communications report.[24]

**Achievements**

78. The Special Rapporteur has continued to draw to the attention of States apparent deficiencies in the management of privacy and ensured that appropriate privacy issues are in the public domain.

**Future activities and opportunities**

79. The Special Rapporteur will seek remedies that are consistent with international obligations for complainants who raise allegations of violations of privacy, and continue working with member States and NGOs to identify and give a voice to complainants who do not have access to national remedies.

## 6. Integrating a gender perspective

**Activities**

80. The conceptualization of privacy as an essential right in itself, enabling the achievement of an overarching fundamental right to the free, unhindered development of personality, drives the Special Rapporteur's thematic work on privacy, personality and flows of information. This initiative commenced in July 2016 in New York with an event attended by 90 experts, regulators, corporations and civil society organizations spanning five continents.

81. The second such consultation, held for the Middle East and North Africa region on 25 and 26 May 2017 in Tunis, was supported by national data protection authorities. The event welcomed approximately 70 participants from Algeria, Egypt, Lebanon, Morocco, the Syrian Arab Republic, Tunisia and Qatar. An important contribution was the session dedicated to a gender perspective, which provided insights into the particular experiences of women.

82. The third consultation was held on 29 and 30 September 2017 in Hong Kong, China, during the International Conference of Data Protection and Privacy Commissioners, in cooperation with the Security, Technology and e-Privacy Research Group at the University of Groningen, the Netherlands, the Department of Information Policy and Governance at the University of Malta and the Managing Alternatives for Privacy, Property and Internet Governance project. Digital Asia Hub, the University of Hong Kong and the privacy commissioner for Hong Kong, China were the local partners and hosts. The event focused on developments and trends in Asia; with separate sessions dedicated to Asian traditions in privacy, surveillance and privacy in Asia; privacy and its relationship to other human rights in Asia; and gender and privacy in Asia.

[22] See www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf.

[23] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E.

[24] See www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx.

83. The fourth such consultation is planned for the first quarter of 2018 with session(s) dedicated to gender issues.

84. A matter of serious concern was raised with one member State, the legal system of which did not adequately provide a remedy for a woman whose genitalia were photographed without permission by a health-care worker on a personal telephone for no professional purpose, during a gynaecological procedure. The effect of this violation of privacy was severe, resulting in emotional, financial and family stress.

85. Another matter concerns the situation in which apparently lawful processes to communicate court proceedings appear to have unintended and differential consequences as regards privacy in matters concerning gender identity. The Special Rapporteur is currently examining the concerns raised.

86. During the official visit of the Special Rapporteur to the United States, a sex worker raised issues concerning the impact of the criminalization of prostitution on the right of sex workers to privacy. It appears that the rules on surveillance by law enforcement officials in cases of sex workers may need revision.[25]

87. Several joint communications in 2017 to States with other mandate holders concerned gender issues[26] and the object and purpose of resolution 34/7, in which the Human Rights Council stated that privacy enabled the development of an individual's personality.

88. The Special Rapporteur will be closely monitoring subsequent cases following the decision of the Supreme Court of India in the case of *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, which considered sexual orientation as an essential attribute of privacy.

89. The Special Rapporteur is keen to examine the impact of a loss of privacy. The proposal has been drafted but the resources have not yet been identified.

**Achievements**

90. The Special Rapporteur held consultations on privacy and gender within the thematic action streams, organized sessions on gender-related aspects of the right to privacy during the three consultations on privacy, personality and flows of information, promoted the exchange of stakeholder information on gender-related aspects of the right to privacy and raised certain matters with member States.

**Future activities and opportunities**

91. The fourth consultation event to be held in the first quarter of 2018 on privacy, personality and flows of information will include a session on the gender-related aspects of the right to privacy. The Special Rapporteur will continue to analyse court decisions as indicated above and conduct research on gender and the right to privacy.

## 7. Reporting on alleged violations, including challenges arising from new technologies

92. The Special Rapporteur has continued to report on the alleged violations of the right to privacy, including the challenges arising from new technologies, and drawn the attention of the Human Rights Council and the United Nations High Commissioner for Human Rights to the situations of particularly serious concern.

[25] See end-of-mission statement: www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

[26] Joint communications with other mandate holders to the Governments of Haiti (22 September 2017), Spain (12 October 2017) and Egypt (31 October 2017).

#### Activities

93. The matter described above by the Special Rapporteur regarding the grievous loss of privacy in a health setting is also relevant here as it involves the need for remedies for such cases.[27] Discussions continue with the State concerned.

#### Achievements

94. The Special Rapporteur has continued to draw the attention of the member States concerned to the allegations of violations of the right to privacy. The Special Rapporteur has also increased awareness within the Human Rights Council of violations of article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights.

#### Future activities and opportunities

95. The Special Rapporteur will continue to report on the alleged violations of the right to privacy and to work with member States to address matters of serious concern.

### 8. Annual reports to the Human Rights Council and to the General Assembly

96. In accordance with his mandate, the Special Rapporteur has reported annually to the Human Rights Council and to the General Assembly.

