United Nations A/HRC/34/60

General Assembly

Distr.: General
6 September 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*

Note by the Secretariat

In his report, prepared pursuant to Human Rights Council resolution 28/16, the Special Rapporteur on the right to privacy focuses on governmental surveillance activities from a national and international perspective. The Special Rapporteur elaborates on the characteristics of the international legal framework and the interpretation thereof. He also describes 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, he outlines first approaches to a more privacy-friendly oversight of government surveillance. In conclusion, the Special Rapporteur reports on his activities in the period covered by his report.

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

Report of the Special Rapporteur on the right to privacy

Contents

I. Introduction

1. Pursuant to Human Rights Council resolution 28/16, the Special Rapporteur on the right to privacy reports annually to the Council and to the General Assembly. The present report is his second report to the Council. In his previous report, the Special Rapporteur outlined a 10-point action plan and a strategy to tackle certain crucial contemporary issues relating to his mandate through activities in "thematic action streams". 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. The Special Rapporteur recently published a statement entitled "Planned thematic reports and call for consultations", in which he presented the issues to be tackled in the present and future reports and set out a timeline for delivery of his reports.[1] The statement should be considered a standing invitation to all stakeholders in all countries around the world who wish to engage with the mandate. Anyone who wishes to contribute to or otherwise be involved in any of the initiatives mentioned should contact the Special Rapporteur or members of his team, preferably by e-mail (srprivacy@ohchr.org) and he or they will respond as quickly as possible.

3. As set out in the summary above, in the present report the Special Rapporteur focuses on the theme of first approaches to a more privacy-friendly oversight of government surveillance. He has already carried out several activities covering the subject during his mandate and will continue to do so. In an attempt to fulfil his tasks as outlined in the previous report of the Special Rapporteur (A/HRC/31/64), and particularly in the surveillance sector, the Special Rapporteur invested considerable effort in organizing the International Intelligence Oversight Forum, held in Bucharest on 11 and 12 October 2016, which was co-hosted by the Joint Committee of the Chamber of Deputies and the Senate for parliamentary oversight of the activities of the Romanian Intelligence Service, the Special Committee of the Chamber of Deputies and the Senate for parliamentary oversight of the activity of the Foreign Intelligence Service and the Committees for Defence, Public Order and National Security in the Chamber of Deputies and in the Senate, in association with the Department of Information Policy and Governance at the University of Malta and the Security, Technology and e-Privacy Research Group at the University of Groningen in the Netherlands. The event was very successful within its understandably modest objectives.[2] The Special Rapporteur therefore intends to continue co-organizing the Forum on an annual basis. In 2017, the plan is to hold it on 20 and 21 November in Brussels, where it will be co-hosted by, among others, the data protection authority of Belgium, the Privacy Commission. It is intended that the Forum will enable the Special Rapporteur to fulfil his mandate by tapping into the practical experience and operational insights obtained by the many oversight bodies which have been set up around the world. That will enable the Special Rapporteur to better understand and reflect upon the realities of trying to achieve effective oversight of the activities of the security and intelligence services and the impact that this may have on privacy. The first Forum brought together nearly 70 participants from some 26 institutions in 20 countries. They included independent oversight authorities, parliamentary committees, some members of civil society and even an oversight tribunal. The Special Rapporteur considers that better thought-out and better resourced oversight of intelligence activities is one of the many complementary initiatives that may help to improve the protection of the right to privacy worldwide. Some would consider this to be

[1] The statement can be accessed at www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx and www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/.

[2] The objectives of the Forum, 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; the distinction between targeted surveillance and mass surveillance; the proportionality of such measures in a democratic society; and the cost-effectiveness and overall efficacy of such measures.

the most promising avenue for concrete measures to protect privacy. That remains to be seen. It is to be hoped that the series of annual Forums will contribute to the identification and sharing of good practices and eventually the considerable strengthening of oversight mechanisms in a large number of Member States. It is also to be hoped that the oversight mechanisms will have a strong basis in detailed and strict domestic laws that provide only the proportionate measures necessary in a democratic society and that appropriate safeguards will be spelled out within the same laws. The laws should also entrench effective oversight of both law enforcement agencies and the security and intelligence services by properly resourced and independent oversight authorities. In the light of the discussions at the annual Forums, the Special Rapporteur expects to make recommendations to ensure the promotion and protection of privacy, including in connection with the challenges arising from new technologies, in fulfilment of his mandate.

