

**ADVANCE UNEDITED
VERSION**

Distr.: General
8 March 2016

Original: English

Human Rights Council

Thirty-first session

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,
Joseph A. Cannataci**

Note by the Secretariat

In the present report, submitted to the Human Rights Council pursuant to Council resolution 28/16, the Special Rapporteur on the right to privacy describes his vision for the mandate, his working methods and provides an insight into the state of privacy at the beginning of 2016 and a work plan for the first three years of the mandate

Contents

	<i>Page</i>
I. Introduction.....	3
II. Working methods of the SRP mandate.....	3
III. Initial observations on the state of Privacy as of early 2016	9
A. Definition and understanding	9
B. The SRP Privacy Landmark Events for 2015-2016	11
IV. Activities of the Special Rapporteur.....	15
V. A Ten Point action plan	18
VI. Conclusions.....	20
Annexes	
Annex I – Some challenges faced by the SRP & a vision of the mandate	22
Annex II – A more in-depth look at Open Data & Big Data	24
Annex III – Further reflections about the understanding of privacy	29
Annex IV – A “State of the Union” approach to Privacy	30

I. Introduction

1. The Human Rights Council established the mandate of the Special Rapporteur on privacy (SRP) in its resolution 28/16 (“The right to privacy in the digital age”). In the resolution the Council emphasizes that Human Rights need to be protected under all circumstances, at all times and in all environments. To achieve this is particularly challenging when it comes to the right to privacy. The rapid development of information technology provides not only new opportunities for social interaction but also raises concerns on how to develop the right further in order to face new challenges.

2. Pursuant to Human Rights Council resolution 28/16, the Special Rapporteur will report annually to the Council and to the General Assembly. In the present report, the Special Rapporteur describes the mandate’s working methods (Section II), the state of privacy in the year 2016 (Section III.), reports the highlight activities in carrying out the mandate up to this moment in time (Section IV.) and proposes a ten point plan which aims at discovering and further developing the new shape of the right to privacy in the 21st century (Section V.). Finally, the Special Rapporteur presents his conclusions (Section VI.).

3. The aims and objectives of this report must perforce be very modest. This first report should be understood as being a very preliminary one and should be taken in context: it is being prepared scarcely six months from the beginning of the mandate’s activities which commenced on 1st August 2015. As such, this initial six month period (most of the report was originally drafted by mid-January 2016) has not been sufficient to meet and consult in-depth with a satisfactorily wide spectrum of stakeholders although considerable effort has been invested in doing so with a significant amount of success. The primary aim of this report therefore is to reflect a period where it has been possible to identify a number of issues but not necessarily to definitively prioritise them. It is expected that the Special Rapporteur would be in a much better position to continue an on-going process of properly prioritising action required on issues some time during the next 6-12 months (January 2016-January 2017) after having had the opportunity to meet with and listen to the concerns of many more stakeholders all around the world. Some more reflections about the vision and the challenges facing the SRP are outlined in Annex I.

II. Working methods of the mandate

4. The SRP immediately set about building up the SRP team composed of persons working for the mandate on a part-time or full-time basis. One of these persons is currently a full-time United Nations (UN) Human rights officer, hired on a temporary contract, while the position is under recruitment. The work of this person is supervised by a more senior UN employee who is also responsible for supporting the work of six other mandate holders. A second part time professional and a part time administrative officer will soon be recruited, as well as a part-time consultant. The SRP is grateful that the Human Rights Council endowed his mandate with this still limited (given the scope of his mandate) but unprecedented level of support to a mandate holder. The other persons in the SRP team are not employed by the UN but are resourced by extra-mural funding obtained by the SRP or may be volunteers.¹ The team is often physically spread across at least three geographical

¹ The SRP is currently in negotiations with both NGOs and Data Protection Agencies which may be willing to second domain-specialists or other staff or otherwise provide resources to assist in the large quantity of complex work required by the mandate. It is expected that these negotiations will later

locations (currently Malta, the Netherlands and Switzerland) and, as befits the digital age, most of the team meetings are carried out in cyber-space with the working day being opened by an on-line conference call involving all team-members who may be available. During the “morning meeting” team members typically report on work carried out in the previous day, consult about tasks planned for the rest of the working day and plan tasks and events for the following weeks and months. When doing so, their tasks reflect the fact that the work of the SRP may be broadly divided into four categories and any team member may be working concurrently on tasks from each of these categories:

1. Country monitoring

5. A database of current policies, legislation, procedures and practices is being developed and populated with documents containing a variety of reports as well as copies of legislation. This database will enable the SRP to identify issues of concern, as well as best practices which could then be shared with others.

2. Thematic studies: analysis and assessment

6. In a world which benefits greatly from *an Internet without borders*, the SRP’s consultations indicate widespread support for a general principle of

- *Safeguards without borders*
- *Remedies across borders*

7. This concern with safeguards aimed at protecting privacy and remedies for privacy breaches underpins each of the following thematic study commenced by the SRP mandate in a number of sectors where risks to privacy appear high, and each of which is expected to eventually lead to an ad hoc report being produced reflecting an on-going process of consultations, interactions and observations:

(a) Privacy and Personality across cultures

8. This study responds to the crying need identified of achieving a better understanding of what privacy is or should be across cultures in 2016 in a way which makes the understanding of the right more relevant to a digital age where the internet operates without borders. In asking the question “Why privacy?” and positing privacy as an enabling right as opposed to being an end in itself, the SRP is pursuing an analysis of privacy as an essential right which enables the achievement of an over-arching fundamental right to the free, unhindered development of one’s personality. This analysis is being carried out in close co-operation with several NGOs and is expected to be the focus of a major international conference which will be organised in 2016. This analysis of privacy is being carried out in a wider context and one where its intersection with other fundamental rights is also being examined. Thus the relationship of privacy with freedom of expression and freedom to access publicly-held information is expected to be examined *inter alia* also through joint action with other UN Special Rapporteurs and discussions are already underway with the Special Rapporteur for Freedom of Expression in order to explore opportunities for joint action about this matter during 2016-2017.

expand to include UN member states and corporations who would likewise be willing to contribute additional resources to provide the capacity and ensure sustainability of work on privacy protection.

(b) *Corporate on-line business models and personal data use*

9. The first 25 years of the existence of the world-wide web have led to a largely unregulated organic growth of private corporations which have sometimes mushroomed into multinational entities operating across national borders and attracting customers from all across the world. One of the hallmarks of this growth has been the collection and use of all forms of personal data: every search, every read, every e-mail or other form of messaging, every product or service purchased leaves hundreds of thousands of electronic tracks about an individual which are capable of being aggregated into forming a very accurate profile of that individual's likes, dislikes, moods, financial capabilities, sexual preferences, medical condition, shopping patterns as well as the intellectual, political, religious and philosophical interests and sometimes even the relevant opinions of the netizen. In general, it should be questioned whether the offering of certain online services by certain service providers has to result necessarily in the tracking of the individual's behaviour to ensure just compensation. This increasingly detailed data-map of consumer behaviour has resulted in personal data becoming a commodity where access to such data or exploitation of such data in a variety of ways is now one of the world's largest industries generating revenues calculated in hundreds of billions most usually in the form of targeted advertising. Very often it would seem that while consumers may be aware of the user-generated content that they themselves consciously put on-line they are much less aware of the quantity, the quality and the specific uses of the metadata they generate when surfing, chatting, shopping and otherwise interacting on-line. The data available for the profiling of individuals is now in order of magnitude larger than it was in 1991-1992 and the extent of the risks for privacy associated with the use or mis-use of that data are not yet completely understood. There is some evidence that the commodification of personal data, especially in sectors traditionally considered to be sensitive such as that of medical and health data, has increased to an extent where the private individual is neither conscious nor consenting to the sale or multiple re-sales of his or her data. There is also not enough evidence available to properly assess the risk inherent in purportedly anonymised data which can be reverse-engineered in a way such to be linked to an identified or identifiable individual. Such a breach of privacy could potentially pose multiple risks to the individual citizen as well as to the community concerned especially if the access is unauthorised and carried out by state authorities intent on acquiring or retaining power, organised crime, commercial corporations acting illegitimately etc. In the early days of digital computers, one of the main concerns was the use of personal data by the state and the state's abilities to correlate data held in various sources to form a detailed picture of an individual's activities and assets. In 2016 it would seem that much more data is held on the individual by corporations than that held by the state. The vast revenues derived from the monetisation of personal data to the extent that it has become a marketable and tradable commodity mean that the incentive for changing the business model simply on account of privacy concerns is not very high. Indeed, it was only when recently risks to privacy threatened the income potential of the business model that some corporations took a stricter more privacy-friendly approach. It would seem opportune that a proper international discussion be held, informed by the collection of an appropriate evidence-base, in order to determine what type of information policy is most suitable to an approach which would maximise protection of and minimise risk to privacy of individual citizens in relation to the data collected about them by corporations. This discussion would be informed about the notions and expectations of privacy that citizens indicate and illustrate in the course of paragraph 8. It is expected that preliminary consultations commenced in 2015, would continue with on-line corporations throughout 2016 with a major public consultation event on this theme being planned for 2017.

