United Nations A/HRC/31/64

General Assembly

Distr.: General
24 November 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*,**

Note by the Secretariat

In his 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 his mandate, together with his working methods and a three-year workplan. The report also contains an overview of the state of privacy at the beginning of 2016.

* The present report was submitted after the deadline in order to reflect the most recent developments.
** The annexes to the present report are circulated in the language of submission only.

GE.16-20847(E)
1620847

Report of the Special Rapporteur on the right to privacy

Contents

I. Introduction

1. The Human Rights Council established the mandate of the Special Rapporteur on privacy in its resolution 28/16 on the right to privacy in the digital age, in which the Council emphasized that States must ensure full compliance with their obligations under international human rights law. As regards the right to privacy, this is particularly challenging to achieve since 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 the above-mentioned resolution, the Special Rapporteur will report annually to both the Council and to the General Assembly. In the present report, the Special Rapporteur describes his working methods (section II), the state of privacy in 2016 (section III), his activities so far (section IV) and a 10-point plan that aims to discover and further develop the right to privacy in the twenty-first century (section V). In addition, he will present his conclusions in section VI.

3. The present report should be seen as being both modest and preliminary in nature, since it was prepared scarcely six months after the appointment of the Special Rapporteur on 1 August 2015. Consequently, despite the considerable efforts of the Special Rapporteur, there was not sufficient time to consult with the full range of stakeholders. The primary aim of the present report is therefore to identify a number of important issues, without necessarily prioritizing them. It is expected that the Special Rapporteur will, after having had the opportunity to listen to the concerns of many more stakeholders from around the world, be in a much better position within the next 12 months (namely, by January 2017) to prioritize the action that is required. The Special Rapporteur's vision for his mandate, together with the expected challenges facing him, are outlined in annex I.

II. Working methods of the Special Rapporteur

A. Country monitoring

4. A database of current policies, legislation, procedures and practices is being developed and populated with a variety of reports and relevant legislation. It will enable the Special Rapporteur to identify issues of concern, as well as best practices, which could then be shared with others.

B. Thematic studies: analysis and assessment

5. In a world that benefits greatly from an Internet without borders, the Special Rapporteur's consultations indicate widespread support for two general principles, namely: safeguards without borders and remedies across borders.

6. This concern for safeguards to protect privacy and remedies for breaches thereto underpins each of the following thematic studies by the Special Rapporteur in a number of sectors in which risks to privacy appear high. Each study is expected to lead to an ad hoc report, which will reflect ongoing consultations, interactions and observations.

1. Privacy and personality across cultures

7. This study responds to the need to achieve a better understanding of what privacy is, or should be, across cultures in 2016, in a way that is relevant to a digital age in which the

Internet operates without borders. In asking the question "why privacy?" and positing privacy as an enabling right as opposed to an end in itself, the Special Rapporteur is analysing privacy as a right that enables the achievement of an overarching fundamental right to the free, unhindered development of one's personality. That analysis is being carried out in close cooperation with several non-governmental organizations (NGOs) and is expected to be the focus of a major international conference, which will be organized in 2016. It is also being carried out in a wider context; one in which its relationship with other fundamental rights is also being examined. Thus, the relationship of privacy to freedom of expression and freedom of access to publicly held information is expected to be examined, inter alia, through joint action with other United Nations Special Rapporteurs. Discussions are already under way with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in order to explore opportunities for joint action on this topic during 2016 and 2017.

2. Corporate online business models and personal data use

8. During the first 25 years of its existence, the world wide web has led to the largely unregulated organic growth of private corporations, which have sometimes mushroomed into multinational entities operating across national borders and attracting customers throughout the world. One of the hallmarks of this growth has been the collection and use of personal data; every search, every item read, every e-mail or other form of messaging, every product or service purchased leaves hundreds of thousands of electronic traces, which can be aggregated to form a very accurate profile of an individual's likes, dislikes, moods, financial capabilities, sexual preferences, medical conditions and shopping patterns, as well as his or her intellectual, political, religious and philosophical interests and opinions. In general, the question arises of whether certain online service providers have the right to track individual behaviour so as to ensure just compensation. This increasingly detailed data map of consumer behaviour has resulted in personal data becoming a commodity. Access to, or exploitation of, such data is now one of the world's largest industries, generating revenues calculated in hundreds of billions of dollars, most usually in the form of targeted advertising. Very often it would seem that while consumers may be aware of the content that they themselves consciously put online they are much less aware of the quantity, quality and specific uses of the metadata that they generate when surfing, chatting, shopping or otherwise interacting online. The data available for the profiling of individuals are now several orders of magnitude greater than they were 25 years ago, while the extent of the risks for privacy associated with the use or misuse 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 those processing medical data, has increased to the point that an individual is not aware of, or does not give his or her consent to, the sale or multiple reselling of such data. There is not enough evidence available to properly assess the risks inherent in purportedly anonymized data, which can be reverse engineered in such a way as to be linked to an identifiable individual. Such a breach of privacy could pose multiple risks to an individual, as well as to the community concerned, especially if access is unauthorized and carried out, among others, by State authorities that are intent on acquiring or retaining power, organized crime syndicates or commercial corporations acting illegitimately. In the early days of digital computers, one of the main concerns was the use of personal data by States and their ability to correlate data held in various sources to form a detailed picture of an individual's activities and assets. In 2016, however, it would seem that much more data on individuals are held by corporations than by States. The vast revenues derived from the monetization of personal data mean that the incentive for changing the business model simply on account of concerns over privacy is not very high. Indeed, it was only when risks to privacy recently threatened the income potential of the business model that some corporations took a stricter, more privacy-friendly approach. It would now seem opportune for a global discussion to take place — one

informed by the collection of appropriate evidence — in order to determine what type of information policy is most suitable for maximizing the protection of, and minimizing the risk to, individuals' privacy in relation to the data collected about them by corporations. This discussion would be informed about the notions and expectations concerning privacy that citizens indicate in the course of paragraph 8. It is expected that the consultations that began in 2015 will involve online corporations in 2016, while a major public consultation event on this theme is being planned for 2017.