4. In relation to surveillance, the Special Rapporteur has focused not only on oversight mechanisms but also, to the extent possible, on a worldwide basis, on relevant new draft laws and reports that concern the use or abuse of surveillance. The Special Rapporteur also monitors to the extent possible, on a worldwide basis, relevant new draft laws and reports that concern the use or abuse of surveillance. As a result, surveillance-related activity is one of his principal considerations when requesting formal country visits. That may be seen especially in the choice of upcoming country visits: the United States of America (19-24 June 2017), France (requested for 13-17 November 2017), the United Kingdom of Great Britain and Northern Ireland (requested for late 2017, possibly 11-17 December), Germany (requested for 29 January-2 February 2018) and the Republic of Korea (requested for 3-15 July 2018). These are States with strong democratic pedigrees that the Special Rapporteur expects to take a leadership role in defining best practices and safeguards in the field of surveillance and fundamental human rights, especially privacy. In addition, they have been particularly active in the area of surveillance during the past several years, in terms of both applied surveillance technologies and new legislation. For each visit, the Special Rapporteur has included a request to meet the intelligence services and oversight authorities and ministers responsible for both law enforcement agencies and the security and intelligence services.

5. Moreover, to avoid reinventing the wheel and with the objective of maximizing synergy, the mandate is very closely following the proceedings and outcomes of other parallel initiatives, such as the project on managing alternatives for privacy, property and Internet governance (MAPPING project) supported by the European Union, which aims to create an all-round and "joined-up" understanding of the many and varied economic, social, legal and ethical aspects of recent developments on the Internet and their consequences for individuals and society at large. Launched in 2014, over a year before the Human Rights Council established the mandate of the Special Rapporteur and 18 months before he took up his role, the MAPPING project has initiated various, relatively well-resourced discussions among stakeholders, including one about the creation of an international legal instrument for regulating surveillance. Those discussions are set to run to the end of February 2018. The Special Rapporteur intends to monitor the outcomes of those discussions and then aims to take a position on the desirability and feasibility of such an international legal instrument between March and July 2018. It is possible that he will set out his position in his report 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, specifically in fulfilment of his mandate.

6. The Special Rapporteur is also in contact and 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 by the Special Rapporteur have established or improved many fruitful working relationships globally, with authorities keen to work on some kind of instrument articulating common standards for the conduct of foreign signals intelligence functions. These are welcome developments that may still be some way from fruition, very likely not within the term of the current mandate holder. However, they are important first steps and the Special Rapporteur will continue to do all he can to promote and facilitate such initiatives.

7. In the present report, the Special Rapporteur deliberately focuses on governmental surveillance. For other areas of activity, he refers to the thematic action streams which were outlined and described in his first report to the General Assembly (A/71/368, paras. 7-17). It must be emphasized that the issues of security and surveillance have been deliberately separated from the 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. They 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 Special Rapporteur. For those reasons, in the present report he focuses on surveillance activities as carried out by a State, on its behalf or at its order.

8. Meanwhile work on the other thematic action streams continues and will be presented in due course, hopefully in accordance with the timelines referred to in paragraph 2 above. In particular, the task force on big data and open data is working on producing its first report, to be discussed at a consultation session in July 2017. The outcome of the consultation is expected to form the main focus of the annual report of the Special Rapporteur to the General Assembly in 2017. In addition, following the success of the workshop on the theme of privacy, personality and flows of information, held in New York in July 2016, the Special Rapporteur has started to prepare the second workshop, which will focus on the Middle East and North Africa. It is planned for 22 and 23 May 2017 in Tunis and will be co-hosted by the Special Rapporteur and the Tunisian data protection authority, in close cooperation with civil society organizations. Preparations have likewise started for the third workshop, which will have a special focus on Asia. It is planned to take place in Hong Kong, China, on 29 and 30 September 2017. If any Government, civil society organization, corporation, data protection authority, academic institution or individual is interested in participating in or supporting these initiatives, they should contact the Special Rapporteur at the earliest opportunity.[3]

9. The Special Rapporteur takes this opportunity to commend the Governments of France, Germany, the Republic of Korea, the United Kingdom and the United States, which responded immediately and positively to his request for a formal country visit, and to lament the lack of response of a number of other countries. That may regrettably be the order of the day with some countries, but it is opportune and necessary to draw public attention to the resistance of Governments with respect to accepting requests for country visits. The Special Rapporteur does not wish to single out particular Governments but the responses or lack thereof to his requests do help to distinguish those that pay lip service to human rights from those that are prepared to engage with fair-minded approaches to improving the protection of privacy.

10. Before moving on to the main focus of the present report, the Special Rapporteur 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 circumstances where it has been alleged that privacy and data protection rights have been erroneously interpreted by the Executive and the national autonomous institute in an attempt to censor information within historical documents, so that access to documents from 30, 40 and even 120 years ago is hampered, clearly violating freedom of expression. Further allegations include worrisome silences of relevant bodies responsible for the protection of the right to privacy in the face of threats to privacy and clear attempts by the authorities to censor information of public interest on the grounds of data protection. The Special Rapporteur has developed good relations with relevant authorities 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 he knows of that the Government of a country is using privacy as an excuse not to release information of public interest into the public domain. That is an area which may be the subject of a separate report and which is mentioned here specifically to invite everybody, and especially civil society

[3] For e-mail, please use srprivacy@ohchr.org or any other addresses listed on the Special Rapporteur's web page at www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

organizations, to report such instances to the Special Rapporteur in order that they may be investigated in more detail.

