Advance unedited version

Distr.: General
24 February 2017

Original: English

Human Rights Council
Thirty-fourth session
27 February-24 March 2017
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*

Note by the Secretariat

In this report, the Special Rapporteur on the right to privacy (SRP) focuses on governmental surveillance activities from a national and international perspective. The SRP will elaborate on the characteristics and the interpretation of the international legal framework. The SRP will also describe recent developments and trends, how these can be studied, and how they interact with the enjoyment of the right to privacy and other interconnected human rights. Consequently, first approaches to a more privacy-friendly oversight of government surveillance will be outlined. Before concluding, the SRP will report on his activities in the relevant period for this report.

* The present document was submitted late so as to include the most up-to-date information possible.

Contents

I. Introduction

1. Pursuant to Human Rights Council resolution 28/16, the Special Rapporteur on the right to privacy (SRP) reports annually to the Council and to the General Assembly. The present report has the SRP reporting for the second time to the Council. In his previous reports, the SRP outlined his 10-point Action Plan and a strategy to tackle certain crucial contemporary issues relating to his mandate through activities in "Thematic Action Streams" (TAS). With these initiatives the Special Rapporteur hopes to contribute to raising the level of respect, protection and fulfilment of the right to privacy, which is challenged particularly by developments in the Digital Age.

2. Recently, the SRP has also published a statement entitled "Planned thematic reports and call for consultations", which presents the issues to be tackled in this and future reports as well as providing a timeline for their delivery.[1] This statement should be considered a standing invitation to all stakeholders in all countries around the world who wish to engage with the mandate. If you wish to contribute to or otherwise be involved in any of the mentioned initiatives all you need to do is to contact me and my team, preferably via e-mail (srprivacy@ohchr.org) and we will get back to you as quickly as possible.

3. As laid out in the opening summary statement, this report will focus on "First approaches to a more privacy-friendly oversight of government surveillance." The special rapporteur has already carried out several activities covering this subject during his mandate and will continue to do so. In an attempt to fulfil his tasks as outlined in Art 4 of A/HRC/31/64, annex and particularly in the surveillance sector, the SRP invested considerable effort in organising the International Intelligence Oversight Forum 2016 (IIOF2016), which was co-hosted by the Joint Permanent Commission of the Chamber of Deputies and of the Senate to exercise parliamentary control over the activity of the Romanian Intelligence Service, the Special Commission of the Chamber of Deputies and the Senate to exercise parliamentary control over the activity of the Foreign Intelligence Service in Romania, the Committee for Defense, Public Order, and National Security in the Romanian Chamber of Deputies and the Committee for Defence, Public Order, and National Security in the Romanian Senate, in association with the Department of Information Policy & Governance at the University of Malta and the Security, Technology & e-Privacy Research Group at the University of Groningen in the Netherlands. The event took place at the Palace of the Parliament in Bucharest, Romania on 11-12 October 2016. The event was very successful within its understandably modest objectives[2], Hence the SRP intends to continue co-organising IIOF on an annual basis. In 2017 it is planned to be held on the 20th and 21st of November in Brussels, Belgium and will be co-hosted by, amongst others, the Data Protection Authority of Belgium. IIOF is intended to enable the mandate of the SRP to tap into the practical experience and operational insights obtained by those many oversight bodies which have been set up around the world. This enables the SRP to

[1] The statement can be accessed via http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx as well as via https://www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/ - accessed on 07.12.2016. See also Annex I

[2] The objectives of IIOF2016, as stated in the formal invitation addressed to states were to start an open and frank debate in a trusted framework on the: adequacy of oversight mechanisms; existing and anticipated surveillance measures which may have a negative impact on privacy; distinction between targeted surveillance and mass surveillance; proportionality of such measures in a democratic society and cost-effectiveness and the overall efficacy of such measures.

better understand and reflect upon the realities of trying to achieve effective oversight of the activities of security and intelligence services (SIS) and the impact that this may have on Privacy. The first IIOF brought together nearly seventy participants from some 26 institutions in 20 countries. These included independent oversight authorities, parliamentary committees, some members of civil society and even an oversight tribunal. **The SRP considers that better thought-out and better resourced oversight of intelligence activities is one of the many complementary initiatives that may help improve the protection of the right to privacy world-wide.** Some would consider this to be THE most promising avenue for concrete measures to protect privacy. This remains to be seen. It is hoped that the series of annual IIOFs will contribute to the identification and sharing of good practices and eventually the considerable strengthening of oversight mechanisms in a large number of UN member states. It is hoped that these oversight mechanisms will have a strong basis in detailed and strict domestic laws that provide only proportionate measures necessary in a democratic society, and spelling out appropriate safeguards within the same law. These laws should also entrench effective oversight of both LEAs and SIS by properly resourced and independent oversight authorities. The series of annual IIOFs are expected to enable the SRP to, in an informed-manner and on as large an evidence-base as possible, "make recommendations to ensure [its] the promotion and protection of privacy, including in connection with the challenges arising from new technologies" in fulfilment of the mandate outlined in Art 4 (a) of A/HRC/31/64, annex.;

4. The oversight of surveillance by SIS is not the only thing that the SRP is doing about surveillance. The SRP monitors to the extent possible relevant new laws drafted world-wide and reports that concern use or abuse of surveillance. As a result, surveillance-related activity is one of the principal considerations when requesting formal country visits. This may be seen especially in the choice of requested country visits: the United States of America (19-24 June 2017), France (requested for 13-17 November 2017), the United Kingdom (late 2017, possibly 11-17 December), Germany (requested for 29 January-02 Feb 2018) and South Korea (03-15 July 2018). These are countries with strong democratic pedigrees and are states that the SRP expects to take a leadership role, in defining best practices and safeguards in the field of surveillance and fundamental human rights, especially privacy. Additionally, these countries have been particularly active in this area during the past several years, both in terms of applied surveillance technologies as well as new legislation. Each of these visits includes requests to meet intelligence services, oversight authorities, and ministers responsible for both law enforcement agencies (LEAs) and security and intelligence services (SIS). Moreover, to avoid re-inventing the wheel and with the objective of maximising synergy, the mandate is very closely following the proceedings and outcomes of other parallel initiatives such as the European Union-supported MAPPING project. The latter, launched in 2014, i.e. over a year before the HRC created the post of SRP and 18 months before the incumbent SRP entered into his role, has initiated various, relatively well-resourced, on-going discussions amongst stakeholders including one about the creation of an international legal instrument regulating surveillance. Those discussions are set to run for at least another year, i.e. end February 2018. The SRP intends to monitor the outcomes of these processes and then aims at taking a position about the desirability and feasibility of such an international legal instrument between March and July of 2018. It is possible that any position will be expressed in the report to be presented to the General Assembly in October 2018, again probably making related "recommendations to ensure the promotion and protection of privacy, including in connection with the challenges arising from new technologies" and this specifically in fulfilment of the mandate outlined in Art 4 (a) of A/HRC/31/64, annex. The SRP is also in contact and is collaborating with other entities or individuals who are taking initiatives to introduce a coherent framework to internationally coordinated intelligence oversight. The past 18 months of intensive work as SRP have established or further improved many fruitful working relationships globally, with authorities keen to work on some kind of