#### Annual reports to the Human Rights Council

97. The present report is the 2018 annual report to the Human Rights Council. It outlines the Special Rapporteur's activities since 2015; gives an account of the successful work on the protection of the right to privacy and on government surveillance; and analyses the mandate provided by the Human Rights Council.

98. The content of the two previous reports to the Council has been outlined above.

#### Annual reports to the General Assembly

99. In his 2017 annual report to the General Assembly, the Special Rapporteur provided a progress report on the thematic action streams and presented the interim report on big data and open data. The Special Rapporteur set out the proposed consultation process and referred to a matter in which publicly released de-identified health data were found to be susceptible to re-identification. This matter is being raised with the State concerned.

100. The content of the two previous reports to the General Assembly has been outlined above.

#### Future activities and opportunities

101. The Special Rapporteur will continue to provide annual reports outlining activities and emerging issues and to present the reports of the thematic action stream task forces as scheduled.

## B. Work of the Special Rapporteur in the priority area of security, surveillance and privacy

102. As OHCHR has stated, the right to privacy in recent years has attracted increasing attention from the General Assembly and human rights mechanisms, in particular with regard to the surveillance policies and practices of many Governments around the world. In 2013, the General Assembly adopted resolution 68/167, in which it expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must

[27] One remedy, a statutory tort of action for serious invasion of privacy, has been recommended by the various Law Reform Commissions of the State on eight separate occasions over the past decade.

also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. National oversight mechanisms, where they exist, are often ineffective as they fail to ensure transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.[28]

103. The terrorist attacks in Belgium, France, Germany and the United Kingdom created national, and sometimes international, approaches that gave priority to reactive and high-profile security responses over carefully nuanced ones that would take into account security interests and the responsibility to protect their citizens' privacy. During the period from 2016 to 2017, Belgium, Germany, the Netherlands, France and the United Kingdom, to mention just a few examples, introduced legislation the effectiveness, proportionality and scope of which varied considerably. There is not one piece of national surveillance legislation that is perfectly compliant with and respectful of international standards on the right to privacy.

104. Despite the momentum created by the revelations of Edward Snowden, privacy and surveillance are topics that few countries are keen to discuss. Civil society, academia and other stakeholders, including a growing number of Governments, have, however, expressed genuine interest in a proper, constructive, international discussion about privacy and surveillance.

105. Consistent with the action plans provided to the Human Rights Council in his first annual report and subsequent reports to the General Assembly, the Special Rapporteur has sought to respond to the concerns expressed by these different actors and to bridge the gap between them, through his convening of various forums for exchange and discussion. He has addressed the major privacy issue of surveillance in collaboration with member States, the European Union-supported Managing Alternatives for Privacy, Property and Internet Governance project and civil society organizations in order to avoid the duplication of efforts.

### 1. The path to an international legal instrument on surveillance and privacy

106. Research and discussions with public policy leaders, law enforcement and intelligence communities and civil society organizations indicated that an essential part of the solution in avoiding a surveillance society was a standard that would be useful both in national and international law.

107. Mindful of the concerns for the right to privacy held by the Human Rights Council and the General Assembly, the Special Rapporteur, in cooperation with the Managing Alternatives project, has held stakeholder consultations, which began in Washington, D.C. in 2015. Workshops were held in Malta and New York in 2016. Participants' thoughts, positions and suggestions were recorded in a document that took the form of a very rough draft of a legal instrument to be utilized for a wide range of purposes, whether as guidelines or as a model for national surveillance law, through to hard law, such as a multilateral international treaty on surveillance.

108. Encouraged by the support within the International Intelligence Oversight Forum, the Special Rapporteur and the Managing Alternatives project undertook further joint consultations on new legal measures in international law to improve the protection of privacy in response to growing surveillance, while also providing a common base for effective oversight of surveillance practices globally.

### 2. Development by an expert group

109. Following the joint meeting with the Work Package 4 Working Group on Internet Governance and Surveillance of the Managing Alternatives for Privacy, Property and Internet Governance project in Miami, United States, in February 2017, a revised draft was produced in March 2017.

[28] See www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

110. Encouraged by the positive reception to the idea of a legal instrument, the Special Rapporteur and the Managing Alternatives project consulted extensively worldwide during 2017. A working group composed of experts from civil society, the Managing Alternatives project and major Internet corporations workshopped the draft legal instrument and surveillance in May 2017 in Malta and in September 2017 in Paris with some 50 experts. The event in Paris was followed by a consultation with law enforcement practitioners at the headquarters of the International Criminal Police Organization (INTERPOL) on 15 September 2017 in Lyon, France.

111. The outcomes of the meetings in Paris and Lyon and the revised draft instrument were circulated at the International Intelligence Oversight Forum on 20 and 21 November 2017 in Brussels. This allowed intelligence oversight authorities and intelligence practitioners to comment on the draft legal instrument and the idea of an international panel of judges and an international data access warrant.

112. These consultations and other measures produced a text sufficiently mature for wider public consultation during 2018. The draft legal instrument was made available online in early January 2018, which coincided with the first public discussion between 17 and 19 January 2018 in Rome.

