联 合 国 A/HRC/46/37/Add.4

大 会

Distr.: General
20 January 2021
Chinese
Original: English

人权理事会
第四十六届会议
2021 年 2 月 22 日至 3 月 19 日
议程项目 3
促进和保护所有人权——公民权利、政治权利、
经济、社会及文化权利，包括发展权

对美利坚合众国的访问

隐私权问题特别报告员约瑟夫·坎纳塔奇的报告* **

概要

隐私权问题特别报告员约瑟夫·卡纳塔奇于 2017 年 6 月 17 日至 28 日对美利坚合众国进行了正式访问。特别报告员对美国制度的一些长处表示称赞，但同时也发现，建制机构的增多造成的分散带来了一些风险，而且有人错误地认为行政部门一定会遵守某些公约。他建议逐步全面修改隐私法，侧重简化，并增加保障措施和补救办法。他尤其建议进一步修改美国法律，以加强现有和新的监督机构的权力，同时使外国情报方面的保障措施和补救办法达到与对国内情报适用的相同的标准。

* 报告概要以所有正式语文分发。报告正文附于概要之后，仅以提交语文分发。

** 因提交方无法控制的情况，经协议，本报告迟于标准发布日期发布。

Annex

Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, on his visit to the United States of America

I. Introduction

1. The present report was finalized in autumn 2020, after evaluating the preliminary results of the country visit in meetings held during the visit, which took place from 17 to 28 June 2017, and cross-checking them with follow-up research and developments to date. The benchmarks used in the present report include the privacy metrics document released by the Special Rapporteur.[1]

2. Much of the content of the present report reflects and builds upon findings already included in the end-of-mission statement published in June 2017,[2] as further validated up to the submission of the present report.

3. The Special Rapporteur thanks the Government of the United States for the open way in which it greeted him and facilitated his visit. Discussions with government officials were held in a cordial, candid and productive atmosphere.

4. The Special Rapporteur likewise thanks members of civil society and of the law enforcement and intelligence communities, governmental officials and other stakeholders who presented him with detailed documentation and organized several meetings with him in order to provide detailed briefings.

5. The Special Rapporteur thanks those members of Congress and their staffers who met with him and answered several questions, providing insights into issues of primary concern regarding privacy.

II. Constitutional and other legal protections of privacy

6. Privacy is not explicitly mentioned in the United States Constitution of 1787–1789, but is considered to be a protected right within the constitutional law of the United States, relying heavily on interpretations of the First and Fourth Amendments of the Constitution introduced in the Bill of Rights of 1791. The protection of privacy in the United States owes a significant debt to its development through the jurisprudence of the Supreme Court of the United States.

7. The right to the free development of an individual's personality, as protected by the Universal Declaration of Human Rights in articles 22 and 29, and as explicitly linked to privacy by the Human Rights Council in its resolution 34/7, is recognized by some eminent

[1] See Professor Joseph A. Cannataci, "Metrics for privacy – a starting point", available at www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf. The document was developed during the period 2017–2019 in order to enable the Special Rapporteur on the right to privacy to maximize the number of common standards against which a country's performance could be measured. It was refined at various stages and then changed status from an internal checklist to a document released for public consultation in March 2019.

[2] See www.ohchr.org/EN/Issues/Privacy/SR/Pages/CountryVisits.aspx. The two documents should be read together, especially since, owing to the wordcount limitation, several detailed observations available in the 2017 statement have been omitted from the present report. The task of compiling and updating the present report included processing 12,200 words in the preliminary observations, and nearly 28,000 words alone, in a United States narrative response provided on 5 November 2017, which it is recommended also be put into the public domain. The Special Rapporteur has additionally consulted thousands of pages of material collected and/or developed since his visit. Hence the official version, subject to the 10,700-word limit imposed on special procedure mandate holders by the General Assembly, is perforce a much less detailed one than it would have been desirable to submit.

United States jurists as subsisting in the United States under the right to privacy. "Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[3] Daniel Solove argues that the conceptualization of privacy:

> can be dealt with under six general headings, which capture the recurrent ideas in the discourse. These headings include: (1) the right to be let alone – Samuel Warren and Louis Brandeis's famous formulation for the right to privacy; (2) limited access to the self – the ability to shield oneself from unwanted access by others; (3) secrecy – the concealment of certain matters from others; (4) control over personal information – the ability to exercise control over information about oneself; (5) personhood – the protection of one's personality, individuality, and dignity; and (6) intimacy – control over, or limited access to, one's intimate relationships or aspects of life.[4]

8. The above summary of the scope of the right would be historically correct in a United States context, but it should be pointed out that certain elements which in the United States would often be discussed under a general heading of privacy, such as "control over one's body", are not universally understood to fall within the scope of the right to privacy. Indeed, many countries find it to be completely possible to discuss privacy without going into the merits of, say, the right to choose whether or not to have an abortion. The latter would appear to be much more significantly linked to the concept of individual autonomy rather than the core notions of privacy.

A. Legislation regarding surveillance

9. While the Special Rapporteur presented a draft legal instrument on government-led surveillance to the Human Rights Council in March 2018,[5] which may be used as an interim benchmark, there is as yet no universally agreed international binding multilateral treaty regulating such matters. States Members of the United Nations have therefore been very much left to "do their own thing" when it comes to safeguards and remedies in the case of State-led surveillance. The United States' approach to the subject reflects a genuine concern to get to grips with the thorny problem of effective oversight of surveillance. The United States remains one of a select group of possibly fewer than 13 countries (out of 193 States Members of the United Nations) which have made serious attempts to address issues of adequate oversight of surveillance following the revelations made by Edward Snowden in 2013 and since then. The United States additionally reaps the benefits of having introduced, or commenced reforms of, such legislation over a period of the four decades preceding those revelations. While there is no doubt that there are multiple legal, operational and structural protections for privacy in the United States, there remain significant question marks as to whether United States legislation is protective enough of the right to privacy.

B. Surveillance

10. With regard to levels of surveillance, the Special Rapporteur understandably asked the basic question: does the Government of the United States carry out more spying or less spying on ordinary citizens than other Governments? The Government provided the following arguments about the level of surveillance carried out in the United States: "The actual number of U.S. persons the U.S. government places under electronic surveillance each year is in fact far below the numbers proposed in the draft report. Any electronic surveillance of U.S. persons takes place either for criminal purposes, pursuant to the Wiretap Act, 18 U.S.C. § 2511, or for a foreign intelligence purpose, pursuant to the FISA [Foreign Intelligence Surveillance Act]".[6] The Wiretap Act requires the Administrative Office of the

[3] Daniel J. Solove, "Conceptualizing privacy", *California Law Review*, vol. 90, No. 4 (July 2002), p. 1088.