instrument articulating common standards for the conduct of particularly foreign signals intelligence functions. These are welcome developments that may still be some way off from fruition, very likely not within the term of the current mandate-holder. However, they are important first steps and the SRP mandate will continue to do all it can to promote and facilitate such initiatives.

5. This report deliberately focuses on governmental surveillance. For other areas of SRP activity it refers to the thematic action streams which have been outlined and described in the first report of the Special Rapporteur to the General Assembly.[3] It needs to be emphasized that the mandate deliberately separates the issue of security and surveillance from personal data held by corporations and other topics, such as Big Data and Open Data. The latter subjects have their own specific challenges and issues with regard to the right to privacy. These are being addressed separately and will, for the time being, and until they are later brought together in a "joined-up approach," continue to be tackled through different parallel initiatives set up by the SRP. For these reasons this report will focus on surveillance activities as carried out by a state, on its behalf or at its order.

6. Meanwhile work on the other TAS continues and will be presented in due course hopefully in accordance with the timelines referred to in para 2 above. In particular, the TAS on Big Data and Open Data is working on producing its first report to be discussed in a consultation session in July 2017. The outcome of this consultation session is expected to form the main focus of the October 2017 report of the SRP to the General Assembly. Additionally, following the success of the July 2016 event in New York, the mandate of the Special Rapporteur for Privacy has started to prepare the second edition of Privacy, Personality and Flows of Information (PPFI 2017 MENA) which will focus on the region of the Middle East and North Africa. It is planned to be held on the 22nd and 23rd of May in Tunis and will be co-hosted by the Tunisian Data Protection authority in close co-operation with Civil Society Organisations (CSOs). Preparations have likewise started for the third edition of PPFI, this time "Privacy, Personality and Flows of Information – Asia 2017". This event will, as the name suggests, have a special focus on Asia. This is planned to take place in Hong Kong on the 29-30th September 2017. If any government, CSO, corporation, Data Protection Authority, academic institution or individual is interested in participating in or supporting these initiatives feel free to contact the Special Rapporteur[4] at the earliest opportunity.

7. The SRP takes this opportunity to commend those governments which responded immediately and positively to his request for a formal country visit: Germany, France, South Korea, United Kingdom and United States and to lament the lack of response of a number of other countries. This may regrettably be the order of the day with some countries, but it is opportune and necessary to draw public attention to the impunity with which some governments deal with requests for country visits, leaving UN OHCHR staff chasing Permanent Missions in Geneva for a response to a request for a country visit to no avail. This is not yet the time to name and shame but it helps distinguish those governments that pay lip service to human rights and those that are prepared to engage with fair-minded approaches to improving the protection of privacy.

8. Before moving on to the main focus of this report, the SRP deems it necessary to draw urgent and immediate attention to a worrying practice in some states concerning the use of privacy laws to muzzle investigative journalism. This may be exemplified by events where it has been alleged that "privacy and data protection rights have been erroneously

[3] United Nations, A/71/368, p. 7 – 11.

[4] Please use the e-mail address srprivacy@ohchr.org or any other venues mentioned under http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

interpreted by the Executive and the national autonomous institute, and this in an attempt to "censor information within historical documents, so the access to documents from 30, 40 and even 120 years ago is hampered, clearly violating freedom of expression"[5] . Further allegations include "worrisome silences of the guarantee body in front of threats to privacy and clear attempts of the authorities to censor information of public interest on the grounds of data protection"[6]. The SRP has developed good relations with that national authority and has started examining such claims without yet making a final determination as to their veracity. It should be stated that this is not the first and only claim that the government of a country is using privacy as an excuse not to release information of public interest into the public domain. This is an area which may be the subject of a separate report and which is here being mentioned specifically to invite everybody and especially civil society organizations to report such instances to the special rapporteur in order that they may be further investigated in more detail.

9. The special rapporteur also welcomes the moves of countries like Brazil to join the family of nations that have adopted domestic privacy and data protection laws and encourages these to meet minimum standards such as those set out in Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS Convention 108).

II. Recent developments and worrying trends in governmental surveillance

A. Governmental surveillance and privacy in the digital age – the Status quo

10. The current dialogue on governmental surveillance has been stimulated by people like Edward Snowden and those supporting him. Albeit controversial from a national perspective, it has to be acknowledged that the information he shared with the public about actual practices of national security services has sparked a necessary debate about what privacy means and should mean in the digital age. His famous quote "I do not want to live in a world where everything I do and say is recorded."[7] has led to many crucial initiatives and actions.

11. The United Nations has followed up in several ways and called upon States in the resolution on privacy in the digital age "to establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data."[8] Regional Human Rights Courts, such as the European Court of Human Rights in Strasbourg, have handed down judgements that establish clear and

[5] Undisclosed source

[6] Undisclosed source

[7] Answer to the question: "Why did you become a whistleblower?"; MacAskill, Edward Snowden, NSA files source: 'If they want to get you, in time they will', The Guardian via https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why - accessed on 08.12.2016.