113. The current draft legal instrument on Government-led surveillance and privacy covers the general principles and basic requirements thereof, covering application, scope, rights, systems and data, multi-stakeholder collaboration and mechanisms for transboundary access to personal data (see appendix 7 to the present report).

### 3. Preliminary options within Internet governance for an international legal instrument on government surveillance

114. There is no question that the global community needs to undertake urgent action to effectively respect and implement article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights by developing a clear and comprehensive legal framework on privacy and surveillance in cyberspace, to operationalize the respect of this right, nationally and across borders. While international human rights law provides high-level universal rules for the protection of the right to privacy, it lacks the level of detail that would constitute the comprehensive legal framework essential to provide adequate protection in a number of applied contexts, including those of national and extraterritorial surveillance. Most regions in the world lack enforcement mechanisms, such as those created over the past 40 years in Europe and North America. Thus, the international legal framework would benefit from vastly increased detail, clarity and comprehensiveness, safeguards and remedies for the daily violations of the right to privacy occurring in cyberspace. The “devil is in the detail”.

115. The draft legal instrument has been complimented by many for its vision and comprehensiveness. Important stakeholders have encouraged its continued development. The recent (18–19 January 2018) consultation co-organized by the Special Rapporteur and the Managing Alternatives project in Rome raised a number of important considerations:

(a) The work achieved to date has identified issues and established potential standards and possible remedies for surveillance in cyberspace and should be publicly released as a tool to nurture thinking and discussion on the subject and provide a draft model for member States currently considering the introduction of legislation and institutional arrangements aimed at ensuring an effective oversight of intelligence activities;

(b) The current draft covers a wide number of issues, and there are strategic and tactical advantages in retaining its current form, but reducing it to two or more smaller instruments of more limited scope may facilitate their adoption;

(c) Strategies are required that address the short and longer term time frames required to achieve wide acceptance and sustainability of the instrument;

(d) An examination of the past development of legal instruments in the United Nations system reveals:

(i) Building international consensus on a legal instrument is a lengthy process;

(ii) Individual member States, regional groups and cross-regional alliances can all play a key role in the adoption of a legal instrument;

(iii) Civil society organizations have a crucial role in promoting the adoption of international legal instruments;

(iv) Even the most laudable initiatives face initial resistance.

(e) Regardless and independently of the work of the Special Rapporteur, the Managing Alternatives for Privacy, Property and Internet Governance project will present the current legal instrument as part of its Policy Brief and Road Map on Internet Governance to the European Commission by 30 April 2018, and eventually to the European Parliament and the European Council. The European Union might be the most appropriate regional grouping to eventually support a legal instrument on surveillance and privacy at the global level;

(f) Preliminary discussions indicate a stronger potential interest in the draft legal instrument in Latin America and Africa, but this needs further exploration and development;

(g) The feedback from stakeholders that participated in the successive consultations indicated:

(i) The regional and global law enforcement community, including the European Police Office and INTERPOL, have shown a strong interest in many of the provisions of the draft legal instrument, although they also indicated that considerable time (between two and three years) would be required for further detailed consultation within their communities;

(ii) Federations of bar associations and lawyers defending privacy cases for activists strongly support the draft legal instrument, including the proposed mechanisms, such as those for an international data access warrant;

(iii) The corporate community indicates a strong interest in the draft legal instrument, especially insofar as it reflects the principles publicly endorsed by the Reform Government Surveillance coalition;[29]

(iv) The intelligence communities indicate that there are some countries with advanced legislation that is 90 per cent in compliance with the current draft legal instrument. More work is required on the definition of targeted surveillance and the limited application of bulk surveillance to make these more practical and appropriate;

(v) The concerns of civil society have focused on the timing of the process, the risk that some States may hijack the text to dilute protections and the specific wording;

(vi) The European region is awaiting the outcomes of certain cases at the Court of Justice of the European Union and the European Court of Human Rights, which are expected in late 2018 or 2019. The outcomes may strengthen the interest of European groupings in a draft legal instrument, but these and other considerations are currently a brake on consensual progress. This may not ease before 2019 or 2021.

### 4. Surveillance-specific recommendations

116. The Human Rights Council should consider the content of appendix 7 in order to identify the issues and some of the solutions that may eventually be considered for inclusion in a future international legal instrument on privacy and surveillance.

117. Member States with an interest in a legal instrument that substantively advances the remedies and solutions aligned with those in appendix 7 should contact the Special

[29] See www.reformgovernmentsurveillance.com.

Rapporteur in order to further explore the options in taking these principles further at national, regional and international levels.

118. Given the timing considerations outlined above, the Special Rapporteur proposes to, if appropriate and timely, report with further recommendations to the Human Rights Council in March 2021.