(c) *Security, surveillance, proportionality and cyberpeace*

10. International concern with security remained at the forefront of developments throughout 2015-2016. The country monitoring process outlined in paragraph 8 above revealed several examples of legislation being rushed through national parliaments in an effort to legitimise the use of certain privacy-intrusive measures by security & intelligence services (SIS) and law enforcement agencies (LEAs) in those particular states. In many of these countries, though unfortunately not all, these legislative measures resulted in public debate about:

- (i) the adequacy of oversight mechanisms;
- (ii) the distinction between targeted surveillance and mass surveillance (or bulk surveillance as it is euphemistically called in some countries);
- (iii) the proportionality of such measures in a democratic society;
- (iv) the cost-effectiveness and the overall efficacy of such measures.

11. Countering terrorism and organised crime as well as other socially-sensitive offences such as paedophilia are the main declared aims of such legislation. Conflicting evidence has been given in these debates, often suggesting that privacy-intrusive measures and especially mass-surveillance will not result in greater security and that intelligence failures need to be addressed by other means. The SRP has continued a programme of continuous engagement with law enforcement agencies and security and intelligence services world-wide in an effort to better understand their legitimate concerns and recognise best practices which could be usefully shared as well as to identify policies, practices and legislation of doubtful usefulness or which present an unacceptable level of risk to privacy nationally and world-wide. In some instances this on-going analysis and assessment becomes almost inextricably entwined with issues of cyber-security and cyber-espionage where a small but growing number of states treat cyber-space as being yet another theatre of operations for a multitude of their security and intelligence agencies and appear as yet unwilling to engage with each other – and sometimes with the SRP - on these issues which not unnaturally also directly impact the privacy of citizens irrespective of their nationality. While not necessarily the primary target of cyber-security and cyber-espionage measures, the ordinary citizen may often get caught in the cross-fire and his or her personal data and on-line activities may end up being monitored in the name of national security in a way which is unnecessary, disproportionate and excessive. Apart from ad hoc investigatory work carried out for the mandate, the SRP is fortunate in having access to a rich evidence-base provided by previous and on-going independent collaborative research in the security field, especially that funded by the European Union² which may be used to the benefit of all nations. The SRP is pursuing this exploration/study on four main fronts: a) State surveillance capabilities which are proportionate in scope and adequately constrained by legislative, procedural and technical safeguards including strong oversight mechanisms; b) a focus on targeted as opposed to mass surveillance; c) the access of LEAs and SIS to personal data held by private corporations and other non-public entities; d) a renewed emphasis on Cyberpeace. The SRP is firmly of the opinion that Cyberspace risks being ruined by Cyberwar and Cyber-surveillance and that Governments and other stakeholders should work towards Cyberpeace. In this sense at least, privacy protection is also part of the Cyberpeace movement. In this way, Cyberspace can truly become a digital space where the citizen can expect both privacy and security, a peaceful space which is not constantly being

² Including projects such as CONSENT, SMART, RESPECT, SiiP, INGRESS, E-CRIME, EVIDENCE, MAPPING, CITYCoP, CARISMAND

put in jeopardy by the activities of some States over and above the threats posed by terrorists and organised crime.

(d) *Open data and Big Data analytics: the impact on privacy*

12. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality. A more detailed insight into the SRP's concerns in this area is available in Annex II.

(e) *Genetics and privacy*

13. The SRP notes that approximately 25% of the UN's member states, have implemented national criminal offender DNA (DeoxyriboNucleic Acid) database programs. Forensic DNA databases can play an important role in solving crimes but they also raise human rights concerns. Issues include potential misuse for government surveillance, including identification of relatives and non-paternity, and the risk of miscarriages of justice. Furthermore it would appear that the use of DNA database in civilian uses, such as for ID cards and immigration is set to increase exponentially and, within the next few years, it is likely that we will see the first country move forward with a citizen-wide DNA database. In a revival of concerns raised in the 1990s about the use of genetic data in the insurance industry, it is being suggested that personalized medicine will cause many citizens to voluntarily submit their full human genomes to the health care industry. In the wake of these and other concerns, there is an ongoing need for greater public and policy debate as DNA databases expand around the world. The SRP intends to continue to engage with projects which aim to set international human rights standards for DNA databases, by establishing best practice and involving experts, policy makers and members of the public in open debate. It is expected that this engagement would contribute to best practice guidelines developed with civil society input, for feedback and discussion.

(f) *Privacy, dignity and reputation*

14. The concern with security and surveillance has possibly been one of the factors deflecting attention from the concern expressed and shared by many citizens about the way that their privacy, their dignity and their reputation are being put at risk on the internet. The digital age has meant that media has developed and changed over the past two decades and this especially in the way that the Internet has enabled normal citizens who do not have the benefit of a formal education in journalism to publish text, audio and video at will at any time of day. This development has empowered citizens in many ways especially in situations where censorship or other obstacles are bypassed and the technology facilitates freedom of expression in a way which benefits democratic aspects of society. On the other hand this new phenomenon of citizen-journalists and bloggers in a fast-moving media world taken together with widespread use of social media has led to a widespread concern that the right to freedom of expression is being abused with a negative impact on other fundamental human rights such as privacy and dignity. Contemporary research over the past five years has highlighted ever-increasing concern of citizens with the ease with which their good name and reputation may be attacked and destroyed on the Internet as well as the sense of helplessness that is felt by many netizens when seeking safeguards and remedies in cases of defamation and/or breach of privacy. The SRP would like to collaborate with the UN Special Rapporteur for Freedom of Expression, civil society as well as other UN agencies like UNESCO with a view to exploring concrete safeguards and remedies for privacy, dignity and reputation on the internet. As with a number of the other thematic

studies outlined above, the relationship between Privacy and Internet Governance remains one of the underlying constant issues which are also relevant to privacy, dignity and reputation.

(g) *Biometrics and privacy*

15. A survey of current research suggests a huge surge in interest in using all forms of biometrics for a variety of purposes ranging from law enforcement to personal access to mobile devices. Thus voice and speaker identification, retina scans, gait recognition, face recognition, fingerprint and sub-cutaneous fingerprint technology are just some examples of the many digital technologies being developed and deployed for various purposes across society in the second decade of the 21st century. The SRP intends to continue long-standing engagement with the biometric research community as well as LEAs, SIS and civil society in an attempt at further identifying appropriate safeguards and remedies in the case of usage of biometric devices.

3. Individual complaints

16. Every so often, and as the mandate will become known, the SRP has received and will presumably continue to receive complaints from individual members of the public residing in a given national territory or from civil society actors of alleged infringements of privacy rights. These complaints are and will be followed up through correspondence with the sources of the complaints and the relevant governments authorities, through the usual communications methodology of Special Procedures mandate holders aimed at clarifying the allegations made, establishing facts and, where necessary, make recommendations for corrective action. These communications may also involve on-line and in-person meetings as appropriate. They will be reported to the Council in the annual reports of the SRP. Should the evidence received warrant particular or urgent attention, and communications prove not to be the appropriate way of responding, the SRP may consider issuing a public expression of concern.

4. Joint actions

17. The SRP receives regularly requests for and may sometimes initiate joint actions with other Special Rapporteurs. Details about these are published separately in the Communications Report of Special Procedures.

18. As at 05 March 2016, there has not been the time or the opportunity to collect enough evidence in any of the four categories listed above to do much beyond adhering to two joint actions. It is expected however that information collected in the four categories above will combine to provide the evidence-base required to pursue SRP dialogue and cooperation with relevant states, including through communications, country visits and other modes of collaboration.

