



**Mandate of the Special Rapporteur on the right to privacy**

**Submission to OHCHR by the Special Rapporteur on the right to privacy, in connection with the workshop on "the right to privacy in the digital age"**

8 June 2018

Office of the High Commissioner for Human Rights

I write in relation to the report that the Office of the High Commissioner for Human Rights is drafting pursuant to Human Rights Council resolution 34/7 on "the right to privacy in the digital age". Paragraph 10 of the resolution requested the United Nations High Commissioner for Human Rights:

"to organize, before the thirty-seventh session of the Human Rights Council, an expert workshop with the purpose of identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard, to prepare a report thereon and to submit it to the Council at its thirty-ninth session."

I commend and support this initiative to better understand the right to privacy in the digital age as captured by this resolution, and the action the Office has set in train. Indeed, I attended the workshop in question and participated fully in all discussions, giving a keynote paper in one session and chairing another. I look forward to contributing further to the report, and to receive its expert input in my mandate's Taskforces, which are also examining various facets of the promotion and protection of the right to privacy in the digital age.

The matters I wish to raise in this letter however concern a document recently brought to my attention and dated 6 April 2018, submitted to the Office in the name of the Electronic Privacy Information Center (EPIC), an NGO based in the United States, in response to the public call for inputs that your Office made following the expert workshop. I note that, regrettably, it contains a section that provides inaccurate statements and impressions not only about the mandate provided to me by the Human Rights Council, but also about the role and procedures of Special Procedures. The relevant excerpt is appended separately as Annex I to this letter.

It is important to correct the inaccuracies in the document submitted, given the exigencies faced by Special Rapporteurs and the Office of the High Commissioner for Human Rights. Hence, I set down for the official record some of the substantive inaccuracies and omissions. In summary:

1. The document fails to take into account the true depth and extent of my work as Special Rapporteur as reflected in my annual reports to the Human Rights Council

and the General Assembly. The document fails to mention that the most significant portion of my mandate's work (at least 75-80 percent of the effort invested and as reflected in my reports and other publicly available material) is spent in areas of focus such as surveillance, Big Data and Open Data, Health data and the use of personal data by corporations. As a consequence, regrettably, the document dated on 6 April completely distorts and misrepresents the true focus and extent of the SRP mandate's activities;

2. My annual report to the Human Rights Council in March 2018 (A/HRC/37/62) is structured to show the full alignment of my work as Special Rapporteur, my priorities and actions, with the mandate contained in Human Rights Council's resolution 28/16. It also pays due attention to the issue of surveillance – the matter that led to the establishment of the mandate of Special Rapporteur on the right to privacy;
3. My annual report to the Human Rights Council in March 2017 (A/HRC/34/60) and to the General Assembly in October 2017 (A/72/43103) concerning the actions, consultations and areas of focus of my mandate are also ignored in the 6 April document submitted to your Office;
4. Special Procedures mandate holders, with the support of your Office, actively seek official country visits, which can only be conducted at the invitation of the receiving State. The 6 April document submitted to your office fails to take into account, even though I highlighted it in my most recent annual report, that I wrote to nine Member States seeking an invitation to conduct an official visit. I am concerned that the 06 April submission in question ignores the fact that the limited number of official visits by my mandate was caused by the refusal or delay in States to accept my requests to visit.
5. The 6 April 2018 submission cites a publication by one of its own co-authors referring readers to an article 'Urgent Mandate, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy' which was significantly dated and correspondingly inaccurate at the time of its publication in May 2017. It so transparently misrepresented the work of the SRP mandate to such an extent that it was not deemed then to be worthy of a public response and is even less so today;

I do not refute the need for scrutiny and accountability. On the contrary, I welcome scrutiny, but I also believe that the efforts of Special Procedures mandate holders and the Office need to be fairly presented and assessed, which the submission by EPIC fails to do.

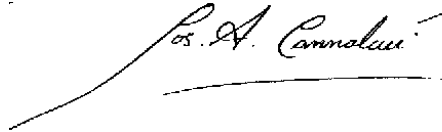
To date, I had chosen not to respond in other occasions when one of the co-authors of the EPIC report had chosen to criticize my mandate, publicly or otherwise, but, given the fact that their submission on 6 April will be included in the upcoming report on "the right to privacy on the digital age" currently being drafted by the Office, it is incumbent for me to correct its inaccuracies and direct attention to the true state of affairs as most recently summarised in my March 2018 report to the Human Rights Council, a copy of which is also attached as Annex Two.

A final consideration to be made is that the credibility of the 6 April document submitted to your office is not only completely demolished by its significant disregard of the facts extensively outlined in the SRP mandate's reports but is then further undermined by its failure to disclose that the primary author of the criticism of my mandate was a candidate

who, in 2015, failed to be short-listed for appointment to the position of Special Rapporteur on the right to Privacy.

I would be grateful if this document can be included with the rest of inputs submitted for the report, and I remain available for any additional information you may require

Respectfully,

A handwritten signature in black ink, reading "Joseph A. Cannataci". The signature is written in a cursive style and is positioned above a horizontal line.

Joseph A. Cannataci – Special Rapporteur on the right to privacy

Annex I: Extract from Submission to ‘Call for Submission on the Right to Privacy in the Digital Age.’

### III. Work of the Special Rapporteur on the Right to Privacy

We would also like to call attention to ongoing concerns about the work of the Special Rapporteur on the Right to Privacy. In 2015, the United Nations (UN) established a Special Rapporteur on the Right to Privacy (SRP) with a broad mandate to “protect” and “promote” the right to privacy set out in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).<sup>77</sup> The mandate set out the expectation that the Special Rapporteur would gather relevant information, make recommendations, raise awareness, report violations, identify emerging issues and report annually on his work. We believe the Special Rapporteur must align his activities with the mandate set out by the UN.

For instance, requirement (a) of the SRP’s mandate concerns “gather[ing] relevant information” on the state of the right to privacy, and requirement (g) of the SRP’s mandate concern calling attention to “alleged violations... of the right to privacy” or “situations of particularly serious concern.” One of the primary mechanisms for Special Rapporteurs to defending a human right is via country visits. Approaching the end of the three-year mandate, the SRP has conducted two country visits to two western nations: the United States and France.<sup>78</sup> He has issued no formal reports from these visits, reports which are often among the most valuable tools to highlight specific situations of concern. EPIC would like to use the opportunity of the OHCHR’s call for input to publicly urge the Special Rapporteur to call attention to the privacy practices of countries around the world, to prioritize finalizing a date for official country visits which have been requested, and to issue country reports on his completed visits promptly.