## C. The capacity of the Special Rapporteur to submit individual communications

119. David Weissbrodt recounts the experience of the first thematic Special Rapporteur (on summary or arbitrary executions) when appealing for the attention of a State in a case. The relevant Government responded to the Special Rapporteur's communication by questioning his ability to make such an appeal.[30]

120. The Special Rapporteur on summary or arbitrary executions wrote to the Human Rights Commission, saying that the issue deserved further examination and he would be grateful for such guidance as the Commission may be able to offer on that question.[31] In that matter, the Commission not only renewed the mandate of the Special Rapporteur on summary or arbitrary executions at its subsequent annual sessions, but could be seen to conclude, as the Norwegian delegate put it, that such cases were within the mandate of the Special Rapporteur and should be included in future reports (Norway was the chief sponsor of the relevant resolution).[32]

121. The Special Rapporteur feels in good company since, during 2017 on two separate occasions, his ability to draw matters to the attention of States was questioned. Sending communications to member States and other stakeholders is an integral part of the core activities of all special procedure mandate holders. This well-documented and regulated procedure allows all mandate holders to intervene directly with Governments and other stakeholders on allegations of violations of human rights that come within their mandates by means of letters, which include urgent appeals and allegation letters, among others.[33]

122. The Special Rapporteur's decision to intervene in the matter regarding the taking of an unauthorized photograph (see para. 84 above) was in accordance with the Human Rights Council resolution establishing the mandate, which explicitly calls upon States to respond promptly to the mandate holder's urgent appeals and other communications.

# III. Conclusions

123. **The Special Rapporteur has used the means normally availed of by other Special Rapporteurs in promoting and protecting privacy, including urgent appeals and allegation letters addressed to States, following up individual complaints, participating in conferences and carrying out country visits, both formally and informally.**

124. **The Special Rapporteur has also developed several innovative means to fulfil his mandate, including: the annual International Intelligence Oversight Forum; the twice-yearly regional events on privacy, personality and flows of information (which have already been held in North America, the Middle East and North Africa and Asia, with Latin America next); and the thematic action stream Task Forces on Big Data and Open Data, Health Data and Privacy and Personality to provide a broader global approach to many issues surrounding privacy.**

[30] David Weissbrodt, "The three 'Theme' Special Rapporteurs of the UN Commission on Human Rights", *American Journal of International Law*, vol. 80, No. 3 (July 1986), pp. 685–699.

[31] E/CN.4/1986/21, at p. 100.

[32] Resolution 1986/36 of the Economic and Social Council.

[33] Special procedures of the Human Rights Council: see www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx.

125. **Acknowledging the seriousness of surveillance as a threat to the enjoyment of the right to privacy, the Special Rapporteur has co-led international efforts in developing a comprehensive international legal framework aimed at regulating surveillance in cyberspace, thus also advancing prospects for cyberpeace.**

126. **Special procedures constitute an important mechanism for the Human Rights Council to implement human rights norms and to develop standards.**[34] **Further developing international standards on the use of Government-led surveillance will enable the international community to guide and assess the use of such technology and practices. Standards for good and best practices are regularly examined in the International Intelligence Oversight Forum.**

127. **The Special Rapporteur believes that a legal instrument regulating surveillance in cyberspace, complementary to other instruments of existing cyberlaw, such as the Council of Europe Convention on Cybercrime, could provide concrete safeguards for privacy on the Internet (A/HRC/34/60 and A/72/540), while also resolving long-standing problems, such as jurisdiction in cyberspace. Work to date has been very successful and encouraging, but the support behind the actual form and content of the legal instrument is as yet still not sufficiently uniform to make a recommendation for the document, as it stands, to be immediately considered by the Human Rights Council. However, with continued effort and time, such a viable instrument could be submitted to the Council in the relatively near future, i.e. possibly even by 2021.**

128. **Special procedure mandate holders are independent experts and an important mechanism for the protection of human rights. Member States must fully accept and cooperate with their communications and enquiries, and cease questioning the legitimacy of their constructive criticism.**

# IV. Recommendations to the Human Rights Council

129. **The Human Rights Council should note the Special Rapporteur's achievements across the mandate through the thematic action streams, the consistency of those achievements with the plan contained in his first report to the Council, the next steps — including the proposal for an additional theme addressing the privacy of children — and the schedule of future thematic action stream reports.**

130. **The Council should note the progress towards international standards on Government-led surveillance, the innovative and successful creation of the International Intelligence Oversight Forum and the intention to develop an instrument in the medium term, which could be considered by the United Nations for its possible eventual development by member States and other interested stakeholders.**

131. **The Council should recommend to the General Assembly that fresh vigour be applied to all efforts by the United Nations to explore the intersection of privacy and security and State behaviour in cyberspace, in synergy with the Special Rapporteur on privacy, in a determined attempt to develop a more comprehensive legal framework for the Internet.**

# V. Guide to supporting documents

132. Due to space constraints, the following documents have been posted on the Special Rapporteur's website:

- Appendix 1: Mandate of the Special Rapporteur on the right to privacy

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix1.docx

[34] Weissbrodt, "The three 'Theme' Special Rapporteurs".

- Appendix 2: Graham Greenleaf, Data Privacy Laws 2017: 120 National Data Privacy Laws, including Indonesia And Turkey

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix2.docx

- Appendix 3: Special Rapporteur on the right to privacy's communications

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix3.docx

- Appendix 4: Interim Report and Preliminary Recommendations of Big Data Open Data Thematic Action Stream Taskforce

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix4.docx

- Appendix 5: Contribution to International Events 2015–2017

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix5.docx

- Appendix 6: Amicus Curiae to the United States Supreme Court in the Matter of the US Government Vs Microsoft Corporation.