[4] Ibid., p. 1092.

[5] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.pdf.

[6] United States narrative response, 5 November 2017.

United States Courts to report the number of federal and state "applications for orders authorizing or approving the interception of wire, oral, or electronic communications".[7] As documented by the Administrative Office in the Wiretap Report 2016, "a total of 3,168 wiretaps were reported as authorized in 2016, with 1,551 authorized by federal judges and 1,617 authorized by state judges". The previous year, according to the Wiretap Report 2015, "a total of 4,148 wiretaps were reported as authorized in 2015, with 1,403 authorized by federal judges and 2,745 authorized by state judges". The reports for every year going back to 1997 are available on the website of the Administrative Office.[8] The Administrative Office is also required by statute to report the number of national security wiretaps.[9] The Administrative Office reported that the Foreign Intelligence Surveillance Court received 1,752 applications in 2016. "After consideration by the court, 1,378 orders were granted, 339 orders were modified, 26 orders were denied in part, and 9 applications were denied in full."[10] In addition, the Foreign Intelligence Surveillance Act requires the Attorney General to report statistics on such surveillance to certain congressional committees. The Director of National Intelligence provides the statistics in the semi-annual Statistical Transparency Report,[11] pursuant to the Intelligence Community's Principles of Intelligence Transparency. The transparency report for the calendar year 2016 reports a total of 1,687 targets in 2016 under titles I and III of the Foreign Intelligence Surveillance Act, as well as sections 703 and 704. That number includes both United States persons and non-United States persons. In 2016, only 336 of the targets were United States persons.[12]

11. The official answer received from the United States, above, is persuasive as to "ordinary wiretaps" and to much of the surveillance carried out about United States persons, but unclear as to whether it includes operations such as (a) scanning the emails of 500 million Yahoo[13] users in the United States and around the world (a claim which remains undenied by United States intelligence); or (b) all the bulk processing carried out by the National Security Agency or other agencies in terms of Executive Order 12333. So the inevitable conclusion is that the existing safeguards, including the Foreign Intelligence Surveillance Act, keep surveillance of United States persons at levels comparable to those in the least intrusive of Western democracies, but remain of significant concern as to what actually happens in terms of non-United States persons as well as of that Executive Order.

[7] 18 U.S. Code § 2519, para. 3.

[8] See www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

[9] Section 107 of Foreign Intelligence Surveillance Act Title I, 50 U.S. Code § 1807, requires the Attorney General to report to Congress and the Administrative Office the number of federal and state "applications for orders authorizing or approving the interception of wire, oral, or electronic communications". 50 U.S. Code § 1873 (a) (2) requires the Director of the Administrative Office to publish the report on the website of the Administrative Office.

[10] See www.uscourts.gov/sites/default/files/ao_foreign_int_surveillance_court_annual_report_2016_final.pdf.

[11] 50 U.S. Code § 1871.

[12] See www.dni.gov/files/icotr/ic_transparecy_report_cy2016_5_2_17.pdf. Those numbers are for collection authorities which may be used to target United States persons, which respond to the Special Rapporteur's observation in his June 2017 end-of-mission statement that "the government scans and copies the contents of millions of Americans' communications for information related to over 90,000 foreign targets". Separately, the same report discloses that under section 702 of the Foreign Intelligence Surveillance Act (which, as discussed in the latter part of the present report, targets the communications of foreign nationals located outside the United States to collect foreign intelligence), in 2016 there were approximately 106,469 individuals targeted, a miniscule fraction of the over 3 billion Internet users throughout the world.

[13] Yahoo is the most popular email service provider in the United States, with tens of millions of United States persons as Yahoo mail users. If all Yahoo mail is scanned at certain moments in time at the orders and to the specifications of the National Security Agency, the Federal Bureau of Investigation or the Central Intelligence Agency, that would translate into millions of United States persons being put under surveillance. That is not to say that such surveillance using selectors can automatically be classified as being disproportionate or unnecessary or that certain adequate safeguards are not implemented, but it does justify the concerns of the Special Rapporteur that there are occasions when tens of millions of United States persons and non-United States persons are placed under some form of surveillance.

12. The Special Rapporteur is especially concerned about the distinction that the Government of the United States continues to make between United States persons and non-United States persons. The Government tries to justify its position on two main grounds: (a) its official interpretation of its adherence to article 17 of the International Covenant on Civil and Political Rights is that it applies only to United States persons (see para. 24 below) and basically that the United States is unshackled by the Covenant when it comes to the privacy of non-United States persons; and (b) most other democracies also protect nationals more than non-nationals. Such an attitude is unacceptable to the Special Rapporteur and, it would appear, also to some Presidents of the United States. President Obama's Presidential Policy Directive 28 establishes, inter alia, the principle of non-arbitrariness which has an effect quasi-identical to the principle of proportionality. The Directive recognizes that non-United States persons deserve to have their privacy protected too. The United States should formally further entrench and enforce the standards established under that Directive. Apart from its intrinsic value for privacy worldwide, such a measure can only lead to increased international respect for the United States. Given that privacy should be treated as a universal right, the Special Rapporteur does not accept the approach of any country which applies lower privacy protection to non-nationals. He respectfully directs the attention of the Government of the United States to relevant good practice emerging in other States Members of the United Nations. Examples are the direction and consequences of the German Constitutional Court in May 2020 requiring a change of law compelling German foreign intelligence to improve the level of safeguards, and the practice of France to de facto apply identical levels of protection to both foreign and domestic intelligence.

13. The Special Rapporteur would like to single out the United States' innovation of creating a statutory Privacy and Civil Liberties Officer within many federal agencies as a good practice to be advanced internationally. All federal agencies have a Senior Agency Official for Privacy, whether that is specifically required by statutes creating Privacy and Civil Liberties Officers or by requirements issued by the Office of Management and Budget pursuant to its statutory authority. Indeed, the Special Rapporteur is reassured by the level of safeguards afforded by United States law in terms of statutory provision for Privacy Officers and accepts the assessment of the Government of the United States that the Department of Justice, the Department of Defense, the Department of State, the Department of the Treasury, the Department of Health and Human Services, the Department of Homeland Security, the Office of the Director of National Intelligence and the Central Intelligence Agency "are all required by statute to have a senior official who is responsible for ensuring that the agency appropriately considers privacy and civil liberties as it completes its mission. Chief privacy officers also have statutory mandates at the Department of the Treasury, General Services Administration, the Federal Elections Commission, the Federal Labor Relations Board and the Federal Maritime Commission.[14] Pursuant to Office of Management and Budget policy, other Executive Branch agencies are required to appoint a Senior Agency Official for Privacy who is responsible for the agency's privacy compliance." [15] As indicated in the recommendations, such statutory provisions, however commendable measures of good practice, are possibly not strong enough if the key holders of such posts are vulnerable to the whims of the Executive.