The SRP also continues to focus a significant portion of his work on what he has designated developing a “better understanding” of the right to privacy.<sup>79</sup> He asserts the “existence and usefulness of” Article 12 of the UDHR and Article 17 of the ICCPR are “seriously handicapped by the lack of a universally agreed and accepted definition of privacy.”<sup>80</sup> EPIC believes this pursuit runs contrary to the purpose of the mandate, particularly since a key responsibility of a UN Special Rapporteur is the vigorous promotion and protection of the right. International law and legal precedents have already defined a fundamental human right to privacy. Cornerstones of the modern right to privacy, set out in Article 12 of the UDHR and Article 17 of the ICCPR, must be preserved.

<sup>75</sup> *Id.*

<sup>76</sup> Harper Neidig, *Senate panel approves Trump's FTC nominees*, Hill (Feb. 28, 2018), <http://thehill.com/policy/technology/375991-senate-commerce-approves-trumps-ftc-nominees>.

<sup>77</sup> Human Rights Council Res. 28/16, U.N. Doc. A/HRS/RES/28/16 (Apr. 1, 2015).

<sup>78</sup> Press release, US could do more on privacy rights, UN rapporteur concludes after official visit (June 27, 2017), <http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=21806&LangID=E>; Press release, France’s leading role in the protection of privacy, despite remaining

concerns, says UN privacy expert (Nov. 17, 2017), <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22413&LangID=E>.

79

---

We described many of these and other concerns in a detailed review last year for the *European Data Protection Law Review*.<sup>80</sup> It remains our view that it is vitally important for the Rapporteur to pursue the mandate set out in the UN Resolution and specifically to seek to promote Article 12 of the UDHR and Article 17 of the ICCPR.

<sup>80</sup> Special Rapporteur on the right to privacy, Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, ¶¶ 21, 25, U.N. Doc. A/HRC/31/64 (Mar. 8, 2016).

<sup>81</sup> Marc Rotenberg, *Urgent Man- date, Unhurried Response: An Evaluation of the UN Special Rapporteur on the Right to Privacy*, 3 Eur. Data Protection L. Rev. 47 (2017).

**ANNEX Two**

**Report of the Special Rapporteur on the right to Privacy to the Human Rights Council  
presented on 07 March 2018**

A/HRC/37/62

---

**Advance unedited version**

Distr.: General  
28 February 2018

Original: English

---

**Human Rights Council**

**Thirty-seventh session**

26 February to 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 this 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 mandate of Special Procedures mandate holders.

---

\* The present report was submitted after the deadline in order to reflect the most recent information.

A/HRC/37/62

---

## Contents

	<i>Page</i>
I. Introduction .....	3
II. The mandate of the Special Rapporteur on the right to privacy .....	4
A. Performance of the mandate 2015-2017 .....	4
B. Work of the Special Rapporteur in the Priority Area ‘Security, Surveillance and Privacy’ .....	18
C. The mandate of the Special Rapporteur on the right to privacy .....	21
III. Conclusions .....	21
IV. Recommendations to the Human Rights Council .....	22
V. Guide to supporting documents .....	23
Annex** .....	24

---

\*\* Reproduced as received, in the language of submission only.



## 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,<sup>1</sup> the Special Rapporteur reports annually to the Human Rights Council and the General Assembly.

2. This report is the Special Rapporteur's third report to the Human Rights 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 activities and achievements as well as elicit some of the lessons learned, and look at the present and the future of the mandate.

3. With this aim in mind, the report is composed of four parts. Following the Introduction, the Special Rapporteur's activities, the achievements and future work are described for each of the eight mandate areas. The third part outlines the successful work undertaken on one of the mandate's key priorities: privacy protection and government and other forms of surveillance. It describes a draft international legal instrument for surveillance, as well as a set of recommendations to be considered. The fourth and final part addresses the terms of the mandate provided by the Human Rights Council to Special Rapporteurs 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<sup>2</sup> and regional<sup>3</sup> levels, and in other human rights instruments,<sup>4</sup> the importance of privacy has been re-affirmed by the Human Rights Council in the resolution consistently with the issue raised on personality in the Special Rapporteur's 2016 report to the Human Rights Council:

“Recognizing that the right to privacy can 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 noting 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...”<sup>5</sup>

5. In his work, the Special Rapporteur is guided not only by the international legal framework on the right to privacy, but also on the resolutions regularly adopted on the topic by the Human Rights Council, including A/HRC/RES/34/7 above.

<sup>1</sup> <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx>; A/HRC/31/64; <https://www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations>.

<sup>2</sup> Universal Declaration on Human Rights: Article 12; International Covenant on Civil and Political Rights: Article 17; Convention on the Rights of the Child: Article 16; International Convention on the Protection of All Migrant Workers and Members of Their Families: Article 14 <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx>.

<sup>3</sup> European Convention for the Protection of Human Rights and Fundamental Freedoms: Article 8; American Convention on Human Rights: Article 11 at <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx>.

<sup>4</sup> For example, the Cairo Declaration on Human Rights in Islam: Article 18; Arab Charter on Human Rights: Articles 16 and 21; African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa; African Charter on the Rights and Welfare of the Child: Article 19; Human Rights Declaration of the Association of Southeast Asian Nations: Article 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 Recommendation No. R(99) 5 for the protection of privacy on the Internet, and the European Union Data Protection Directive.

<sup>5</sup> Human Rights Council Resolution A/HRC/RES/34/7.

## II. The mandate of the Special Rapporteur on the right to privacy

6. Activities conducted by the Special Rapporteur typically relate to more than one area of his mandate, so matters are reported under several mandate areas. The mandate terms are at Appendix 1.

### A. Performance of the mandate 2015-2017

#### 1. Gathering relevant information and study matters

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

8. To meet this first aim, the Special Rapporteur has established five Thematic Action Stream (TAS) and utilizes the tools of official country visits, consultations, liaison with non-governmental organizations, examination of matters brought to his attention, letters of allegations, public privacy debates, international conferences and promotional events such as the Asia Pacific Privacy Authorities' annual Privacy Awareness Week, and other means to study relevant matters.