3. Security, surveillance, proportionality and cyberpeace

9. International concern with security remained at the forefront of developments throughout 2015 and into 2016. The country-monitoring process outlined above revealed several examples of legislation being rushed through national parliaments in an effort to legitimize the use of certain privacy-intrusive measures by security and intelligence services and law enforcement agencies in those particular States. In many of those countries, though unfortunately not all, the introduction of legislative measures resulted in public debate on:

(a) The adequacy of oversight mechanisms;

(b) The distinction between targeted surveillance and mass surveillance (or bulk surveillance as it is euphemistically called in some countries);

(c) The proportionality of such measures in a democratic society;

(d) The cost-effectiveness and the overall efficacy of such measures.

10. Countering terrorism and organized 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 Special Rapporteur has continued a programme of continuous engagement with law enforcement agencies and security and intelligence services worldwide in an effort to understand better their legitimate concerns, recognize best practices, which could be usefully shared, and identify policies, practices and legislation of doubtful usefulness or which present an unacceptable level of risk to privacy, both nationally and globally. In some instances, this ongoing analysis becomes almost inextricably entwined with issues of cybersecurity and cyberespionage. A small but growing number of States treat cyberspace as yet another theatre of operations for a multitude of security and intelligence agencies; they appear as yet unwilling to engage with each other — and sometimes with the Special Rapporteur — on these issues, which not unnaturally also has a direct impact on the privacy of citizens irrespective of their nationality. While not necessarily the primary target of cybersecurity and cyberespionage measures, the ordinary citizen may often get caught in the crossfire and his or her personal data and online activities may end up being monitored in the name of national security in a way that is unnecessary, disproportionate and excessive. Apart from the ad hoc investigatory work carried out to fulfil his mandate, the Special Rapporteur is fortunate to have access to a rich evidence base provided by previous and ongoing independent collaborative research in the security field, especially that funded by the European Union.[a] The Special Rapporteur is pursuing this study on four main fronts: (a) State surveillance capabilities that are proportionate in scope and adequately constrained by legislative, procedural and technical safeguards, including strong oversight mechanisms; (b) a focus on

[a] Including projects such as CONSENT, SMART, RESPECT, SiiP, INGRESS, E-CRIME, EVIDENCE, MAPPING, CITYCoP and CARISMAND.

targeted, as opposed to mass, surveillance; (c) the access of law enforcement agencies and security and intelligence services to personal data held by private corporations and other non-public entities; and (d) a renewed emphasis on cyberpeace. The Special Rapporteur strongly believes that cyberspace risks being ruined by cyberwar and cybersurveillance and that Governments and other stakeholders should work towards cyberpeace. In that sense at least, the protection of privacy is also part of the movement towards cyberpeace. In that way, cyberspace can truly become a digital space in which an individual can expect both privacy and security, a peaceful space that is not constantly being put in jeopardy by the activities of certain States over and above the threats posed by terrorists and organized crime.

4. Open data and big data analytics: the impact on privacy

11. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the appropriate balance between, on the one hand, the use of data for the benefit of society according to the principles of open data and, on the other hand, the established principles that have been developed so far with a view to protecting fundamental rights, like privacy, autonomy and the free development of one's personality. A more detailed account of the Special Rapporteur's concerns in this area is available in annex II.

5. Genetics and privacy

12. The Special Rapporteur notes that approximately one quarter of Member States have implemented national criminal offender DNA databases. Forensic DNA databases can play an important role in solving crimes but they also raise human rights concerns, including potential misuse of government surveillance (for example, identification of relatives and non-paternity) and the risk of miscarriages of justice. Furthermore, it would appear that the use of DNA databases for administrative ends, such as for identity cards or immigration, is set to increase exponentially. Moreover, within the next few years, it is likely that there will be moves towards 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 people 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 become more prevalent around the world. The Special Rapporteur intends to continue to engage with projects that aim to set international human rights standards for DNA databases, by establishing best practices and involving experts, policymakers and members of the public in open debate. It is expected that this engagement will contribute to the formulation of guidelines on best practices, to be developed with input and feedback from civil society actors.

6. Privacy, dignity and reputation

13. Concerns over security and surveillance have possibly been responsible for deflecting attention away from the other concerns shared by many citizens about the way in which their privacy, dignity and reputation are being put at risk on the Internet. The digital age means that media has developed and changed over the past two decades, especially in the way that the Internet has enabled normal citizens who do not have the benefit of formal training in journalism to publish text, audio and video content at will, at any time of day. That development has empowered citizens in many ways, especially in situations where censorship or other obstacles are bypassed or where technology facilitates freedom of expression in a way that enhances democracy in society. On the other hand, this new phenomenon of citizen-journalists and bloggers in a fast-moving media world, combined with widespread use of social media, has led to a generalized concern that the right to

freedom of expression is being abused with a consequent negative impact on other fundamental human rights, such as privacy and dignity. Research over the past five years has highlighted the ever-increasing concern of citizens as regards 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 breaches of privacy. The Special Rapporteur would like to collaborate with the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, civil society and other United Nations agencies, such as the United Nations Educational, Scientific and Cultural Organization, with a view to exploring concrete safeguards for one's privacy, dignity and reputation on the Internet, together with remedies for breaches thereto. As with a number of the other thematic studies outlined above, the relationship between privacy and Internet governance remains one of the underlying recurrent issues that is also relevant for privacy, dignity and reputation.