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix6.pdf

- Appendix 7: Draft Legal Instrument on Government Led Surveillance

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix7.docx

- Appendix 8: Acknowledgements

http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix8.docx

# Annex

## Paper presented at Expert workshop on the right to privacy in the digital age

### Office of the High Commissioner for Human Rights

**Geneva, 19–20 February 2018**

1. Privacy is a fundamental human right recognized as such under international law. It is also a universal right, one which should be enjoyed everywhere by everybody, as such it should be respected everywhere by everybody, by States as well as by non-State actors, irrespective of the ethnicity, nationality, gender, religious, philosophical or political beliefs of any given individual or any other status. The recognition of the universal right to privacy is part of the set of fundamental norms established in the development of human rights law since World War II.

2. Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. These contexts may be as diverse as medical and health, insurance, statistics, national security, finance, police, social security, education and many others. Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context and an identification of safeguards that protect it, and remedies available to citizens which may be specific to that context. The devil, literally, is in the detail, and privacy requires very detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular context as well as the remedies that a citizen may resort to if his or her privacy is breached in that context. The importance of this level of detail is even greater in the case of privacy since there exists no universally accepted definition of privacy. In other words, people across the world have agreed that the right to privacy exists and that everybody is entitled to such a right but they have not spelt out precisely what the right is or what it entitles a person to in a wide variety of circumstances. This fact has both advantages and disadvantages: too narrow a definition of privacy would restrict its ability to be protected as circumstances and privacy-threats change and also as we develop our understanding of what constitutes privacy-infringing behaviour in a number of changing or new contexts.

3. The rules and remedies provided for at national law come together with those established under international law to constitute the international legal framework available for the protection of privacy. Those at the national level are most often to be found in an amalgam of principal and subsidiary legislation complemented by the case law of that particular country. The courts of all countries and especially those with constitutional competences interpret the extent — and occasionally the limits — of the right to privacy in accordance with their understanding of that country's constitution, the national law on privacy — if it exists — as well as, often enough, the precepts of international law on the subject. Very importantly, over the past forty years we have witnessed a huge growth in the impact of international law on national law in the sphere of privacy protection. We have seen the concerted development of international law at the regional level, most notably in Europe, which has then guided the development of national law and practices in diverse contexts where privacy may be threatened.

4. Moreover, privacy is not an absolute right. It is a qualified right. There exist a small number of very special occasions when limitations to the right to privacy may be introduced subject to a number of special measures which are normally best spelt out under international law as well as necessarily having a clear legal basis in domestic law. Some of these will be explored below in the context of security. The way that the right to privacy is qualified needs to be spelt out in great detail in a given context. If limitations to the right to privacy are not adequately defined the gaps in privacy protection will increase.

5. An additional but essential overall consideration is that constantly developing technologies pose important challenges for the protection of privacy: these technologies may reveal the most intimate behaviour, wishes, preferences and indeed the very thoughts of individuals in ways that previously were not possible. Smartphones, credit cards and the Internet are three good examples of the types of technology that bring significant new challenges to the protection of privacy.