#### Thematic Action Streams

9. The Special Rapporteur outlined his work plan in 2016 in his reports to the Human Rights Council and the General Assembly. He invited all stakeholders to engage in "Planned thematic reports and call for consultations", all of which relate to the five Thematic Action Streams (TAS).

10. The five TAS 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 Taskforce to build on the work of the others. For example, the Big Data Taskforce sets the scene for the 'Health Data' and 'Use of Personal Data by Corporations' Thematic Action Streams. Each Taskforce is co-ordinated by a Chairperson 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 best practices safeguards regarding surveillance on the internet, the Special Rapporteur created the International Intelligence Oversight Forum (IIOF) - an annual gathering of national agencies and parliamentary committees tasked with the oversight of domestic and foreign intelligence in their respective countries. The IIOF serves as a platform to share information, exchange experiences and identify best practices at an international level.

12. The IIOF has been an unqualified success. The organizing committee membership is refreshed regularly. Its 2016 edition 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. Its 2017 edition was held in the Belgian Parliament with the support of data protection authorities of Belgium, Luxembourg and Netherlands: 80 delegates from 30 countries participated. The 2018 edition is scheduled to take place in Portugal in autumn. Oversight authorities of several countries are increasingly co-owners of the process, and are working towards the identification of issues and remedies in intelligence oversight as a collective international concern, responding to a latent need and leading to the adoption of best practices important for the protection of privacy.

13. It is precisely the intersection of privacy with 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 Snowden revelations ongoing since June 2013. The Special Rapporteur shares the impressions of the Chair of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) who, in October 2017 *inter alia* noted the following:

“Recommendation by experts about “raising awareness about the link between international peace and security, human rights and development as it applies to the ICT environment”.

“Sharing lessons and practices in countering the use of ICTs 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 ICTs 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. Experts stressed that in this States should consider their commitment to and respect for and protection of human rights and fundamental freedoms”.

Experts offered various recommendations to support implementation of the voluntary, non-binding norms for responsible State behavior presented in the 2015 GGE report (A/70/174) *inter alia* “States in ensuring the secure use of ICTs, should respect Human Rights Council resolution A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet) as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights including the right to freedom of expression” “Experts underscored that personal data held on, transmitted through or processed by ICTs 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 GGE to reach a consensus on a final report, the Special Rapporteur submits that the need is greater than ever to achieve synergy between all actors at the international level whose mandates touch upon the use of information and communication technologies where these involve personal data.

15. The Special Rapporteur consistently maintains that cyberpeace depends on States' willingness and ability to achieve synergy between security interests and privacy in cyberspace. Avoidance of cyberwar must therefore also contemplate measures to limit surveillance and other privacy-intrusive measures in cyberspace. As part of an effort to explore options for such measures, in synergy with the European Union-supported MAPPING (Managing Alternatives for Privacy, Property and Internet Governance) project<sup>6</sup>, the Special Rapporteur has explored options for a draft legal instrument on surveillance and privacy to strengthen standards and create protection mechanisms to address massive infringements of the privacy of people around the world.

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

(a) A set of principles and model provisions for their integration into national legislations embodying and enforcing the highest principles of international human rights law, especially the right to privacy, when it comes to surveillance;

<sup>6</sup> In IIOF as in events organized for example for Privacy & Personality Flows of Information, the Special Rapporteur receives logistical support from the University of Malta and the University of Groningen (STEP) and via joint events from the EU supported MAPPING project. Since 2014, the Special Rapporteur has been the overall scientific co-ordinator of the MAPPING project which deals with internet governance, privacy and intellectual property. Within this project which formally ends in February 2018, the Special Rapporteur is also personally responsible for internet governance with responsibility for privacy within that project, exercised by the Institute of Legal Informatics from Leibovitz University, Hanover, Germany.

A/HRC/37/62

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

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 states practice, as hard law as 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 a maturity where I can confidently assure the Human Rights Council that the instrument has unanimous or even 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 – Open Data was presented to the United Nations General Assembly in October 2017 as an introductory study identifying key issues. 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 the data privacy protections including a privacy impact assessment; and

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

19. Consultation is underway with a call for submissions closing 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 situations of de-identification failure.

**(c) Health Data**

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

21. All interested actors, States as well as other stakeholders, including non-governmental organizations 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 informed consent of the individuals concerned.<sup>7</sup> During the official visit to the United States in June 2017, meetings with corporations canvassed the way corporations react to requests from Governments regarding personal data they hold. The concerns of the Special Rapporteur regarding such requests led to the submission of an Amicus Curiae to the United States Supreme Court in late 2017.<sup>8</sup>

<sup>7</sup> <http://www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf>

<sup>8</sup> Amicus Curiae of the U.N. Special Rapporteur on the Right to Privacy Joseph Cannataci in support of neither party in Matter No. 17-2 Supreme Court United States UNITED STATES OF AMERICA, Petitioner, v. MICROSOFT CORPORATION, Respondent. On Writ Of Certiorari To The United States Court Of Appeals For The Second Circuit, filed 13 December 2017.

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 assisting the Thematic Action Stream Taskforce 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<sup>9</sup> is explored by the Taskforce on "A better understanding of privacy", chaired by Dr. Elizabeth Coombs (Australia), in consultations, communications received, 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 themed "Privacy, Personality & Information Flows". The first (Western countries) was held in July 2016 in New York. The second (Middle East and Northern Africa) was held in Tunisia in May 2017, the third (Asia) took place in September 2017 in Hong Kong, and the fourth (Latin America) is planned for May 2018.

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

(a) Examination of landmark decisions such as the Indian Supreme Court in 2017 in Justice K. S. Puttaswamy (Retd.) and Anr. vs Union of India And Ors. The judgment states: "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" [169];<sup>10</sup>

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

(c) Examining cyber-violence, with an emphasis on perspective gender-based analysis, and vulnerable sections of the community;<sup>11</sup>

(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. Official country visits dates and timing of country visits are negotiated with the Member States hosting the visits. Countries are selected largely on the basis of privacy-related developments.