7. Biometrics and privacy

14. A survey of current research suggests that there has been a huge surge in interest in using biometrics for a variety of purposes, ranging from law enforcement to personal access to mobile devices. Thus, voice identification, retina scans, gait and face recognition, and fingerprint and subcutaneous fingerprint technology are just some examples of the many digital technologies that are being developed and deployed for various purposes in the second decade of the twenty-first century. The Special Rapporteur intends to continue cooperating with the biometric research community as well as with law enforcement agencies, security and intelligence services and civil society in an attempt at further identifying appropriate safeguards and remedies concerning the use of biometric devices.

C. Individual complaints

15. The Special Rapporteur has received, and will presumably continue to receive, especially as his mandate becomes more widely known, complaints of alleged infringements of privacy rights from individuals and civil society actors. These complaints are followed up through correspondence with both the complainants and the relevant government authorities. Such follow-up communication is carried out in accordance with the methodology used by special procedure mandate holders, which aim to clarify the allegations made, establish the facts and, where necessary, make recommendations for corrective action. These communications may also involve online or in-person meetings as appropriate. Should the evidence that has been received warrant particular or urgent attention, and the normal forms of communication prove not to be an appropriate response, the Special Rapporteur may consider issuing a public expression of concern.

D. Joint actions

16. The Special Rapporteur receives regular requests for, and sometimes initiates, joint action with other Special Rapporteurs. Details of such joint action are published separately in the communications report under special procedures.

17. As at 5 March 2016, there has not been the time to collect enough evidence in any of the categories listed above to do more than take part in two joint actions. It is expected, however, that the information collected in each category will be combined to provide the evidence base required to pursue Special Rapporteur dialogue and cooperation with relevant States, including through communications, country visits and other means of collaboration.

E. Building bridges and a policy of engagement

18. The Special Rapporteur has used his mandate to continue and expand the work previously carried out to build bridges with, and among, stakeholders. That has led to an ongoing policy of engagement with all types of stakeholders, including: government officials and ministers in their capitals or at bilateral meetings in international forums; meetings with several data protection and privacy commissioners, in particular with the Chair of the Article 29 Working Party of the European Union and the Chair of the Council of Europe's Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; discussions with technical standards bodies such as the International Telecommunication Union (ITU) and the Institute of Electrical and Electronic Engineers; in-depth meetings with civil society actors either individually or in groups; and meetings with human rights specialists or other officials from the permanent missions in Geneva. This list is merely illustrative and not complete. Invitations to deliver keynote speeches, participate in panel discussions and conferences and to meet with members of civil society are received almost daily. While many such invitations are accepted, especially those relating directly to the seven thematic studies indicated above, several others have had to be declined, especially in cases where time and/or budgetary constraints make such participation unfeasible. Among many other results, that policy of engagement has also witnessed the adoption of a resolution formalizing cooperation with data protection and privacy authorities,[b] which was adopted by the International Conference of Data Protection and Privacy Commissioners.

III. Privacy at the beginning of 2016

A. Definition and understanding

19. While the concept of privacy exists in all societies and cultures — and has done so throughout the history of humankind — there is no binding and universally accepted definition of such a notion.[c] To understand the right to privacy better it is necessary to consider it from two different perspectives. First, one should consider what the positive core of the right encompasses. Second, the question arises of how to delimit the right in the form of a negative definition. However, these two tasks have yet to be completed.

20. As reaffirmed by the Human Rights Council in its resolution 28/16, article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights form 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 relevant legislation, this means that worldwide there exists a considerable legal framework that could be useful for the protection and promotion of privacy. The usefulness of that legal framework is, however, seriously handicapped by the lack of a universally agreed and accepted definition of privacy. Even if 193 nations were signed up to the principle of protecting privacy, it would mean very little unless there was a clear understanding of what they had agreed to protect.

[b] Adopted at the International Conference of Data Protection and Privacy Commissioners, 27 October 2015, Amsterdam. Available from https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

[c] For a much more detailed insight into the Special Rapporteur'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*. *Volume I* (Oxford, Ashgate, 2015).

21. The absence of a universally agreed and accepted definition of privacy is not the only major challenge facing the Special Rapporteur. Even if the drafters of all the relevant legal instruments had included a universally agreed definition of privacy, there would still be the dimensions of time, place, economy and technology to consider. The passage of time and the impact of technology, taken together with the different rates of economic development and deployment of technology in different geographical locations, mean that the legal principles established 50 years ago (when the International Covenant on Civil and Political Rights was adopted) or even 35 years ago (for example, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) let alone 70 years ago (Universal Declaration of Human Rights) may need to be revisited, further developed and possibly supplemented and complemented to make them more relevant to the realities of today.

22. Given the lack of a universally agreed definition of privacy and considerations of time, place, economy and technology, it is clear that there is a need to establish an understanding of what privacy means to different people in different places in different circumstances across the planet. Such an endeavour would therefore seem *prima facie* to be not only a fundamentally important task but also a priority for the Special Rapporteur.