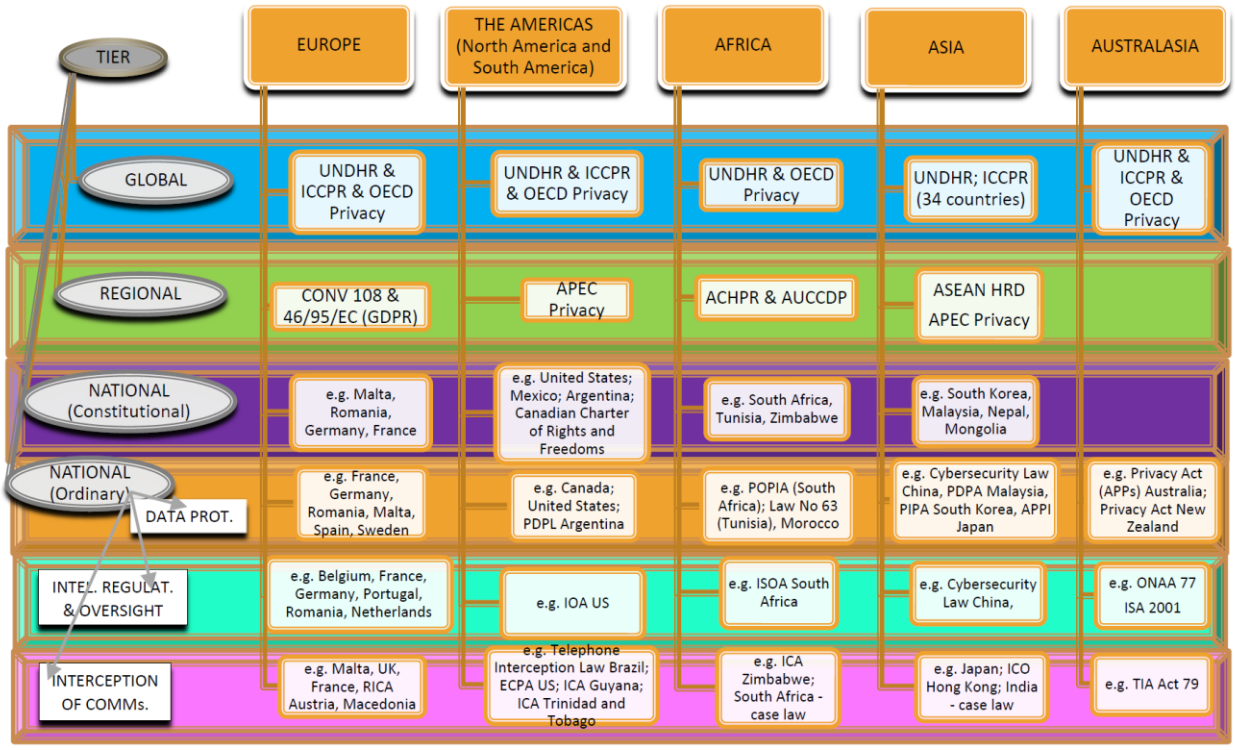
6. When dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that "whatever is protected off-line is protected on-line". That is a hopelessly inadequate approach to the protection of privacy in 2018. International law such as Art. 12 UDHR and Art 17 ICPPR only provides an answer to the question "Why?" as in "Why should we protect privacy" i.e. because we have agreed that it is a universal fundamental human right. They however do not provide answers to the questions: When? Which? What? How? Who? When should privacy be protected? How should privacy be protected? Which are the privacy-relevant safeguards to be created in a particular context? Which new contexts pose the greatest risks to privacy? What should be done to protect privacy in given circumstances? Which are the remedies most appropriate and possible in those cases where, despite all the safeguards provided, a breach of privacy still occurs? Who has special duties and obligations in the case of privacy protection, in which circumstances, what measures are the minimum to discharge these obligations and how should such persons be held accountable? The answers to these and other questions can only be found if the international and national legal framework is detailed enough.

7. Over the past fifty years some countries and some inter-governmental organizations have taken the initiative to develop their legal framework with respect to privacy but others have not. As a consequence, in 2018 more than a third of United Nations Member States have no privacy laws at all[1] while most of the other 125 states have laws which cover some of the contexts where privacy may be threatened but not all. Some important threats to privacy especially those arising in the context of national security, intelligence and surveillance are inadequately regulated in most countries of the world. International law, especially in the form of some regional initiatives, helps provide a level of co-ordinated response to some privacy threats for some countries but these remain, at best, a significant minority. The result is a patchwork quilt, in many places crocheted in stitches which are far too open to keep in the warmth and which, in any case, is not large enough to cover all of the bed. This patchwork quilt can in no way be characterized as a comprehensive and sufficiently detailed legal framework through which persons anywhere and everywhere can enjoy the universal right to privacy. It is the duty of the Special Rapporteur on the right to privacy, in conformity with his mandate, to identify the lack of a comprehensive, detailed and universal legal framework as a serious obstacle to the protection of the right to privacy world-wide. The rest of this paper, for reasons of time and space, mostly focuses on the lack of an adequate legal framework in two often-related contexts: national security and the prevention, detection, investigation and prosecution of crime but this is not to say that all other contexts are well served by the international legal framework.

**The current international legal framework**

8. The diagram below attempts to sketch out the international legal framework for the protection of privacy which exists so far:

[1] Though this does not exclude the possibility that their constitutional courts could be seized of privacy-related matters.




9. The diagram above is intended primarily to illustrate the tiered structure of the international legal framework but limitations of space do not permit one to clearly see that the tiers in Asia and Africa contain many more gaps and vacant spaces than those in Europe and North America. These gaps are however summarized in the overview text below.

**Gaps in protection from government-led surveillance.**

10. The surveillance of citizen behaviour on the internet can be broadly categorized into two main types: Government-led surveillance, and, surveillance or monitoring of citizens behaviour by private corporations that track citizens browsing, purchasing and other activities on the internet.

11. This overview analysis is focused on Government-led surveillance and the gaps in protection which currently exist in the international legal framework.

12. The surveillance and/or monitoring and/or profiling of citizens by corporations will be the subject of a separate report.

**What do we understand by a comprehensive legal framework?**

13. A comprehensive legal framework protecting citizens' privacy in cyberspace is one which provides both safeguards and remedies for all facets of the citizens' presence in cyberspace, irrespective of the fact if the threat to privacy comes from inside that citizen's country or from outside it.

14. Tension has continued to build up in cyberspace, with the privacy of many responsible citizens being put at risk by the behaviour of State actors in the form of cyber-surveillance, cyber-espionage and elements of cyber-war.

**Problem Statement**

15. In cyberspace, the citizen may be surveyed in both a domestic situation by his or her own Government, or else in a transboundary/transnational situation by a Government which is not his/her own. The case studies referenced below outline a fraction of some of the ways in which a citizen in one country finds him/herself subject to infringement of their privacy by their own Government or another State actor.