11. The Special Rapporteur welcomes the moves of countries such as Brazil to join the family of nations that have adopted domestic privacy and data protection laws and encourages them to meet minimum standards, such as those set out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

II. Recent developments and worrying trends in governmental surveillance

A. Governmental surveillance and privacy in the digital age: the status quo

12. The current dialogue on governmental surveillance has been stimulated by people such as Edward Snowden and those supporting him. Although it is controversial from a national perspective, it has to be acknowledged that the information Mr. Snowden shared with the public about the actual practices of some national security services has sparked a necessary debate about what privacy means and should mean in the digital age. The famous quote from an interview he gave to The Guardian newspaper: "I do not want to live in a world where everything I do and say is recorded",[4] has led to many crucial initiatives and actions.

13. The United Nations has contributed to the debate on governmental surveillance in a number of ways. In its resolution 69/166, the General Assembly called upon States 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. Regional human rights courts, such as the European Court of Human Rights, have handed down judgments that establish clear and binding requirements that Governments must respect when establishing the means of carrying out surveillance and in its implementation.[5]

14. The Special Rapporteur follows developments in government surveillance worldwide in a number of ways, including through regular contact with a number of national and international civil society organizations. Many of the latter do an excellent job in bringing various matters of concern to the attention of the Special Rapporteur, to that of national Governments and the world in general. Without in any way detracting from the value of the work of other organizations, the Special Rapporteur would like to single out for attention the usefulness of the efforts of the American Civil Liberties Union,[6] Access Now,[7] Amnesty International,[8] the Association for Progressive Communications,[9] Article19,[10] Human Rights Watch,[11] the International Network of Civil Liberties Organizations[12] and Privacy International,[13] with which his mandate collaborates in a variety of ways. It is extremely beneficial when relevant reports by those and other civil society organizations are published, since the word limit afforded to the Special Rapporteur

[4] Available from www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why, accessed on 08.12.2016.

[5] See, for example, European Court of Human Rights, *Zakharov v. Russia*, judgment of 4 December 2015, available from hudoc.echr.coe.int/eng?i=001-159324.

[6] See www.aclu.org/issues/national-security/privacy-and-surveillance.

[7] See www.accessnow.org/issue/privacy/.

[8] See www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance and www.amnesty.org.uk/issues/Mass-surveillance.

[9] See www.apc.org/en/pubs/research.

[10] See www.article19.org/cgi-bin/search.cgi?q=privacy.

[11] See www.hrw.org/sitesearch/surveillance.

[12] See www.inclo.net/.

[13] See www.privacyinternational.org/reports.

by the United Nations for formal reports does not permit him to include a narrative on, say, developments on surveillance, such as may be found in the briefing submitted to him by Privacy International in November 2016 and since published on the Privacy International website.[14] It is important to state that the Special Rapporteur shares the concerns of Privacy International about related developments in surveillance in Colombia, Estonia, France, Mexico, Morocco, New Zealand, Poland, the Russian Federation, Rwanda, South Africa, Sweden, the Former Yugoslav Republic of Macedonia, Uganda, the United Kingdom, the United States of America, Venezuela (Bolivarian Republic of) and Zimbabwe, and is independently following up on those developments. The Special Rapporteur hereby invites the Governments of those States to take note of the concerns expressed in the submissions by Privacy International and preferably respond publicly to such concerns and/or communicate directly with the Special Rapporteur, as appropriate.

15. However, and it is deeply concerning, since resolution 69/166 was adopted and despite such judgments as are mentioned in paragraph 13 above, the status of the right to privacy in the area of surveillance has not improved since the previous report of the Special Rapporteur. The States that did react started to work on and pass new laws on the subject that contain only minor improvements in limited areas, if any at all. In general, those laws have been drafted and rushed through the legislative process to legitimize practices that should never have been implemented.

16. On 21 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 other rights in the digital age. With regard to legal obligations, which require the retention of data in bulk by telecommunications providers, the Court 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 are the subject of constant surveillance”.[15] It also mentioned the negative potential consequences for the exercise of freedom of expression.

17. The Court further recognized that “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”.[16] Furthermore, the Court made clear that the retention of traffic data must be the exception, not the rule. When there were 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 reiterated that the people concerned needed safeguards and remedies and that there must be effective oversight mechanisms in place involving checks and balances.[17]

18. While privacy advocates understandably welcomed the judgment, the other dimensions of the decision were perhaps most usefully summed up by David Anderson, Q.C., the Independent Reviewer of Terrorism Legislation in the United Kingdom: “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

[14] Privacy International, “Monitoring and oversight of communications surveillance”, November 2016, available from www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html.