[8] United Nations, A/RES/69/166.

binding requirements that governments have to respect when establishing means to, and carrying out, surveillance.[9]

12. The SRP mandate follows developments in government surveillance world-wide in a number of ways, including regular contact with a number of national and international CSOs. Many of the latter do an excellent job in bringing various matters of concern to the attention of the SRP as well as to national governments and the world in general. Without in any way detracting from the value of the work of other CSOs, the SRP would like to single out for attention the usefulness of the efforts of the following CSOs with whom the mandate collaborates in a variety of ways: ACLU[10], Access Now[11], Amnesty International[12], APC[13], Article19[14], Human Rights Watch[15], INCLO[16] and Privacy International[17]. It is extremely beneficial when relevant reports by these and other CSOs are published since the 10,300 word limit afforded to the SRP in formal reports does not permit him to include a narrative on, say, developments on surveillance as one may find in the report submitted to him by Privacy International in November 2016 and since published on the PI website[18]. It is important to state that the SRP mandate share's PI's concerns about, and is independently following up related developments, in surveillance in Colombia, Estonia, France, Former Yugoslav Republic of Macedonia, (FYRM), Mexico, Morocco, New Zealand, Poland, Russia, Rwanda, South Africa, Sweden, Uganda, United Kingdom, United States of America, Venezuela and Zimbabwe. The SRP hereby invites the governments of these states to take note of the concerns expressed in the PI submissions and very preferably respond publicly to such concerns and/or communicate directly to the SRP mandate as may be appropriate to the circumstances.

13. However, and deeply concerning, since the day the above-mentioned UN resolution has been passed and despite such judgments as mentioned in the preceding paragraph, the status of the right to privacy in the surveillance area of activity has not improved since the last SRP report. The states that reacted, started to work on and pass new laws on the subject that only, if at all, contain minor improvements in limited areas. In general, these laws have been drafted and rushed through the legislative process with political majorities to legitimize practices that should never have been implemented.

14. Recently, on the 21st of December 2016, the Court of Justice of the European Union delivered a very important and welcome judgment to remind the member states of the European Union of their duties to respect, promote and protect the human right to privacy and others in the digital age. With regards to legal obligations which require the retention of data in bulk by Telecommunication providers it stated: "The interference entailed by such legislation in the fundamental rights […] is very far-reaching and must be considered to be particularly serious. The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives

[9] European Court of Human Rights, Zakharov vs. Russia, App. No. 47143/06, available via http://hudoc.echr.coe.int/eng?i=001-159324 – accessed on 08.12.2016.

[10] https://www.aclu.org/issues/national-security/privacy-and-surveillance

[11] https://www.accessnow.org/issue/privacy/

[12] http://www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance and https://www.amnesty.org.uk/issues/Mass-surveillance

[13] https://www.apc.org/en/pubs/research

[14] https://www.article19.org/cgi-bin/search.cgi?q=privacy

[15] https://www.hrw.org/sitesearch/surveillance

[16] http://www.inclo.net/

[17] https://www.privacyinternational.org/reports

[18] https://www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html

are the subject of constant surveillance […].”[19]It also mentioned the negative potential consequences for the exercise of freedom of expression.

15. The judges further recognised “[…] while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight […]”.[20]Furthermore, the Court of Justice of the European Union made clear that the retention of traffic data must be the exception, not the rule. When there are concrete indications that such data must be kept for the fight against terrorism and serious crime, there must be limiting criteria in place such as precise geographical limitations. Additionally, the Court reiterates that people concerned need safeguards and remedies and there must be effective oversight mechanisms in place which involve checks and balances.[21]

16. While privacy advocates understandably welcomed this judgement, the other dimensions of the decision were perhaps most usefully summed up by David Anderson, the UK’s Independent Reviewer of Terrorism legislation “The judgment of the CJEU was thus a genuinely radical one. The proven utility of existing data retention powers, and the limitations now placed on those powers, is likely to mean that it will be of serious concern to law enforcement both in the UK and in other Member States. On the other side of the balance, not everyone will agree with the Court’s view that these powers constitute a “*particularly serious*” interference with privacy rights, or that they are “*likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance*” (para 100). A more rigorous analysis of proportionality would have focussed on any actual harm that this useful power might be shown to have caused over its years of operation, and sought to avoid assertions based on theory or on informal predictions of popular feeling”[22]

17. The SRP comes from a tradition deeply committed to evidence-based policy making which is why he shares Anderson’s desire for a more rigorous analysis of proportionality. To date, the SRP has not yet been granted (in the UK at least) access to certain (sometimes classified) data which would confirm that the utility of bulk acquisition of data is both necessary and proportional to the risk. Indeed, the SRP welcomes the CJEU’s judgement precisely because this evidence has not yet been made available that would persuade the SRP of the proportionality or necessity of laws regulating surveillance which permit bulk acquisition of all kinds of data including metadata as well as content.

18. It is important to draw attention to the cultural dimensions also noted by Anderson in this context:

> “*It must be acknowledged, however, that feelings on these matters do vary at least to some extent across Europe. Thus:*
>
> - *The comments of the CJEU in relation to the seriousness of the interference with privacy find no real echo in the three parliamentary and expert reports which led to the introduction of the Investigatory Powers Bill, nor in the regular reports of the Interception of Communications Commissioner, the senior former Judge who conducts detailed oversight of this activity in the UK.*

[19] European Court of Justice, Tele 2 Sverige, C-203/15, ECLI:EU:C:2016:970, 21.12.2016, mn. 100.
[20] Ibidem, mn. 103.
[21] Ibid. mn. 103 – 111.
[22] https://terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/

- *But in the eastern part of Europe and in Germany, historic experience, coupled with a relative lack of exposure (until recently) to terrorism have induced greater circumspection. National data retention rules have proved controversial and were annulled even before Digital Rights Ireland in Bulgaria, Romania, Germany, Cyprus and the Czech Republic.*

This may reflect what I have previously described as "marked and consistent differences of opinion between the European Courts and the British judges … which owe something at least to varying perceptions of police and security forces and to different (but equally legitimate) conclusions that are drawn from 20th century history in different parts of Europe" (A Question of Trust, 2.24)."[23]

B. Challenges and worrying trends

19. Through various research activities of the mandate of the SRP and through other related research projects it has been found that the surveillance activities of LEAs and SIS are sometimes increasingly hard to distinguish from one another. While the activities of the one branch are typically directed towards the inside of a national territory and the activities of the latter towards foreign territory, the nature of trans-border dataflows and the technical needs required to interfere with them often result in the use of the same or very similar equipment in the digital age.