C. Surveillance for the purposes of law enforcement

14. There may occasionally be some blurring of lines as to surveillance carried out for the purposes of law enforcement and that carried out for agencies which are recognized as being members of the United States intelligence community. The concept of "police intelligence" is not a new one and there may be an understandable necessity to have such a standing function, but in that case, it is recommendable that the safeguards and remedies at state level should be at least as strong had the same activity been carried out by an intelligence agency or other agency operating at the federal level. It has proved difficult to accurately and

[14] Section 522 of the Consolidated Appropriations Act of 2005, Public Law 108–447, 118 Stat. 2809, Division H (2004). Available at www.gpo.gov/fdsys/pkg/PLAW-108publ447/pdf/PLAW-108publ447.pdf.

[15] United States narrative response, 5 November 2017.

comprehensively establish the safeguards protecting United States citizens from surveillance by non-federal law enforcement agencies across some 18,000 different law enforcement jurisdictions that exist in the United States.

D. Surveillance for the purposes of national security (domestic and foreign surveillance)

15. Surveillance for the purposes of national security is carried out by a combination of 16 different United States government agencies operating at the federal level subjected to a complex legal system providing various levels of privacy protection and oversight.

E. Oversight of agencies carrying out surveillance

16. The Intelligence Community in the United States is not left to its own devices. There is a complex system of oversight of surveillance, both ex ante and ex post. The United States has a strong system of ex-post oversight of surveillance including the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Foreign Intelligence Surveillance Court itself, the Privacy and Civil Liberties Oversight Board and others. It is a multilayered system that required the Special Rapporteur to hunt down multiple annual reports and other periodic or ad hoc reports, many of which run to several hundred pages. They may be scattered around on different websites, occasionally heavily redacted and published only after several months' delay because of a declassification process, but they contain a treasure trove of thousands of pages of evidence that surveillance methods and cases are regularly subjected to rigorous scrutiny. The persons who carry out that oversight and their reporting are very often a credit to the United States system, and the Special Rapporteur notes that they are an essential part of "a self-healing mechanism": their reports highlight flaws in the system which both the agencies and the legislators then try to fix. The oversight system of the United States may be at least partially credited with raising the awareness of the legislative branch, which contributed to the attempts to increase privacy safeguards by the United States Congress in 2020.

Privacy and Civil Liberties Oversight Board

17. The Special Rapporteur generally commends the work of the Privacy and Civil Liberties Oversight Board. He especially noted the Board's Strategic Plan for 2019–2022,[16] which envisages a range of actions. He looks forward to examining all the relevant reports, once they are published.

F. Privacy laws not directly concerned with government-led surveillance, including health-related data

18. In order to properly understand the complex patchwork of privacy protection provided by United States federal laws, regulations and policies, one needs to start by examining some 60 separate documents,[17] fewer than 10 of which are related to government-led surveillance. As may be seen from the foregoing, outside the scope of federal agencies as covered by the Privacy Act 1974 and those laws or policies pertinent to government surveillance, the United States has so far contented itself with a situation where it mostly takes a fragmentary approach to privacy protection. That is in contrast to the European omnibus approach which often applies identical standards to personal information, irrespective of whether it is processed by the public sector or the private sector. That does not mean that, in many cases, the protection of privacy is inferior in the United States, but all the available evidence does suggest that the fragmented approach taken by the United States makes it more expensive to administer and certainly more difficult for anybody, especially normal citizens, to understand. Indeed, "63% of Americans say they understand very little or nothing at all about

[16] See https://documents.pclob.gov/prod/Documents/StrategicPlans/10/StrategicPlan_2019-2022.pdf.
[17] United States narrative response, 5 November 2017.

the laws and regulations that are currently in place to protect their data privacy".[18] It is also time for the emphasis to change and become a more rights-based one. Put differently, it is time for the Government of the United States to emphasize that people are citizens first and consumers second. People enjoy a right to privacy irrespective of what, when, why and how they consume. That notwithstanding, the Special Rapporteur would like to mention the sterling work carried out by the Federal Trade Commission which, in the United States, carries out many of the functions similarly exercised by a data protection authority in other countries. Although the focus continues to be on "consumers", it is clear that the Commission's efforts contribute significantly to the protection of privacy of United States persons.

III. Conclusions and recommendations

A. Intelligence oversight, security and surveillance

1. Background and context

19. **The mandate of the Special Rapporteur was created in the wake of the Snowden revelations and thus much attention continues to be paid to the Special Rapporteur's findings on surveillance globally, but especially those involving the United States. The Special Rapporteur has spent the past five years, inter alia, observing a small group of States which are not in any way willing to open themselves to his scrutiny, yet which are more than willing to seize on each and every opportunity as an excuse to condemn the international surveillance activities, real or alleged, of the United States of America. Indeed, that has been one of his major disappointments while serving the United Nations: instead of engaging in good faith in order to protect human rights, some countries continue to "play the system". Their public statements in United Nations meetings and their criticism of other countries in no way contradict a mounting body of evidence that they themselves are possibly the worst possible transgressors of human rights, especially the right to privacy, both domestically and internationally. The Special Rapporteur is also conscious of the risk that some States may seek to instrumentalize anything he may say, and therefore invites States and civil society to always clarify with him the real intention that he wishes to convey in the present and any other report. He also cautions against the dangers of cherry-picking from the recommendations that he makes: they are intended to be a package of measures and subtracting one could significantly detract from the effect of the others.**

20. **To put things into their proper context, it should be unequivocally stated that during the five years of his tenure, there have been occasions in which the Special Rapporteur felt that some States were attempting to intimidate him and that his personal safety and liberty were threatened. None of those States accepted his formal or informal proposals that they invite him to carry out official country visits in order to investigate at first hand the extent to which privacy is protected or menaced in their territory. The first thing that should be stated therefore is that the Government of the United States welcomed the Special Rapporteur's visit and acted in the most open of manners, as befits a true democracy. Likewise, when its officials disagreed with his findings, they did so respectfully, however robustly.[19] On some matters they may have persuaded him, on others not, but in no way did he ever feel intimidated or under threat from the United States. The vast majority of the officials he dealt with have earned and continue to enjoy his deepest respect. They believe in their country and in their system**

[18] See www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[19] The Government of the United States also provided the Special Rapporteur with references to dozens of official websites, scores of laws at federal and state level, and thus thousands of pages of evidence to examine. The evaluation of the evidence gathered during the visit on-site in the United States and follow-up with various stakeholders also included waiting for and evaluating a number of key reports from the Privacy and Civil Liberties Oversight Board and the Foreign Intelligence Surveillance Court, the most recent of which considered in the present report was declassified in September 2020.

and, understandably enough, do their best to paint things in a good light. Those members of the United States justice, health, security and other spheres of activity give credence to the United States claim of a growing professionalism in their sectors which favours the respect of privacy.