[15] See European Court of Justice, *Tele 2 Sverige AB v. Swedish Post and Telecom Authority*, judgment of 21 December 2016.

[16] Ibid.

[17] Ibid.

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.”[18]

19. The Special Rapporteur comes from a tradition deeply committed to evidence-based policymaking, which is why he shares the Independent Reviewer’s desire for a more rigorous analysis of proportionality. To date, the Special Rapporteur has not yet been granted (in the United Kingdom 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 Special Rapporteur welcomes the judgment of the Court precisely because the evidence has not yet been made available that would persuade the Special Rapporteur of the proportionality or necessity of laws regulating surveillance which permit bulk acquisition of all kinds of data, including metadata and content.

20. It is important to draw attention to the cultural dimensions also noted by the Independent Reviewer 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.
> - 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).”[19]

B. Challenges and worrying trends

21. Through various research activities related to the mandate of the Special Rapporteur and through other related research projects, the surveillance activities of law enforcement agencies and the security and intelligence services have been found to be increasingly hard to distinguish from one another at times. While the activities of one branch are typically directed towards surveillance within the borders of the national territory and the activities of the latter towards foreign territories, the nature of transborder data flows 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.

22. Increasingly, personal data ends up in the same “bucket” of data which can be used and reused for all kinds of known and unknown purposes. That poses critical questions in areas such as requirements for gathering, storing, analysing and ultimately erasing data. As a concrete example, a recent study carried out by the Center on Privacy and Technology at Georgetown Law Center in Washington, D.C. found that one in two American adults is in a law enforcement face recognition network. As the authors of the study put it: “We know

[18] See www.terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/.

[19] Ibid.

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."[20]

23. These and similar insights lead to a couple of considerations. First, the nature of transborder 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 the substantial advantages that has brought and will continue to bring for humankind, there needs to be a consistent and trustworthy environment in which it 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.

24. 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 and specifically in his first report to the General Assembly (see A/71/368, paras. 19-40). In addition, other mandate holders, such as the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, have already carried out significant and welcome work in this area (see A/HRC/29/32).

25. If law enforcement agencies and the security and intelligence services are concerned about their inability 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 channels. Humans have started to share so much information through digital means that even if a few of them are not accessible to the State, that does not mean that there are no other ways to follow people with bad intentions. In particular, the vast amounts of metadata created by smartphones and connected devices, which are often as revealing as the actual content of communications, provide ample opportunities for analysing people's behaviour.[21] 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.

26. It is to be welcomed that some countries and organizations have already started to increase their efforts to tackle these challenges. The Council of Europe, in particular, has made a contribution in this area, with an initiative in the context of law enforcement in cloud-computing environments. That is connected with the Convention on Cybercrime and is aimed at developing a new legal tool.[22]

27. It is, however, worrying that modern laws on surveillance increasingly allow for the creation, access and analysis of personal data without adequate authorization and supervision. An adequate authorization 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."[23] While "traditional" methods, such as the interception of telephone calls and communications in general, are often subject to judicial authorization 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, telephone calls, use of applications, etc.) are subject to much weaker safeguards. That 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.

[20] Clare Garvie, Alvaro Bedoya and Jonathan Frankle, "The perpetual line-up: unregulated police face recognition in America", October 2016, available from www.perpetuallineup.org/.

[21] See, for example, a report by the Berkman Center for Internet and Society at Harvard University, "Don't panic. Making progress on the 'going dark' debate", 2016, available from cyber.harvard.edu /pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

[22] See www.coe.int/en/web/portal/-/cybercrime-towards-a-new-legal-tool-on-electronic-evidence.

[23] European Court of Human Rights, *Zakharov v. Russia*.

28. While judicial authorization of intrusive measures generally raises the degree of privacy protection, it must also be guaranteed that the judges themselves are independent and impartial in their decision-making processes in individual cases. Furthermore, they must have the knowledge and facts necessary to consider requests for such measures 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 to equip judges for this complicated task.

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

30. In most countries that will be hard to achieve, given the large volume of data involved. The authorities carrying out surveillance should take measures to guarantee 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.

31. Another area which attracts a lot of attention is the international nature of oversight activities. There are two particular dimensions to this phenomenon that require increased attention. First, it is of the utmost importance that States respect the right to privacy, which is based on human dignity, at the 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 that 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

32. Research and exchange with several national authorities, civil society and corporations from different global regions, especially during the International Intelligence Oversight Forum in 2016, have shown the emergence of several themes in the area of governmental surveillance. They include:

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

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

(c) The promotion and protection of fundamental human rights in relation to the methods used;

(d) Safeguards and remedies, preferably at an international level;

(e) Accountability and transparency;

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

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

(h) Answers to the question as to how to engage with the public;

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

(j) A need for more forums to make progress on the subject.