20. Increasingly, personal data ends up in the same "bucket" of data which can be used and re-used for all kinds of known and unknown purposes. This poses critical questions in areas such as requirements for gathering data, storing data, analysing data and ultimately erasing data. As a concrete example a recent study carried out by the Georgetown Center on Privacy and Technology in the United States has found that "one in two American adults is in a law enforcement face recognition network."[24] As the authors of the study put it: "We know very little about these systems. We don't know how they impact privacy and civil liberties. We don't know how they address accuracy problems. And we don't know how any of these systems—local, state, or federal—affect racial and ethnic minorities."

21. These and similar insights lead to a couple of considerations: *First*, the nature of trans-border data flows and modern information technology requires a global approach to the protection and promotion of human rights and particularly the right to privacy. If the flow of information is to remain a global affair – with all of the substantial advantages that has brought and will continue to bring for humankind – there needs to be a consistent and trustworthy environment in which this happens. Such an environment cannot discriminate between people of different nations, origins, races, sex, age, abilities, confessions, etc. There needs to be a core of rights and values which is consistently respected, protected and promoted throughout the international community.

22. Secondly, the increasing importance of the exchange of information in the virtual space needs private, trustworthy and secure methods. Technologies such as encryption have already been discussed broadly by the Special Rapporteur on the right to privacy, and specifically in the first report to the General Assembly.[25] Additionally, other Special

[23] Ibid.

[24] Garvie, Bedoya, Frankle, The Perpetual Line-up – unregulated Police Face Recognition in America, available via https://www.perpetuallineup.org/ - accessed on 08.12.2016.

[25] A/71/368, p. 13 - 22.

Rapporteurs, such as the one on Freedom of Expression, have already carried out significant and welcome work in this area.[26]

23. If LEAs and SIS are concerned about their inability not to intercept or read every message sent and received between anybody who uses modern information technology, they should not forget that we live in an age where information exchange happens through thousands of venues. Humans have started to share so much information through digital means that even if a couple of them are not accessible to the state, that does not mean that there are no other traces and venues to follow those people with bad intentions. Particularly, the vast amounts of metadata created by smartphones and connected devices, which often is as revealing as the actual content of communications, provides ample opportunities for the analysis of people's behaviour.[27] On the other hand, if the state is capable of potentially interfering with every flow of information, even retroactively through bulk data retention and technologies such as "quick freeze", the right to privacy will simply not experience a full transition to the digital age.

24. It is to be welcomed that some countries and organizations have already started to increase their efforts to tackle these challenges. Particularly, the Council of Europe has contributed in this area with an initiative in the context of law enforcement in cloud computing environments. This is connected with the Cybercrime Convention and is aiming at developing a new legal tool.[28]

25. Additionally, it is worrying that modern laws on surveillance increasingly allow for the creation, access and analysis of personal data without adequate authorisation and supervision. An adequate authorisation and supervision requirement should be in place when the measure "is first ordered, while it is being carried out, or after it has been terminated."[29] While often "traditional" methods, such as the interception of phone calls and communications in general, are subject to judicial authorisation before the measure can be employed, other techniques such as the collection and analysis of metadata referring to protocols of internet browsing history or data originating from the use of smartphones (location, phone calls, usage of applications, etc.) are subject to much weaker safeguards. This is not justified since the latter categories of data are at least as revealing of a person's individual activity as the actual content of a conversation. Hence, appropriate safeguards must also be in place for these measures.

26. While judicial authorisation of intrusive measures generally raises the degree of privacy protection, it also must be guaranteed that the judges themselves are independent and impartial in their decision-making process in individual cases. Furthermore, they must have the knowledge and facts necessary to consider the requests thoroughly and understand the potential implications of their decisions, particularly in terms of the technology to be employed, and the consequences of using that technology. Hence, states should provide the required training and resources necessary for judges to live up to this complicated task.

27. In principle, the same applies to the oversight of surveillance activities by specialized bodies of parliamentary assemblies. They need not only to have the relevant

[26] A/HRC/29/32.

[27] Cf. A report by the Harvard Berkman Center released earlier in 2016 on the issue, Groing Dark available via https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf - accessed on 09.12.2016.

[28] Council of Europe, Cybercrime: towards a new legal tool on electronic evidence via https://www.coe.int/en/web/portal/-/cybercrime-towards-a-new-legal-tool-on-electronic-evidence - accessed on 12.12.2016.

[29] European Court of Human Rights, Zakharov vs. Russia, App. No. 47143/06, available via http://hudoc.echr.coe.int/eng?i=001-159324 – accessed on 08.12.2016, mn. 233.

information to understand the activities of law enforcement agencies and security and information services, they also need to have adequate resources to comprehend and digest them.

28. In most countries this will be hard to achieve given the large volume of data involved. The authorities carrying out surveillance should take measures to guarantee internally that oversight practices are reviewed and controlled permanently and in detail. Oversight, particularly if carried out in the political sphere, should be able to focus on structural issues and be able to address the general direction of operations.

29. Another area which attracts a lot of attention is the international nature of oversight activities. There are particularly two dimensions to this phenomenon that require increased attention: First, it is of utmost importance that states respect the right to privacy, which is based on human dignity, on a global level. Surveillance activities, regardless of whether they are directed towards foreigners or citizens, must only be carried out in compliance with fundamental human rights such as privacy. Any national laws or international agreements disregarding this fact, must be considered outdated and incompatible with the universal nature of privacy and fundamental rights in the digital age.

III. First approaches to a more privacy-friendly oversight of government surveillance

A. Comprehensive overview of approaches and themes

30. Research and exchange with several national authorities, civil society and corporations from different global regions, especially within IIOF2016, have shown the emergence of several themes in the area of governmental surveillance. These are:

(1) A need for internationalization and standardization of terms and language used;

(2) A need for a confidential and open dialogue to better understand national systems, their similarities and differences;

(3) The promotion and protection of Fundamental Human Rights in relation to the methods used;

(4) Safeguards and Remedies – preferably on an international level;

(5) Accountability and transparency;

(6) Collection and discussion of good and bad practices;

(7) A more evolved discussion on how to structure oversight of governmental surveillance;

(8) Answers to the question on how to engage with the public;

(9) The need to be less secretive and more proactive in explaining the work of secret services and law enforcement authorities when carrying out surveillance;

(10) A need for more fora to make progress on the subject.