21. **Some States Members of the United Nations or indeed internal critics in the United States itself will doubtless attempt to quote selectively from the present report in order to suggest that the United States is a major power which flagrantly disrespects privacy and that it compares unfavourably to, say, Europe when it comes to safeguards regarding surveillance. That would be a gross misrepresentation of the situation that the Special Rapporteur is faced with. His findings confirm that the United States is easily one of the top 10 or 20 countries in the world when it comes to the extent to which the right to privacy is protected in the realm of surveillance, but that does not mean that things are perfect or cannot be improved significantly. It just means that out of the 193 States Members of the United Nations, most are quite lax, inefficient or downright deceitful when it comes to effective safeguards and proper oversight of surveillance and that the United States is doing a reasonably good job within the system it has currently devised. The main point remains whether that system is good enough. The short answer is that in some instances it is and in others it is not. The present report contains recommendations which should resolve long-standing bones of contention, address any possible existing levels of complacency and improve the system to everybody's benefit.**

22. **The recommendations made by the Special Rapporteur relate to what type of oversight should be made (ad hoc substituting prior generic), when it should be made (ex ante – before the surveillance is carried out as well as ex post – after the surveillance is carried out), and why surveillance should be authorized (i.e., because it is necessary and proportionate). The Special Rapporteur respectfully also evaluates existing suggestions as to who should carry out the oversight.**

23. **The constant comparisons between the United States and the European Union are unavoidable, but often unhelpful in that they are often superficial and do not properly take into account the complexities of the situation. Many people will doubtless agree with the assessment of the European Court of Justice (*Schrems II*) that United States surveillance authorities, including pursuant to section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, create the possibility or outright permit large-scale surveillance that is not strictly necessary to the needs of the State. That is something which the Special Rapporteur thinks should be remedied irrespective of relations between the European Union and the United States, but again, that deficiency in the United States system does not mean that privacy is totally or almost always disrespected, nor does it mean that all or indeed most European Union member States have safeguards for privacy in matters of surveillance that are as protective as those in the United States. Put another way, let it be unequivocally stated that the United States has more safeguards for privacy in matters of surveillance than the vast majority (around 20) of the 27 European Union member States. That stark fact being recognized, some other basic facts remain, with one positive fact being unable to negate or counterbalance less positive facts, as indicated in paragraph 24 and 25 below.**

24. **The United Nations system, and the European system with it, expect any interference with privacy to meet the tests of necessity and proportionality. The Government of the United States has formally rejected that position. The Court of Justice of the European Union in Luxembourg correctly finds that necessity and proportionality are not formally key tests in the United States system, which encompasses section 702 of the Foreign Intelligence Surveillance Act and Executive Order 12333, hence they cannot be trusted to deliver against such metrics.**

25. **The European system, comprising the 27 member States of the European Union and the wider family of the 47 member States of the Council of Europe, which adhere to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of the Council of Europe (European Treaty Series No. 108), requires Governments to respect the principles of necessity and proportionality in matters of national security as a matter of**

binding international law. Even if many European Union or Council of Europe member States do not currently have the same detailed legal and/or operational safeguards for privacy protection in matters of surveillance as the United States, the citizens and residents of Europe have remedies in their domestic legislation and all the way up to the European Court of Justice and the European Court of Human Rights. The sad truth is that European citizens do not enjoy the same standards of necessity and proportionality, protections and remedies as in the United States, nor, let it be said immediately, in a host of other countries for that matter, say China, the Democratic People's Republic of Korea, India, the Islamic Republic of Iran and Japan, to name but a few. As it happens, to date, the Court of Justice of the European Union has been called in to decide the matter about the transfer of personal data to the United States. What would it have to say if it had to apply the same metrics that it has applied to the United States in *Schrems II* to, say China or Japan? All available evidence would suggest that both China and Japan – and many other States – would fail one or more of the *Schrems* tests, yet it remains a fitting irony that the State Member of the United Nations which has probably the most effective privacy protections for surveillance out of those countries dealing with Europe, that is, the United States (in addition to Canada, New Zealand and a few others), is the one receiving a very public castigation for the inadequacy of the safeguards and remedies in its current legislative framework.

26. **The Special Rapporteur has not received adequate and persuasive evidence that the use of technology in surveillance in the United States is always necessary and proportionate, whether the surveillance is carried out at the state or the federal level. On the contrary, evidence continues to pile up that it is not always so.**[20] **That does not mean that the vast majority of cases of surveillance do not actually meet the tests of necessity and proportionality. Neither does it mean that privacy safeguards are not in place or are generally not applied. It means especially that some types and instances of surveillance, especially those involving non-United States persons and bulk processing of data, need to be further examined in an independent and credible manner in much more detail in order to quell doubts about necessity and proportionality. The result of such scrutiny in Europe has led to some instances of bulk processing being declared to be unlawful and other instances of bulk processing to be notionally acceptable. The Special Rapporteur finds that the United States needs to carry out the same level of scrutiny as that carried out in Europe – and possibly even more given that the level of surveillance that it carries out may be much wider and deeper than most European States. If instances are detected where surveillance was either unnecessary or disproportionate, if the right safeguards and/or remedies were not in place (e.g., ex ante authorization on an ad hoc basis), then they should be legislated into being and deployed without delay. Again, the current situation should not be misconstrued: the Special Rapporteur is not saying here that there currently exists no independent scrutiny: the very cases which have brought the overreach of United States intelligence agencies to the Special Rapporteur's attention are the result of existing rigorous scrutiny within the United States which also contains evidence that some remedial action is taken immediately by the agencies concerned.**[21]

[20] See all examples cited in the Foreign Intelligence Surveillance Court reports, especially those published between 2016 and 2020. In one such case, it transpires that the Court in its decision of 6 December 2019 in practice applied the principle of necessity in declaring thousands of queries requested by the Federal Bureau of Investigation in August 2019 to be unnecessary and, in essence, disproportionate. The Federal Bureau of Investigation had put in the standard justification that the entire search met the standard of being reasonably likely to retrieve foreign-intelligence information or evidence of a crime, but Judge Boasberg called that position "unsupportable" and characterized all but 7 out of the 16,000 queries as "broad, suspicionless queries". There appear to have been dozens of other cases of surveillance which infringed existing safeguards. See www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf. See also the reports by Inspector General Horowitz of 2019 and 2020.