23. In some cultures, the privacy debate includes a debate on abortion. Without entering into the merits of such an approach, and so as to avoid any doubt, it should be stated that, at this preliminary stage of the mandate, the focus of the Special Rapporteur will be on informational privacy. Such an approach will focus on the function and role of privacy in determining the flows of information in society and the consequent impact on the development of an individual's personality. It will also include related issues, such as the distribution of power and wealth within society. When doing so, however, it becomes clear that it is not only privacy that has an impact on the flow of information in society, but also other rights, such as freedom of expression and freedom of access to publicly held information. All of these rights are important and a commitment to one right should not detract from the importance and protection of another right. Considering rights in conjunction wherever possible is more productive than seeing them as being in opposition to each other. Thus, properly speaking, it is not helpful to talk of "privacy versus security" but rather of "privacy and security", since both privacy and security are needed. Both rights can be taken to be enabling rights rather than ends in themselves. Security is an enabling right for the overarching 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 of fundamental importance as regards autonomy and the ability of individuals to identify and choose between options in an informed manner as they develop their own personality throughout life.

24. When launching the debate on what privacy is and should be, the Special Rapporteur wishes to focus on fundamentals and to avoid the debate being sidetracked by what may be perceived, or indeed real, local or cultural differences at the fringes of privacy, as opposed to the strong core of privacy values that may eventually be found to enjoy universal consensus. In order to help focus a fresh, structured debate on fundamentals, the Special Rapporteur intends, with a certain degree of provocation, to posit privacy as being an enabling right as opposed to an end in itself. Several countries around the world have identified an overarching fundamental right to dignity and the free, unhindered development of one's personality. Countries as geographically disparate as Brazil and Germany have this right written into their constitutions and it is the Special Rapporteur'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 recognized rights, such as those to privacy, freedom of expression and freedom of access to information, constitute a triad of enabling rights that are best considered in the context of their usefulness in enabling a human being to develop freely his or her personality. 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. That type of approach should help all participants in the debate, irrespective of which country or culture they may hail from, to focus on the fundamentals of developing one's personality and what kind of a life one would like privacy to help protect, rather than losing too much time on what privacy-relevant traditions in any given culture they would need to focus on or defend/promote.

25. It will be seen that, in many cases, the debate on privacy cannot be meaningfully divorced from that on the value of autonomy or self-determination. The latter term is one that has been discussed at length and, when related to privacy and personality rights, it has since 1983 in Germany given 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 on the protection and promotion of the fundamental right to dignity and the free, unhindered development of one's personality.

26. The triad 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, however, has had an enormous impact on these rights, both offline (for example, through credit cards, radio-frequency identification and other electronic systems) and online where, today, netizens generate tens of thousands of more data sets about themselves than they did two decades ago, before they started going online. Mobile devices and converging technologies, such as mobile smartphones — where telephony, the Internet and photography converge — create a new way of life, new comforts and new expectations both in terms of convenience and privacy.

27. The impact of new technologies also means that the distinctions between individual and collective privacy may have to be revisited, along with expectations of privacy in both public and private spaces, in the context of dignity and the free, unhindered development of one's personality.

B. Initial observations in 2015 and 2016

28. Choosing which were the most important events as regards privacy since taking up his mandate is a difficult task, especially as the necessary resources were not available to carry out a rigorous investigation into such events. Moreover, the Special Rapporteur does not wish to infringe on the important role played by civil society actors, such as Privacy International and its affiliates, which for the best part of 20 years have organized their Big Brother Awards,[d] shining a light on privacy deeds and misdeeds. On the other hand, the Special Rapporteur would like to commend good practices, laws, court decisions or indeed ideas that might promote and increase the protection of privacy. Therefore, without wishing to claim that this is an exhaustive list, and in no particular order, the Special Rapporteur would like to bring the following important developments to the attention of the Human Rights Council.

1. Wise restraint — a no to back-door communications from the Netherlands and the United States of America

29. The Governments of the Netherlands and the United States of America should be complimented on the restraint that they demonstrated in their unwillingness to allow the

[d] www.bigbrotherawards.org.

law to be used to engineer back doors in communications. On 4 January 2016, it was announced that the Government of the Netherlands formally opposed the introduction of back doors in encryption products. In a government position paper,[e] published by the Ministry of Security and Justice and signed by the security and business ministers, the Government claimed that it was currently not appropriate to adopt restrictive legal measures against the development, availability and use of encryption in the Netherlands. The conclusion came at the end of a five-page run-through of the arguments for greater encryption and the counterarguments for allowing the authorities access to information. By introducing a technique into an encryption product that would give the authorities access, encrypted files would also be made more vulnerable to access by criminals, terrorists and foreign intelligence services. It could have undesirable consequences for the security of information communicated and stored, and the integrity of information and communications technology systems, which are increasingly of importance for the functioning of society.

30. The position of the Government of the Netherlands seems to be more clear-cut than that of the Government of the United States, which preceded it by some three months. In early October 2015, the Director of the Federal Bureau of Investigation, James Comey, Jr., said in testimony on Capitol Hill that the administration was not, for now, pressing for legislation that would force companies to decrypt customer data. What is of greater concern, which came to the fore in the recent case brought against Apple, is that the United States 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. The Special Rapporteur's position on that case has been largely, though independently, articulated in the statement of the United Nations High Commissioner for Human Rights on 4 March 2016.[f] It is encouraging to note the latest comments made by the United States Secretary of Defense, Ashton Carter, when he declared that strong encryption was essential to the nation's security. Speaking to an audience composed of specialists from the technology industry on 2 March 2016, he said that he was not a believer in back doors or encryption programmes that leave openings for outsiders to read coded files. This is consistent with his statements in October 2015[g] and is a position that should be encouraged and reinforced.