B. Discussion

31. The Internationalization and Standardization of terms and language aims at defining words such as “surveillance”, “mass surveillance”, “bulk collection”, “bulk interception”, “bulk hacking”, “equipment interference”, etc. The British authorities have published a useful albeit controversial document entitled “Operational case for Bulk Powers”[30] which provides some aspirational descriptions for some of these terms.[31] It is important that government authorities carrying out surveillance, as well as civil society and other stake-holders, have a clear view on what they actually mean when they use these terms relating to surveillance. Some of these terms, such as “mass surveillance” are highly loaded and controversial. What is necessary is a more comprehensive and harmonized use of terms and their understanding in exchanges between governmental authorities carrying out surveillance. However, also oversight bodies of the judicial and political branch, civil society, security research and corporations should be able to understand and use these terms appropriately.

32. Since surveillance has an international dimension it is necessary to talk about it in an international arena, which is confidential and trustworthy. It is important to increase the dialogue between national authorities carrying out surveillance. Furthermore, while having such discussions it must also be ensured that experts from civil society can provide their input and share their concerns.

33. It is crucial that fundamental human rights, particularly privacy, freedom of expression and the right to information, remain at the core of the assessment of governmental surveillance measures of all types and kinds. While the protection of the right to life and to rest unharmed is a basic precondition for human existence, it has to be borne in mind that there is no strict hierarchy between human rights. They typically reinforce each other. This means, in other terms, that there is a need for a broad promotion of the catalogue of rights without a specific focus on one or two.

34. A right is only worth as much as its delimitations and enforcement mechanisms allow it to be. This is crucial in the area of governmental surveillance, since we need safeguards without borders as well as remedies across borders. Mutual legal assistance, as already mentioned, needs to be enforced and upgraded. If there is no possibility for a common global approach, and that is not yet excluded, we need more regional and cross-regional initiatives.

35. The structure of accountability and transparency within governmental organizations carrying out surveillance need to be clear. It also needs to be clear why a particular set of data is being collected, what purpose the analysis has and which purposes are not legal. Enforcement of these mechanisms needs to be embedded first and foremost within the authorities carrying out surveillance and it needs to be clear who is accountable for compliance after appropriate legal requirements have been defined.

36. It is helpful in this exercise to collect examples of good and bad practices. For example, some Intelligence Oversight Agencies have established expert consultation bodies consisting of trusted external experts to counsel them on specific issues. Additionally, evaluation of operations and reflection on their implications for the promotion and protection of fundamental human rights is crucial. As a third example, members of authorities carrying out surveillance have to be trained not to put too much trust in

[30] Accessible via https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf - accessed on 09.12.2016.

[31] Ibid. P.6.

technology and that ultimately a human decision must be made based on technological assistance and not vice versa.

37. If internal mechanisms of accountability and transparency fail, there need to be other checks and balances in place. States need to have the capability to detect and assess structural problems in those agencies which are entitled to carry out surveillance. In some states parliamentary committees carry out these functions. However, oversight authorities often suffer from a lack of domain knowledge, resources and/or access to relevant information. The same applies to mechanisms of judicial oversight where these exist.

38. Furthermore, the Snowden revelations and their aftermath have clearly shown that there is a pressing need for government authorities to explain their work. This may partially be achieved through *ex post* notification of those individuals who are subject to surveillance. Once this can be done safely, those should be notified and explained the consequences of such operations. They also should be entitled to alter and/or delete irrelevant personal information provided that information is not needed any longer to carry out any current or pending investigation for which the collection and use of that information had been appropriately authorised.

39. Additionally, the general public needs to regain trust in the operations of those agencies which carry out surveillance. It is obvious that security is a valid concern for everybody. Hence, while it is not necessary for the general public to understand the characteristics and applications of each and every operation in detail, there needs to be information available in order to grasp the general dimension of operations undertaken to protect the public. A passenger does not need to know how to fly an aircraft in order to book a flight with it. But they will not pay for a ticket if they do not trust the general capability and safety of the aircraft traffic and safety systems.

IV. Activities of the Special Rapporteur

40. As usual, the Special Rapporteur on the right to privacy is reporting the main public or semi-public activities carried out as part of his mandate. This report covers the activities from Privacy, Personality and Free Flows of Information 2016, held on the 19th and 20th of July 2016 to the beginning of February 2017

(a) 2016 European Privacy Protection Innovation Workshop, Huawei German Research Center, Munich, Germany, 3 August 2016;

(b) Key note speaker, Council of Europe Conference “Internet Freedom; A Constant Factor of Democratic Security in Europe”, Strasbourg, France, 9 September 2016;

(c) Panel chair, Biometrics and Privacy, Darmstadt EAB-Research Projects Conference 2016, Darmstadt, Germany, 19 September 2016;

(d) Protection And Security Advisory Group (PASAG) – European Union Commission DG Home, Brussels, Belgium, 27 September 2016;

(e) Special Rapporteur for Privacy event “International Intelligence Oversight Forum” (IIOF) Bucharest, Romania, 11-12 October 2016;

(f) Keynote Speaker and Panel Chair, Intelligence in the Knowledge Society, Bucharest, Romania, 13-14 October 2016;

(g) Keynote Speaker, 38th International Conference of Data Protection and Privacy Commissioners, Marrakech, Morocco, 18-22 October 2016;

(h) MAPPING Second Annual General Assembly, Prague, Czech Republic, 31 October – 2 November 2016;

(i) Keynote Speaker, Cyberspace Conference 2016 Brno, Czech Republic, 25 November 2016;

(j) Keynote Speaker, APPA Forum Manzanillo, Colima, Mexico, 30 November – 2 December 2016;

(k) Keynote Speaker and Panellist, Irish Civil Liberties Union, Surveillance, 7th December 2016

(l) Keynote Speaker, Northern Ireland Human Rights Commission's annual statement in Belfast at Stormont House, United Kingdom, 8 December 2016;

(m) Preparatory meetings Privacy Personality and Free Flows of Information 2017, 12-14 December 2016, Tunisia.