B. Discussion

33. The internationalization and standardization of terms and language aims to define 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”, which provides some aspirational descriptions for some of these terms.[24] It is important that government authorities carrying out surveillance, civil society and other stakeholders, have a clear view as to what they actually mean when they use such terms relating to surveillance. Some of them, such as “mass surveillance” are very loaded and highly controversial. What is necessary is a more comprehensive and harmonized use of terms and the understanding of them in exchanges between governmental authorities carrying out surveillance. However, oversight bodies of the judicial and political branch, civil society, researchers in the field of security and corporations should also be able to understand and use these terms appropriately.

34. 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 such discussions are being held, experts from civil society must be able to provide their input and share their concerns.

35. It is crucial that fundamental human rights, particularly privacy, freedom of expression and the right to information, remain at the core of any assessment of governmental surveillance measures of all types and kinds. While the protection of the rights to life and to physical integrity is a basic precondition for human existence, it has to be borne in mind that there is no strict hierarchy of human rights. They typically reinforce each other. That 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 of them.

36. A right is only worth as much as its delimitations and enforcement mechanisms allow it to be. That is crucial in the area of governmental surveillance, since safeguards without borders are needed, 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, more regional and cross-regional initiatives are needed.

37. The structure of accountability and transparency within governmental organizations carrying out surveillance needs 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 those 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.

38. 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, an evaluation of operations and a 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 technology and to understand that ultimately technology should assist, not drive, decision-making by humans.

39. 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

[24] Available from www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

often suffer from a lack of knowledge in this field, resources and/or access to relevant information. The same applies to mechanisms of judicial oversight, where these exist.

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

41. In addition, 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, information must be available, so that the general dimension of operations undertaken to protect the public can be grasped. A passenger does not need to know how to fly an aircraft in order to book a flight with it, but he or she will not pay for a ticket if he or she does not trust the general capability and safety of the aircraft traffic and safety systems.

IV. Activities of the Special Rapporteur

42. The Special Rapporteur on the right to privacy is reporting on the main public or semi-public activities carried out as part of his mandate. The present report covers his activities from July 2016 to the beginning of February 2017. They include:

(a) European privacy protection innovation workshop, Huawei German Research Center, held in Munich, Germany, on 3 August 2016;

(b) Keynote speaker, Council of Europe conference on the theme of “Internet freedom: a constant factor of democratic security in Europe”, held in Strasbourg, France, on 9 September 2016;

(c) Chair of a panel on biometrics and privacy, European Association for Biometrics research projects conference, held in Darmstadt, Germany, on 19 and 20 September 2016;

(d) Horizon 2020 Protection and Security Advisory Group meeting, European Commission Directorate-General for Migration and Home Affairs, held in Brussels on 27 September 2016;

(e) Special Rapporteur for the International Intelligence Oversight Forum, held in Bucharest on 11 and 12 October 2016;

(f) Keynote speaker and panel Chair, Intelligence in the Knowledge Society conference, held in Bucharest on 13 and 14 October 2016;

(g) Keynote speaker, 38th International Conference of Data Protection and Privacy Commissioners, held in Marrakesh, Morocco, from 18 to 22 October 2016;

(h) MAPPING second annual general assembly, held in Prague from 31 October to 2 November 2016;

(i) Keynote speaker, Cyberspace Conference 2016, held in Brno, Czechia, on 25 and 26 November 2016;

(j) Keynote speaker, Asia Pacific Privacy Authorities Forum, held in Manzanillo, Mexico, from 30 November to 2 December 2016;

(k) Keynote speaker and panellist, Irish Council for Civil Liberties, symposium on surveillance, held in Dublin on 7 December 2016;

(l) Keynote speaker, Northern Ireland Human Rights Commission, annual statement, held in Belfast, United Kingdom, on 8 December 2016;

(m) Preparatory meetings for the second workshop on privacy, personality and free flows of information, held in Tunisia from 12 to 14 December 2016;

(n) Panellist on artificial intelligence and privacy, Computers, Privacy and Data Protection tenth International Conference, held in Brussels from 25 to 27 January 2017;

(o) Keynote speaker on privacy and security, ninth ISMS Privacy Forum, held in Madrid on 1 and 2 February 2017.