27. Requests for official country visits in the period from 2015 to 2017:

<i>COUNTRY</i>	<i>REQUEST DATE</i>
Republic of Korea	31 March 2016
South Africa	31 March 2016
China	31 March 2016
United States	20 September 2016
India	21 October 2016
Germany	21 October 2016
United Kingdom	21 October 2016
France	29 November 2016
Argentina	20 December 2017

<sup>9</sup> UN Human Rights Council, Resolution (UN A/HRC/L.17/Rev – March 2017).

<sup>10</sup> [http://supremecourtsofindia.nic.in/pdf/jud/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtsofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf).

<sup>11</sup> Hadeel al-Alosi, Cyber-violence: digital abuse in the context of domestic violence, UNSW Law Journal Volume 40(4), pps 1573-1603.

A/HRC/37/62

<i>COUNTRY</i>	<i>REQUEST DATE</i>
Uruguay	8 January 2018

28. Delays in conducting country visits generally arise from Governments' late or non-responses to visit requests and circumstances which 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. The meeting schedule accordingly involves:

- (a) Official authorities, such as intelligence services, law enforcement, regulators/oversight authorities, and their responsible ministers;
- (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 priorities, as well as assessment 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 which 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 of America. 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 amongst 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 engagements took the Special Rapporteur to over 30 different cities, some in Asia, North Africa and Central America, with a fourth in the United States and over a half in Europe.

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

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

#### **Achievements**

33. Below are the thematic reports submitted to date:

- Security and Surveillance: "First approaches to a more privacy-friendly oversight of government surveillance", Human Rights Council, March 2017;
- Security and Surveillance, General Assembly, October 2017;
- Big Data – Open Data: "Interim Report", General Assembly, October 2017;

- Security and Surveillance: “Some preliminary options within Internet Governance for an international legal instrument on government surveillance”, Human Rights Council, March 2018.

### **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 is currently under consultation; and a draft legal instrument on surveillance and privacy that addresses issues identified.

35. The Special Rapporteur has held consultation events, such as the ‘2017 Privacy and Personality Flows of Information in Asia’ conference.

36. The Special Rapporteur has commenced the work of the Health Data Thematic Action Stream Taskforce.

37. The Special Rapporteur gathered support for the Taskforce on Use of Personal Data by Corporate Sector and the associated Amicus Curiae brief to the United States Supreme Court on the ‘Microsoft case’<sup>12</sup>.

### **Official country visits**

38. The Special Rapporteur has conducted two official country visits the United States of America (June 2017<sup>13</sup>) and France (November 2017<sup>14</sup>). 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. These have included events organized by the Irish Civil Liberties Council, the Japanese Civil Liberties Union, the Japan Federation of Bar Associations, the Northern Ireland Commission for Human Rights, multiple activities at the Internet Governance Forum, RightsCon, are a few examples.

### **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**

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

#### **(b) To the General Assembly**

- “Improving safeguards and remedies for privacy and health data”, General Assembly, October 2018;

<sup>12</sup> United States v. Microsoft Corp. (No. 17-2), see: <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22560&LangID=E>.

<sup>13</sup> End of mission statement: [http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/VisitUSA\\_EndStatementJune2017.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx).

<sup>14</sup> Preliminary findings: <http://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F>.

A/HRC/37/62

- “Profits and Privacy: the monetisation of personal data as a business model and the responsibilities of corporations”, October 2019;
- “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;
- “The transborder 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 - Open Data; health data; corporate use of personal information; 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); privacy issues in the digital age.

42. The Special Rapporteur’s next planned official visits are the United Kingdom (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 MAPPING conference held in Rome on 19-20 January, the Latin America Privacy, Personality and flows of information event planned to be held in May 2018 and the Health Data Taskforce consultation and the consultation on Big Data and Open data to be held in Australia in July 2018.

## 2. Seeking, receiving and responding to information

### Consultations

44. The Special Rapporteur exchanged information with officials and ministries and institutions of various Governments (at national and sub-national levels); data protection and privacy commissioners; the Chairperson of the European Union’s “Article 29 Working Party”<sup>15</sup>; the Chairperson of the Council of Europe’s Consultative Committee on Data Protection (T-PD); standards setting organizations, such as the International Telecommunication Union (ITU) and the Institute of Electrical and Electronics Engineers; civil society organizations; Permanent Missions to the United Nations in Geneva; other Special Procedures mandate holders, officials of the Office of the High Commissioner for Human Rights, 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 - a core constituency for his mandate. At the 2015 edition of the International Conference of Data Protection and Privacy Commissioners, the Special Rapporteur sought their feedback on the mandate’s ten-point plan. At the 2016 conference, the Special Rapporteur reported progress on the ten-point plan and, at the 2017 Conference in Hong Kong, China, he spoke and participated in parallel events and held his third “Privacy, Personality and Flows of Information” event complementing the Conference.

### Correspondence

46. The Special Rapporteur receives correspondence from various sources. Of those, only those received via the official registry of the Office of the High Commissioner for Human Rights are registered and counted, making it difficult to report the total number of communications received. Nevertheless, since the commencement of the mandate, the Office of the High Commissioner for Human Rights has registered the following correspondence received on behalf of the Special Rapporteur.

<sup>15</sup> Data Protection Working Party established by Article 29 of Directive 95/46/EC.



47. Registered Special Rapporteur correspondence 2015-2017<sup>16</sup>:

2015	2016	2017	Total
Not available	3	47	50

48. The disaggregation of the letters received by country or issue is not available, but in 2017 most of the correspondence was received from Permanent Missions, non-governmental organizations and international organizations.<sup>17</sup> These figures do not take into account the hundreds, possibly thousands, of other e-mail messages received at the mandate's official email address: srprivacy@ohchr.org.

**Achievements**

49. The International Conference of Data Protection and Privacy Commissioners adopted a Resolution on Co-operation with the United Nations Special Rapporteur on the right to privacy<sup>18</sup> in October 2015.

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

51. The Special Rapporteur identified and responded to emerging matters and 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 activities, emphasizing engagement with all stakeholders (particularly security and surveillance issues, including cyber security 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 Procedures mandate holders in 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 security and surveillance field as befitting the core issue leading 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, domestically and globally. An overview of the gaps identified in privacy protection may be found in the Annex.