5. Building Bridges and a policy of engagement

19. The SRP has used the mandate to continue and expand previous work aimed at building bridges with and between stakeholders. This leads to an on-going policy of engagement with all classes of stakeholders, including officials and ministers of various governments in their capitals or at bilateral meetings in international fora; meetings with several Data Protection and Privacy Commissioners and especially with the Chairperson of the Art 29 Committee of the EU and the Chairperson of the Council of Europe's Consultative Committee on Data Protection (T-PD); discussions with technical standards bodies such as the ITU and IEEE; in-depth meetings with civil society either one-to-one or in groups; one-to-one meetings with Human rights specialists or other officials from the Permanent Missions of States to the UN in Geneva, etc. etc. Invitations to deliver keynote

speeches, participate in panel discussions, conferences and to meet with members of civil society are received almost literally on a daily basis. Many are accepted, especially those in line with the seven thematic studies indicated in Section II paras 6 to 15 above while several others are regrettably declined especially where time and/or budgetary constraints make such participation unfeasible. Amongst many other results, this policy of engagement has also witnessed the adoption of a Resolution on Cooperation with the UN Special Rapporteur for Privacy³ adopted in October 2015 by the International Conference of Data Protection and Privacy Commissioners.

III. Privacy at the beginning of the year 2016

A. Definition and understanding

20. While the concept of privacy is known in all human societies and cultures at all stages of development and throughout all of the known history of humankind it has to be pointed out that there is no binding and universally accepted definition of privacy.⁴ To understand the right better it is necessary to think of it from two perspectives. First, it should be considered what the positive core of the right encompasses. Secondly, the question arises how to delimit the right in the form of a negative definition. It would appear that we are some distance from having completed these two tasks.

21. As reaffirmed by the Human Rights Council in resolution 28/16 article 12 of the Universal Declaration of Human Rights (UDHR) and article 17 of the International Covenant on Civil and Political Rights (ICCPR) constitute the basis of the right to privacy in international human rights law. Taken together with a number of other international and national legal instruments including constitutions and ad hoc legislation, this means that there exists world-wide, a considerable legal framework which can be useful to the protection and promotion of privacy. The existence and usefulness of this legal framework is however seriously handicapped by the lack of a universally agreed and accepted definition of privacy. In some cases it may prove to be next to useless if we were to have 193 nations signed up to the principle of protecting privacy if we do not have a clear understanding of what we have agreed to protect.

22. The absence of a universally agreed and accepted definition of privacy is not the only major handicap faced by the Special Rapporteur on Privacy (SRP). Even had the drafters of all the existing legal instruments, UN and otherwise, included a universally agreed definition of privacy in those instruments we would still have had to deal with what can be conveniently summed up as the Time, Place, Economy and Technology (TPET) dimensions. For the passage of time and the impact of technology, taken together with the different rate of economic development and technology deployment in different geographical locations means that legal principles established fifty years ago (ICCPR) or even thirty-five years ago (e.g. the European Convention on Data Protection) let alone seventy years ago (UDHR) may need to be re-visited, further developed and possibly supplemented and complemented to make them more relevant and useful to the realities of 2016.

³ <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf>

⁴ For a much more detailed insight into the SRP's assessment of the existence and time, place and space dimensions of privacy across the millennia see Joseph A Cannataci (ed) *The Individual and Privacy* Publisher: Ashgate; Extent: 552 pages; ISBN-10: 1409447170 ISBN-13: 9781409447177 Sku: 246532549; Publish Date: 19/03/2015 - <http://www.ashgate.com/isbn/9781409447177>

23. Against a background of a lack of a universally agreed definition and TPET, it is clear that for the foundations of “the privacy house” to be strong and fit-for-purpose we first require to establish a re-freshened understanding of what privacy means to different people in different places in different circumstances across the planet. This therefore would *prima facie* seem to be not only a fundamentally important task but also a priority task for the SRP.

24. A debate on privacy in some cultures includes the debate on abortion. Without entering into the merits of whether this is correct or otherwise, for the avoidance of doubt, it is being stated that, at this preliminary stage, the focus of the SRP shall be on informational privacy i.e. on the function and role of privacy in determining the flows of information in society and the resultant impact on the development of the personality of individual citizens as well as almost inextricably related issues such as the distribution of power and wealth within society, and this to the exclusion of subjects such as abortion. When doing so however it becomes clear that it is not only privacy that impacts the flows of information in society but also other rights like freedom of expression and freedom of access to publicly-held information. All of these rights are important and commitment to one right should not detract from the importance and protection of another right. Taking rights in conjunction wherever possible is healthier than taking rights in opposition to each other. Thus, properly speaking, it is not helpful to talk of “privacy vs. security” but rather of “privacy **and** security” since both privacy and security are desiderata ... and both can be taken to be enabling rights rather than ends in themselves. Security is an enabling right for the over-arching right to life while privacy may also be viewed as an enabling right in the overall complex web of information flows in society which are fundamentally important to the value of autonomy and the ability of the individual to identify and choose between options in an informed manner as he or she develops is or her own personality throughout life.

25. When launching the debate on the understanding of what privacy is and should be in 2016, the SRP wishes to focus on fundamentals and to avoid the debate being side-tracked by what may be perceived or real local or cultural differences at the fringes of privacy as opposed to the strong core of privacy-values which may eventually be found to enjoy universal consensus. In order to help focus a fresh, structured debate on fundamentals the SRP intends to provocatively posit privacy as being an enabling right as opposed to being an end in itself. Several countries around the world have identified an over-arching fundamental right to dignity and the free, unhindered development of one’s personality. Countries as geographically far apart as Brazil and Germany have this right written into their constitution and it is the SRP’s contention that a) such a right to dignity and the free, unhindered development of one’s personality should be considered to be universally applicable and b) that already-recognised rights such as privacy, freedom of expression and freedom of access to information constitute a tripod of enabling rights which are best considered in the context of their usefulness in enabling a human being to develop his or her personality in the freest of manners. Positing privacy and better still, the question “Why Privacy?” in the context of a wider debate about the fundamental right to dignity and the free, unhindered development of one’s personality reflects the realities of life in the digital age and should help all participants in the debate, irrespective of which country or culture they may hail from, to focus on the fundamentals of the development of one’s personality and what kind of a life they would like privacy to help protect rather than lose too much time on what privacy-relevant traditions in any given culture they would need to focus upon or defend/promote.

26. It will be seen that, in many cases, the debate on privacy cannot be usefully divorced from that on the value of autonomy or self-determination. The latter term is one which has been discussed often within UN and other circles and, when related to privacy and personality rights, in some countries such as Germany where it has, since 1983, given additionally rise to a constitutional right to “informational self-determination”. The appeal

and validity of this concept needs to be evaluated further in the context of a global discussion on how the right to privacy should be better understood in 2016, possibly in the context of a discussion of the protection and promotion of the fundamental right to dignity and the free, unhindered development of one's personality.

27. The tripod of enabling rights mentioned above – privacy, freedom of expression and freedom of access to information – existed before the advent of digital technologies. As did the right to dignity and the free, unhindered development of one's personality. Digital technology has however resulted in a huge impact on these rights since both off-line (eg through credit cards, RFID and other electronic devices) and on-line where, today, netizens generate tens of thousands of more data-sets about themselves than they did two decades ago before they started going on-line in droves. Mobile devices and converging technologies such as mobile smart phones - where telephony, the Internet and photography converge - create a new way of life, new comforts and new expectations both in terms of convenience as well as for privacy.

28. The impact of new technologies also means that we may have to re-visit the distinctions between individual and collective privacy as well as expectations of privacy in both public and private spaces, always in the context of dignity and the free, unhindered development of one's personality.