V. Conclusions and recommendations

43. **At this stage, the Special Rapporteur wishes to make five distinct recommendations arising from his 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 the right to privacy could possibly be better protected through developments in domestic and international law;**

(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.**

Why populism and privacy are inimical to security

44. **To be more precise perhaps, this section should be headed security, populism and privacy. The period from 2015 to 2017 has seen a growing tendency, especially, although not exclusively, in Europe, to indulge in "gesture politics". In other words, the past 18 months have seen politicians who wish to be seen to be doing something about security legislating powers that are intrusive of privacy into being — or legalizing existing practices — without in any way demonstrating that this is either a proportionate or indeed an effective way to tackle terrorism.**

45. **The new laws that have been introduced are predicated on the psychology of fear: the disproportionate, although understandable, fear that electorates may have in the face of the threat of terrorism. The level of fear prevents the electorate from objectively assessing the effectiveness of the measures proposed.**

46. **There is little or no evidence to persuade the Special Rapporteur 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 United Kingdom and the United States. Like the judge in a recent case on the immigration ban in the United States, the Special Rapporteur must seek evidence for the proportionality of the measures provided for by laws.[25] In the same way as the judge asked precisely how many acts of terrorism had been carried out since 2001 by nationals of the States that were the subject of the immigration ban, the Special Rapporteur must ask whether it would not be much more proportional, let alone more cost-effective and less intrusive of privacy if more money was spent on the human resources required to carry out targeted surveillance and infiltration and if less effort was expended on electronic surveillance. That, at a time when the vast majority of terrorist attacks have been carried out by suspects already known to the authorities.**

47. **There is also growing evidence that the information held by States, including information collected through bulk acquisition or mass surveillance, is increasingly**

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

vulnerable to being hacked by hostile Governments or organized 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.

48. **Furthermore, the abuse of data collected by bulk acquisition remains a primary source of concern. Without necessarily casting aspersions on the incoming United States administration, the concerns expressed in that context by a senior researcher at Human Rights Watch 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."**[26] **While the checks and balances existing in the United States or indeed the ethical standards of the Executive itself may hopefully push the country away from the realization of such risks, the point being made here by the Special Rapporteur 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 as to preclude its very collection in the first place.**

49. **The Special Rapporteur therefore recommends that States desist from playing the fear card and improve security through proportionate and effective measures, not through privacy-intrusive laws that are unduly disproportionate. To quote Cardinal Vincent Nichols, Archbishop of Westminster, "I don't believe that any form of leadership is best exercised by using fear. True political leadership does not play the fear card."**[27]

How States may engage to improve privacy protection through better oversight of intelligence

50. **The 2016 International Intelligence Oversight Forum (IIOF) demonstrated that the discussion on how to manage the oversight of intelligence in a way that reinforces privacy safeguards is a complex process requiring much time, resources, occasional culture changes, political will and the generation of trust. There are no short cuts to identifying and further developing best practices.**

51. **The recommendation of the Special Rapporteur is a simple but important one: all States Members of the United Nations should engage in the painstaking discussion of the oversight of intelligence initiated by the Special Rapporteur at the 2016 International Intelligence Oversight Forum, which will be continued the next Forums in 2017. Governments should encourage oversight bodies and intelligence agencies to take part in the Forums and facilitate their participation.**

Who deserves to enjoy the right to privacy

52. **The Special Rapporteur recommends that States prepare themselves to ensure that both domestically and internationally, privacy is respected as a truly universal right and that, especially when it comes to surveillance carried out on the Internet, privacy is not a right that depends on the passport in your pocket.**

53. **That recommendation requires some space to develop and will be illustrated using examples here restricted (purely for reasons of space) to United States case law and legislative change. It should be clear at the outset that whatever is here recommended for the United States is likewise recommended in analogous situations for all States Members of the United Nations.**

[26] Cynthia M. Wong, "Surveillance in the age of populism", Human Rights Watch, February 2017, available from www.hrw.org/news/2017/02/07/surveillance-age-populism.

[27] Cardinal Vincent Nichols speaking on the BBC Radio 4 programme, the Westminster Hour, on 5 February 2017.

54. **On 6 February 2017, the United States House of Representatives did something very commendable, for which the Special Rapporteur had long been waiting. It unanimously passed the Email Privacy Act, which closed a gap in United States law by requiring a judicial warrant in order to permit access to e-mail more than six months old that is stored in the cloud or elsewhere. That is a development which the Special Rapporteur heartily welcomes and which he trusts will also be acceptable to the Senate, which derailed the process last time it was attempted in April 2016. Indeed the Special Rapporteur invites the Senate to seize upon a historic opportunity and go a step further, thereby demonstrating the commitment of the United States to human rights worldwide and simultaneously putting paid to one of the xenophobic fallacies that some Governments consciously or unwittingly promote, that only "nasty foreigners" are out "to get us" and that therefore they do not deserve to have their fundamental human rights respected by the law.**