54. In Big Data, information no longer needs to be 'personal' to identify an individual.<sup>19</sup> Technological capacities and data analytics only require information that 'lead to' an individual and their connections, to pose a threat to privacy.

55. The Thematic Action Streams are identifying contemporary obstacles to protecting and promoting the right to privacy, such as technologically based incursions in the health sphere; the smartphone in the witness box; cyber-based violence; differential vulnerability across communities; embedded gender and other biases in algorithms; government access of private sector data; facial recognition and other technological tools.

<sup>16</sup> Excludes emails sent to srprivacy@ohchr.org.

<sup>17</sup> Advice from OHCHR 19 December 2017.

<sup>18</sup> <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf>.

<sup>19</sup> 'Submission on the white paper of the committee of experts on a data protection framework for India', Graham Greenleaf AM FAAL, Professor of Law and Information Systems, UNSW Australia, January 2018, SSRN.

A/HRC/37/62

### **Responding to obstacles – promoting privacy**

56. For surveillance, the Special Rapporteur has embarked upon a strategy to build a consensus about 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 or 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 Indian Government, the United Kingdom Government and the Australian Parliament.<sup>20</sup> The Special Rapporteur also submitted letters expressing his concern, some of which remain confidential,<sup>21</sup> and some 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 - Open Data are in Appendix 4 to this 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 2008 Amendments Act of the 1978 Foreign Intelligence Surveillance Act); smart surveillance in urban environments and surveillance carried out for law enforcement purposes; Executive Order 12333 situations; personal data held by corporations; extending the protection provided by the 1996 Health Insurance Portability and Accountability Act to all health data; identity management of sex workers; the simplification of privacy; and fostering privacy-positive initiatives at State level. On surveillance, the Special Rapporteur recommended the cessation of any discrimination between United States citizens and residents and those who are neither citizens nor residents in the country, when it comes to privacy safeguards and remedies, and action by the United States Congress to introduce new legislation that treats 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 the Human Rights Council (2015-2017) and in communications concerning violations of the right to privacy by Member States.

63. The Special Rapporteur has responded to the obstacles to the enjoyment of the right to privacy through advocacy with Governments in order to address initiatives and programs that could violate the right to privacy; the creation of Thematic Action Stream Taskforces; 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 outlined above: Ten Point Action Plan, 2015; the Mandate Priorities (Thematic Action Streams), 2016; preliminary recommendations in the end of mission statement on his official

<sup>20</sup> Submission Australian Parliament, Joint Parliamentary Committee on Intelligence and Security, inquiry into National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, 24 January 2018.

<sup>21</sup> Confidential pending expiration of a 60-day response allowance.

United States visit, 2017<sup>22</sup> and those on Government led surveillance<sup>23</sup> and Big Data Open Data,<sup>24</sup> 2017.

#### **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 where Executive Order 12333 applies. His report on the official visit to France is due March 2019 as announced on the website.

66. Presentation of the report on privacy and health data to the General Assembly October 2018.

67. Submission of his final proposals and recommendations on Big Data and Open Data following international consultation in mid 2018.

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

##### **Activities**

68. The Special Rapporteur speaks at many events, including as keynote speaker thereby reaching key stakeholders, and widely reflected in the media.

69. An ongoing strategic contribution of the mandate holder is the cooperation with the International Conference of Data Protection and Privacy Commissioners. On 19-20 February 2018, the Special Rapporteur presented and moderated a session at the 'Expert workshop on the right to privacy in the digital age', for the Office of the High Commissioner for Human Rights. Following this workshop a report will go to the Human Rights Council's thirty-ninth session as per Human Rights Council (Resolution 34/7).

70. The Special Rapporteur is implementing his Ten Point Action Plan presented to the Human Rights Council in March 2016, comprising:<sup>25</sup>

(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 non-governmental organizations, data protection and privacy commissioners, law enforcement agencies and security and intelligence services as interlocutors;

(d) Comprehensive approach to legal, procedural and operational safeguards and remedies: for example, the draft legal instrument and the amicus curiae brief submitted in the United States v. Microsoft Corp. (No. 17-2) case;

(e) Technical safeguards discussed with the General Assembly, October 2017, and 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

<sup>22</sup> [http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/VisitUSA\\_EndStatementJune2017.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx).

<sup>23</sup> A/HRC/34/60.

<sup>24</sup> A/72/43103.

<sup>25</sup> See A/HRC/31/64, para. 46.

regional developments in privacy-protection mechanisms.<sup>26</sup> Contact with Privacy and data protection authorities world-wide facilitates this promotion;

(h) Cooperation with civil society. The Special Rapporteur met with 40 non-governmental organizations during his first six months in office and continues to engage via the work of Thematic Taskforces; meetings and in public events, such as Privacy and Personality Flows of Information;

(i) Cyberspace, Cyber-privacy, Cyber-espionage, 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 relevant is cyber-violence 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 late 2017, the Special Rapporteur collaborated with the Harvard University Cyberlaw Clinic to file an amicus curiae brief to the United States Supreme Court in the *United States v. Microsoft Corp.* (No. 17-2) case, due to its potential impact upon international law (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 Anr. vs Union Of India And Ors, ruling unanimously that privacy is a constitutionally protected right in India. This landmark case may lead to constitutional challenges to other Indian legislation<sup>27</sup> affecting gender matters, which the Special Rapporteur will monitor closely.

#### Achievements

71. The Special Rapporteur has delivered over 100 addresses since March 2015 promoting the protection of the right to privacy (Appendix 5); created a blog on privacy and personality ([www.privacyandpersonality.org](http://www.privacyandpersonality.org)); submitted an amicus curiae brief to the United States Supreme Court in the *United States v. Microsoft Corp.* (No. 17-2) matter (Appendix 6); provided feedback to the Consultation of the Government of the United Kingdom on the Investigatory Powers Act 2016 and Proposed 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 Indian Government on the White Paper on Data Protection legislation; and collaborated with the Harvard University Cyberlaw Clinic.

#### Future activities and opportunities

72. The Special Rapporteur will continue to contribute to and organize international events, such as the Privacy and Personality and Flows of Information conferences, 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 one in ten 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 practitioners and patients. The Special Rapporteur has written twice to the Member State concerned. The correspondence

<sup>26</sup> Eg *Data Sharing (Government Sector) Act 2015* NSW, Australia requiring data sharing within legislative privacy provisions.