B. Initial observations in 2015-2016

29. Choosing which were the most important events in the Privacy calendar for 2015-2016 is a difficult task and the resources were not available to the SRP to carry this out rigorously and scientifically during the first six months of the mandate. Moreover the SRP does not wish to substitute the important role played by civil society actors such as Privacy International and its affiliates which for the best part of twenty years have organised their Big Brother Awards⁵ which shine a light on privacy deeds and misdeeds. These succeed in delivering in considerable more detail and at a national level much more than can be done in this brief report to the HRC. On the other hand, the SRP would like to commend good practices, good laws, good court decisions indeed any good ideas which may promote and increase the protection of privacy so, without the pretension of the following being in any way an exhaustive list, and in no particular order, the following important developments are being brought to the attention of the HRC:

Wise restraint – a no to back doors from the Netherlands and the USA

30. Jointly to the governments of the United States of America and the Kingdom of the Netherlands which should be complimented on the restraint demonstrated in their unwillingness to permit the law to be used to engineer back-doors in communications. On the 4th January 2016, it was announced that the Dutch government has formally opposed the introduction of backdoors in encryption products. A government position paper⁶, published by the Ministry of Security and Justice and signed by the security and business ministers, concludes that "the government believes that it is currently not appropriate to adopt restrictive legal measures against the development, availability and use of encryption within the Netherlands." The conclusion comes at the end of a five-page run-through of the arguments for greater encryption and the counter-arguments for allowing the authorities access to the information. "By introducing a technical input into an encryption product that

⁵ <http://www.bigbrotherawards.org/>

⁶ http://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015

would give the authorities access would also make encrypted files vulnerable to criminals, terrorists and foreign intelligence services," the paper noted. "This could have undesirable consequences for the security of information communicated and stored, and the integrity of ICT systems, which are increasingly of importance for the functioning of the society."⁷

31. The Dutch position seems to be more clear cut than the similar US position which preceded it by some three months when, in early October 2015 FBI Director James Comey Jr. said in testimony on Capitol Hill that the administration is not pressing legislation, for now, that would force companies to decrypt customer data. "After months of deliberation, the Obama administration has made a long-awaited decision on the thorny issue of how to deal with encrypted communications: It will not — for now — call for legislation requiring companies to decode messages for law enforcement"⁸. What is of greater concern and which came to the fore in the recent Apple vs FBI Case, is the position that the US administration "will continue trying to persuade companies that have moved to encrypt their customers' data to create a way for the government to still peer into people's data when needed for criminal or terrorism investigations."⁹ The SRP's position on the Apple vs FBI case has been largely though independently articulated in the High Commissioner's statement of 4 March 2016¹⁰. It is encouraging to note the latest comments made by US Defense Secretary Ash Carter when he declared "that strong encryption is essential to the nation's security... Defense Secretary Ash Carter told a tech industry audience on Wednesday 2 March 2016 that he's "not a believer in back doors," or encryption programs that leave openings for outsiders to read coded files."¹¹ This is consistent with his statements in October 2015¹² and is a position which should be encouraged and reinforced.

The beginning of the judicial end for mass surveillance – the substantive issue

32. On 06 October 2015, the Court of Justice of the European Union delivered a judgment in the case of Maximillian Schrems versus the Data Protection Commissioner of the Republic of Ireland. The Court declared void a decision by the European Commission which established the so-called "Safe Harbour" framework and which was based on Directive 95/46/EC. The SRP directs attention to what is probably one of the most important parts of that decision from a precedent-confirming (and setting) point of view:

"94. In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter"

33. Some debate will doubtless ensue over the precise meaning of "access on a generalised basis" and here the court is clearly referring to content of communications as opposed to metadata but it will be interesting to see which European law legitimising mass surveillance, if any would pass the test of such a standard if the ECJ would be inclined to continue to apply it strictly in future. The ambiguity however is at least partially dispelled when the *Schrems* decision is read together with the *Zakharov* judgement indicated below

⁷ http://www.theregister.co.uk/2016/01/04/dutch_government_says_no_to_backdoors/

⁸ https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data-for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html

⁹ ditto

¹⁰ <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E>

¹¹ <http://gadgets.ndtv.com/mobiles/news/us-defense-secretary-says-favours-strong-encryption-not-back-doors-809437>

¹² <http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu>

which forms as much a part of EU law as it does for other Council of Europe member states.

The importance of having a remedy – enforcement and procedural issues

34. Again, with reference to the Schrems case just quoted above, the SRP welcomes that the ECJ has become a forum for people like the applicant. Max Schrems started the case as an individual concerned about the consequences of the development of modern information technology for his dignity as a human being in a democratic society. The opportunity for individuals to argue their case and to defend their rights before a supra-national public institution, challenging existing power relations, is essential for creating knowledge to enhance the welfare of our society, and consistent with the development of international human rights law. The existence of such mechanisms is absolutely crucial to protect human rights and to restore trust in the use of technology by States or other actors.

35. It is also the harbinger of a new development in society, one pointing out that if you have a right this needs to be respected and enforced anywhere not just the place where servers are based.

36. The judgment of the ECJ also demonstrates the added-value of regional policy approaches which may possibly serve in future to promote bottom-up, participatory legal instruments with a wider, global reach.

Mere existence of a secret surveillance measure is a violation of the right to private life

37. The Grand Chamber of the European Court of Human Rights - in its decision *Roman Zakharov v Russia* [2015] Eur Court HR (No 47143/06) (4 December 2015)¹³ - has unanimously held that the Russian system of secret interception of mobile telephone communications was a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom. In addition, and very interestingly, the Court accepted that if certain conditions are satisfied an applicant can claim to be the victim of a violation of article 8 due to the mere existence of a secret surveillance measure. Perhaps most importantly was the declaration by the court that basically outlawed mass surveillance systems in a way which is even more explicit than that of the ECJ in *Schrems*.

“270. The Court considers that the manner in which the system of secret surveillance operates in Russia gives the security services and the police technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation. Although the possibility of improper action by a dishonest, negligent or over-zealous official can never be completely ruled out whatever the system (see *Klass and Others*, cited above, § 59), the Court considers that a system, such as the Russian one, which enables the secret services and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse. The need for safeguards against arbitrariness and abuse appears therefore to be particularly great.”

38. This decision sets up a very important benchmark highlighting as it does the requirements for reasonable suspicion and prior judicial authorisation as well as the unacceptable nature of “a system...which enables the secret service and the police to intercept directly the communications of each and every citizen without requiring them to show an interception authorisation”. This then would be the test against which all existing and new proposed legislation about surveillance in any European country must be

¹³ [http://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-159324%22\]}](http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]})

measured. The SRP also notes with grave concern various reports about a decision of the Russian Duma (Parliament) which would enable decisions of the European Court of Human Rights to be overruled¹⁴. If these reports are true, this may, in practice, remove a very important remedy available to citizens of countries which have ratified the European Convention on Human Rights including remedies in the case of violation of the right to private life. The SRP invites the Government of the Russian Federation to assist the SRP in further verifying these reports, examining the law in question more deeply for nuance and, if the reports are fundamentally accurate, persuade the Duma to revoke the law of 4 December 2015 and thus restore the efficacy of the remedies available to Russian citizens in terms of the European Convention on Human Rights including their remedies against the state in cases where their right to privacy is infringed.

The UK's Investigatory Powers Bill

39. Recognition is due to the three joint UK Parliamentary committees: the science and technology committee on February 1, the intelligence and security committee on February 9 and most importantly, the joint committee for the bill itself on February 11, 2016 for their consistent, strong, if occasionally over-polite, criticism of the UK Government's Investigatory Powers Bill. The joint committee for the draft investigatory powers bill made 86 recommendations for changes to the bill in its report, concentrating on issues of clarity, judicial oversight and justification of the various powers. Recognition is also due to the UK Government which has taken heed of advice from various quarters and which is using the IPB to introduce much-needed reinforcement of oversight mechanisms. While there may still be some room for improvement in this area too, these are steps in the right direction. At the time of the submission of this SRP report to the HRC, the SRP's initial assessment of the latest version of the Bill published on 1 March 2016 however leads to serious concern about the value of some of the revisions most recently introduced. At the time of writing, not only do some of the UK Government's proposals appear to run counter to the logic and findings of UN Special Rapporteur on Counter-terrorism Ben Emmerson in his 2014 report dealing *inter alia* with mass surveillance¹⁵, but they *prima facie* fail the benchmarks set by the ECJ in *Schrems* and the ECHR in *Zakharov*. The SRP firmly encourages the three committees of the UK Parliament commended above to continue, with renewed vigour and determination, to exert their influence in order that disproportionate, privacy-intrusive measures such as bulk surveillance and bulk hacking as contemplated in the Investigatory Powers Bill be outlawed rather than legitimised. It would appear that the serious and possibly unintended consequences of legitimising bulk interception and bulk hacking are not being fully appreciated by the UK Government. Bearing in mind the huge influence that UK legislation still has in over 25% of the UN's members states that still form part of the Commonwealth, as well as its proud tradition as a democracy which was one of the founders of leading regional human rights bodies such as the Council of Europe, the SRP encourages the UK Government to take this golden opportunity to set a good example and step back from taking disproportionate measures which may have negative ramifications far beyond the shores of the United Kingdom. More specifically, the SRP invites the UK Government to show greater commitment to protecting the fundamental right to privacy of its own citizens and those of others and also to desist from setting a bad example to other states by continuing to propose measures, especially bulk interception and bulk hacking, which *prima facie* fail the standards of several UK Parliamentary Committees, run counter to the most recent judgements of the European Court of Justice and the European Court of Human Rights, and undermine the spirit of the very right to privacy. Finally, the SRP

¹⁴ Russia has adopted a law allowing it to overrule judgements from the European Court of Human Rights (ECHR). <http://www.bbc.com/news/world-europe-35007059>

¹⁵ <http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf>

invites the UK Government to work closely with the mandate, especially in the context of its thematic study on surveillance, in an effort to identify proportionate measures which enhance security without being overly privacy-intrusive.