[21] See Judge Boasberg's positive assessment of new procedures which require analysts to provide a written justification for why their searches met the applicable standards. Boasberg said the latest procedures met legal and constitutional requirements. Available at

27. **The Special Rapporteur notes that many of the problems noted in practice by one of the existing principal United States independent oversight authorities, the Foreign Intelligence Surveillance Court,**[22] **largely arise from the current system of permitting warrantless searches by authorizing them to be carried out against a system of rules which are reviewed annually. Part of the official explanation given on a government website is that "Because of this change in communication technology, the government had to seek individual court orders, based on a finding of probable cause, to obtain the communications of non-U.S. persons located abroad. This proved costly because of the resources required and because the government couldn't always meet the probable cause standard, which was designed to protect U.S. persons and persons in the U.S."**[23] **The Special Rapporteur has examined very closely the reasons why that takes place and notes that in practice, it largely boils downs to resources. Weakening privacy protection is not the answer, whereas increasing resources could be a very significant part of the remedy. The Special Rapporteur observes that there is no shortage of excellent law graduates in the United States, coupled with a tradition for a strong and independent judiciary. Likewise, an increase in resources in the intelligence community would not only enable the ex ante authorization to be carried out, but would also increase the ability to meet the probable cause standard already established for United States persons. He therefore strongly recommends that the existing legal framework created by Foreign Intelligence Surveillance Act be reinforced further by:**

(a) **Significantly expanding the strength of the Foreign Intelligence Surveillance Court with the adequate number of independent judges;**

(b) **Training those judges adequately in matters of technology law and security science;**

(c) **Possibly amending the composition of the Foreign Intelligence Surveillance Court into a more tribunal-like setting with judges sitting together with at least one information and communications technology technical and one operational expert;**

(d) **Correspondingly increasing the required resources in the intelligence community to equip both the Foreign Intelligence Surveillance Court and the Intelligence Community for the task of handling the larger amount of ex ante oversight requests that would result from amending Foreign Intelligence Surveillance Act section 702.**

That will prove to be costly, but like other human rights, privacy does not come cheap. In voting the necessary resources, the United States Congress would be putting its money where the country's mouth is. It would thus set an example and demonstrate to the world that it is worthy of leadership since it is also investing significant funds to ensure that everybody's privacy is protected around the world and that United States protection of human rights has lost its narrow focus on United States persons and regained a global dimension.

28. **In line with the previous recommendations on resources and training, the Special Rapporteur therefore strongly recommends that the Foreign Intelligence Surveillance Act be amended to require that authorization for surveillance is always granted on: (a)**

www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf.

[22] See, for example, cases examined by Judge Boasberg, available at www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf. His concern is such that he has ordered the Government of the United States to "promptly submit in writing a report concerning each instance in which FBI personnel accessed unminimized Section 702-acquired contents information that was returned by a query that used a U.S.-person query term and was not designed to find and extract foreign-intelligence information. The report should include a detailed description of the information at issue and the manner in which it has been or will be used for analytical, investigative, or evidentiary purposes. It shall also identify the query terms used to elicit the information and provide the FBI's basis for concluding that the query was consistent with applicable procedures" (p. 81).

[23] See www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf.

an ex ante basis; and (b) an ad hoc case-by-case basis by the Foreign Intelligence Surveillance Court or an equivalent authority. The same safeguards should be applied in each and every case of surveillance carried out under Executive Order 12333 and any other relevant executive authorizations. It should be clear that the Special Rapporteur is recommending that the United States revert to protections that it had already devised in the versions of the Foreign Intelligence Surveillance Act that existed for almost 30 years between 1977 and 2007. [24] **The Special Rapporteur's recommendation requires undoing some amendments made to the Act in 2007**[25] **and 2008 by, for example, reintroducing into the definition of "electronic surveillance" in the Act any surveillance directed at a person reasonably believed to be located outside the United States, as well as radically amending section 702.**

29. **The Special Rapporteur notes that the United States continues to have what, at first glance, appears to be a serious formal disagreement with the United Nations system regarding some of the most important metrics applied in the present report. The Special Rapporteur, in line with internationally accepted rules and best practice, holds that any action interfering with privacy should be necessary and proportionate in a democratic society. The United States does not accept that concept as an accepted legal basis for determining whether an interference with privacy is arbitrary or unlawful under the International Covenant on Civil and Political Rights. As the United States indicated to the Human Rights Committee in its one-year follow-up response on the Committee's concluding observations, it does not share the Committee's view as to the applicability of the legal concepts of "necessity" and "proportionality" to article 17 of the Covenant. It asserted that those legal concepts were derived from certain regional jurisprudence, were not broadly accepted internationally, and were not supported by the *travaux* of the treaty.**[26] **Also of relevance in that context are the Government's observations on**[27] **the Committee's draft general comment No. 35, addressing the Committee's application of such concepts in relation to its interpretation of the term "arbitrary" under article 9.**[28]

30. **It is to be immediately noted that the United States' disagreement with the test of proportionality as cited officially to the Special Rapporteur and reproduced above is prima facie primarily a procedural one. That is not surprising, especially given that "some areas of U.S. constitutional law embrace proportionality as a principle, as in Eighth Amendment case law, or contain other elements of the structured 'proportionality review' widely used in foreign constitutional jurisprudence, including the inquiry into 'narrow tailoring' or 'less restrictive alternatives' found in U.S. strict scrutiny".**[29] **While it is true that some scholars have demonstrated how United States law, including constitutional law, could benefit from further developing the principle of proportionality, that is not the same thing as saying that there are not already strong elements of the principle in United States law or that United States law is completely inimical to the further development of that principle. The United States has not advanced any persuasive substantive (as opposed to legal procedural) reasons as to why "necessity and proportionality" are not the correct tests, nor has it persuaded the Special Rapporteur in any way that those tests should not be more fully applied within United States law.**

[24] Although some people claim that the protection offered then was unintended on the part of the legislator.

[25] Under the Protect America Act of 2007.

[26] Available at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fFCO%2fUSA%2f19957&Lang=en, para. 33.

[27] The key legalese here is "arbitrary and unlawful" under the International Covenant on Civil and Political Rights. In other words, the United States is here attempting to present arguments which would deflect criticisms that it is not adhering to its international law obligations if there were to be any instances where it is not applying the principles.

[28] See https://2001-2009.state.gov/s/l/2007/112674.htm.

[29] Vicki C. Jackson, "Constitutional law in an age of proportionality", *Yale Law Journal*, vol. 124, (2015), p. 3096.