(n) Conference on Privacy and Data Protection, Brussels, Panelist on AI and Privacy, 25 January 2017

(o) Keynote speaker on Privacy and Security, ISMS Privacy Forum, Madrid, 1st February 2017

V. Conclusions and Recommendations

41. **At this stage, the SRP mandate is making five clear, distinct recommendations arising from interim conclusions. They deal with:**

(a) WHY populism and privacy are inimical to security;

(b) HOW states may engage to improve privacy protection through better oversight of intelligence;

(c) WHO deserves to enjoy the right to privacy i.e. everybody, everywhere – the universality of the right to privacy has a special meaning in this context

(d) HOW this right to privacy could possibly be better protected through developments in domestic and international law and

(e) WHEN some developments in international law, especially those concerning a legal instrument regulating surveillance may possibly soon be at a stage of maturity where they could benefit from a wider discussion;

42. **WHY - Populism and Privacy**

a. To be more precise perhaps, this section should be entitled Security, Populism and Privacy. 2015-2017 have seen a growing tendency, especially though not exclusively in Europe, to indulge in "gesture-politics". In other words, the past eighteen months have seen politicians who wish to be seen to be doing something about security, legislating privacy-intrusive powers into being – or legalise existing practices – without in any way demonstrating that this is either a proportionate or indeed an effective way to tackle terrorism.

b. The new laws introduced are predicated on the psychology of fear: the disproportionate though understandable fear that electorates may have in the face of the threat of terrorism. The level of the fear prevents the electorate from objectively assessing the effectiveness of the privacy-intrusive measures proposed.

c. There is little or no evidence to persuade the SRP of either the efficacy or the proportionality of some of the extremely privacy-intrusive measures that have been introduced by new surveillance laws in France, Germany, the UK and the USA. Like Judge Robart in the recent case on the immigration ban in the USA, the SRP must seek evidence for the proportionality of the measures provided for by law[32]s. In the same way as Judge Robart asked as to precisely how many cases of terrorism were carried out since 2001 by nationals of the states subjected to the immigration ban, the SRP must ask as to whether it would not be much more proportional, never mind more cost-effective and less privacy-intrusive if more money was spent on the human resources required to carry out targeted surveillance and infiltration and if less effort were expended on electronic surveillance. This, in a time when the vast majority of all terrorist attacks were carried out by suspects already known to the authorities prior to the attacks.

d. There is also growing evidence that the information held by states, including that collected through bulk acquisition or "mass surveillance" is increasingly vulnerable to being hacked by hostile governments or organised crime. The risk created by the collection of such data has nowhere been demonstrated to be proportional to the reduction of risk achieved by bulk acquisition.

e. Furthermore, the abuse of data collected by bulk acquisition remains a primary source of concern. Without necessarily casting aspersions on the incoming US administration, the concerns expressed in that context by a senior HRW researcher are worth reproducing: *"In the US, the National Security Agency continues its information dragnet on millions of people every day, despite modest reforms in 2015. Now the keys to the world's most sophisticated surveillance apparatus have been handed over to a candidate (who) threatened to imprison his political opponent, register and ban Muslims, deport millions of immigrants, and menace the free press."*[33] While the checks and balances existing in the USA or indeed the ethical standards of the Executive itself may hopefully push the US away from the realisation of such risks, the point being made here by the SRP is that once the data sets produced by mass surveillance or bulk acquisition exist and a new unscrupulous administration comes into power anywhere in the world, the potential for abuse of such data is such so as to preclude its very collection in the first place.

f. RECOMMENDATION: Desist from playing the fear card, and improve security through proportionate and effective measures not with unduly disproportionate privacy-intrusive laws "I don't believe that any form of leadership is best exercised by using fear. True political leadership does not play the fear card" [34]

43. **HOW - Assist the SRP in identifying and developing best practices in the oversight of intelligence.**

[32] http://www.npr.org/2017/02/04/513446463/who-is-judge-james-l-robart-and-why-did-he-block-trumps-immigration-order

[33] Cynthia Wong, Surveillance in the age of populism" Human Rights Watch last accessed on 12th Feb 2017 at https://www.hrw.org/news/2017/02/07/surveillance-age-populism

[34] Cardinal Vincent Nichols speaking to the BBC on Sunday 05 February 2017 –Westminster hour website

a. IIOF2016 has demonstrated that the discussion on oversight of intelligence in a way that reinforces privacy safeguards is a complex process which requires much time, resources, occasionally culture change, political will and the generation of trust. There are no short cuts to identifying and further developing best practices.

b. The ensuing recommendation is a simple but important one: all member states of the UN should engage in the painstaking discussion of oversight of intelligence initiated by the SRP in IIOF2016 and to be continued in IIOF2017. Governments should encourage and facilitate participation in IIOF2017 by oversight bodies and intelligence agencies.

44. **WHO deserves the right to privacy = everybody, everywhere. RECOMMENDATION: States should prepare themselves to ensure that both domestically and internationally, Privacy be respected as a truly universal right – and, especially when it comes to surveillance carried out on the Internet, privacy should not be a right that depends on the passport in your pocket**

a. This recommendation requires some space to develop and will be illustrated using examples here restricted (purely for reasons of space) to USA case-law and legislative change. It should be clear at the outset that whatever is here recommended for the USA is being likewise recommended in analogous situations for all UN members states.

b. The US House of Representatives did something very commendable on 6th February 2017. Something which the SRP had long been waiting for: it unanimously passed the Email Privacy Act which closes a gap in US law by requiring a judicial warrant in order to permit access to e-mail older than six months stored on the cloud or elsewhere. This is a development which the SRP heartily welcomes and which he trusts will also be acceptable to the US Senate which derailed the process last time it was attempted in April 2016. Indeed the SRP invites the Senate to seize upon a historic opportunity and go a step further thereby demonstrating the US commitment to human rights world-wide as well as simultaneously putting paid to one of the xenophobic fallacies that some governments consciously or unwittingly promote i.e. that 'it's only nasty foreigners who are out to get us…and that therefore they don't deserve their fundamental human rights to be respected by our laws'. This is not a fault we only witness in some US law-making. For example, the German government has recently been equally guilty of making such a law which distinguishes between German and EU citizens on the one hand and everybody else on the other hand[35]. One could of course attack such laws purely on the ground of logic: if one were to take the vast majority of terrorist attacks in Europe these were not carried out by "Johnny Foreigner" but mostly by EU citizens holding EU ID cards and EU passports. Likewise, it would seem to be a similar situation for most recent terror attacks in the USA. So why pander to this fallacy that it is logical and sensible to discriminate against people who are not citizens of the lawmakers' own jurisdiction? If Governments sincerely wish to prevent and reduce terrorism, logic suggests that they should tackle the heart of the problem, the *radix malorum* or root causes such as radicalisation. Investing much more in anti-radicalisation measures and allocating more resources for long-term targeted surveillance and cell infiltration would seem to be far more effective than indulging in gesture-politics. Trying to appear tough