16. Where a citizen is subject to surveillance by his/her own Government then the safeguards and remedies must normally be sought within domestic law. Where a citizen is subject to surveillance by a State which is not his own, obligations of both the State conducting the surveillance and the State where that person is physically located are relevant; yet a remedy becomes harder to seek, because in practice most states accord the citizens of other States a lower level of protection than that accorded to their own citizens, in breach of the prohibition of discrimination found in articles 4, and 26 of the ICCPR.

17. For individuals not to suffer interferences in their right to privacy, they firstly need to benefit from safeguards which exist within domestic law, in other words, their Government should be subject to a whole set of regulatory procedures provided for by the law of that State, and which would include precautionary measures designed to ensure that surveillance cannot be initiated until or unless, it is proven to an independent and competent authority that this surveillance is legal, necessary and proportionate to objective pursued, "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UDHR, Art. 29(2).

**Summary overview of protection gaps**

18. In summary: the United Nations has 193 sovereign Member States and two non-member observer States, all of them capable of having their own independent systems/structures such as domestic legislation and data protection authorities.

19. More than 33 percent of United Nations Member States, i.e. over 70 countries, have no privacy law at all.

20. Out of the remaining 125 United Nations Member States which do have one form of privacy law or another, (for an outline of these states please see article by Professor Graham Greenleaf in Appendix Two attached) less than 65 have certain key fundamental characteristics such as a truly independent data protection authority or truly strict enforceable safeguards and remedies. Thus, these laws are not homogeneous and the level of protection of privacy differs quite widely from one country to the next.

21. The types of laws mentioned in Graham Greenleaf's article are mostly those intended to cover the use of personal data by companies or state departments outside the law enforcement and national security sector. Most of them are therefore not intended to adequately and comprehensively cover the use of surveillance by intelligence agencies.

22. More than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance.

23. 100 percent of existing State legislations concerning the oversight of domestic intelligence within United Nations Member States require amendment and reinforcement.

24. 75 percent of United Nations Member States have no system of detailed safeguards or remedies to which they can readily turn to for cases of surveillance upon their citizens by other states. Even where remedies for citizens exist within the courts of those States, these courts often lack jurisdiction over the surveillance behaviour of other State actors.

25. 25 percent of United Nations Member States — those within the European region encompassed by the Council of Europe, have agreed to a basic principle in the application of privacy law to state security: by agreeing to Article 9 of Convention 108 they have accepted that measures can only limit the right to privacy where these measures are provided for by law and are necessary and proportionate in a democratic society.

26. This however means that it is only the very highest principles that have been agreed to, even in European states with more developed legislation on the right to privacy and this is mostly applied in the case of domestic intelligence. The situation relating to foreign intelligence is much more fluid, elastic. What actually constitutes a necessary and proportionate measure in a democratic society then needs to be translated into very detailed legislation and this is still very much work-in-progress all across Europe. Belgium, the Netherlands and the United Kingdom are some of the European states currently reviewing

their legislation in order to improve compliance with basic principles in a detailed manner. France has done so in 2015 but intends to re-visit its legislative framework in the near future.

27. Even where legislation exists regarding the oversight of intelligence it is often largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases.

28. In the absence of more detailed regulation, several United Nations Member States have to rely on their existing legislative and judicial frameworks, often at the national constitutional or the regional level in order to develop remedies and safeguards on the hoof. This works slowly but relatively well at the European levels where the European Court of Justice and the European Court of Human Rights often have pan European reach with their judgments about surveillance and privacy.[2] This however is not a completely satisfactory solution since it is one ex post. Very preferably citizens wish to have their privacy protection provided ex ante and this, especially to protect themselves against or minimize intrusion. In order to resolve problems of jurisdiction in cyberspace, this can be only provided by detailed international law which does not yet exist in the surveillance sector, including in the European region. If the remedies are unclear and imperfect in Europe where the European Court of Human Rights has relatively worked well with over 100,000 cases decided since it was established in 1959, the situation outside Europe is even more concerning. In the Americas, the Inter-American Court of Justice established in 1979 has cross-country reach, as so has in in Africa the recently set-up (2006) African Court for Human and People's Rights. Both courts strive but struggle. The United States signed but never ratified the American Convention on Human Rights and, unlike the European human rights system, individual citizens of Member States of the Organization of American States cannot take their cases directly to the Inter-American Court, having to refer first to the Inter-American Commission on Human Rights. Likewise, only seven African states have signed the protocol empowering their regional court to receive petitions from non-governmental organizations and individuals. These limitations substantially weaken the reach of these regional courts. Moreover, in Asia or the Pacific there is no regional court to turn for infringements of privacy whether caused by domestic intelligence or foreign intelligence.

29. The United Nations Human Rights Committee plays a very important role in the protection of human rights, but once again is largely an ex post forum and cannot be expected to provide in-depth regulation and governance structures, which are the required minimum adequate legal response to questions like transborder data flows and cross-border espionage and surveillance.