2. The beginning of the judicial end for mass surveillance — the substantive issue

31. On 6 October 2015, the Court of Justice of the European Union delivered a judgment in the case of *Maximillian Schrems v. Data Protection Commissioner*. The Court declared void a decision by the European Commission that established the so-called "safe harbour" framework and which was based on directive 95/46/EC. The Special Rapporteur would like to highlight 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 ….

[e] Available from www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015 (accessed 23 August 2016).

[f] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E.

[g] See http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu.

32. Some debate will doubtless ensue over the precise meaning of "access on a generalized basis" and here the Court is clearly referring to the content of communications as opposed to metadata, but it will be interesting to see which European law legitimizing mass surveillance, if any, would pass the test of such a standard if the Court is inclined to continue to apply it strictly. The ambiguity, however, is at least partially dispelled when the *Schrems* decision is read together with the *Zakharov* judgment indicated below, which constitutes European Union law as much as it does law in other Council of Europe member States.

3. The importance of having a remedy — enforcement and procedural issues

33. Again with reference to the *Schrems* case, the Special Rapporteur welcomes the fact that the Court of Justice has become a forum for people such as the applicant, who 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 supranational public institution, challenging existing power relations, is essential in creating knowledge to enhance the welfare of our society and is consistent with the development of international human rights law. The existence of such mechanisms is absolutely crucial in protecting human rights and restoring trust in the use of technology by States or other actors.

34. It is also the harbinger of a new development in society; it points to the fact that rights need to be respected and enforced everywhere not just in the place where servers are based.

35. The Court of Justice judgment 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.

4. The mere existence of a secret surveillance measure is a violation of the right to respect for private life

36. The Grand Chamber of the European Court of Human Rights — in its judgment of 4 December 2015 in the case Roman *Zakharov v. Russia*[h] — 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 Freedoms (European Convention on Human Rights). In addition, and very interestingly, the Court accepted that, if certain conditions were satisfied, an applicant could claim to be a victim of a violation of article 8 owing to the mere existence of a secret surveillance measure. Perhaps most importantly was the declaration by the Court that outlawed mass surveillance systems in a way that was even more explicit than that of the Court of Justice in the *Schrems* case:

> 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

[h] *Roman Zakharov v. Russia* [GC], 4 December 2015, no. 47143/06, Reports of Judgments and Decisions.

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.

37. That decision sets up a very important benchmark highlighting the requirements for reasonable suspicion and prior judicial authorization 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". That would then be the test against which all existing and new proposed legislation about surveillance in any European country must be measured. The Special Rapporteur also notes with grave concern various reports about a decision of the Russian Duma (Parliament) that would enable decisions of the European Court of Human Rights to be overruled.[i] If those reports are true, that may, in practice, remove a very important remedy available to citizens of countries that have ratified the European Convention on Human Rights, including remedies in the case of violation of the right to respect for private life. The Special Rapporteur invites the Government of the Russian Federation to assist him in further verifying those 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 its remedies against the State in cases where their right to privacy is infringed.

5. The investigatory powers bill of the United Kingdom of Great Britain and Northern Ireland

38. Recognition is due to three United Kingdom parliamentary committees — the Science and Technology Committee (on 1 February 2016), the Intelligence and Security Committee of Parliament (on 9 February 2016) and, most importantly, the Joint Committee on the Draft Investigatory Powers Bill itself (on 11 February 2016) — for their consistent, strong, if occasionally overpolite, criticism of the draft investigatory powers bill, which is currently making its way through Parliament. The Joint Committee on 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 Government of the United Kingdom, which has taken heed of advice from various quarters and which is using the bill to introduce much-needed reinforcement of oversight mechanisms. While there may still be some room for improvement in this area, the steps taken are in the right direction. However, at the time of submission of the present report, the Special Rapporteur has serious concerns about the value of some of the revisions most recently introduced to the latest version of the bill, which was published on 1 March 2016. At the time of writing, not only do some of the Government's proposals appear to run counter to the logic and findings of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism in his 2014 report dealing, inter alia, with mass surveillance,[j] but they prima facie fail the benchmarks set by the Court of Justice in the *Schrems* case and the European Court of Human Rights in the *Zakharov* case. The Special Rapporteur strongly encourages the three committees commended above to continue, with renewed vigour and determination, to exert their influence so that disproportionate, privacy-intrusive measures, such as bulk surveillance and bulk hacking as contemplated in the bill, are outlawed rather than legitimized. It would appear that the serious and possibly unintended consequences of

[i] See www.bbc.com/news/world-europe-35007059.

[j] A/69/397.

legitimising bulk interception and bulk hacking are not being fully appreciated by the Government. Bearing in mind the huge influence that United Kingdom legislation still has in more than a quarter of the Members States of the United Nations that still form part of the Commonwealth, as well as its proud tradition as a democracy that was one of the founders of leading regional human rights bodies, such as the Council of Europe, the Special Rapporteur encourages the Government to take this golden opportunity to set a good example and step back from taking disproportionate measures that may have negative ramifications far beyond the shores of the United Kingdom. More specifically, the Special Rapporteur invites the 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 United Kingdom parliamentary committees, run counter to the most recent judgments of the Court of Justice and the European Court of Human Rights and undermine the spirit of the very right to privacy. Finally, the Special Rapporteur invites the Government to work closely with him, especially in the context of his thematic study on surveillance, in an effort to identify proportionate measures that enhance security without being overly privacy intrusive.

6. First small steps towards cyberpeace?

39. The lead taken by China and the United States to start defusing the situation in cyberspace deserves recognition.

40. There are possibly three main dimensions to cyberpeace, which are all threatened by online espionage:

(a) Sabotage and warfare;

(b) Intellectual property rights and economic espionage;

(c) Civil rights and surveillance.