<sup>27</sup> <https://inform.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/>.

remains confidential for 60 days. This matter is closely linked to the mandate's Thematic Action Streams: Big Data - 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 website of the Office of the High Commissioner for Human Rights<sup>28</sup> and is now awaiting an invitation from the Japanese Government to engage in discussions regarding standards of international human rights law.

76. On 19 July 2017, the Special Rapporteur issued, together with other Special Procedures 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.<sup>29</sup>

77. The Special Rapporteur wrote to a Member State concerning the lack of remedies available for an individual who experienced a gross invasion of her privacy. The Special Rapporteur had the consent of the complainant using the pseudonym requested. The correspondence is published in the Special Procedures communications report.<sup>30</sup>

#### **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 consistent with international obligations for complainants raising allegations of violations of privacy, continue working with Member States and non-governmental organizations to identify and give a voice to complainants who do not have access to domestic remedies.

### **6. Integrating a gender perspective**

#### **Activities**

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

81. Its second edition, held for the Middle East and North African region in Tunis on 25-26 May 2017, was supported by the national data protection authorities. The event welcomed 65-70 participants from Algeria, Egypt, Lebanon, Morocco, Syria, Tunisia and Qatar. An important contribution was the session dedicated to gender perspective which provided insights into the particular experiences of women.

82. The third edition was held in Hong Kong, China, on 29-30 September 2017 during the International Conference of Data Protection and Privacy Commissioners, in cooperation with the Security, Technology & e-Privacy Research Group (STeP) at the University of Groningen, Netherlands, the Department of Information Policy and Governance, University of Malta and the MAPPING Project (Managing Alternatives for Privacy, Property and Internet Governance). Digital Asia Hub, the University Hong Kong and the Hong Kong Data Protection Commissioner were local partners and hosts. This engagement 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.

<sup>28</sup> [http://www.ohchr.org/Documents/Issues/Privacy/OL\\_JPN.pdf](http://www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf).

<sup>29</sup> <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E>.

<sup>30</sup> <http://www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx>.

A/HRC/37/62

83. The fourth edition is planned for spring 2018 with session(s) dedicated to gender issues.

84. A matter of serious concern and raised with the State concerned, involves the legal system of one Member State, which does not adequately provide a remedy for a woman whose genitalia were photographed without permission by a healthcare worker on a personal phone for no professional purpose, during a gynecological procedure. The effect of this privacy incursion was severe, resulting in emotional, financial and family stress.

85. Another matter concerns the situation where apparently lawful processes for communication of court proceedings appear to have unintended and differential privacy consequences in gender identity matters. The Special Rapporteur is currently examining the concerns raised.

86. In the official visit to the United States, a sex worker raised issues concerning the impact of criminalization of prostitution on the right of sex workers to privacy. It appears the rules of engagement for surveillance by law enforcement in cases of sex workers may need revision.<sup>31</sup>

87. Joint communications to States with other mandate holders in 2017 concerned gender issues<sup>32</sup> and which relate to the advancing the intent of the Human Rights Council Resolution of 2017<sup>33</sup> stating privacy enables the development of the personality.

88. The Special Rapporteur will be closely monitoring subsequent cases following the Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors decision by the Indian Supreme Court which considered sexual orientation as an essential attribute of privacy.

89. The Special Rapporteur is keen to examine the impacts of loss of privacy. The proposal is drafted but resourcing has not been identified.

#### **Achievements**

90. The Special Rapporteur held consultations on privacy and gender within the Thematic Action Streams, held sessions on gender-related aspects of the right to privacy in the three Privacy, Personality and Flows of Information editions, promoted the exchange of stakeholder information working on gender-related aspects of the right to privacy, and raised certain matters with Member States.

#### **Future activities and opportunities**

91. The fourth edition of the Privacy, Personality and Flows of Information in spring 2018, which will include a session on gender-related aspects of the right to privacy. He will continue to analyze 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 reporting on alleged violations of the right to privacy, including challenges arising from new technologies, and drawn the attention of the Council and the High Commissioner for Human Rights to situations of particularly serious concern.

<sup>31</sup> 'Preliminary observations by the United Nations Special Rapporteur on the right to privacy at the end of his visit to the United States of America' at OHCHR website.

<sup>32</sup> Joint communications with other mandate holders to the Governments of Spain (12 October); Egypt (31 October); Haiti (22 September).

<sup>33</sup> UN A/HRC/L.17/Rev-March 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.<sup>34</sup> Discussions continue with the State concerned.

### **Achievements**

94. The Special Rapporteur has continued to draw the attention of relevant Member States to allegations of violations of the right to privacy. The Special Rapporteur has also increased awareness of the Human Rights Council on violations of article 12 of the UDHR and article 17 of the ICCPR.

### **Future activities and opportunities**

95. The Special Rapporteur will continue to report on 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 the General Assembly**

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

### **Annual reports to the Human Rights Council**

97. The 2018 report is before 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 analyzes the mandate provided by the Human Rights Council.

98. Previous points above have outlined the content of the reports to the Human Rights Council.

### **Annual reports to the General Assembly**

99. In his 2017 annual report, the Special Rapporteur provided a progress report on the thematic action streams and presented the "Big Data & Open Data" Interim Report.<sup>35</sup> The Special Rapporteur set out the proposed consultation process and referred to a matter where supposedly de-identified health data was publicly released but re-identification was possible. This matter is being raised with the State concerned.

100. Previous points above have outlined the content of the reports to the Human Rights Council.

### **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 Taskforces as per schedule.

## **B. Work of the Special Rapporteur in the priority area 'Security, Surveillance and Privacy'**

102. "The right to privacy in recent years has attracted increasing attention from the United Nations General Assembly and human rights mechanisms, in particular with regard to surveillance policies and practices of many governments across the globe. 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

<sup>34</sup> One remedy, a statutory tort of action for serious invasion of privacy has been recommended by various Law Reform Commissions of the State on eight separate occasions over the past decade.

<sup>35</sup> A/72/43103 and supporting document.