55. **This is not a fault only of some United States law-making. For example, the Government of Germany has recently been equally guilty of adopting a law which distinguishes between German and European Union citizens on the one hand and everybody else on the other hand (see A/71/368, paras. 35-36). 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, they were not carried out by foreigners, but mostly by citizens of the European Union holding European Union identity cards and passports. Likewise, it would seem to be a similar situation for most recent terror attacks in the United States. So why pander to the 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 root causes of the problem, such as radicalization. Investing much more in measures to combat radicalization and allocating more resources to long-term targeted surveillance and cell infiltration would seem to be far more effective than indulging in gesture politics. Trying to appear tough on security by legitimizing 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.**

56. **The Special Rapporteur 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 United States law were to be aligned with the principles recently articulated in Europe by both the European Court of Human Rights in the case of *Zakharov v. Russia* and the European Court of Justice in the case of *Tele 2 Sverige AB v. Swedish Post and Telecom Authority*, namely that the key requirement for carrying out targeted surveillance is reasonable suspicion and not citizenship. If a security and intelligence service or law enforcement agency can demonstrate reasonable suspicion, then judicial permission to obtain an access warrant should be granted, irrespective of the passport held by the suspect. 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 held. The Universal Declaration of Human Rights very rightly does not state that only United States citizens have the right to privacy. Instead it states that everyone has the right to the protection of the law against such interference or attacks (see art. 12), by which the Special Rapporteur takes it to mean United States law also. Here, therefore, is an opportunity for United States legislators to set an example to others around the world, follow in the spirit and the words of the Universal Declaration and take concrete steps to make United States 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.**

57. **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. That is the truth to which the Special Rapporteur calls the United States Senate also to give witness. On so many occasions, Governments of the United States 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 citizens of the United States and other citizens, by extending the privacy safeguards afforded to citizens of the United States 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 Union and Council of Europe privacy and data protection laws, which make no distinction between the privacy rights of citizens and non-citizens.

How the right to privacy could possibly be better protected through developments in domestic and international law

58. **Whereas the previous recommendation deals largely with opportunities to protect the universality of privacy within domestic law, next few paragraphs contemplate opportunities to complement domestic measures through international law.**

59. **Another key concern raised by the current wording of the United States Email Privacy Act is whether the safeguards that are strengthened within the law are also applicable to data, wherever it is held, whether in the United States or elsewhere. To illustrate this issue, it is useful to cite the case of Microsoft contesting the global reach of United States search warrants relating to data held outside the country.**[28] **One can very easily understand the reluctance displayed by Microsoft to allow access to data held outside the United States. Not only does that have a potentially negative impact on its own competitiveness worldwide, but it also presents a particularly thorny problem when trying to decide how to deal with all kinds of requests for data from all kinds of Governments from around the world. That is not a problem which Microsoft faces alone. Most of the other industry technology giants predominantly of United States origin, such as Google, Facebook, Apple and Twitter (to name but a few) are faced annually with thousands of requests for access to data from Governments around the world.**

60. **If the United States 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 and one which would not put American firms at a commercial disadvantage, it should realize that the answer cannot lie solely in domestic law. It must also realize that this particular area of law is not being well served by tools such as mutual legal assistance, which are decades old. Congress should realize that while the Convention on Cybercrime made considerable progress in some areas, it has not yet managed to make the transfer of personal data across borders and access to the data required for investigations as fast and as problem-free as some would have hoped. One of the main reasons for that relative failure is that it has continued to rely too much on the nineteenth-century mindset of the sovereign nation State, rather than catering for the reality of the borderless Internet of the twenty-first century. While it is perhaps a good example of what may be achieved with "baby steps" and while it has certainly scored some successes, including the identification and codification of computer- and Internet-based offences, the Convention has not delivered on timely transborder flows of personal data, which are suitable for the detection, investigation and prevention of crime in the Internet age. One of the main possible reasons why it has not done so, is that it did not go the extra step of creating a mechanism, such as an international body tasked with authorizing international access to data and given the authority to do so.**

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

61. **In the same way that other forms of international law have provided for agencies to be established, tasked with creating trust and implementing appropriate safeguards in areas as diverse as maritime law, space law, atomic weapons, chemical weapons etc., the Convention on Cybercrime, in tandem with other multilateral treaties, including new ones created for the purpose, has the potential to be expanded in such a way as to create an international authority, which would be able to grant the equivalent of an international surveillance warrant or international data access warrant that would be enforceable in cyberspace. Countries signing up to such a new treaty, or an additional protocol, could contribute their own specialized independent judges to a pool where, sitting as a panel, they could conceivably act as a one-stop shop for relevant judicial warrants enforceable worldwide — in those countries which were party to the treaty. In that way, to return to the previous example of the decision of July 2016 in the Microsoft case, companies like Microsoft, Google, Facebook, Amazon, Apple and other technology giants operating data centres internationally would not need to worry about any State overstepping its boundaries, but would rather be faced with an international data access warrant issued on grounds of reasonable suspicion under clear international law. Likewise, citizens worldwide would be assured that their right to privacy, not to mention other rights, such as freedom of expression and of association, were 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 worldwide basis.**