[35] See A/71/368

on security by legitimising largely useless, hugely expensive and totally disproportionate measures which are intrusive on so many people's privacy – and other rights - is patently not the way governments should go.

c. The SRP very respectfully suggests that it would be much more sensible – and effective – as well as setting an example to the rest of the world – if US law were to align itself with the principles recently articulated in Europe by both the European Court of Human Rights in the Sakharov case and the European Court of Justice in the Sverige2 & Watson case i.e. that the key requirement in order to carry out targeted surveillance is reasonable suspicion and not citizenship. If an SIS or LEA can demonstrate reasonable suspicion then judicial permission to obtain an access warrant should be granted irrespective of the passport held by the suspect. Here, the key consideration is that of risk and should remain that of risk-management. If a person demonstrably poses a risk then he or she should be subject to surveillance anywhere and everywhere irrespective of his or her passport status. The same safeguards which are applied against unreasonable search and seizure – in this case a judicial warrant - are likewise appropriate irrespective of the passport of the citizen. The Universal Declaration of Human Rights, launched in December 1948 in the United States with much credit going to that remarkable US First Lady, Eleanor Roosevelt, very rightly does not state that "Only US Citizens have the right to privacy etc". Instead it states that "Everyone has the right to the protection of the law against such interference or attacks". By which I take it to mean US law too. Here therefore is an opportunity for US legislators to set an example to others around the world and follow in the spirit and the words of the Universal Declaration and take concrete steps to make US law truly respect the universality of the right to privacy by amending the Email Privacy Act in the right directions, some of which are outlined below.

45. **If privacy, like freedom from torture or so many other rights, is a fundamental human right it is also a universal right which means that everybody all over the world has the right to privacy, irrespective of where he or she may be, irrespective of whatever passport he or she may hold and likewise irrespective of colour, creed, ethnic origin, political philosophy or sexual orientation. This is the truth to which the SRP calls the US Senate to give witness too. On so many occasions, US Governments have sought to punish human rights violations in other countries, often leading the way in drawing red-lines and creating sanctions to improve the chances of their observance. In removing distinctions between US citizens and other citizens, by extending privacy safeguards afforded to US citizens to all the citizens of the world, the Senate would be striking a sensible blow for the universality of the fundamental human right to privacy and one against xenophobic trends in law-making. In so doing it will also match European privacy and data protection law which makes no distinction between the privacy rights of citizens and non-citizens.**

46. **HOW – a role for international law**

a. Whereas the previous recommendation dealt largely with opportunities to protect the universality of privacy within domestic law, this section will contemplate opportunities to complement domestic measures through international law.

b. There is another key concern that is raised by the current wording of the US Email Privacy Bill. That is whether the safeguards being strengthened within the law are also applicable to data wherever it is held, whether inside the United States or outside it. To illustrate this issue it is useful to cite the Microsoft case contesting the global reach of US search warrants on data held

outside the US[36]. One can very easily understand the reluctance displayed by Microsoft to give access to data held outside the USA. Not only does this have a potentially negative impact on Microsoft's competitiveness world-wide but also it represents a particularly thorny problem when trying to decide how to deal with all kinds of requests for data from all kinds of governments from all around the world. This is not a problem which Microsoft faces alone. Most of the other predominantly US origin industry tech giants such as Google, Facebook, Apple and Twitter (to name but a few) are faced yearly with thousands of requests of access to data from governments all around the world.

c. If the US Congress wishes to find a sensible way forward on this score, not to mention providing a solution which is sound from a fundamental human rights point of view as well as one which would not put US firms at a commercial disadvantage, it should realise that the answer cannot lie solely in domestic law. It must also realise that this particular area of law is not being well served by decades-old tools such as mutual legal assistance (MLA). Congress should realise that while the Cybercrime convention did make considerable progress in some areas, it has not yet managed to make the transfer of personal data across borders and access to data required for investigations as fast and as problem-free as some would have hoped for. One of the main reasons for this relative failure is that it has continued to rely too much on the 19th century mind-set of the sovereign nation state rather than cater for the reality of the borderless internet of the 21st century. While perhaps a good example of what may be achieved with "baby steps" and while it certainly scored some successes including the identification and codification of computer and internet based offences, the Cybercrime Convention has not delivered on timely transborder flows of personal data which are suitable for detection, investigation and prevention of crime in the Internet age. One of the main reasons for not doing so is possibly that it did not go that extra step of creating a mechanism such as an international body tasked with – and granted the authority to authorise - international access to data, internationally. In the same way that other forms of international law have set up agencies tasked with creating trust and implementing appropriate safeguards in other "spaces", in areas as diverse as maritime law, space law, atomic weapons, chemical weapons etc., the Cybercrime Convention, in tandem with other multilateral treaties, including new ones created for the purpose, has the potential to be expanded in such a way so as to create an international authority which would be able to grant the equivalent of an international surveillance warrant or international data access warrant (IDAW) that would be enforceable in cyberspace. Countries signing up to such a new treaty or additional protocol could be contributing their own specialised independent judges to a pool who would, sitting as a panel, conceivably act as a one-stop shop for relevant judicial warrants enforceable world-wide – naturally in those countries which would become party to the treaty. In this way, to return to our previous example of the July 2015 decision, companies like Microsoft, Google, Facebook, Amazon, Apple and other tech giants operating data centres internationally would not need to worry about any state overstepping its boundaries but rather would be faced with an international data access warrant issued on grounds of reasonable suspicion under clear international law. Likewise, citizens world-

[36] https://blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0019d8sjw1492dnrz7k1yawh09b46

wide would be assured that their right to privacy, not to mention other rights such as freedom of expression and freedom of association, is being protected with appropriate safeguards, even-handedly and universally. If one really wishes the right to privacy to be universal then it stands to reason that this would be advanced by having mechanisms which are both international and universal applying the same standards and safeguards on a world-wide basis.