A/HRC/37/62

rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and called upon all States to respect and protect the right to privacy in digital communication. Domestic oversight mechanisms, where they exist, often are ineffective as they fail to ensure transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data.”<sup>36</sup>

103. The terrorist attacks in Belgium, France, Germany and the United Kingdom created national and sometimes international moods, which gave priority to reactive and high-profile security responses over carefully nuanced approaches 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 a few examples, introduced legislation whose effectiveness, proportionality and scope varies considerably. There is no one piece of national surveillance legislation 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 fora for exchange and discussions. He has addressed the major privacy issue of surveillance in collaboration with Member States, the European Union-supported MAPPING project<sup>37</sup> 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 is 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 MAPPING project, has held stakeholder consultations commencing 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 which took the form of a very rough draft of a legal instrument to be utilised for a wide range of purposes, whether as guidelines or model for domestic surveillance law, through to hard law such as a multilateral international treaty on surveillance.

108. Encouraged by the support within IIOF, the Special Rapporteur and the MAPPING project undertook further joint consultations on new legal measures at international law to improve the protection of privacy in response to growing surveillance, 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 MAPPING Work Package 4 Working Group on Internet Governance and Surveillance in Miami, United States, in February 2017, a revised draft was produced in March 2017.

110. Encouraged by the positive reception to the idea of a legal instrument, the Special Rapporteur and the MAPPING Project extensively consulted world-wide during 2017. A working group composed of experts from civil society, the MAPPING Project and major internet corporations workshopped the draft legal instrument and surveillance in Malta in

<sup>36</sup> <http://www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf> viewed 23/12/2017.

<sup>37</sup> <https://mappingtheinternet.eu/>.



May 2017 and in Paris, 13-14 September 2017 with some 50 experts. The Paris event was followed by a consultation with law enforcement practitioners at INTERPOL's headquarters in Lyon, France, on 15 September 2017.

111. The outcomes of the meetings in Paris and Lyon in September 2017 and the revised draft were circulated at the International Intelligence Oversight Forum in Brussels, 20- 21 November 2017. This allowed intelligence oversight authorities and intelligence practitioners to comment on the draft legal instrument and the notions 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 coinciding with the first public discussion in Rome on 17-19 January 2018.

113. The current draft legal instrument on government-led surveillance and privacy covers general principles and basic requirements for government-led surveillance covering application, scope, rights, systems and data, multi-stakeholder collaboration and mechanisms for transborder access to personal data (see Appendix 7 to this 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 UDHR and article 17 of the ICPPR by developing a clear and comprehensive legal framework on privacy and surveillance in cyberspace, to operationalise the respect of this right, domestically 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 which would constitute the comprehensive legal framework essential to provide adequate protection in a number of applied contexts including that of domestic and extra territorial 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-organised by the Special Rapporteur mandate with the MAPPING project in Rome, Italy raised a number of important considerations:

(a) The work achieved to date has identified issues, 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 timeframes required to achieve wide acceptance and sustainability of the instrument;

d. Examination of past development of legal instruments in the United Nations system reveal:

- Building international consensus on a legal instrument is a lengthy process;
- Individual Member States, regional groups and cross-regional alliances can all play a key role in the adoption of a legal instrument;
- Civil society organizations have a crucial role in promoting the adoption of international legal instruments;
- Even the most laudable initiatives face initial resistance.

A/HRC/37/62

e. Regardless and independently of the work of the Special Rapporteur, the MAPPING 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 would possibly be one of the first important regional groupings situated 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 in Africa, but this needs further exploration and development.

g. The feedback from stakeholders which participated in the successive consultations indicated:

- The regional and global law enforcement community, including EUROPOL and INTERPOL, have shown strong interest in many of the provisions of the draft legal instrument, but also indicated that considerable time (between two and three years) would be required for further detailed consultation within their communities;
- Federations of bar associations and lawyers defending privacy cases for activists very strongly support the draft legal instrument, including the proposed mechanisms such as those for International Data Access Warrant;
- 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;<sup>38</sup>
- The intelligence communities indicate there are some countries with advanced legislation that are 90 percent 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;
- 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 specific wording;
- The European region is awaiting the outcomes from some cases in the European Court of Justice 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 2019-2021.

#### 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 within a future international legal instrument on privacy and surveillance.

117. Member States with an interest in a legal instrument substantively advancing remedies and solutions aligned with those in Appendix 7 should contact the Special Rapporteur in order to further explore 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.

<sup>38</sup> <https://www.reformgovernmentsurveillance.com>.

### C. The mandate of the Special Rapporteur on the right to privacy

119. David Weissbrodt (1986) recounts the experience of the first thematic Special Rapporteur (the Special Rapporteur against summary or arbitrary executions) when appealing for the attention of a State to a case. The relevant government responded to the Rapporteur's communication by questioning the Special Rapporteur's ability to make such an appeal.<sup>39</sup>

120. The Special Rapporteur on summary or arbitrary executions wrote to the Human Rights Commission saying "this issue deserves further examination and he would be grateful for such guidance as the Commission may be able to offer on this question."<sup>40</sup> In that matter the Commission not only renewed the mandate of Special Rapporteur on summary or arbitrary executions in its subsequent annual sessions, but affirmed "such cases are within the Mandate of the Special Rapporteur and should be included in future reports."<sup>41</sup>

121. The Special Rapporteur feels in good company that during 2017, on two separate occasions, his mandate's 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 Procedures mandates. 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, allegations letters and other letters.<sup>42</sup>

122. The Special Rapporteur's decision to intervene in the matter described in par. 84 was made according to his mandate, which explicitly mentions the Special Rapporteur's capacity to bring upon States urgent appeals and other communications, and which calls upon all States to promptly respond to his 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 or Letters of Allegation to States, following up individual complaints, participating in conferences and carrying out country visits, both formal and informal.**

124. **The Special Rapporteur also developed several innovative means to fulfilling his mandate: including the annual International Intelligence Oversight Forum (IIOF); the twice-yearly regional events on Privacy, Personality and flows of Information (held in North America, Middle East and Northern Africa and Asia regions, with Latin America next); created the Thematic Action Streams 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.**

125. **Acknowledging the seriousness of surveillance as a threat to the enjoyment of the right to privacy, he 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 right norms and to develop standards.<sup>43</sup> Further developing international standards in the use of government-led surveillance will enable**

<sup>39</sup> Weissbrodt, D. 'The Three "Theme" Special Rapporteurs of the UN Commission on Human Rights', *The American Journal of International Law*, Vol 80, No. 3 (July 1986), pp685-599.