41. While privacy is mostly concerned with the third dimension, it also often appears in discussions involving the other two dimensions. In September 2015, it was announced that the United States 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 behaviour in cyberspace within the international community. The countries also agreed to create a senior experts group for further cyber affairs discussion."[k] Not only did the United States 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."[l] That is still some way off from achieving complete agreements about cyberwar or online surveillance and the impact of espionage on the privacy of citizens, but at least it is a start and the Special Rapporteur can but try to persuade all parties concerned that the discussions should extend to include concrete measures for the respect of online privacy, too.

[k] See www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

[l] See http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement.

IV. Highlight activities of the Special Rapporteur

A. Resourcing the Special Rapporteur's mandate

42. 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 1 August 2015 — that is, when most of Europe was on holiday — it took several weeks for the Special Rapporteur to be provided with any form of support by the Office of the United Nations High Commissioner for Human Rights. For the time being, such administrative support is being provided on a temporary basis, pending recruitment of staff, which is expected to be completed by June 2016. On assessing the resourcing situation, the Special Rapporteur took immediate steps to source funding from outside the United Nations. A post-doctoral researcher (with a PhD in privacy and the right to be forgotten) was recruited with effect from October 2015 on a part-time basis and, with effect from January 2016, on a full-time basis in order to provide assistance on substantive issues. The external funding will continue until the situation regarding human resources is resolved. Voluntary assistance has also been very kindly provided by specialists and other staff from institutions for which the Special Rapporteur is working, namely the Department of Information Policy and Governance within the Faculty of Media and Knowledge Sciences at the University of Malta and the Security, Technology and e-Privacy Research Group at the Faculty of Law at the University of Groningen in the Netherlands. That assistance, which — together with that of United Nations staff in Geneva — is very gratefully acknowledged, enables the Special Rapporteur to carry out his functions until capacity is suitably increased and a more sustainable support structure, which is fit for purpose, can come into being.

B. A road map for the Special Rapporteur's mandate — formulating the 10-point plan

43. Over and above the daily activities outlined in section II, considerable time has been invested in developing the 10-point plan outlined in section V below and in consultations with the many stakeholders.

C. Engagement in multiple events

44. The Special Rapporteur accepted invitations for meetings, conferences and panels and individual consultations, especially those that helped maintain an ongoing policy of engagement on the seven thematic studies outlined above. The following is a non-exhaustive list of such events:

(a) Panel discussion on "Inextricably intertwined: freedom of expression and privacy in Internet governance", MAPPING, First General Assembly, Hannover, Germany, 22 September 2015;

(b) Meeting with the Director of Global Affairs, Human Rights Watch, 30 September 2015;

(c) Participated in, and made presentation at, the Seminar on Data Protection and Privacy in Statistics, Geneva, 13-14 October 2015;

(d) Held a meeting with the Deputy Secretary-General of ITU, Geneva, 14 October 2015;

(e) Organized and led the panel on privacy and surveillance at the Conference on Intelligence in the Knowledge Society 2015, Bucharest, 16 October 2015;

(f) Delivered a keynote speech on privacy in the digital age at the International Conference of Data Protection and Privacy Commissioners, closed session, Amsterdam, 27 October 2015;

(g) Participated in the round-table discussion "tour du monde" at the International Conference of Data Protection and Privacy Commissioners, Amsterdam, 29 October 2015;

(h) Participated in multiple sessions, public and bilateral, at the Internet Governance Forum, João Pessoa, Brazil, 9-13 November 2015;[m]

(i) Delivered keynote speech during a closed meeting at the Big Data in the Global South International Workshop, Rio de Janeiro, Brazil, 16-17 November 2015;[n]

(j) Held meetings with officials at the Ministry of Justice of Brazil during an in-depth analysis of a new Brazilian draft law on privacy, Brasilia, 18 November 2015;

(k) Held joint meeting with officials from the Ministries of Telecommunications, Justice and the Interior of Brazil, regarding a new Brazilian draft law on privacy, Brasilia, 18 November 2015;

(l) Held meeting at the Prosecutor General's Office, Brasilia, 18 November 2015;

(m) Held meeting with the Director of Human Rights, Ministry of Foreign Affairs of Brazil, Brasilia, 19 November 2015;

(n) Delivered speech (by video link) at the Consumers International World Congress, Brasilia, 19 November 2015;[o]

(o) Held in-depth meetings and consultations with the founder and director of Patient Privacy Rights, Malta, 25 November 2015;

(p) Delivered a speech during the session on setting the scene at the High-level Conference on Protecting Online Privacy by Enhancing IT Security and EU IT Autonomy, which was jointly organized by the Committee on Civil Liberties, Justice and Home Affairs and the Science and Technology Options Assessment Panel of the European Parliament, Brussels, 8 December 2015;[p]

(q) Delivered a keynote speech at a conference on security and privacy in the context of a safe harbour 2.0, Rome, 9 December 2015;[q]

(r) Delivered a keynote speech on privacy, identity, security and freedom at the Privacy and Identity Lab annual congress, Utrecht, Netherlands, 11 December 2015;[r]

(s) Participated in an induction session for Special Rapporteurs, Geneva, 14-16 December 2015;

(t) Meeting with a delegation of the United Kingdom, Geneva, 17 December 2015;

[m] See www.intgovforum.org/cms/igf-2015-schedule.

[n] See http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global.

[o] See http://congressprogramme.consumersinternational.org/speakers.html.