First small steps towards cyberpeace?

40. The efforts of the USA and China in leading efforts to start defusing the situation in cyberspace deserve recognition.

41. There are possibly three main dimensions to cyberpeace all threatened by on-line espionage:

- (i) sabotage and warfare;
- (ii) intellectual property rights and economic espionage
- (iii) civil rights and surveillance.

42. While privacy is mostly concerned with the third dimension i.e. civil rights and surveillance, this is often also caught up in discussions about the first and second dimensions. In September 2015 it was announced that the USA and China had agreed “that neither government would support or conduct cyber-enabled theft of intellectual property” and that “both countries are committed to finding appropriate norms of state behavior in cyberspace within the international community. The countries also agreed to create a senior experts group for further cyber affairs discussion”¹⁶ Not only did the US and China follow up this important step forward with cyber talks in December 2015 but they seem to have set an example for other countries too: “the U.S. announcement was followed by a similar agreement between the UK and China, and a report that Berlin would sign a “no cyber theft” deal with Beijing in 2016. In November 2015, China, Brazil, Russia, the United States, and other members of the G20 accepted the norm against conducting or supporting the cyber-enabled theft of intellectual property.”¹⁷ This is still some way off from achieving complete agreements about cyber-war or on-line surveillance and the impact of espionage on privacy of citizens but at least it is a start and the SRP cannot but try to persuade all parties concerned that the discussions should extend to include concrete measures for respect of on-line privacy too.

IV. Activities of the Special Rapporteur

Highlight Activities carried out by the Special Rapporteur

Resourcing the SRP mandate

43. Since the mandate is a new one, since the formal budget for the mandate was not approved until January 2016 and since the mandate commenced on 01 August 2015 i.e. when most of Europe – and certainly many members of the UN OHCHR secretariat in Geneva – were on holiday, it took several weeks for the Mandate to be provided any form of support by UN OHCHR staff and to date such administrative support is provided on a stopgap basis pending recruitment of staff which process is expected to be completed by June 2016. On assessing the resourcing situation SRP took immediate steps to source extra-mural funding outside UN sources. A post-doc researcher (with a PhD in privacy and the right to be forgotten) was recruited with effect from October 2015 on a part time and, with

¹⁶ <http://www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html>

¹⁷ <http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement/>

effect from January 2016 on a full-time basis in order to secure some assistance with the substantive part of the work required by the mandate. This non-UN funded full-time resource will be maintained in post until the human resource situation for the mandate stabilises. Volunteer assistance has also been very kindly provided by domain specialists and other staff from the SRP's home institutions i.e. the Department of Information Policy & Governance within the Faculty of Media & Knowledge Sciences of the University of Malta and the STeP (Security, Technology & e-Privacy) Research Group at the Faculty of Law in the University of Groningen in the Netherlands. This assistance which, together with that of the UN staff in Geneva, is very gratefully acknowledged, enables the mandate to live on until capacity is suitably increased and a more sustainable support structure which is fit-for-purpose can come into being.

A road-map for the SRP mandate - Formulating the ten-point plan

44. Over and above the daily activities outlined in Section II – Working Methods of the SRP mandate, considerable time was invested in developing the ten-point plan outlined in Section V below and in consultation with many stakeholders about the plan.

Engagement in multiple events

45. The SRP accepted invitations for meetings, conferences, panels and 1:1 consultations especially those which helped maintain an on-going policy of engagement about the seven thematic studies outlined in Para 4.2 above. These included (non-exhaustive list follows):

(a) Panel discussion *Inextricably intertwined: freedom of expression and privacy in Internet Governance* MAPPING Annual Stakeholders Assembly, Hannover Germany – 22 Sep 2015

(b) Meeting with Director of Global Affairs, Human Rights Watch, 30 Sep 2015 Participation in and presentation to seminar on *Data protection and privacy in statistics*, UN, Geneva, 13-14 October 2015;

(c) Meeting with the Deputy Secretary General of the International Telecommunications Union (ITU), Geneva, 14 October 2015;

(d) Organised and led Panel on *Privacy and Surveillance* at conference for intelligence services *Intelligence in the Knowledge Society 2015*, Bucharest, Romania – 16 October 2015

(e) Keynote Speech – *Privacy in the Digital Age* - International Conference of Data Protection & Privacy Commissioners, Closed session, Amsterdam 27 October 2015

(f) Participated in Round Table discussion *Tour du Monde*¹⁸ International Conference of Data Protection & Privacy Commissioners, Open session, Amsterdam 29 October 2015

(g) Participated in multiple sessions, public and bilateral, at the Internet Governance Forum, Joao Pessoa, Brazil 09-13 November 2015¹⁹

(h) Delivered keynote speech, during closed workshop *Big Data in the Global South* International Workshop, ITS, Rio De Janeiro, Brazil 16-17 November 2015,²⁰

¹⁸ <https://www.privacyconference2015.org/wp-content/uploads/2015/01/Tour-Du-Monde-Report.pdf>

¹⁹ <https://www.intgovforum.org/cms/igf-2015-schedule>

²⁰ <http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global/>

- (i) Held meetings with Ministry of Justice officials, in an in-depth analysis of new Brazilian draft law on privacy, Brasilia, 18 November 2015
- (j) Held joint meeting with officials from Ministry of Telecommunications, Ministry of Justice, Ministry of the Interior, etc. regarding new Brazilian draft law on privacy, Brasilia, 18 November 2015
- (k) Held meeting with Procurator General responsible at Procurator General's office, Brasilia, 18 November 2015
- (l) Held meeting with Director of Human Rights, Ministry of Foreign Affairs, Brasilia, 19 November 2015
- (m) Delivered (video address) speech at Consumer International Conference, 19 November 2015, Brasilia, Brasil²¹
- (n) Held in-depth meetings and consultations with founder director of Patient Privacy Rights, Malta 25 November 2015
- (o) Delivered setting the scene panel contribution at High Level Conference "Protecting on-line privacy by enhancing IT Security and EU IT autonomy" jointly organised by LIBE Committee of the European Parliament - European Parliament, Brussels 8th December 2015²²
- (p) Delivered keynote speech Conference: "Sicurezza e privacy verso un Safe Harbour 2.0
- (q) 9th Rome, December 2015²³
- (r) Delivered keynote speech, on *Privacy, Identity, Security & freedom*, IPLab Conference Utrecht, 10th December 2015²⁴
- (s) Participated in induction session for Special Rapporteurs, Palais des Nations, Geneva 14-16 December 2015
- (t) *Meeting with UK*, Geneva 17 December 2015
- (u) *Meeting with China*, Geneva 17 December 2015
- (v) *Meeting with Russia*, 17 December 2015
- (w) Participated in *Technical meeting of the Counter-Terrorism Committee Executive Directorate, on "Preventing Terrorists from Exploiting the Internet and Social Media to Recruit Terrorists and Incite Terrorist Acts, While Respecting Human Rights and Fundamental Freedoms"*
- (x) Presentation via Video Conference on "The threat and challenges relating to the use of the Internet and social media for terrorist purposes, 17 December 2015
- (y) Made presentation to and led discussion with *NGO roundtable: Privacy International, Amnesty International, Reporters without Borders, Internet Society, HRW, ACLU*, Geneva, 18 December 2015
- (z) Meeting with ITU's Deputy Director of the Telecommunication Standardization Bureau, (joined by ITU Legal Unit) 18 December 2015

²¹ <http://congressprogramme.consumersinternational.org/speakers.h>

²² <http://www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy>

²³ <http://www.dimt.it/tag/cannataci/>

²⁴ <https://www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published/>

- (aa) Intervened through video conferencing and gave presentation “Privacy, quality of life & smart cities: Scaling-up “surveillable” to ITU conference on Smart Cities, Singapore, 18 January 2016
- (bb) In-depth meetings with Helen Wallace and Andrew Jackson of GeneWatch UK, Malta, 03 February 2016
- (cc) Delivered keynote speech (via live video conference) at Fifth workshop on data protection as part of good governance in international organisations, Geneva, 05 February 2016²⁵
- (dd) Delivered keynote speech and participated in general meeting for stakeholders, Dutch Ministry of Foreign Affairs, The Hague, The Netherlands, 03 March 2016.