<sup>40</sup> UN Doc.E/CN.4/1986/2/ at 100.

<sup>41</sup> UNDoc.E/CN.4/1986/L.68 adopted without a vote 11 March 1986.

<sup>42</sup> Special Procedures of the Human Rights Council, <http://www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx>.

<sup>43</sup> Weissbrodt, D. 'The Three "Theme" Special Rapporteurs of the UN Commission on Human Rights', *The American Journal of International Law*, Vol 80, No. 3 (July 1986), pp685-599.

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 a legal instrument regulating surveillance in cyberspace, complementary to other pieces of existing cyberlaw such as the Convention on Cybercrime of the Council of Europe (CETS No.185), could provide concrete safeguards to privacy on the Internet,<sup>44</sup> while also resolving long-standing problems like 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 to date not sufficiently uniform to make a recommendation that the document as it stands should be immediately considered by the Human Rights Council. With continued effort and time, this is achievable and a viable option to place before the Human Rights Council in the relatively near future, i.e. possibly even by 2021.

128. Special Procedures 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 via Thematic Action Streams, the consistency with the plan in the Special Rapporteur's first report to the Human Rights 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 Human Rights Council should note the progress towards international standards on government-led surveillance, the innovative, 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 Human Rights Council should recommend to the General Assembly that fresh vigour be applied to all UN efforts exploring the intersection of privacy with security and state behaviour in cyberspace in synergy with the mandate of the UN Special Rapporteur on Privacy in a determined attempt to develop a more comprehensive legal framework for the Internet.

---

<sup>44</sup> See UN Special Rapporteur for Privacy, Annual Report, UN Human Rights Council in Geneva March 2017 and General Assembly, October, 2017 at [www.ohchr.org/Documents/Issues/Privacy/A\\_HRC\\_34\\_60\\_EN.docx](http://www.ohchr.org/Documents/Issues/Privacy/A_HRC_34_60_EN.docx).

---

## V. Guide to supporting documents

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](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix1.docx)
- 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/2018AnnualReportAppendix2.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix2.docx)
- Appendix 3: Special Rapporteur on the right to privacy's communications  
[http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/2018AnnualReportAppendix3.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix3.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/2018AnnualReportAppendix4.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix4.docx)
- Appendix 5: Contribution to International Events 2015 – 2017  
[http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/2018AnnualReportAppendix5.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix5.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/2018AnnualReportAppendix6.pdf](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf)
- Appendix 7: Draft Legal Instrument on Government Led Surveillance  
[http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/2018AnnualReportAppendix7.pdf](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf)
- Appendix 8: Acknowledgements  
[http://www.ohchr.org/Documents/Issues/Privacy/SR\\_Privacy/2018AnnualReportAppendix8.docx](http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix8.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 behavior, 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.

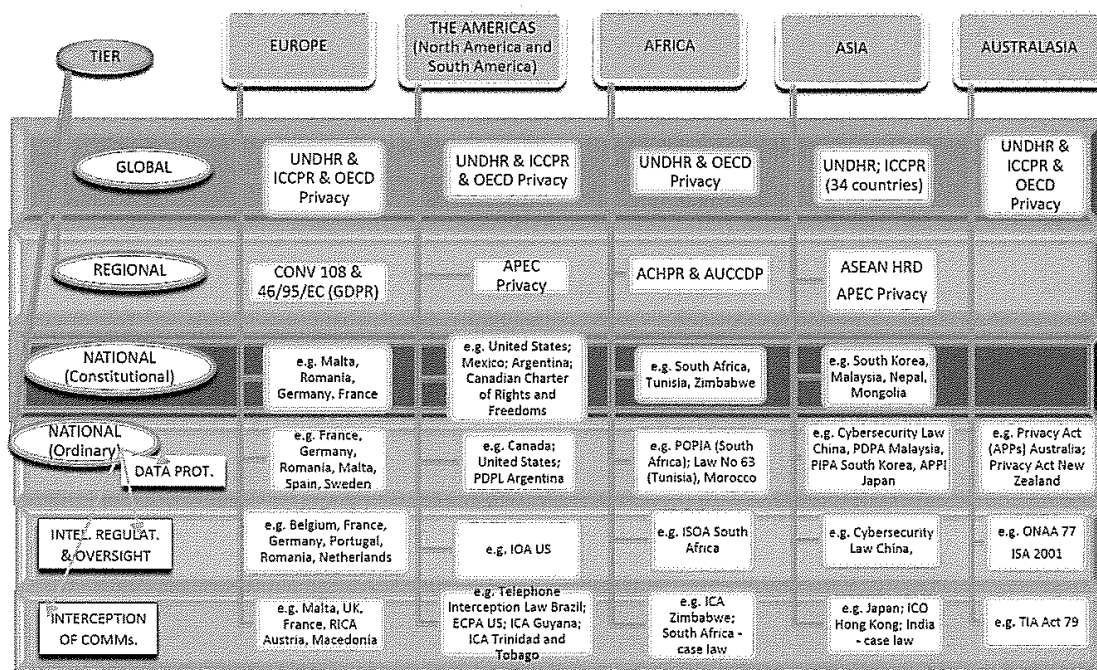
7. Over the past fifty years some countries and some inter-governmental organizations have taken the initiative to develop their legal framework with respect to privacy but others have not. As a consequence, in 2018 more than a third of United Nations Member States have no privacy laws at all<sup>45</sup> 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:

<sup>45</sup> Though this does not exclude the possibility that their constitutional courts could be seized of privacy-related matters.

A/HRC/37/62



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 behavior on the internet can be broadly categorized into two main types: Government-led surveillance, and, surveillance or monitoring of citizens behavior 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 behavior 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 surveilled in both a domestic situation by his or her own Government, or else in a transborder/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 behavior 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

A/HRC/37/62

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<sup>46</sup>. 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 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.

<sup>46</sup> *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<sup>47</sup> 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.

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

<sup>47</sup> 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.

*A/HRC/37/62*

---

principles to establish what state behavior in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when.

---