62. **This is not utopia. It 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 cyberpeace, as recently advocated by the President and Chief Legal Officer of Microsoft.**[29]

63. **At present, the evidence available to the Special Rapporteur would suggest that a number of States, even some leading democracies, regrettably treat the Internet in an opportunistic manner, as somewhere where their law enforcement agencies and especially their security and intelligence services can operate relatively unfettered, intercepting data and hacking millions of devices, (smartphones, tablets and laptops as much as servers) worldwide. In doing so, between 15 and 25 States treat the Internet as their own playground, over which they can squabble for spoils, forever seeking to gain the upper hand, whether in terms of cyberwar, espionage and counter-espionage, or industrial espionage. The list of motivations is long while the other approximately 175 States look on powerless, unable to do much, except hope that somehow cyberpeace will prevail.**

64. **To state this frankly, a tiny minority of States have actively tried to informally discourage the Special Rapporteur from exploring options for solutions in this area, but it is his 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 organization, one corporation, indeed one reasonable law enforcement agency or 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 whether this can being achieved any time soon.**

65. **The only way that such clarity can be achieved and those safeguards and remedies introduced in such a way that their enforcement becomes more timely, even-handed and expedient is through multilateral agreements enshrined in international law. What the world needs is not more State-sponsored shenanigans on the Internet, but rational, civilized agreement about appropriate State behaviour in cyberspace, which brings the present report back to the subject of surveillance.**

[29] See 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.

66. **Some of the improved international mechanisms mentioned above would be very useful in law enforcement in cyberspace, something which is currently regulated by the Convention on Cybercrime. As its name suggests, however, the Convention, to which some 25 per cent of the States Members of the United Nations have already subscribed, deals only with the criminal justice sector. It does not deal with national security or 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 Convention and for them to be regulated satisfactorily the scope of the Convention would need to be considerably extended, or there would have to be a separate but complementary treaty that adequately covered surveillance in cyberspace. That would be much more preferable to a situation in which a number of democracies, such as France, Germany, the United Kingdom and the United States, are scrambling to introduce new laws regulating surveillance and where the mindset appears to be unduly influenced by the concept of the nineteenth-century sovereign nation State.**

67. **While nationalism and jingoism, not to mention populism, appear to be going through what history might demonstrate to be a cyclical rise in their 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 recognized — even by politicians speaking at the national level — that the vast majority of Member States have no interest in promoting acts of organized 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, Brazil, France, Germany, Ghana, India, the United Kingdom and the United States — to mention some countries randomly — there should be little fear that such a panel, or a panel similarly composed for the purpose, would not grant a warrant to access data about a person if reasonable suspicion was demonstrated. Once that process leads to an international data access warrant, that would considerably simplify things for Governments and corporations within the jurisdictions of States which have agreed on such mechanisms through an international treaty.**

68. **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 would be that very important yet often neglected other part of article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, namely, the right to protection of reputation, which is both distinct from yet akin to privacy.**

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

69. **In summary therefore, a legal instrument regulating surveillance in cyberspace would be a complementary step to other pieces of existing cyberlaw, such as the Convention on Cybercrime, and one which could do much to provide concrete safeguards to privacy on the Internet. Happily for the Special Rapporteur's mandate, a pre-existing initiative, the project on managing alternatives for privacy, property and Internet governance (MAPPING project) supported by the European Union is currently 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 is expected to get a public airing some time in 2017 and certainly before the spring of 2018. It would be premature for anybody, including the Special Rapporteur, to take a position on such a text, or a similar one, at this early stage of exploring options, but it is possible that it could eventually prove to be a useful springboard for discussion by Governments within intergovernmental organizations, including and perhaps especially the United Nations.**

70. **In the same way that the Special Rapporteur is preparing to deliberate on this subject, in particular 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 and 2018 — to actively explore such options for the proper regulation of surveillance and the introduction of privacy-friendly safeguards and remedies in cyberspace. That 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, which 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 that it not only protects privacy but also other fundamental human rights.**

71. **However difficult it may be to bring this 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. That 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. That has been the lesson learned from the development of international law over the past couple of centuries. There is no reason why that lesson should be ignored when it comes to privacy, surveillance and cyberspace. It may not come to fruition during the tenure of the Special Rapporteur, but it is at least the possibly most promising path on which to start. Everything the Special Rapporteur has seen in the course of his mandate to date has persuaded him that this may be the wisest path to tread when its time will come. That time may be sooner than some may wish to think.**