V. A Ten Point action plan

46. In order to facilitate the process of further elaboration on the dimensions of the right to privacy and its relationship with other human rights the Special Rapporteur has developed an outline Ten Point Action plan. It should be kept in mind that the points mentioned in the plan are brought forward in no particular order and do not imply a specifically prioritised working programme. The Special Rapporteur understands his function similarly to that of a pathfinder. In other words the aim is to seek a way forward while at the same time identifying urgent issues to be tackled or reacting to the needs of individuals or of countries who require urgent work in the sector of responsibility. The Ten Point Action Plan below is a TO DO LIST and not a mere wish-list. The SRP has embarked on each of the ten points below but naturally at the speed dictated by time-availability and resource constraints

(a) *Going beyond the existing legal framework to a deeper understanding of what it is that we have pledged to protect:* There is a need to work on developing a better, more detailed and more universal understanding of what is meant by “the right to privacy”. What does it mean and what should it mean in the 21st century? How can it be better protected in the digital age? Activities will be organised and research will be supported to examine possible answers to these key questions which will help provide essential foundations for other parts of the SRP’s action plan.

(b) *Increasing awareness:* Another important issue is the development of greater awareness amongst citizens in order to help them understand what privacy is. It is important to have a general discourse on what their privacy rights are, how their privacy may be infringed upon especially by new technologies and by their behaviour in cyberspace. They need to learn on how their personal data has been monetised and what are the existing safeguards and remedies. What can they do to minimize privacy risk and how can they interact with their law-makers and the corporate sector to improve privacy protection? This creation of awareness is a massive task in its own right, and the Special Rapporteur will contribute to this awareness-raising throughout on-going engagement with all stakeholders and especially civil society for the entire duration of his mandate.

(c) *The creation of a structured, on-going dialogue about privacy.* The establishment of a more structured, more open, more comprehensive, more effective and most importantly permanent dialogue between the different stakeholders is crucial. In order to achieve the protection of privacy bridges are required and need to be built. The Special

²⁵ <https://www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations>

Rapporteur would like to put great emphasis on this activity and will use existing fora as well as creating new fora. To be included are particularly the facilitating of a structured dialogue between Non-Governmental Organizations, Data Protection and Privacy Commissioners, Law Enforcement Agencies (LEAs) and Security and Intelligence Services (SIS). It is essential to work with all classes of stakeholders in order to improve internal procedures, increase the level of privacy by design in the technologies they deploy and the procedures they follow. It is important to maximise transparency and accountability and reinforce impartial and effective oversight to the point where it becomes significantly more effective and credible. Without genuinely engaging with key stakeholders including those whose role may be completely necessary and legitimate in a modern society, progress cannot be achieved.

(d) *A comprehensive approach to legal, procedural and operational safeguards and remedies:* Appropriate safeguards and effective remedies have been part of the “raison d’être” of data protection law since its inception aimed at providing guidance and protection at the correct level of detail required in a world rendered more complex by constant technological change. Clearer and more effective protection for citizens should be provided in order to prevent the infringement of privacy. Real remedies need to be available to all concerned in those cases where an infringement actually occurs. The search for safeguards and remedies is transversal and underlies all of the SRP’s thematic studies identified in Section II paras 6 to 15.

(e) *A renewed emphasis on technical safeguards:* The safeguards and remedies available to citizens cannot ever be purely legal or operational. Law alone is not enough. The SRP will continue to engage with the technical community in an effort to promote the development of effective technical safeguards including encryption, overlay software and various other technical solutions where privacy-by-design is genuinely put into practice.

(f) *A specially-focused dialogue with the corporate world.* An increasing number of corporations today already gather much more personal data than most governments ever can or will. What are the acceptable alternatives to or the key modifications that society should expect from current business models where personal data has been heavily monetised? Which are the safeguards applicable in cases where data held by private corporations are requested by state authorities? This dimension of the mandate requires much time and attention. The SRP has already commenced direct contacts with industry and will maintain a privacy-focused dialogue relevant to these issues with a range of industry players with the intention of informing new developments in the corporate sector as well as other parts of the SRP’s mandate.

(g) *Promoting national and regional developments in privacy-protection mechanisms* The value of national and regional developments in privacy-protection mechanisms should be appreciated more at the global level. The SRP has an important complementary role to play when working in close co-operation with Data Protection and Privacy Commissioners world-wide. Through mutual cooperation and dialogue the global standards of privacy protection could be raised significantly. The SRP has commenced a series of global activities planned and executed with Data Protection Authorities world-wide. These include events planned for Australia, Morocco, New Zealand, Northern Ireland and Tunisia for 2016 with many others in the pipeline for future years.

(h) *Harnessing the energy and influence of civil society.* Having already met with representatives of over forty (40) NGOs during his first six months in office, the SRP intends to continue dedicating considerable time to listening to and working with those representatives of civil society who are putting in so much effort to better protect privacy world-wide.

(i) *Cyberspace, Cyber-privacy, Cyber-espionage, Cyberwar and Cyberpeace*

The global community needs to be inquisitive, frank and open about what is really going on in cyberspace, including the realities of mass surveillance, cyber-espionage and cyberwar. Tackling these realities will build upon the results of other action points outlined above as well as the results of the thematic studies indicate in Section II paras 6 to 15. The Special Rapporteur expects these issues to be a constant feature of a number of his reports as well as in many of the country visits and, by transparently engaging with stakeholders about these issues, hopes to play a constructive role in improving the protection of privacy in the digital age.

(j) *Investing further in International Law.*

While law alone is not enough it is very important. The potential for development of international law relevant to privacy should be explored in all forms and the SRP is open to examining the value of any legal instrument irrespective of whether this is classed as soft law or hard law. A priority issue such as up-dating legal instruments through an expanded understanding of what is meant by the right to privacy would seem to be an essential starting point. There appears to be a consensus amongst several stakeholders that one of these legal instruments could take the form of an additional protocol to Art. 17 of the ICCPR²⁶ wherein the SRP is being urged “to promote the opening of negotiations on this additional protocol during his first mandate”²⁷. The precise timing of this however should probably be contingent on the duration and outcome of in-depth and wide-ranging discussions invoked through action point a) above – i.e. achieving a better universal understanding of what the core values in privacy are or may be. Some other privacy-relevant matters, especially issues of jurisdiction and territoriality in cyberspace cannot be addressed satisfactorily unless there is a clear international agreement to that effect, one which would normally take the form of agreement in a multilateral treaty most probably on a specific topic or set of issues. For the avoidance of doubt it should be stated that what is envisaged is not one new global all-encompassing international convention covering all of privacy or Internet governance. It is far more realistic to expect that protection of privacy can be increased through incremental growth of international law and thus the clarification and eventually the extension of existing legal instruments as well as even, in the mid to long term, the development of entirely new legal instruments. On-going discussions about international law and new legal instruments in the field of internet governance will also be monitored by the SRP in order to determine the timing of initiation of action within UN bodies as well as the type and scope of the legal instrument that the SRP may possibly eventually wish to recommend to the HRC and the GA.

VI. Conclusions

47. **The SRP has been impressed by the overwhelmingly warm and enthusiastic welcome that he has received from most sectors of society, most classes of stakeholders;**

48. **Privacy has never been more at the forefront of political, judicial and personal consciousness than in 2016;**

49. **The tensions between security, corporate business models and privacy continue to take centre stage but the last twelve months have been marked by contradictory indicators: some governments have continued, in practice and/or in their parliaments to take privacy-hostile attitudes while courts world-wide but especially in the USA and**

²⁶ <https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf>

²⁷ Ibid.

Europe have struck clear blows in favour of privacy and especially against disproportionate, privacy-intrusive measures such as mass surveillance or breaking of encryption.

50. There are strong indicators that Privacy has become an important commercial consideration with some major vendors adopting it as a selling point. If there is a market for privacy, market forces will provide for that market. The rapid increase in the availability of encrypted devices and software services is a strong indicator that consumers world-wide are increasingly aware of risks to their privacy and the fact that they will increasingly choose privacy-friendly products and services over ones which are privacy-neutral or privacy-unfriendly;

51. While some governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimise or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures such as bulk collection, bulk hacking, warrantless interception etc. other governments led, in this case by the Netherlands and the USA have moved more openly towards a policy of no back doors to encryption. The SRP would encourage many more governments to coalesce around this position.