[p] See www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy.

[q] See www.dimt.it/tag/cannataci.

[r] See www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published.

(u) Meeting with a delegation of China, Geneva, 17 December 2015;

(v) Meeting with a delegation of the Russian Federation, 17 December 2015;

(w) Participated by means of a video link in the special meeting of the Counter-Terrorism Committee on preventing terrorists from exploiting the Internet and social media to recruit terrorists and incite terrorist acts, while respecting human rights and fundamental freedoms, New York, 17 December 2015;

(x) Made presentation to, and led discussions with, an NGO round table, including representatives of Privacy International, Amnesty International, Reporters without Borders, Internet Society, Human Rights Watch and the American Civil Liberties Union, Geneva, 18 December 2015;

(y) Meeting with the Deputy Director of the ITU Telecommunication Standardization Bureau (joined by the ITU Legal Unit), Geneva, 18 December 2015;

(z) Intervened and gave presentation by video link on privacy, quality of life and smart cities: scaling-up "surveillable" to an ITU conference on smart cities, Singapore, 18 January 2016;

(aa) Meetings with Helen Wallace and Andrew Jackson of GeneWatch UK, Malta, 3 February 2016;

(bb) Delivered keynote speech (by video link) at the Fifth Workshop on Data Protection in International Organisations, Geneva, 5 February 2016;[s]

(cc) Delivered keynote speech and participated in a general meeting for stakeholders of the Ministry of Foreign Affairs of the Netherlands, The Hague, Netherlands, 3 March 2016.

V. Ten-point action plan

45. In order to further elaborate on the dimensions of the right to privacy and its relationship with other human rights, the Special Rapporteur has developed an outline 10-point action plan. It should be borne in mind that the points mentioned in the plan are presented in no particular order and do not imply a specifically prioritized working programme. The Special Rapporteur sees his role as akin 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 countries that require urgent work to be done regarding the issue of responsibility. The 10-point action plan below is a to-do list and not a mere wish list. The Special Rapporteur has already started work on each of the 10 points, but progress will be determined by the availability of time and resources.

1. The meaning of the "the right to privacy"

46. Going beyond the existing legal framework to a deeper understanding of what has been 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 twenty-first century? How can it be better protected in the digital age? Activities will be organized and research will be supported to examine possible answers to those key questions, which will help provide essential foundations for other parts of the Special Rapporteur's action plan.

[s] See www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations.

2. Increasing awareness

47. Another important issue is the development of greater awareness among citizens in order to help them understand what privacy is. It is important to have a general discourse on what their privacy rights are and how their privacy may be infringed upon, especially by new technologies and their behaviour in cyberspace. They need to learn how their personal data is monetized and what are the existing safeguards and remedies to protect their right to privacy. What can they do to minimize the risk of infringements to their right to privacy and how can they interact with lawmakers and the corporate sector to improve privacy protection? Raising awareness is a considerable undertaking, and the Special Rapporteur intends to contribute throughout his mandate to this task through his ongoing engagement with all stakeholders, especially civil society.

3. The creation of a structured, ongoing dialogue about privacy

48. The establishment of a more structured, open, comprehensive, effective and, most importantly, permanent dialogue among the different stakeholders is crucial. In order to protect privacy, bridges need to be built. The Special Rapporteur intends to place great emphasis on that activity, using existing forums as well as creating new ones. Of great importance in that respect is the facilitation of structured dialogue among NGOs, data protection and privacy commissioners, law enforcement agencies and security and intelligence services. It is essential to work with all categories of stakeholders in order to improve internal procedures, increase the level of privacy by incorporating measures to protect it in the design of the technologies they deploy and the procedures they follow. It is important to maximize transparency and accountability and reinforce impartial and effective oversight to the point at which it becomes significantly more effective and credible.

4. A comprehensive approach to legal, procedural and operational safeguards and remedies

49. Appropriate safeguards and effective remedies have been part of the raison d'être of data protection law since its inception. Such law aims to provide guidance and protection at the appropriate level 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 cases in which an infringement actually occurs. The search for safeguards and remedies is transversal and underlies all of the Special Rapporteur's thematic studies, which were identified in section II above.

5. A renewed emphasis on technical safeguards

50. The safeguards and remedies available to citizens can never be purely legal or operational. Law alone is not enough. The Special Rapporteur 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.

6. A specially focused dialogue with the corporate world

51. Today, an increasing number of corporations 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 in which personal data has been heavily monetized? 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 Special Rapporteur has already

commenced direct contacts with representatives from the corporate world and will maintain a privacy-focused dialogue relevant to these issues with a range of industry players with the intention of staying informed about new developments in the corporate sector as well as providing information to them on other parts of his mandate.

7. Promoting national and regional developments in privacy protection mechanisms

52. The value of national and regional developments in privacy protection mechanisms should be more appreciated at the global level. The Special Rapporteur has an important complementary role to play when working in close cooperation with data protection and privacy commissioners worldwide. Through mutual cooperation and dialogue, the global standards of privacy protection could be raised significantly. The Special Rapporteur has commenced a series of global activities planned and executed with data protection authorities. Those include events planned to take place in Australia, Morocco, New Zealand and Tunisia, as well as in Northern Ireland for 2016, with many others in the pipeline in the coming years.

8. Harnessing the energy and influence of civil society

53. Having already met with representatives of 40 NGOs during his first six months in office, the Special Rapporteur 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 worldwide.