[2] *The Snowden revelations – 6 June 2013 –ongoing reverberations across Europe*

The revelations over mass surveillance and other privacy –intrusive programmes carried out by the signals intelligence arms of the United Kingdom and United States intelligence communities have not really receded. They have been followed by legislative changes in both countries, sometimes imposing more constraints and safeguards, on other occasions legitimizing existing practices. The unilateral nature of transborder forays by United States and/or United Kingdom agencies into Belgium, Brazil, France, Germany and other countries led to a great deal of concern which still finds its reverberations in various fora, international and otherwise. Both countries are still struggling to find the right formula to frame their behaviour in cyberspace such that, for example, the legislative measures of the United Kingdom would be found necessary and proportionate by either the European Court of Human Rights or the European Court of Justice. The United Kingdom's intelligence services were found to be in default on several counts by the UK's own Investigatory Powers Tribunal while the United Kingdom law on bulk collection of metadata has been declared disproportionate by the European Court of Justice on the 21st December 2016. An important decision in this respect is also being expected in a case first heard by the European Court of Human Rights on 7th November 2017, Big Brother Watch and Others v. the United Kingdom (no. 58170/13), Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14) and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15).

30. In order to better understand the protection needs in the privacy area, one has to take the Yahoo cases[3] cited below and ask "which ex ante safeguards should have been applied by which country in order to protect citizens in, say France, from having their Yahoo e-mail account privacy infringed and what ex post remedies are available to that same French citizen?" The answers to these questions can only be provided by a detailed international law regime which has yet to be worked out. The Human Rights Committee's interpretative advice of ICCPR's article 17 should be a last resort; it cannot be the primary mechanism designed to protect the privacy of billions of people who use the Internet on a daily basis.

[3] The following two cases are being cited for purposes of illustrating a problem area but are not here being represented as facts proving certain types of behaviour by the United States or Russian authorities. The Special Rapporteur on the right to privacy reserves the right to investigate these cases separately through Letters of Allegation and until doing so remains neutral on the accuracy or otherwise of media and governmental reports on the subject:

*Case 1: Privacy of 500 million Yahoo! users infringed – 15 March 2017*

Formal indictments were brought in the United States of America by the Justice Department, which announced on 15 March 2017 that the "indictments of two Russian spies and two criminal hackers in connection with the heist of 500 million Yahoo user accounts in 2014, marking the first United States criminal cyber charges ever against Russian government officials. The indictments target two members of the Russian intelligence agency FSB, and two hackers hired by the Russians. The charges include hacking, wire fraud, trade secret theft and economic espionage, according to officials."

While this case remains sub judice and therefore the evidence available has not yet had time to be exhaustively evaluated by the court in question, the nationality of the accused and the locus of the judicial proceedings are almost immaterial for the purposes of this observation. The point here is that the spread of the damage was global, possibly the largest or one of the largest intrusions in history on the private e-mail accounts of five hundred million Yahoo! users spread across the planet. If it transpires that the men indicted were not responsible after all, we are still left with the problem of the nature and scale of the attack in addition to the instability induced by public accusations made against Russia. If the guilt of the accused is eventually proved beyond reasonable doubt then the problem would be compounded by the involvement of state officials who may or may not have been acting on instructions. Either way the suspicion of their acting as agents of the Russian state is already a destabilising factor in international relations and threatening all forms of peace, above and beyond cyber-peace. The violation of the personal space of hundreds of millions of internet users has not, to date, attracted much attention but it remains a source of major concern to those involved, over and above the charges actually made in the indictment.

*Case 2: Privacy of 500 million (?) Yahoo! users breached by United States agency (reported 4th October 2016)*

If you're a Yahoo! e-mail user, if it's not one government hacking into your e-mail account or scanning your incoming e-mail, then it's another. Or at least un-contradicted media reports so suggest. For some time during the period 2014–2016, hundreds of millions of Yahoo! e-mail users apparently not only suffered the most massive hack in history as already mentioned above (allegedly by a combination of Russian criminal and state-connected persons) but also had their incoming mail scan-read on the orders of a United States Government agency. There are multiple causes for concern here. Firstly, all those Yahoo! users within the United States may arguably claim that such searches violated their Fourth Amendment rights under the United States constitution, although the scan-reading was carried out in terms of lower-level United States law (FISA). Secondly, it should be clear to all concerned that well more than half of those five hundred million Yahoo users are not United States citizens and would need to seek recourse elsewhere for protection of their fundamental and universal right to privacy…but where to do so is the obvious question. Even if this were ever to be considered a proportional measure – and that is a contentious point in its own right, unless there were to be an international agreement that this would constitute appropriate state behaviour in cyberspace, hundreds of millions of citizens world-wide yet again find themselves without any effective safeguards or remedies when it comes to their fundamental right to privacy.

31. Thus it should be glaringly evident from the above summary that huge gaps exist in the legal protection of privacy at both the national and international levels. Unless and until it will be possible for any citizen, anywhere, irrespective of passport held, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that "a clear and comprehensive legal framework exists". In order to create such a clear and comprehensive legal framework it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles to establish what state behaviour in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when.