31. **In the light of the above, the Special Rapporteur finds that all the evidence available to him bears out the following assessment made in 2016:**

> **While the Proportionality Principle is reflected on paper in both constitutional law and statutory law, the government's actual use of new surveillance technologies runs contrary to this principle. Again, the result is that violations of the Proportionality Principle are widespread, including in the National Security Agency's bulk collection of data and the powerful broad surveillance tools increasingly used by local law enforcement agencies. Even as courts struggle to reach a consensus on how aging laws will apply to new surveillance technologies, some state legislatures are innovating to protect the privacy of their citizens. Ultimately, in order to create a unified standard for government access to a range of different types of electronic data, it may be necessary for the United States Congress to adopt comprehensive communication surveillance reform.**[30]

32. **The Special Rapporteur therefore respectfully but strongly recommends that the United States change its formal stance and, instead of looking into the *travaux* for justifications to maintain its current position, it should formally accept that the tests of necessity and proportionality are the right ones to apply for those measures provided for by law which permit interference with privacy in certain well-defined instances. In so doing, the United States would simply reflect many of its own internal developments, some of which already directly or indirectly accept and promote necessity and proportionality.**

33. **The Special Rapporteur recommends that the Government immediately repeal section 14 of President Trump's Executive Order entitled "Enhancing Public Safety in the Interior of the United States", which directs federal agencies to "ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information". That section goes against international human rights law and practice, but just as importantly, is inherently nonsensical. As he does with all other Governments, the Special Rapporteur draws the attention of the Government to the fact that, in matters of security, what is relevant is the element of risk and not nationality or residence. Is somebody a risk or not? A person's nationality or place of residence should not automatically create a presumption in his or her favour or against it. A survey of terrorist attacks carried out in most States worldwide suggests that most terrorists are "home-grown" so provisions such as section 14 make no sense at all in practice. Nevertheless, such provisions, in essence, do reflect a universal reality in the field of surveillance law: many politicians are perfectly comfortable with restricting the rights of people on whose votes they do not depend.**

(a) The "who" in the oversight of surveillance – ex ante

34. **One of the healthier aspects of United States law on the subject of surveillance is that, since it requires periodic review and renewal, it regularly generates an important debate about the subject. The Special Rapporteur has observed with great interest the process in the United States legislature, especially in May 2020 regarding the renewal of Foreign Intelligence Surveillance Act. During that process, an amendment proposed by Senator Rand Paul would have required the Government to go to a traditional federal court instead of the Foreign Intelligence Surveillance Court to get a warrant to eavesdrop on an American. That amendment was defeated. The Special Rapporteur would respectfully discourage a development such as that advocated by Senator Paul not only, or primarily, because of the unwarranted distinction it creates between United States persons and non-United States persons. The Special Rapporteur expresses a strong preference for the United States to continue to develop a strong cadre of specialized judges within a much-expanded Foreign Intelligence Surveillance Court, better equipped with significant training in technology law and security science. The**

[30] Rumold Mark, "Assessing the legality and proportionality of communications surveillance in United States law" (2016). Available at https://necessaryandproportionate.org/country-reports/united-states-america/twenty-sixteen/.

Special Rapporteur bases that view on the fact that, in the United States, as in most other States Members of the United Nations, legal training and judicial training are inadequate in the areas of technology law and security science and it is far preferable to have such sensitive matters decided by specially trained judges, ideally sitting as part of a tribunal that also incorporates technical and operational expertise.

35. **A small but growing number of countries have adopted or are seriously considering the creation of an independent oversight tribunal which is responsible for some of the oversight in matters of intelligence. While they tend to be more secretive than normal courts, they do permit independent scrutiny in a discreet manner more fitting to sensitive material and operations dealt with by both law enforcement and intelligence agencies. The United States has followed that model in the Foreign Intelligence Surveillance Court and in May 2020, its Congress attempted to introduce further safeguards which the Special Rapporteur recommends as a model of good practice. Specifically, the amendment "requires FISA court judges to appoint an amicus curiae (a neutral third-party observer) in any case involving a 'sensitive investigative matter' so long as the FISA court does not determine it to be inappropriate. The amendment will also empower the amicus to raise any issue with the court at any time and give both the amicus and the FISA court access to all documents and information related to the surveillance application".[31] The idea of an independent counsel who is appointed on an ad hoc basis to defend the interests of the person or persons being placed under surveillance is something which should be explored further both inside and outside the United States. It may contribute to increasing much-needed synergy between security and privacy.**

36. **While noting favourably the improvement achieved by the successful amicus curiae amendment, from Republican Senator Mike Lee of Utah and Democratic Senator Patrick Leahy of Vermont, which would increase third-party oversight to protect individuals in some surveillance cases, the Special Rapporteur regrets that neither the Senate nor the House of Representatives has succeeded in introducing a further safeguard. He notes that another proposal that fell just short of 60 votes would have prevented federal law enforcement from obtaining Internet browsing information or search history without seeking a warrant. "Should law-abiding Americans have to worry about their government looking over their shoulders from the moment they wake up in the morning and turn on their computers to when they go to bed at night?"[32] The Special Rapporteur shares Senator Ron Wyden's view that they should not have to do so and was pleased to see that the amendment was reintroduced in the House of Representatives in May 2020. It would appear that the House has, however, since suspended discussions on the issue. That and other safeguards should be included in the next major reform of United States law on surveillance.**

37. **In many instances, the stars have to be properly aligned for the right laws to be made at the right time by the right people in the right way. In the 2017 Foreign Intelligence Surveillance Act review, an opportunity was missed to introduce major reform in United States surveillance law. The time was not right, some of the players were possibly not the right ones, and the mood about surveillance was not right. In May 2020, the closeness of the Senate vote on Internet browsing was taken to be an indicator of a mood swing. It is possible that the changes brought about by the November 2020 elections in the United States could bring the stars into perfect alignment for the amendments to the Foreign Intelligence Surveillance Act and increased oversight of Executive Order 12333 and any other relevant legislation. For such endeavours, the Special Rapporteur strongly recommends ensuring that:**

(a) **Necessity and proportionality are entrenched as criteria applied when giving authorization ex ante to surveillance;**

[31] See www.lee.senate.gov/public/index.cfm/2020/5/senate-passes-lee-leahy-fisa-amendment.

[32] See www.wyden.senate.gov/news/press-releases/wyden-opposes-warrantless-government-surveillance-of-americans-internet-browsing-history-.