d. This is not utopia. This is cold, stark reality, something which will mark out the true democracies from those states intent mainly on using the internet as a means of social control and retaining power within their own jurisdictions. It is also something which could be linked to other initiatives aimed at preserving the cyber-peace as recently advocated by Microsoft's Brad Smith.[37]

e. At this moment in time, the evidence available to the SRP would suggest that a number of states, even some leading democracies, regrettably treat the Internet in an opportunistic manner, as somewhere where their LEAs and especially their SIS can operate relatively unfettered, intercepting data and hacking millions of devices, (smartphones, tablets and laptops as much as servers) world-wide. In doing so, approximately 15-25 states treat the Internet as their own playground over which they can squabble for spoils, ever seeking to gain the upper hand whether in terms of cyber-war, or espionage or counter-espionage, or industrial espionage. The list of motivations goes on while the other 175-odd states look on powerless, unable to do much about it except hope that somehow cyber-peace will prevail.

f. Let me state this frankly: a tiny minority of states have actively tried to informally discourage the SRP from exploring options for solutions in this area but as a Rapporteur it is my duty to report back that these seem to be the only people who don't wish to have internationally enforceable safeguards and remedies on the internet. I have yet to meet one civil society organisation, one corporation, indeed one reasonable law enforcement agency and security and intelligence service that does not wish to have greater clarity and universally applicable safeguards and remedies, although they may be discouraged as to this being achieved any time soon.

g. It's no use beating round the bush: the only way this clarity can be achieved, the only way that these safeguards and remedies can be introduced in a way where their enforcement becomes more timely, more even-handed and expedient is through multilateral agreement enshrined in international law. What the world needs is not more state-sponsored shenanigans on the Internet but rational, civilised agreement about appropriate state behaviour in cyberspace. Which again brings me back to the subject of surveillance.

h. Some of the improved international mechanisms mentioned above would be very useful in law enforcement in cyberspace, something which is currently regulated by the Cybercrime convention. As its name suggests however that multilateral treaty to which some 25% of the UN's member states have already subscribed only deals with the criminal justice sector. It does not deal with national security nor surveillance carried out in the name of national security. In other words the type of activities revealed by Edward Snowden lie outside the scope of the Cybercrime Convention and for these to be regulated

[37] http://www.itpro.co.uk/security/28134/how-can-nation-states-win-the-unfolding-cyberwar?_mout=1&utm_campaign=newsletter&utm_medium=email&utm_source=newsletter&tpid=109380765640

satisfactorily the scope of Convention 185 would need to be considerably extended or else we would need to have a separate but complementary treaty that adequately covers surveillance in cyberspace. This would be much more preferable to a situation where we have a number of democracies like France, Germany, the UK and the USA scrambling to introduce new laws regulating surveillance where the mindset appears to be unduly influenced by the concept of the 19th century sovereign nation state. While nationalism and jingoism, not to mention populism, appear to be going through what history might demonstrate to be a cyclical rise in fortunes, their usefulness at the polling booth should not be confused with their efficiency in providing true security both domestically and internationally. It should be recognised – even by politicians speaking at the national level - that the vast majority of UN member states have no interest in promoting organised crime or terrorism wherever they may take place and by whomsoever they are perpetrated. To put it simply, if one were to be an investigator in Belgium going to an international panel composed of judges from, say the USA, France, the UK, Germany, Ghana, India and Brazil – to mention some countries randomly – there should be little fear that such a panel – or panel similarly composed for the purpose - would not grant a warrant to access data about a person if reasonable suspicion is demonstrated. Once that process leads to an international data access warrant (IDAW) that would considerably simplify things for governments and corporations within the jurisdictions of states which would have agreed on such mechanisms through an international treaty.

i. Such a legal instrument should not be confused with an all-embracing Internet Governance Treaty or a "Geneva Convention for the Internet" as some have called it. There are many other parts of Internet Governance which would remain untouched by a legal instrument regulating surveillance in cyberspace, not least of which that very important yet oft-neglected other part of Art. 12 and Art 17 i.e. the right to protection of reputation which is both distinct from yet akin to privacy.

j. In summary therefore, a legal instrument regulating surveillance in cyberspace would be another step, complementary to other pieces of existing cyberlaw such as the Cybercrime Convention, one which could do much to provide concrete safeguards to privacy on the Internet. Happily for the SRP's mandate, a pre-existing initiative, the EU-supported MAPPING project is actually exploring options for a legal instrument regulating surveillance in cyberspace. A draft text exists, is being debated by experts from civil society and some of the larger international corporations and it is expected that this text will get a public airing some time in 2017 and certainly before the spring of 2018. It would be premature for anybody including the SRP to take a position on such a text or a similar one at this early stage of exploring options but it is possible that this could eventually prove to be a useful spring-board for discussion by governments within inter-governmental organisations including and perhaps especially the UN.

k. RECOMMENDATION. In the same way that the SRP is preparing to deliberate on this subject, especially between March and July 2018, it would appear sensible for many executive branches of government to be given a mandate by their parliaments – and their electorates where elections are being held in 2017-2018 - to actively explore such options for proper regulation of surveillance and the introduction of privacy-friendly safeguards and remedies in cyberspace. This would not only be of great intrinsic value to citizens worldwide but would also send a clear signal to those states, democracies,

pseudo-democracies and otherwise who mistakenly believe that the best way to deal with cyberspace is to claim sovereignty over chunks of the Internet or what its citizens get up to on the Internet. Human rights are universal and cyberlaw should exist in such a way not only to protect privacy but also other fundamental human rights.

l. However difficult for it to be brought about, it is not impossible, indeed it is both plausible and reasonable that a significant number of states would eventually coalesce around a legal instrument which would regulate surveillance and protect privacy in cyberspace. This would be good for citizens, good for governments, good for privacy and good for business. The number of states coalescing around newly-articulated principles and newly created mechanisms could gradually grow to provide critical mass. This has been the lesson we have learned from the development of international law over the past couple of centuries. There is no reason as to why we should ignore this lesson when it comes to privacy, surveillance and cyberspace. It may probably not come to fruition during my tenure as SRP but at least it is possibly the most promising path to start off upon. Everything I have seen in my role as SRP to date has persuaded me that this may be the wisest path to tread when its time will come. That time may be sooner than some may wish us to think.