52. Countries world-wide are not only waking up to their responsibilities and to the realities of technical safeguards such as encryption. They are also slowly but surely realising the limitations of gains and the enormity of risks should they bring ruin to cyberspace through cyberwar and cyberespionage. We are still some way away from sufficient progress in this area but 2015 has seen some important beginnings so the SRP encourages Governments – and not just from the G20 - to come to the table to discuss appropriate state behaviour and related governance measures for cyberspace, ones which inter alia address civil rights especially privacy, freedom of expression and surveillance.

53. The working methods of the SRP and the ten-point plan should be indicative of a holistic approach to the subject of privacy protection and promotion in the digital age. A holistic approach helps determine the overall picture of what needs to be done but the timing of precisely what needs to be done by whom and when will depend on two main factors: i) the resources available to pursue the action plan and to complete the thematic studies and ii) the willingness of various stakeholders to accept and promote a privacy-friendly agenda as opposed to clinging on to a “command and control mentality”. To those who at first glance may find the Action Plan to be not only ambitious but possibly over-ambitious, the SRP’s message is clear and simple: if you agree with the objectives of the plan and with its integration of a number of complex but inter-related issues then come forward and contribute additional resources for the implementation of part or all of the plan. This would help achieve the transition from over-ambitious to ambitious. The SRP is building on his experience as an experienced project manager with a successful track record in raising tens of millions of Euro/dollars for privacy-related research to work on a strategy to increase the resources available to the mandate and the ten-point plan is posited on the success of that strategy. Even if this strategy is completely successful, the SRP fully expects that continuation and completion (if ever) of parts of the Ten Point Action Plan would fall upon the next mandate holder. The challenge at this stage is to provide a clear comprehensive vision and strong foundations which can form the basis of solid, evidence-based policy making in the field of privacy protection.

Annexes

Annex I. Some challenges faced by the SRP & a vision of the mandate

1. The fact that the mandate on privacy is a new one presents both advantages and disadvantages. Amongst other things it means that the Special Rapporteur on Privacy (SRP) had no roadmap to follow and indeed one of his first priorities in this case is to work on designing and developing such a roadmap. This means that some of the issues identified in this and later reports are not necessarily capable of being resolved within the time-constraints imposed by one or even two three-year mandates. They are mentioned however in order to provide a more holistic picture of what needs to be done in the short, mid and long-term. In doing so, this incumbent is conscious of possibly identifying issues which may possibly be more appropriately tackled in a more timely manner by later holders of the mandate.
2. One of the recurring themes of this and later reports will undoubtedly be the time dimension. The rapid pace of technology and its effects on privacy means that action on some already-identified issues may increase or decrease in priority as time goes by while new issues may emerge fairly suddenly. It may also mean that sometimes it may be more opportune to launch or intensify action on a particular issue not necessarily because it is much more important than other issues but rather because the timing is right, because the different international audiences and classes of stakeholders may be far more sensitive and receptive to that particular issue for reasons and circumstances over which the Special Rapporteur may have absolutely no control but in which case it would be foolish not to take advantage of favourable opportunities which may result in the creation or improvement of privacy safeguards and remedies.
3. The later prioritisation of action will also depend on the extent of the resources made available to the Special Rapporteur and the extent to which he can succeed in attracting fresh resources to support the mandate on privacy. This resource issue is fundamentally important and will directly affect the extent of the impact the mandate on Privacy may have in practice in real life. It is clear that, however good in quality in some respects, the quantity of resources provided to the mandate by the UN is woefully inadequate and even if the mandate's human and financial resources are increased ten-fold, it would still be hard-pressed to achieve the minimum required to persuade the incumbent that the work of the mandate is really making a difference to the protection of privacy of ordinary citizens around the world. The experience of the first six months in office has persuaded the mandate-holder that not only must the SRP be omni-present 24/7 on the many privacy-related issues which arise literally every day in many countries around the world but that he must also act as rainmaker, somehow attracting funds and human resources in order to make the work of the mandate both possible and sustainable in the short, mid and long-term. The effort required by what is, in essence, a part-time, un-paid position which must, by definition, co-exist with a demanding day-job, should not be under-estimated. This effort can be encouraged by the positive response of all stakeholders not least that of the nation-states, members of the UN to whom this report is addressed. If these stakeholders do not support the mandate adequately, if they do not put their money where their mouth is, then this will only serve to increase the frustrations already inherent to any work being carried out within the UN's systems and bureaucracy.
4. The incumbent's vision of the mandate is therefore analogous to the process required to design, finance, project manage and complete the building of a house or other building suitable for human beings to live and/or work in safely. Firstly we need to understand the function of the building: is it a residence for an individual living alone or for one nuclear family, or for a large and extended family or indeed for several of such

individuals and families? Should it include a working space and if so for what type of work: is this to be a farm-house, a baker's *casa bottega* or a black-smith's lodge or an urban block of multi-rise apartments? Form follows function so the function or functions must be clearly identified and understood in-depth. Secondly, form follows function so the design of the house – or the mandate's range of activities – must be completed on the basis of the function. Thirdly, the size of the building and its interior may be basic, cramped, spartan i.e. just barely enough to provide basic shelter and sanitation or else it may be more comfortable and spacious and functional or else it may be downright luxurious. Whether it is one or the other will depend on the resources and especially the finances which can be projected to be available to the builder – and these will influence the final design of the plan for the building – and the mandate. Fourthly, the time available to complete essential parts of the building will also influence the design of the plan. Fifth, it will need to be borne in mind that life gets in the way of the best-laid plans and the design may, from time to time, have to be more of an emergent design process rather than the fulfilment of a rigid, prescriptive pre-ordinate design. This analogy is useful to explaining the scope of this report especially to emphasize that while the building itself may not necessarily be capable of completion within the time-frame of one or even two three-year mandates, it is very important to decide on what the final building needs to be like, otherwise we would be unable to design the type of the foundations we require to build...and unless the foundations are sound and fit-for-purpose the building will ultimately prove to be unsustainable and collapse.

Annex II. A more in-depth look at Open Data & Big Data

1. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality.

2. At first sight Open Data sounds fine as a concept, a noble and altruistic approach to dealing with data as a common good, if not quite "common heritage of mankind". Who could object to data sets being used and re-used in order to benefit various parts of society and eventually hopefully all of humanity? It is what you can do with Open Data that is of concern, especially when you deploy the power of Big Data analytical methods on the data sets which may have been made publicly available thanks to Open Data policies. Of course, it is important to differentiate between data sets of one type and another. If what is put into the public domain consists of, say, the raw data arising out of tens of thousands of questionnaire responses about perceptions of privacy which responses would have been gleaned from across 27 EU member states and processed in an anonymised manner, the risk to individual privacy from aggregated data sets would appear to be very low if not non-existent. If, on the other hand, one uses Big Data analytical methods to develop links between supposedly anonymized medical data and publicly available electoral registers in a way that links identified or identifiable individuals to sensitive patient information then society has genuine cause for concern. Pioneers like Latanya Sweeney in the USA have demonstrated these abilities and exposed these risks on numerous occasions over the past two decades but the question remains: how should society intervene? More precisely how should policy-makers act in the face of such risks? Which is the correct information policy to develop and adopt? Especially since society has already intervened in a number of ways. Open Data is an information policy born out of specific information politics. For example, the EU legislated in favour of re-utilising public data more than 12 years ago (Directive 2003/98/EC), indeed five years after Prof Sweeney's first eye-opening discoveries.²⁸ Is this one of many cases where Open Data Policies were embraced before unintended consequences were properly understood and may now need to be remedied?

3. It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide. For the best part of forty years, our entire *forma mentis* has been founded upon something we call the purpose-specification principle. Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose. Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.

²⁸ "In 2000, Sweeney analyzed data from the 1990 census and revealed that, surprisingly, 87 percent of the U.S. population could be identified by just a ZIP code, date of birth, and gender" according to Caroline Perry, SEAS Communications "You're not so anonymous" October 18, 2011 last accessed on 13 Jan 2016 at <http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/>. However, in testimony to the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS") on 15 June 2005 Sweeney states that it was in 1997 that she "was able to show how the medical record of William Weld, the governor of Massachusetts of the time could be re-identified using only his date of birth, gender and ZIP. In fact, 87% of the population of the United States is uniquely identified by date of birth (e.g., month, day and year), gender, and their 5-digit ZIP codes. The point is that data that may look anonymous is not necessarily anonymous". http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf last accessed on 13 January 2016

4. The purpose-specification principle is not something invented by Europeans. One of the first places where it is articulated as such is in a 1973 report by an Advisory Committee to the US Department of Health²⁹ where it was held that “There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent” This quickly became a fundamental value in many other fora. The OECD Guidelines of 1980 have the Purpose specification Principle as the third out of eight principles “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose”. In this context it is also important to note the OECD’s corollary fourth principle usually recognised as the Use Limitation Principle whereby “Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3 above except a) with the consent of the data subject; or b) by the authority of law” These principles are also found in the Council of Europe’s influential Data Protection Convention of 1981 and the EU’s Data Protection Directive (46/95).

5. In an important regional development, the European Union is now at an advanced stage of devising and implementing the next generation of its data protection laws. When one examines the texts produced by the EU between 2012 and 2015, it is not as if the European Union appears ready to abandon the principle of purpose limitation. In the latest available version³⁰ of the draft text of the EU’s General Data Protection Regulation (GDPR) the importance of the purpose specification principle does not appear to be in any way to be diminished. Article 5 b retains the principle prominently, stipulating that personal data shall be

- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

an approach reinforced by the next principle to be found in the GDPR’s Article 5 which lays down that personal data shall be

- (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

6. The meaning of these key principles had been similarly announced in the recitals of the GDPR

²⁹ DHEW Secretary’s Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41

³⁰ s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf

- (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

7. It is clear therefore that the current thinking in Europe on Data Protection still relies on the purpose specification principle taken in tandem with anonymization or deletion despite all the risks inherent in the use of Big Data Analytics and Open Data. Likewise, in the United States where on May 9, 2013, President Obama signed an executive order³¹ that made open and machine-readable data the new default for government information³², some have attempted to downplay the concerns raised by Latanya Sweeney and have generally held that the risks of de-identification are not as great as previously made out.³³ Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab³⁴ and some of her more recent research³⁵ persuade the SRP that we are running the risk of using outmoded safeguards, almost twenty years after our attention was drawn to the fact that stripping personal data of some basic identifiers may not be enough to protect privacy.

8. A careful examination of the pivotal thinking in Europe in 2015-2016 does not provide much reassurance especially if one carefully examines the pertinent part of the latest version³⁶ available of the draft EU General Data Protection Regulation which holds that

- (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

9. This latest version from December 2015 after negotiation with the Council is less detailed than the one approved by the Parliament in October 2013 which held that

³¹ <https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government>- last accessed on 13 Jan 2016

³² <https://www.whitehouse.gov/open> last accessed on 13 January 2016

³³ See for example Barth-Jones, Daniel C. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now" June 2012 last accessed on 13th January at <https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf>

³⁴ <http://dataprivacylab.org/index.html>

³⁵ Sweeney L, Matching Known Patients to Health Records in Washington State Data, 2012 last accessed on 13th January 2016 at <http://dataprivacylab.org/projects/wa/1089-1.pdf>

³⁶ http://www.emeeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 last accessed on 13th January 2016

- (23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

10. Is the change an improvement, a factor which strengthens privacy protection in the era of Open Data or Big Data or is it a compromise which weakens protection? Whereas, it seems to the SRP that the very standard formulation of October 2013,³⁷ dependant as it was on the costs and time required to identify an individual, is rapidly becoming archaic in the era of big data analytics, the rather vaguer 2015 version seems to be a bit more elastic, but that could be a double-edged sword. If we are to insist on maintaining information policies built around the principles of Open Data then we need to develop much stronger, complex algorithmic solutions and procedural safeguards. The application of the newest EU proposals pivot almost entirely on what constitutes anonymous data yet Latanya Sweeney³⁸ and others have clearly demonstrated that there are huge limits to anonymization and it would seem that practically most personal data may actually be identifiable with such minimal effort that they would not meet eligibility criteria to qualify as anonymous data, thus bringing the GDPR into play.

11. Things get even more complicated when taking into consideration the factors legitimising research³⁹

- (88) For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

12. While the issue of sensitive data such as health information still presents a quandary within the EU's GDPR

³⁷ "unofficial consolidated version" <https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-unofficial-consolidated-LIBE.pdf> last accessed on 13th January 2016

³⁸ <http://latanyasweeney.org/publications.html>

³⁹ Though this recital 88 has been expanded in the latest 17 Dec 2015 version

- (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

13. How do Open Data and Big Data analytical capabilities fit into the scenarios and thinking portrayed above? Which would be the suitable safeguards to apply in Open Data policies which would protect privacy in the era of Big Data? Are the latest legal innovations being contemplated in Europe the right response to the evidence presented by Sweeney and do they represent best practice for the world to follow or dubious practice for the world to shun? The only thing that is certain is that if we are to get things right then it is clear that we need much more in-depth analysis of both the risks of Open Data as well as existing and new safeguards. Moreover, in this field too there appears to be a huge need for increasing public awareness. Relatively few people seem to know about the existence of open data policies or the consequences of applying big data analytics to different data sets put into the public domain by Open Data policies. In the course of participating in debates about Open data and Big data during tenure as SRP, one reinforced the impression that Open Data policies and their privacy and autonomy implications remain very much an area of interest to a tiny group of domain specialists and then again may be restricted further by the language in which they are made available to the public. The SRP is very sensitive to and is working with NGOs interested in protecting personal data in a number of sectors, including medical data and will, during 2016-2017 be engaging in events aimed at promoting discussion and on-going, in-depth investigation of related matters. The SRP is also very concerned that entire nations or trading blocs including major nations or regional federations such as China, the European Union and the United States have adopted or are adopting Open Data and Big Data policies the far-reaching consequences of which may not as yet be properly understood and which may unintentionally put in peril long-standing social values as well as the fundamental rights to privacy, dignity and free development of one's personality. Some studies on posthumous privacy suggest that in 2016 the citizens of some countries may be better off dead from a privacy point of view since their rights to privacy are better protected by law if they are dead than if they are alive in a world where Open data and big data analytics are a way of life endorsed by the information policies of the countries concerned. These developments may well be unintentional but the impact on privacy, autonomy, dignity and free development of personality may be far-reaching.

Annex III. Further reflections about the understanding of privacy

A. Core Values and Cultural Differences

1. As a result of the processes described in Section III of the report, an improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age.

2. This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to restrict privacy in a proportionate manner. The Special Rapporteur invites all actors in the field to contribute to the development of this urgently needed and improved understanding of the right to privacy and is convinced that significant progress is possible.

B. Enforcement

3. Apart from the absence of a clear universal understanding of privacy, the lack of effective enforcement of the right is an issue which is evident at most turns of the debate. Thus, not only is it not entirely clear what needs to be protected but also how to do it. Regretfully though perhaps hitherto inevitably, the super-fast development of privacy-relevant technologies and especially the Internet has led to a huge organic growth in the way in which personal data is generated and the exponential growth in the quantity of such data. This is especially evident in an on-line environment where, when seen from a global perspective, it would appear that the triangle of actors consisting of legislators, private (mostly corporate) actors and citizens all try to shape cyberspace using their possibilities in an uncoordinated manner. This may lead to a situation where none of the three is able to unleash the full potential of modern information technology.

4. In order to disentangle this triangular relationship an ongoing and open dialogue needs to be set up which eventually would provide for a more clear and harmonious regulation of cyberspace. This can only be achieved as a result of a sincere, open and committed dialogue of all parties which is to be held in a respectful and open manner. Sturdy and reliable bridges need to be built between all actors which are shaping the developments. It is the intention of the Special Rapporteur to listen closely to all parties and to facilitate this dialogue. In this way a basis for a positive and sustainable long-term development in the field of privacy protection should be achieved.

Annex IV A “State of the Union” approach to Privacy

1. It would appear to be useful to, at least once a year, have the SRP present an independent stocktaking report on where the right to privacy stands and this may be one of the primary functions of both the reports to be made to the Human Rights Council (HRC) and the General Assembly (GA). Since these reports are constrained by a word-limit it is clear that they can be little more than an extended executive summary of the findings and activities of the mandate throughout the reporting period. It should follow that the reports will also reflect the working methods of the mandate as outlined in Section II of the main report, in particular the thematic investigations as well as salient developments identified in the country monitoring activities carried out by the SRP team. It is expected that the report presented to the March 2017 session of the Human Rights Council would be the first such report reflecting a “State of the Union” approach. The report to the March 2016 session of the HRC will not attempt to prioritise risks or landmark improvements in privacy protection but simply refer to a few cases which illustrate particular progress or difficulties.