(b) **Bulk processing of data is authorized only in the most targeted of manners and always in conformity with the principles of necessity and proportionality.**

38. **The United States Congress exerts significant oversight over the activities of intelligence agencies, relying heavily on the findings of the professional full-time oversight bodies such as the Foreign Intelligence Surveillance Court and the various Inspectors General. Increased bipartisanship in that sector, as witnessed in 2020, is encouraged as are the various legislative next steps recommended in the present report.**

(b) The "who" in the oversight of surveillance – ex post

39. **The ex post oversight system of federal agencies is a complex one because of the size of the United States intelligence community, but the Special Rapporteur does not express any preference as to the method of organization of such oversight, since the current one appears in practice to sufficiently maintain focus. The increasingly effective coordination brought about by the privacy function inside the Office of the Director of National Intelligence is impressive in itself, as are the holders of the posts with whom the Special Rapporteur has met on several occasions. One of the areas of United States good practice that the Special Rapporteur would wish to highlight is that in many cases,[33] the oversight ex post is carried out by somebody quite different from the person or persons who granted authorization ex ante. That helps avoid any perceptions or accusations of "marking one's own homework".**

40. **Do the very positive points noted above and previously mean that the ex post oversight of surveillance in the United States cannot be strengthened further, and indeed that such strengthening is not absolutely necessary? The short answer is that urgent action needs to be taken in order to protect the holders of office entrusted to carry out oversight. During his visit to the United States, the Special Rapporteur was struck by the sincere belief of many career senior officials in the integrity and independence of the office holders involved in the oversight of surveillance and their belief that the Executive would not dream of interfering with their independence of action. There was ample evidence of that independence of action, to the extent that the approach taken by then Inspector General of the Intelligence Community, Michael Atkinson, was highlighted by the Special Rapporteur as good practice during the International Intelligence Oversight Forum he co-hosted with the authorities of the United Kingdom of Great Britain and Northern Ireland in London in October 2019.**

41. **The Special Rapporteur however shares the view endorsed by many United States legislators, as articulated by James Madison: men are not angels.[34] The Special Rapporteur's experience with less-than-angelic politicians worldwide, including in his home country, has fostered a strong preference for safeguards for independence which are built into the law. Indeed, the Special Rapporteur has separately and publicly, through a detailed letter sent to the Government on 7 July 2020,[35] expressed deep dissatisfaction with United States law which permits a maverick President the discretion to dismiss the Inspector General of the Intelligence Community without oversight from the Senate. For reasons of space, the case outlined in that letter is not reproduced here in full, but it contains a specific recommendation which needs to be reiterated. The Special Rapporteur's chief concern is with Statute 50 U.S. Code section 3033 (c) (4) (Inspector General of the Intelligence Community), which provides that: "The Inspector General may be removed from office only by the President. The President shall communicate in writing to the congressional intelligence committees the**

[33] With the notable exception of the Foreign Intelligence Surveillance Court.

[34] "If Men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and the next place, oblige it to control itself." From *The Federalist*, No. 51, "The Structure of the Government Must Furnish the Proper Checks and Balances Between the Different Departments".

[35] See https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25193.

reasons for the removal not later than 30 days prior to the effective date of such removal. Nothing in this paragraph shall be construed to prohibit a personnel action otherwise authorized by law, other than transfer or removal." The Special Rapporteur respectfully submits that Statute 50 U.S. Code section 3033 (c) (4) be amended to ensure that the oversight of intelligence agencies is carried out in an independent manner. Regrettably, current United States law does not provide adequate statutory protection of office for the Inspector General of the Intelligence Community, nor for most of the other key senior figures who provide oversight of United States intelligence operations. True independence can be significantly reinforced by statutory independence of office. The Special Rapporteur therefore strongly recommends that section 3033 (c) (4) be amended to read that the Inspector General may be removed from office only by a motion backed by no less than two thirds of the members of the Senate.

42. **The above-mentioned recommendations of the Special Rapporteur regarding the protection of tenure of the Inspector General of the Intelligence Community should be extended to all those Inspectors involved in oversight of surveillance, especially the Inspector General of the Department of Justice, and preferably all Inspectors General established in terms of 5a U.S. Code section 12.**

43. **With regard to the Privacy and Civil Liberties Oversight Board, the main recommendation is that both the Executive and Congress make a greater effort to ensure the timely nomination and appointment of Board members, since the lack of quorum and late nominations and appointment of its members have hampered the timeliness of its work over the years.**

2. Clarifying Lawful Overseas Use of Data Act (CLOUD Act)

44. **The Clarifying Lawful Overseas Use of Data Act (known as the CLOUD Act) is a unilateral and bilateral approach to regulating criminal justice sector data flows to and from the United States and is therefore, almost by definition, a suboptimal way of tackling the issue on a global level. The Special Rapporteur contends that the matter cannot be settled definitively and satisfactorily unless there is a proper multilateral approach that regulates the matter in terms of public international law through binding multilateral agreements. The Special Rapporteur however recognizes that in the current climate characterized by a lack of the required political will among States Members of the United Nations, bilateral approaches such as the CLOUD Act may have a positive effect in the interim until a multilateral approach is achievable. The Special Rapporteur therefore encourages States to engage with the United States of America in order to explore how the CLOUD Act could be implemented in a way which fully respects the right to privacy. That is in keeping with the Special Rapporteur's stated position of encouraging regional and bottom-up approaches to discussing privacy-related matters, since the devil is in the detail and detailed discussion enables States to identify where privacy may be at risk and how such risks may be mitigated through procedural and substantive measures.**

B. Further modernization of United States' privacy and data protection laws

45. **The Special Rapporteur recommends that the Government set 1 May 2024, the date of the fiftieth anniversary of the introduction of the Privacy Act into Congress by Senator Sam Ervin, as the latest target date for updating that Act. That would grant the federal Government ample time for the necessary consultations at both the federal and state levels. Senator Ervin based his arguments for the Privacy Act of 1974 on the First and Fourth Amendments of the United States Constitution, and his trailblazing legislation helped establish United States leadership in thinking and action about the matter. It helped set a good example for Europe to follow, build and expand upon. It is time for a rethink, especially as to how the principles of privacy law in the United States should apply evenly to both the public and private sectors. The power of personal data held by the latter has never been more visible than in 2020, when United States-based corporations actually determined what otherwise-sovereign Governments worldwide**

would have access to in the course of the coronavirus disease (COVID-19) pandemic. The United States federal and state governments should set out to learn from the experience of the implementation in California of its Consumer Privacy Act and then update the 1974 Act accordingly in the spirit of Senator Ervin's commitment to the protection of the freedom of the individual. That exercise would have been essential had the United States been the only country on planet Earth. As it is not, updating its Privacy Act in the direction of the California Consumer Privacy Act would also greatly facilitate the transfer of personal data to and from other countries or regional groupings such as the European Union.