9. Cyberspace, cyberprivacy, cyberespionage, cyberwar and cyberpeace

54. The global community needs to be inquisitive, frank and open about what is really going on in cyberspace, including the realities of mass surveillance, cyberespionage 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 indicated in section II above. The Special Rapporteur expects these issues to be a constant feature of a number of his reports, as well as many of the country visits and, by transparently engaging with stakeholders on these issues, he hopes to play a constructive role in improving the protection of privacy in the digital age.

10. Investing further in international law

55. While law alone is not enough, it is very important. The potential for developing international law concerning privacy should be explored in all its forms; the Special Rapporteur is open to examining the value of any legal instrument irrespective of whether it is classified as soft or hard law. A priority issue such as updating 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 among several stakeholders that one of these legal instruments could take the form of an additional protocol to article 17 of the International Covenant on Civil and Political Rights,[t] on the subject of which the Special Rapporteur is being urged "to promote the start of negotiations on such a protocol within his first mandate".[u] The precise timing of this should, however, probably be contingent on the duration and outcome of in-depth and wide-ranging discussions under point 1 above — that is, achieving a better universal understanding of what the core values are or may be in privacy. Some other privacy-relevant matters, especially issues of

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

[u] Ibid.

jurisdiction and territoriality in cyberspace, cannot be addressed satisfactorily unless there is a clear international agreement to that effect; one that would normally take the form of a multilateral treaty, most probably on a specific topic or set of issues. So as to avoid doubt, it should be stated that what is envisaged is not a new, global, all-encompassing international convention, covering all issues related to privacy or Internet governance. It is far more realistic to expect that the protection of privacy can be enhanced through the incremental growth of international law and thus the clarification and, eventually, the extension of existing legal instruments. In the mid to long term, that might include the development of entirely new legal instruments. Ongoing discussions about international law and new legal instruments in the field of Internet governance will also be monitored by the Special Rapporteur in order to determine the timing of action within United Nations bodies, as well as the type and scope of the legal instrument that the Special Rapporteur may eventually wish to recommend to the Human Rights Council and the General Assembly.

VI. Conclusions

56. **The Special Rapporteur has been impressed by the overwhelmingly warm and enthusiastic welcome that he has received from most sectors of society and most categories of stakeholders.**

57. **Privacy has never been more at the forefront of political, judicial or personal consciousness than in 2016.**

58. **The tensions between security, corporate business models and privacy continue to take centre stage, but the past 12 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 worldwide, especially in the United States and Europe, have struck clear blows in favour of the right to privacy and especially against disproportionate, privacy-intrusive measures, such as mass surveillance or breaking encryption.**

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

60. **While some Governments continue with ill-conceived, ill-advised, ill-judged, ill-timed and occasionally ill-mannered attempts to legitimize or otherwise hang on to disproportionate, unjustifiable privacy-intrusive measures, such as bulk collection, bulk hacking and warrantless interception, other Governments, led in this case by the Netherlands and the United States, have moved more openly towards a policy of no back doors to encryption. The Special Rapporteur would encourage more Governments to coalesce around this position.**

61. **Countries worldwide are not only waking up to their responsibilities and to the realities of technical safeguards such as encryption, they are also slowly but surely realizing the limitations of gains and the enormity of risks should they bring ruin to cyberspace through cyberwar and cyberespionage. Progress still remains to be made in that area, but 2015 has seen some important beginnings. Therefore, the Special Rapporteur encourages Governments — and not just those from the Group of 20 — to come to the table to discuss appropriate State behaviour and related governance**

measures for cyberspace; ones that, inter alia, address civil rights, especially privacy, freedom of expression and surveillance.

62. **The working methods of the Special Rapporteur and the 10-point plan should be indicative of a holistic approach to the subject of protecting and promoting privacy in the digital age. A holistic approach helps determine the overall picture of what needs to be done, although the timing of precisely what needs to be done by whom and when will depend on two main factors: first, the resources available to pursue the action plan and to complete the thematic studies; and, second, 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 overambitious, the Special Rapporteur'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 interrelated issues, then come forward and contribute additional resources for its implementation. This would help make the plan more feasible. The Special Rapporteur is building on his experience as a project manager with a successful track record in raising tens of millions of dollars for privacy-related research to work on a strategy to increase the resources available to the mandate holder; indeed, the 10-point plan is posited on the success of that strategy. Even if that strategy is completely successful, the Special Rapporteur fully expects that continuation and (possible) completion of parts of the 10-point plan would fall to the next mandate holder. The challenge at this stage is to provide a clear, comprehensive vision and strong foundations that can form the basis of solid, evidence-based policymaking in the field of protecting privacy.**

Annex I

Challenges faced by the Special Rapporteur and his vision for the mandate

1. The Special Rapporteur immediately set about building up his 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. The team is often physically spread across at least three geographical 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.

2. 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.

3. 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.

4. 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 tenfold, 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.

5. 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 and 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.[v] 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

[v] "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.

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.

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 Health[w] 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 version[x] 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;

[w] 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.

[x] s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf.

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

> (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 order[y] that made open and machine-readable data the new default for government information",[z] 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.[aa] Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab[bb] and some of her more recent research[cc] 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 version[dd] 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.

[y] 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.

[z] https://www.whitehouse.gov/open last accessed on 13 January 2016.

[aa] 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.

[bb] http://dataprivacylab.org/index.html.

[cc] 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.

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

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

> (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,[ee] 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 Sweeney[ff] 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 research[gg]

> (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

> (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.

[ee] "inofficial consolidated version" https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf last accessed on 13th January 2016.

[ff] http://latanyasweeney.org/publications.html.

[gg] Though this recital 88 has been expanded in the latest 17 Dec 2015 version.

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 on the notion 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

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.