C. Privacy and health-related data

46. **The Special Rapporteur found a general if quiet consensus that the Health Insurance Portability and Accountability Act of 1996 is in sore need of updating. Furthermore, the COVID-19 pandemic has provided an opportunity for reflection. Most, if not all, of the issues raised by wearables, computerization of health records, related use of artificial intelligence, technology applications in contact tracing and standards to be respected, even in a pandemic, are addressed by the Special Rapporteur's recommendation on the subject,**[36] **as explained in the accompanying explanatory memorandum.**[37] **The Special Rapporteur therefore respectfully draws the attention of the Government to the recommendation on the protection and use of health-related data, which he presented to the General Assembly in October 2019 (A/74/277, annex), and urges the Government to update the Health Insurance Portability and Accountability Act accordingly. He also urges the Government to reflect on the successes and failures in attempts to use applied technologies, especially smartphone applications, in efforts to fight the COVID-19 pandemic.**

D. Gender and privacy

47. **During the course of his visit, the Special Rapporteur observed instances, especially in his discussions with representatives of sex workers, where gender could impact the way that privacy is experienced. The Special Rapporteur therefore respectfully draws the attention of the Government to his findings and recommendations for protecting against gender-based infringements of privacy, which he presented to the Human Rights Council in March 2020 (A/HRC/43/52). The principles outlined therein should be closely respected and implemented in any forthcoming reform of the United States' contribution to the debate about review and reform of its applicable data protection law(s), in the current case, the General Data Protection Regulation.**

E. Big data analytics, open data, children and privacy

48. **During an event supported by the United Nations Children's Fund (UNICEF) in Paris in April 2017, the Special Rapporteur appreciated the genuine concern of civil society with the privacy of children. In some instances, advanced technologies, including big data analytical techniques, had been deployed and/or contemplated. The Special Rapporteur therefore respectfully draws the attention of the Government to his findings and recommendations on big data and open data (A/73/438), which he presented to the General Assembly in October 2018, and his recommendations on gender and privacy (A/HRC/43/52), as well as his findings and recommendations to the Human Rights Council on children's privacy (A/HRC/46/37).**

[36] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.pdf.

[37] See www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

F. Harmonizing federal and state legislation, policy and practice

49. **Given the increasing availability and affordability of a range of privacy-intrusive technologies, coordinated and harmonized action to set minimum standards at state level across all 50 states in the United States would seem to be highly recommendable. There is huge reliance on the ordinary courts to issue wiretap orders at state level and some non-governmental organizations claim that those courts and wiretap orders are not subjected to sufficient scrutiny. While oversight of surveillance by federal agencies at all levels grows tighter and tighter, that of law enforcement agencies at state level does not seem to benefit from an even and harmonized approach that would in practice better protect the privacy of citizens faced with an array of technologies, including closed-circuit television, face and gait recognition and smartphone application malware.**

G. The United States' role on the international stage

50. **There may be no legal obligations under international law for the United States to take a leadership role in privacy matters or to set an example, but the world would be a better place for it.**

51. **The Special Rapporteur respectfully submits that privacy on the Internet is impossible with a unilateralist approach. No one single country can impose and/or enforce privacy safeguards and remedies across the Internet without the collaboration of several other countries. In other words, in the Internet age, both privacy and security on the Internet require real multilateralism. The United States helped establish the noble principles and backed much of the work of the United Nations through multilateralism. The United States now has the opportunity to revert to form and again lead through a renewed focus on principled multilateralism.**

52. **If the United States were to accept and adopt the Special Rapporteur's other recommendations on surveillance alone (see A/HRC/37/62), then it is respectfully submitted that it would regain the international credibility required to provide much-needed leadership in devising and securing a multilateral consensus on privacy and security on the Internet. That should be built on the United Nations-endorsed principles of necessity and proportionality for any measures which interfere with privacy. It is true that that may not prevent the Internet from continuing to break up into "splinternets", roughly divided into those where human rights are respected and those where they are not. The United States may not be powerful enough to prevent that from happening, but it should certainly be among that growing group of countries effectively working together to create and enforce the right privacy safeguards and remedies on the Internet. The Special Rapporteur is confident that the United States is uniquely positioned to prove to the world that it is perfectly possible to achieve security while explicitly respecting the principles of necessity and proportionality as basic tests for the protection of privacy universally.**

53. **If the United States were to go beyond reform of surveillance law and gradually also reform the Privacy Act of 1974 into something more closely resembling the California Consumer Privacy Act, then the way would be open to joining the world's largest privacy and data protection law club. The Special Rapporteur strongly recommends that the Government follow up reform of United States laws on surveillance with reform of the Privacy Act of 1974 and then ratification without delay of Convention 108+.**[38]

54. **The Special Rapporteur strongly encourages the Government to take a leading role in seeking the widest possible international consensus on matters regarding**

[38] Convention for the protection of individuals with regard to the processing of personal data as modernised by the Amending Protocol Council of Europe Treaty Series 223. Available at https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

privacy, especially the safeguards and remedies which should be applicable in the case of government-led surveillance. He notes with satisfaction the participation of the United States in the workings of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cybersecurity in the Context of International Security and reminds the United States that the Group provides an opportunity for it to demonstrate leadership by inserting privacy safeguards into the considerations of that and other United Nations working groups dealing with cyberspace.

55. **The Special Rapporteur invites the Government to follow the lead of the Governments of the United Kingdom (2019), Malta (2018), Belgium, Luxembourg and the Netherlands (2017) and Romania (2016) in supporting the United States Congress to host a special session of the International Intelligence Oversight Forum with a special focus on bulk processing and those instances where targeting and trend/new threat detection may be properly considered in an open dialogue with the intelligence community.**

56. **The Special Rapporteur notes the letter dated 4 October 2019 co-signed by the United States Attorney General, William Barr, and the United States Acting Secretary of Homeland Security, Kevin McAleenan, requesting Facebook not to proceed with its plan to implement end-to-end encryption across its messaging services without "including a means for lawful access to the content of communications to protect our citizens".**[39] **The Special Rapporteur notes that that request is in line with Attorney General Barr's position on encryption, as indicated in his speech of July 2019.**[40] **The Special Rapporteur strongly recommends that the Government of the United States reconsider its position on encryption in the spirit of the Special Rapporteur's multiple pronouncements on the subject since 2016. He also directs the attention of the Government to the paper published on 22 October 2019 by one of its former senior officials encouraging it to rethink its position on encryption.**[41] **The Special Rapporteur shares most of the views expressed in that paper, which are in turn very much in line with the identification of risks outlined in the paper published by the Government of the Netherlands on 4 January 2016.**[42] **The Special Rapporteur additionally contends that there may also be certain technical means which, without weakening end-to-end encryption, may be used to mitigate some of the more serious risks to public safety and national security arising out of the use of encryption.**

57. **The Special Rapporteur sees the United States as being especially well-positioned to take a leadership role in building bridges with Europe and other democratic countries around the world in matters concerning privacy and surveillance.**

---

[39] See www.nextgov.com/media/gbc/docs/pdfs_edit/open_letter_to_mark_zuckerberg.pdf.

[40] See www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber.

[41] Jim Baker, "Rethinking encryption", Lawfare, 22 October 2019.

[42] See www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption.