联 合 国 A/HRC/37/62

大 会

Distr.: General
25 October 2018
Chinese
Original: English

人权理事会
第三十七届会议
2018 年 2 月 26 日至 3 月 23 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

隐私权问题特别报告员的报告* **

秘书处的说明

隐私权问题特别报告员在依照人权理事会第 28/16 号决议编写的报告当中重点介绍了自己就任头三年开展的工作，尤其是围绕监控与隐私问题开展的工作，并对特别程序任务负责人的作用和任务进行了反思。

* 本报告迟交，以反映最新信息。

** 附件不译，原文照发。

隐私权问题特别报告员的报告

目录

页次

一. 导言 3

二. 特别报告员的任务 4

A. 特别报告员的活动(2015-2017 年) 4

B. 特别报告员在安全、监控与隐私这一重点领域内开展的工作 18

C. 特别报告员个别致函的资格 22

三. 结论 22

四. 向人权理事会提出的建议 23

五. 辅助文件导引 23

附件

Paper presented at the Expert workshop on the right to privacy in the digital age 25

一. 导言

1. 隐私权问题特别报告员的任务始于 2015 年 8 月 1 日。根据人权理事会第 28/16 号决议，特别报告员向理事会和大会进行年度汇报。[1]

2. 本报告是特别报告员向理事会提交的第三份报告，因而是首任即现任隐私权问题特别报告员任务中的最后一份报告。正因如此，借此机会回顾过去三年，概括介绍活动和成就，由此引出所汲取的一些经验教训，并对当前和未来的任务进行审视，这是妥当的做法。

3. 带着上述目标，本报告由四个部分组成。继导言之后，逐一围绕本任务的八个领域介绍特别报告员的活动、成就及今后的工作。在本报告第三部分，特别报告员概括介绍就本任务的主要重点领域之一，即隐私保护与政府监控及其他形式监控所开展的成功工作。特别报告员介绍了一项有关监控问题的国际法律文书草案，以及一系列待审议的建议。在报告第四部分，即最后部分，特别报告员谈到本任务的条件，以及条件当中需要澄清和进一步充实的内容。

4. 自本任务开始以来，除隐私权被载入国际文书[2] 和区域文书[3] 以及其他人权文书[4] 并得到保护外，隐私的重要性也被理事会重申，尤其是在第 34/7 号决议当中。理事会在该决议当中确认隐私权可促进个人享有其他权利，自由发展个人的个性和身份特征，培养个人参与政治、经济、社会和文化生活的能力。理事会在该决议中还关切地注意到，侵犯或践踏隐私权可能影响个人享有其他人权，包括自由发表意见和持有主张不受干涉的权利，以及和平集会和结社自由的权利。这与特别报告员 2016 年向理事会提交的报告(A/HRC/31/64)当中对个性问题采取的处理方针是一致的。

5. 特别报告员在工作当中不仅遵循有关隐私权的国际法律框架，而且奉行理事会定期就该议题通过的各项决议，包括上文提到的决议。

[1] 见 www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx。

[2] 见：《世界人权宣言》，第十二条；《公民权利和政治权利国际公约》，第十七条；《儿童权利公约》，第十六条；《保护所有移徙工人及其家庭成员权利国际公约》，第 14 条。另见：www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx。

[3] 见《保护人权与基本自由公约》，第 8 条；《美洲人权公约》，第 11 条。另见：www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx。

[4] 举例来说，见：《开罗伊斯兰人权宣言》，第 18 条；《阿拉伯人权宪章》，第 16 和第 21 条；非洲人权和民族权委员会的《非洲表达自由原则宣言》；《非洲儿童权利与福利宪章》，第 10 条；《东南亚国家联盟人权宣言》，第 21 条；《亚太经济合作组织隐私框架》；欧洲委员会《关于在自动处理个人数据方面保护个人的公约》；《<关于在自动处理个人数据方面保护个人的公约>有关监管当局和跨境数据流动的附加议定书》；欧洲委员会部长理事会关于保护因特网上的隐私的第 R(99)5 号建议；欧洲议会和欧盟理事会 1995 年 10 月 24 日关于在处理个人数据方面保护个人以及此类数据的自由传输问题的第 95/46/EC 号指令。

二. 特别报告员的任务

6. 一般来说，特别报告员所开展的活动不止涉及其任务的一个领域，因此相关事项系在几个任务领域之下汇报。特别报告员的任务见附件 1, 可在网上查阅(见第五部分)。

A. 特别报告员的活动(2015-2017 年)

1. 收集相关信息并研究问题

7. 本任务开篇第一段指出，特别报告员应收集相关信息、研究隐私权所涉问题，并就隐私权的促进和保护问题，包括就新技术带来的挑战提出建议。

8. 为达到上述第一项目标，特别报告员建立了五个专题行动系列。为了对相关问题进行研究，除其他手段外，特别报告员利用正式国别访问、磋商活动、与非政府组织的接触、围绕隐私问题举行的公共辩论、国际会议以及诸如亚太隐私问题主管部门论坛年度“隐私意识周”等推广活动，并对提请其关注的问题和提出指称的信函进行了审查。

专题行动系列

9. 特别报告员于 2016 年在向理事会和大会提交的报告当中概述了他的工作计划。他邀请所有利益攸关方参与拟予编写的专题报告，并要求开展磋商活动。所有的磋商活动均与五大专题行动系列有关。

10. 五大专题行动系列是：加深对隐私的理解；安全与监控；大数据和开放数据；健康数据；企业对个人数据的使用。上述专题行动系列均针对数字时代隐私所面临的挑战，彼此相互关连，一环套一环，从而使每个工作队均可在其他组工作的基础上开展工作。举例来说，大数据和开放数据工作队为有关健康数据以及企业对个人数据的使用问题的专题行动系列设置了场景。每个工作队均由一名主席负责协调。工作队主席在自愿的基础上，通过收集研究结果和信息、发现问题以及尽可能广泛地开展磋商活动，向特别报告员提供协助。

(a) 安全与监控

11. 为了确定针对因特网监测提供保障的最佳做法，特别报告员创建了“国际情报监督论坛”。该论坛是在各自国家负责国内外情报监督工作的国家机构和议会委员会的一场年度聚会，充当着一个在国际上分享信息、交流经验和确定最佳做法的平台。

12. 该论坛取得了完全的成功。组委会成员中定期注入新鲜血液。2016 年，在罗马尼亚议会四个监督委员会的支持下，该论坛在布加勒斯特举办。论坛迎来了 20 个国家 26 家机构派出的 60 多位代表。2017 年，在比利时、卢森堡和荷兰数据保护主管部门的支持下，该论坛在比利时议会举办。来自 30 个国家的 80 位代表出席了论坛。2018 年，该论坛计划于秋季在葡萄牙举办。几个国家的监督主管部门越来越多地主动承担起论坛进程的工作，努力找出作为集体国际关注事项的情报监督中的问题和对策，应答一种隐性存在的需求，即争取使对于隐私保护具有重要意义的最佳做法得到采用。

13. 正是隐私与国家安全利益和网络监控之间存在的交叉，使特别报告员的任务在 2013 年 6 月以来一直在持续的爱德华·斯诺登揭露事件后，于 2015 年应运而生。特别报告员同意关于从国际安全角度看信息和电信领域的发展政府专家组主席的意见，后者 2017 年 10 月谈到一项有关在信息和通信技术(信通技术)领域提高人们对国际和平与安全、人权以及发展之间联系的认识的建议，指出，在针对将信通技术用于恐怖主义目的和其他犯罪目的实施打击方面分享经验教训和实践方法，包括就国家之间以及国家与私营部门之间的合作分享经验教训和实践方法，以防范和制止恐怖主义和极端主义团体将信通技术用于招募人员和煽动暴力以及用于其活动的筹资、计划和准备时，以及在确定哪些领域可能需要开展更多工作时，各国应当考虑到本国对人权和基本自由的承诺以及尊重和保护人权和基本自由的问题。政府专家组提出了多项建议，以支持实施其 2015 年报告(A/70/174)当中就负责任的国家行为提出的自愿、非约束性规范，其中一条是：各国在确保安全使用信通技术方面，应遵守关于促进、保护和享有因特网上的人权理事会第 20/8 和 26/13 号决议，以及关于数字时代的隐私权问题的大会第 68/167 和 69/166 号决议，以保证充分尊重人权，包括表达自由权。政府专家组强调，通过信通技术存储、传输或处理的个人数据，有可能对生活和安全产生深远的影响。各国应采取妥善举措保护个人数据，包括保护个人数据的保密性、完整性、访问便利性以及真实性，与此同时遵守相关的国际法律人权文书。

14. 特别报告员注意到政府专家组未能就最后报告达成一致意见，因此认为现在比以往任何时候都更有必要在其任务涉及到采用信息和通信技术处理个人数据的国际一级所有行为体之间实现协同增效。

15. 特别报告员一贯认为，网络和平取决于各国在安全利益与网络空间隐私之间实现协同增效的意愿和能力。为了避免网络战争，还必须考虑旨在对网络空间中的监控以及其他对隐私造成侵犯的措施加以限制的举措。作为为探讨此类备选措施付出的部分努力，特别报告员协同欧洲联盟赞助下的“隐私、产权和因特网治理替代管理方案”项目，[5] 探讨了起草一项有关监控与隐私问题的法律文书草案，以加强相关标准并创建保护机制，从而解决全世界范围内个人隐私权遭大规模侵犯问题的备选方案。

16. 在联合国内讨论和通过一项有关监控与隐私问题的法律文书，可通过为各国提供以下内容，同时实现两个主要目标：

(a) 一系列体现和贯彻国际人权法最高标准，尤其是在监控问题上体现和贯彻隐私权的原则和示范性规定，以供纳入各国的法律法规；

(b) 若干以国际最佳做法为基础，旨在于安全利益和监控关切与保护隐私权之间取得平衡的备选方案。

[5] 在“国际情报监督论坛”和其他活动(例如有关隐私、个性和信息流动的活动)上，特别报告员得到了马耳他大学和格罗宁根大学提供的后勤支持，以及通过与欧洲联盟赞助下的“隐私、产权和因特网治理替代管理方案”项目的联合活动提供的后勤支持。自 2014 年以来，特别报告员一直担任“替代管理方案”项目的科学问题总协调人。该项目针对的是因特网治理、隐私以及知识产权问题，于 2018 年 2 月正式结束。在该项目中，特别报告员还亲自负责因特网治理与因特网上的隐私专题。该专题由德国汉诺威莱布尼兹大学法律信息学研究所开发。

17. 一项某种形式的文书是必要的，无论是以建议形式推出的软法，甚或是以国际多边条约形式推出的硬法——鉴于当前国家一级推行的做法，硬法更为妥当。特别报告员迄今的工作非常成功。考虑到其中涉及的挑战，尤其如此。但是，条件尚不够成熟，无法使特别报告员向人权理事会保证该文书已得到各国的一致支持，甚至无法使特别报告员向人权理事会保证该文书已得到多数国家的支持。尽管迫切需要这样一项法律文书，但还是有必要顾及时机问题。

(b) 大数据——开放数据

18. 特别报告员于 2017 年 10 月作为一项确定主要问题的介绍性研究报告，向大会提交了关于大数据和开放数据的报告(A/72/540)。初步建议触及以下方面：

(a) 治理、监管、研究以及与民间社会组织的磋商；

(b) 基于国际标准和原则对使用个人信息施加的限制，包括个人信息的豁免类别；

(c) 强有力的执行机制；

(d) 需要对数据隐私保护情况进行严格、公开和科学的分析，包括评估对隐私造成的影响；

(e) 政府和企业积极支持创造和使用增强隐私的技术。

19. 磋商工作正在进行，已要求于 2018 年 4 月 28 日前提交材料，并计划于 2018 年 7 月举办一场公共磋商活动。正在开展的工作将触及以下问题：

(a) 大数据背景下提供指导和保护隐私的原则；

(b) 就报告以及大数据给隐私带来的挑战开展磋商；

(c) 促进“去识别化”方面的研究；

(d) 应对“去识别化”未能成功的情况。

(c) 健康数据

20. 特别报告员的健康数据工作队正在美国德克萨斯大学戴尔医学院副教授 Steve Steffensen 博士带领下对问题进行审视。计划于 2018 年举办一场磋商活动。最大的可能性是在美国举办。

21. 邀请所有感兴趣的行为体、各国以及包括非政府组织在内的其他利益攸关方为制定最佳做法相关指导原则建言献策。

(d) 企业对个人数据的使用

22. 一些企业，包括规模最大的企业在内，日益依赖于压榨式利用(收集、处理、转用和出售)个人信息，往往未能确保足够的透明度，也未能确保取得相关个人的知情同意。[6] 特别报告员 2017 年 6 月对美国进行正式国别访问期间，就一些企业如何应对政府就其掌握的个人数据所提出的要求的方式向其进行了游

[6] 见 www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf。

说。对于此类要求的关切促使特别报告员于 2017 年 12 月向美国最高法院提交了一份“法庭之友”材料。[7]

23. 整个 2017 年间，特别报告员还与若干美国企业举行了会晤，讨论后者商业模式当中使用个人数据的问题。这样的对话协助企业对个人数据的使用问题工作队于 2018 年正式开始工作。

(e) 隐私与个性

24. 人权理事会承认隐私权是民主社会的一项基本权利。[8] 由 Elizabeth Coombs (澳大利亚)主持的隐私与个性工作队通过磋商活动、所收到的来文以及仔细研究现有文献，对此进行了探讨。为了增进对数字时代隐私问题的理解，特别报告员一直在就隐私、个性以及信息流动等主题举办区域磋商活动。第一次区域磋商活动(西方国家)于 2016 年 7 月在纽约举办。第二次区域磋商活动(中东和北非国家)于 2017 年 5 月在突尼斯举办。第三次(亚洲)于 2017 年 9 月在中国香港举办。第四次(拉丁美洲)计划于 2018 年 5 月举办。

25. 此外，特别报告员还开展了以下工作：

(a) 对里程碑性质的裁定进行仔细研究，例如印度最高法院 2017 年在 K.S. Puttaswamy 法官(已退休)及另一人诉印度联邦及其他方一案中作出的裁定。最高法院在该项判决中指出：“隐私是个人神圣不可侵犯性的终极体现。隐私是一种宪法价值，贯穿于基本权利范畴，保护个人享有一片作出选择和自主自决的范围”；[9]

(b) 报告隐私权遭剥夺给个人及其自身发展造成的影响；

(c) 侧重于以性别为基础进行分析，并重点着眼于社会当中的弱势群体，对网络暴力问题进行审视；[10]

(d) 探讨隐私对于个人的充分发展以及对于个人所生活并为之作出贡献的社会所具有的重要意义。

正式国别访问

26. 正式国别访问的日期和时机安排系与相关成员国商定。选择哪些国家在很大程度上基于与隐私有关的动态。

[7] 美利坚合众国诉微软公司，案件号 17-2，2017 年 12 月 13 日提交。见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf。

[8] 人权理事会第 34/7 号决议。

[9] 见 http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf。

[10] Hadeel al-Alosi, “Cyber-violence: digital abuse in the context of domestic violence”, University of New South Wales Law Journal, vol. 40 (4), pp. 1573–1603。

27. 2016 至 2018 年间提出的正式国别访问要求如下：

国家	提出要求的日期
中国	2016 年 3 月 31 日
大韩民国	2016 年 3 月 31 日
南非	2016 年 3 月 31 日
美利坚合众国	2016 年 9 月 20 日
德国	2016 年 10 月 21 日
印度	2016 年 10 月 21 日
联合王国	2016 年 10 月 21 日
法国	2016 年 11 月 29 日
阿根廷	2017 年 12 月 20 日
乌拉圭	2018 年 1 月 8 日

28. 进行国别访问方面出现的延误，一般是因为相关政府对访问要求迟答复或不答复，或是因为形势使特别报告员不宜按照先前的计划如期访问。访问是特别报告员对隐私权进行监测职责一个不可或缺的组成部分。因此，会晤日程安排包括：

(a) 官方主管部门，例如情报部门、执法和监管/监督主管部门，以及负责此类主管部门的部长；

(b) 民间社会以及其他利益攸关方的代表，包括活动人士、记者、学者及其他人士。

29. 会晤议程一般包括：

(a) 宪法、法律和制度框架；

(b) 大数据、监控、隐私面临的威胁、特别报告员的五大专题行动系列，以及情报监督机制评估；

(c) 专家和民间社会组织向特别报告员表达的关切。

非正式国别访问

30. 特别报告员出于出席国际会议等其他目的访问各国，并收集可用于其专题行动系列的信息。举例来说，在 2016 年向大会汇报之前的五个月内，特别报告员参与了在 11 个国家举办的多项活动。这 11 个国家形形色色、相距遥远，包括澳大利亚、奥地利、丹麦、法国、德国、意大利、拉脱维亚、荷兰、新西兰、瑞士和美国。参与上述活动确定了对于促进隐私具有重要意义的领域，例如保护儿童的隐私、隐私的结构性和机构性安排以及数据监管部门，等等。

磋商

31. 特别报告员接触了非洲、美洲(北美洲、中美洲和南美洲)、亚洲、大洋洲和欧洲的民间社会、政府、执法部门、情报部门、数据保护主管部门、情报监督主管部门、学术界、企业以及其他利益攸关方。仅 2016 年和 2017 年，特别报告员

就为参与 26 个活动而前往了 30 多个不同城市，其中一些位于亚洲、北部非洲和中美洲，四分之一位于美国，超过一半位于欧洲。

为促进和保护隐私权起草建议，其中涵盖新技术带来的挑战

32. 特别报告员在上文概述的活动当中收集的信息有助于他为提交人权理事会和大会的报告编写建议。

成就

33. 迄今为止提交的专题报告如下：

- 对政府监控活动进行更注重隐私的监督基本方针，人权理事会，2017 年 3 月(A/HRC/34/60)；
- 安全与监控，人权理事会，2017 年 3 月(A/HRC/31/64)；
- 大数据和开放数据工作队中期报告，大会，2017 年 10 月(A/72/540)；
- 因特网治理领域内有关政府监控问题的国际法律文书的一些初步备选方案，人权理事会，2018 年 3 月(见本报告以及可在网上查阅的本报告附录 7)。

专题行动系列方面不断取得的进展

34. 特别报告员起草了大数据问题指导意见，已于 2017 年 10 月提交大会，现正在磋商当中。特别报告员还针对所发现的问题，起草了监控与隐私问题国际法律文书草案。

35. 特别报告员还举办了磋商活动，例如 2017 年的“隐私、个性与信息流动大会：隐私作为一项全球人权的亚洲视角”。

36. 健康数据问题工作队已在特别报告员指导之下开始工作。

37. 特别报告员为企业对个人数据的使用问题工作队集结了支持，并就微软一案向美国最高法院提交了相关的“法庭之友”简评。

正式国别访问

38. 特别报告员已进行了两次正式国别访问，一次是访问美国(2017 年 6 月)，[11] 另一次是访问法国(2017 年 11 月)。[12] 相关报告将于 2019 年 3 月提交人权理事会，以容许有更多时间与相关国家的政府进行后续交流。

磋商

39. 磋商活动提高了各不同司法管辖区、不同层级以及社会不同阶层对隐私相关问题的认识，其中包括爱尔兰公民自由委员会、日本公民自由联盟、日本律师

[11] 见 end-of-mission statement: www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx。

[12] 初步结论见：www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F。

协会联合会和北爱尔兰人权委员会组织的活动，还包括在因特网监督论坛和“权会(RightsCon)”等平台组织的多项活动。

未来的活动和机遇

40. 若人权理事会延长特别报告员的任务，特别报告员计划提交以下报告：

(a) 向人权理事会提交：

(一) “对政府监控活动进行有效监督方面所吸取的有助于改进保障措施和补救措施的经验教训”，2019 年 3 月；

(二) “政府监控、执法以及个人信息跨界流动方面的适度性、必要性和法律：现有法律保障措施和补救措施的有效性及改进问题”，2020 年 3 月；

(三) “对政府监控活动进行有效监督方面的进展、倒退以及其他方面”，2021 年 3 月。

(b) 向大会提交：

(一) “改进隐私和健康数据的相关保障措施和补救措施”，2018 年 10 月；

(二) “利润与隐私：个人数据货币化的商业模式与企业的责任”，2019 年 10 月；

(三) “隐私、个性与信息流动：首次从时间、地点和空间角度对具有普遍性的隐私权进行全球概述”，2020 年 10 月；

(四) “个人信息在企业、执法与监控之间的跨界流动”，2021 年 10 月。

41. 在时间和资源允许的情况下，特别报告员还可能就与隐私权有关的其他问题提交报告：大数据和开放数据；健康数据；企业对个人信息的使用；儿童和年轻人的隐私；解决监控活动中隐私面临的固有挑战的策略；采用以性别为基础的方针处理隐私权问题；大数据未能实现“去识别化”等隐私泄露情况的应对之策；特别报告员收到的投诉；正式国别访问；正在与一些国家讨论的问题(公共领域信函)；数字时代的隐私问题。

42. 特别报告员接下来计划进行的正式访问是访问大不列颠及北爱尔兰联合王国(2018 年 6 月)和德国(2018 年秋)。

43. 特别报告员将继续就隐私权问题与国家机关、个人和组织磋商。2018 年的主要活动包括：1 月 19 日和 20 日在罗马召开的“隐私、产权和因特网治理替代管理方案大会”；计划于 5 月举办的拉丁美洲隐私、个性与信息流动相关活动；监控数据工作队的磋商活动；拟于 7 月在澳大利亚举办的大数据和开放数据相关磋商活动。

2. 搜集、接收和应对信息

磋商

44. 特别报告员与以下各方交流了信息：多个不同国家政府的官员、部委和机构(国家和国家以下一级)；数据保护与隐私专员；欧洲联盟“第 29 条工作组”[13]主席；欧洲委员会《关于在自动处理个人数据方面保护个人的公约》磋商委员会主席；国际电信联盟以及电机和电子工程师学会等确立标准的组织；民间社会组织；常驻联合国日内瓦办事处和日内瓦其他国际组织代表团；其他特别程序任务负责人、联合国人权事务高级专员办事处(人权高专办)官员；研究人员、学者和专业团体。特别报告员广泛参与各类大会和民间社会会议并作主旨发言。

45. 特别报告员与数据保护与隐私专员们进行了尤其富有成效的接触。数据保护与隐私专员是特别报告员任务当中的一个核心组成群体。在 2015 年召开的数据保护与隐私专员国际会议上，特别报告员就其“10 点计划”征求了各位专员的反馈意见。在 2016 年召开的会议上，特别报告员报告了上述计划的进展情况。在 2017 年于中国香港召开的会议上，特别报告员致辞并参与了几场并行举办的活动，还举办了他的第三次“隐私、个性与信息流动”活动，以对会议起到补充作用。

函件

46. 特别报告员收到各种不同来源的函件。不过，只有通过人权高专办官方登记系统收到的函件才会登记并被计入统计，使特别报告员难以汇报所收到函件的总量。尽管如此，自本任务开始以来，人权高专办已替特别报告员登记了以下函件。

47. 2015-2017 年间登记的函件：[14]

2015 年	2016 年	2017 年	总量
不详	3	47	50

48. 未按国别或议题对所收到的信件进行分列。不过，2017 年收到的多数函件系来自常驻代表团、非政府组织和国际组织。[15] 特别报告员官方电子邮件地址(srprivacy@ohchr.org)所收到的数以百计，有可能是数以千计的其他邮件未计入上述数字。

成就

49. 2015 年 10 月数据保护与隐私专员国际会议通过了一项关于与特别报告员合作的决议。[16]

[13] 根据第 95/46/EC 号指令第 29 条建立的数据保护工作组。

[14] 不包括发往 srprivacy@ohchr.org 的电子邮件。

[15] 人权高专办的建议，2017 年 12 月 19 日。

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

50. 特别报告员与其他任务负责人就埃及、海地、洪都拉斯、墨西哥和西班牙的情况联合发出了函件。

51. 特别报告员发现并应对了新兴问题、有关隐私泄露的指称，以及诸如人脸识别软件等有可能以技术为基础对隐私造成的侵犯。

未来的活动和机遇

52. 特别报告员将以下列内容为重点，继续开展他的活动：与所有利益攸关方接触(尤其是就安全与监控相关问题，包括信息系统的网络安全问题)；在民间社会组织及其他利益攸关方的建言献策之下，就新兴问题起草指导材料和建议；就数字时代隐私权面临的日益加剧且多种多样的风险，提供技术援助；就保护人权问题与其他特别程序任务负责人协作。

3. 发现阻碍、推广原则并提交建议

隐私面临的阻碍

53. 特别报告员最重要的举措之一是在安全与监控领域，与推动人权理事会创立特别报告员任务的核心问题正相符。保护监控之下的隐私权方面所面临的阻碍包括，目前在国家一级和全球一级均没有或缺少可确保对监控进行独立、可靠和有效控制的详细的规则、实用的程序和适当的监管机制。附件当中可查阅隐私保护方面所发现差距的概括介绍。

54. 就大数据而言，用以识别个人的信息不再需要是“个人信息”。[17] 只需有“引向”某一个人及其联系人的信息，技术能力和数据分析即可对隐私造成威胁。

55. 各专题行动系列确定保护和促进隐私权方面当前所面临的阻碍，例如：健康领域以技术为基础对隐私造成侵犯；智能手机进入证人席；网络暴力；社群间各有区别的脆弱之处；深植于算法当中的性别偏见及其他偏见；政府获取私营部门数据；人脸识别以及其他技术工具。

应对阻碍—— 促进隐私

56. 在监控专题上，特别报告员已着手推行一项战略，以就如何针对全球的监控活动加强国际法律框架和创建妥善监督机制建立共识。

57. 特别报告员应时下关注的隐私问题、正式国别访问以及需要与其他任务负责人联合应对的问题发出了正式函文(见附录 3)。

推广原则和最佳做法

58. 除其他外，特别报告员为印度政府、联合王国政府以及澳大利亚议会[18] 就法律草案举行的公共磋商活动提供了意见建议。特别报告员还致函表达自己的关

[17] Graham Greenleaf, “Data protection: a necessary part of India’s fundamental inalienable right of privacy — submission on the White Paper of the Committee of Experts on a Data Protection Framework for India”, University of New South Wales Law Research Paper No. 6, January 2018. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810。

[18] 就《国家安全法修正案(间谍和外国干涉)法案(2017 年)》函询澳大利亚议会情报与安全联合委员会，2018 年 1 月 24 日。

切，其中一些信函仍未解密，[19] 另一些信函已经公开，例如致日本政府和墨西哥政府的信函。

向人权理事会提出的提案和建议

59. 特别报告员有关大数据和开放数据的建议载于本报告附录 4。

60. 特别报告员继对美国进行正式访问后提出的初步建议涵盖：出于国家安全目的进行监控的问题(隐私与公民自由监督委员会成员问题，以及 2008 年的《1978 年外国情报监控法修正案法》第 702 条)；城市环境中的智能监控，以及出于执法目的进行的监控；第 12333 号行政命令所涵盖的情况；企业掌握的个人数据；将 1996 年《健康保险流通与责任法案》的保护范围扩大到所有健康数据；性工作者的身份管理；简化隐私问题；在国家一级支持有利于隐私的举措。在监控问题上，特别报告员建议，联系隐私相关保障和补救，停止在美国公民和居民与既非公民又非居民者之间的任何区别对待，并建议国会采取行动推出新法律，规定大规模监控在民主社会中既不适当又不必要。

61. 特别报告员在向人权理事会提交的年度报告当中，还就安全与监控问题提出了其他建议。

成就

62. 特别报告员在向大会和人权理事会提交的年度报告(2015 年至 2017 年间)以及有关成员国侵犯隐私权的函文当中，报告了新出现的阻碍。

63. 特别报告员通过以下手段应对上述阻碍：向各国政府进行宣传，以便解决有可能侵犯隐私权的举措和方案；就各专题行动系列创建工作队；在技术公司中间推广“从设计着手保护隐私”；就政府主导的监控问题起草法律文书草案(见第二部分)；开展公共磋商；参与国际活动；发表论文。

64. 特别报告员提交了下列提案和建议，其中一些上文已概括介绍：“10 点行动计划”，2015 年；本任务的工作重点(专题行动系列)，2016 年；对美国的正式访问结束之际的总结报告当中提出的初步建议，2017 年；就政府主导的监控活动提出的初步建议(A/HRC/34/60)；就大数据和开放数据提出的初步建议，2017 年(A/72/540)。

未来的活动和机遇

65. 特别报告员将于 2019 年 3 月提交他对美国正式访问的最后报告。该报告将以第 12333 号行政命令所适用情况中的现有监督机制为重点。特别报告员对法国正式访问的报告需于 2019 年 3 月提交。

66. 特别报告员关于隐私与健康数据的报告将于 2018 年 10 月提交大会。

67. 继 2018 年年中开展的国际磋商后，将发布特别报告员关于大数据和开放数据的最终提案和建议。

[19] 在 60 日的答复期限到期前保密。

4. 为国际活动作出贡献，以推动采取系统、连贯的方针处理隐私权问题

活动

68. 特别报告员曾在很多活动中发言，包括作为主旨发言人发言，从而触及了主要利益攸关方并引发了广泛的媒体报道。

69. 本任务负责人一项正在持续的战略性贡献是与数据保护与隐私专员国际会议之间的合作。2018 年 2 月 19 日和 20 日，特别报告员在数据时代的隐私权问题专家研讨会上为人权高专办启动并主持了一场会议。将向人权理事会第三十九届会议提交该研讨会的报告(根据理事会第 34/7 号决议)。

70. 特别报告员正在落实“10 点行动计划”。该行动计划曾于 2016 年 3 月提交人权理事会，其中包含(见 A/HRC/31/64,第 45 至第 55 段)：

(a) 就数字时代保护隐私权的问题开展研究与磋商，着重强调有必要加大对儿童和年轻人隐私权的保护力度，并着重强调隐私与性别相关问题；

(b) 提高认识工作，例如隐私问题主管部门论坛的“隐私意识周”，以及针对社群成员、监管人员以及公共和私营部门组织开展的其他活动；

(c) 就安全与监控中的隐私问题开展结构性对话，包括与非政府组织、数据保护与隐私专员、执法机构以及安全与情报部门对话；

(d) 采取综合方法处理法律、程序以及行动中的保障和补救问题。例如，上文提到的法律文书草案和“法庭之友”简评；

(e) 2017 年 10 月与大会讨论过的技术保障问题，以及正在以促进有效的技术保障为目的与技术界进行的接触；

(f) 上文概括介绍的与企业界进行的对话；

(g) 促进国家一级和区域一级在隐私保护机制方面的发展。特别报告员强调国家一级和区域一级在隐私保护机制方面的发展在全球一级具有的价值。[20] 与全世界隐私和数据保护主管部门的接触为上述促进工作提供了便利；

(h) 与民间社会合作。特别报告员在上任的头六个月内会晤了 40 个非政府组织，并继续通过以下途径与其接触：专题工作队的工作；会议；公共活动，例如有关隐私、个性和信息流动的公共活动；

(i) 网络空间、网络隐私、网络间谍、网络战、网络和平：正如有关安全与监控的专题行动系列工作所表明的那样，上述问题经常会成为特别报告员报告的主要内容。同样具有相关意义的是针对较弱势者的网络暴力，包括借助数字设备得以实施的家庭暴力、未经同意传播亲密影像，也包括幼童隐私所面临的风险；

(j) 推动制定国际法。上文提到，鉴于有望给国际法带来的影响，特别报告员于 2017 年 12 月与哈佛法学院的“网络法律诊所”协作，就微软一案向美国最高法院提交了“法庭之友”简评(见附录 6)。2017 年 8 月 24 日，印度最高法院就具有重要意义的宪法相关案件 K.S. Puttaswamy 法官(已退休)及另一人诉印度联

[20] 举例来说，澳大利亚新南威尔士州 2015 年的《数据共享(政府部门)法》。该法规定，数据共享须符合隐私相关法律法规的规定。

邦及其他方一案下达裁定，一致判定隐私在印度是一项受宪法保护的权利。这一里程碑性质的案件有可能带来从宪法上质疑印度其他影响性别问题的法律。[21] 特别报告员将对此进行密切的监测。

成就

71. 特别报告员：自 2015 年以来，为了促进对隐私权的保护，发表了 100 多次讲话(见附录 5)；就隐私与个性问题开通了博客(www.privacyandpersonality.org)；向美国最高法院提交了“法庭之友”简评；就联合王国政府就 2016 年《调查权力法》提出的咨询提供反馈，并就欧洲联盟法院的裁决提出应对提议；针对澳大利亚议会就信息和通信技术的发展对执法机构的影响提出的问询提供了材料，并就《国家安全法修正案(间谍和外国干涉)法案(2017 年)》提出问询；就数据保护框架白皮书向印度政府提出意见建议；与哈佛法学院“网络法律诊所”协作。

未来的活动和机遇

72. 特别报告员将继续为隐私、个性与信息流动相关会议等国际活动作出贡献、组织此类国际活动，并对有关隐私与个性(包括性别相关问题)的里程碑性质的法庭裁定进行仔细研究。

5. 就隐私权(包括相关挑战和切实补救措施)提高认识

73. 特别报告员继续着眼于数字时代面临的特定挑战，就促进和保护隐私权的重要性提高人们的认识。特别报告员还继续就按照国际人权义务向隐私权遭侵犯的个人提供获得切实补救的机会所具有的重要意义，提高人们的认识。

74. 2016 年年中，随着据称已进行“去识别化”处理的健康与药品福利使用情况数据库被公开发布，某成员国每 10 位公民中就有 1 位的隐私被置于风险之下。据查，相关从业人员和患者有可能被重新识别出来。特别报告员两次致函相关成员国。函件保密 60 天。该项事宜与本任务有关大数据和开放数据以及有关健康数据的专题行动系列密切相关。

75. 2017 年 5 月 18 日，特别报告员采取了非同寻常的举措，在人权高专办网站上发布了一封致日本政府的公开的指称函。[22] 特别报告员现正在等待日本政府发出邀请，以便就国际人权法的标准问题展开讨论。

76. 2017 年 7 月 19 日，特别报告员与其他特别程序任务负责人一道，联合向墨西哥政府发出呼吁，要求对方针对有关人权维护者、社会活动人士和记者遭到监视和非法监控的指称展开透明、独立和公正的调查。[23]

77. 特别报告员就隐私遭严重侵犯的某位个人得不到补救的问题致函某成员国。该函件发布在特别程序的来文报告当中。[24]

[21] 见 https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/。

[22] 见 www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf。

[23] 见 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=E。

[24] 见 www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx。

成就

78. 特别报告员一直在提请各国注意处理隐私方面所明显存在的不足之处，并确保适当的隐私相关问题属于公共领域。

未来的活动和机遇

79. 特别报告员将争取为提出隐私遭侵犯指称的申诉人获得与国际义务相符的补救，并继续与成员国和非政府组织合作，发现在国内无法获得补救的申诉人并赋予其发声的机会。

6. 纳入性别视角

活动

80. 将隐私本身构想为一项必不可少的权利，从而使自由地、不受阻碍地发展个性这一包罗万象的基本权利得以实现，这是特别报告员隐私、个性与信息流动专题工作背后的驱动力量。该项举措随着 2016 年 7 月在纽约举办的一项活动而启动。来自五个大洲的 90 个专家、监管人员、企业和民间社会组织出席了该活动。

81. 第二个此类磋商活动系在国家数据保护主管部门的支持下，于 2017 年 5 月 25 日和 26 日在突尼斯针对中东和北非区域举办。该活动迎来了来自阿尔及利亚、埃及、黎巴嫩、摩洛哥、阿拉伯叙利亚共和国、突尼斯和卡塔尔的大约 70 位与会人员。一项具有重要意义的贡献是那场专门讨论性别观的会议。该会议让与会人员对妇女的特定经历有了深入的了解。

82. 第三个磋商活动系在数据保护与隐私专员国际会议期间，于 2017 年 9 月 29 日和 30 日在中国香港与以下各方合作举办的：荷兰格罗宁根大学安全、技术与电子隐私研究小组；马耳他大学信息政策与治理系；“隐私、产权和因特网治理替代管理方案”项目。“数字亚洲中心”、香港大学以及中国香港隐私问题专员是当地的合作伙伴和承办方。该活动重点关注亚洲的动态和趋势，包含几场分别专门讨论以下内容的会议：亚洲在隐私方面的传统；亚洲的监控与隐私；亚洲的隐私及其与其他人权之间的关系；亚洲的性别与隐私。

83. 第四个此类磋商活动计划于 2018 年第一季度举办。活动中将召开一场或多场专门讨论性别问题的会议。

84. 向一个成员国提出了一个令人严重关切的问题。该国的法律制度未能为一位妇女充分提供补救。在一次妇科检查过程中，该妇女的生殖器官被一名保健工作者在未经许可的情况下，出于非专业目的用个人电话拍了照。这一侵犯隐私行为的影响是严重的，造成了情绪、经济以及家庭方面的压力。

85. 另一个问题涉及到的情况是，在与性别认同有关的事宜中，表面看上去合法的法庭诉讼材料送达程序似乎在隐私方面产生了意料之外、差别不同的后果。特别报告员现正对所提出的关切进行审视。

86. 特别报告员正式访问美国期间，一名性工作者就将卖淫定为犯罪对性工作者隐私权造成的影响提出了问题。执法官员在性工作者相关案件中的监控规则似乎可能有待修订。[25]

87. 2017 年与其他任务负责人联合向一些国家发出的几份函件涉及到性别相关问题[26] 以及第 34/7 号决议的目标和宗旨。人权理事会在该决议中指出，隐私使个人得以发展自己的个性。

88. 特别报告员将对继印度最高法院在 K.S. Puttaswamy 法官(已退休)及另一人诉印度联邦及其他方一案中作出裁定后出现的案件进行密切的监测。该案的裁定认定性取向是隐私的一项基本属性。

89. 特别报告员很想对失去隐私的影响进行审视。相关提案已经起草，但资源尚未确定。

成就

90. 特别报告员在各专题行动系列中就隐私与性别问题进行了磋商，在围绕隐私、个性与信息流动举办的三次磋商活动中就隐私权的性别相关内容组织了会议，推动了利益攸关方就隐私权的性别相关内容交流信息，并向成员国提出了某些问题。

未来的活动和机遇

91. 拟于 2018 年第一季度就隐私、个性与信息流动举办的第四次磋商活动将包含一场有关隐私权的性别相关内容的会议。特别报告员将继续如上文所述对法庭裁定进行分析，并就性别与隐私权开展研究。

7. 报告据称发生的侵权情事，包括新技术带来的挑战

92. 特别报告员继续报告据称发生的侵犯隐私权情事，包括继续报告新技术带来的挑战，并提请人权理事会和联合国人权事务高级专员注意特别严重的令人关切问题的现状。

活动

93. 特别报告员上文讲述的有关健康情境中严重丧失隐私一事在此处也具有相关意义，因为该事件涉及到有必要为此类案件提供补救的问题。[27] 与相关国家的讨论在继续。

[25] 见访问结束之际的总结报告：www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx。

[26] 与其他任务负责人联合向海地政府(2017 年 9 月 22 日)、西班牙政府(2017 年 10 月 12 日)和埃及政府(2017 年 10 月 31 日)发出的函文。

[27] 过去十年间，该国的各种法律改革委员会已在八个不同场合建议提供一种补救，即就严重侵犯隐私行为出台法定诉讼理由。

成就

94. 特别报告员继续提请相关成员国注意有关隐私权遭侵犯的指称。特别报告员还在人权理事会内提高了对《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条遭违反情事的认识。

未来的活动和机遇

95. 特别报告员将继续报告隐私权据称遭到侵犯的情事，并与成员国合作解决令人严重关切的问题。

8. 向人权理事会和大会提交年度报告

96. 特别报告员依照其任务，向人权理事会和大会提交年度报告。

提交人权理事会的年度报告

97. 本报告系提交人权理事会的 2018 年度报告。本报告概述了特别报告员自 2015 年以来开展的活动，介绍了就保护隐私权以及政府监控问题开展的卓有成效的工作，并对人权理事会赋予的任务进行了分析。

98. 此前向理事会提交的两份报告的内容，上文已进行了概括介绍。

提交大会的年度报告

99. 特别报告员在 2017 年提交大会的年度报告当中提供了各专题行动系列的进展报告，并就大数据和开放数据提交了中期报告。特别报告员启动了拟予开展的磋商进程，并提及了一起公开发布的经“去识别化”处理的健康数据被发现易于被重新识别的事件。正在向相关国家提出这一问题。

100. 此前向大会提交的两份报告的内容，上文已进行了概括介绍。

未来的活动和机遇

101. 特别报告员将继续提交年度报告，概括介绍所开展的活动和新出现的问题，并将继续如期提交各专题行动系列工作队的报告。

B. 特别报告员在安全、监控与隐私这一重点领域内开展的工作

102. 正如人权高专办所指出的那样，近年来隐私权越来越引起大会和各项人权机制的关注，尤其是在世界各地很多国家的政府所推行的监控政策和做法问题上。大会于 2013 年通过了第 68/167 号决议，其中对监控和拦截通信可能给人权造成的不利影响深表关切。大会确认人们在线下享有的权利在线上也必须得到保护，并呼吁所有国家尊重和保护数字通信中的隐私权。即便存在国家监督机制，这种机制也往往效果不彰，有的是因为未能确保适当的透明度，也有的是因为未能确保对国家监控通信、拦截通信和收集个人数据的做法实行问责。[28]

[28] 见 www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf。

103. 比利时、法国、德国和联合王国发生的恐袭事件在国家一级、有时在国际一级引发的处理方法是：优先考虑反应型的高调安全对策，而非经仔细斟酌的既虑及安全利益又虑及保护公民隐私之责的对策。谨稍举几例，2016 年至 2017 年间，比利时、德国、荷兰、法国和联合王国推出了有效性、适度性和覆盖范围迥异的法律。没有一项有关国家监控的法律完全符合并尊重隐私权方面的国际标准。

104. 爱德华·斯诺登的揭露制造了某种势头，但尽管如此，仍鲜有国家很愿意讨论隐私与监控议题。不过，民间社会、学术界以及其他利益攸关方，包括越来越多国家的政府在内，已表示真有兴趣就隐私与监控问题开展妥善的、建设性的、国际性的讨论。

105. 特别报告员力求对上述各种不同行为体所表达的关切作出反应，并通过召集各种供交流和讨论的论坛来弥合各种行为体之间的分歧。这与特别报告员在提交人权理事会的第一份年度报告和随后提交大会的报告当中所提供的行动计划是一致的。为了避免重复劳动，特别报告员与成员国、欧洲联盟赞助下的“隐私、产权和因特网治理替代管理方案”项目以及民间社会组织协作处理监控当中的主要隐私问题。

1. 通往有关监控与隐私的国际法律文书的途径

106. 研究工作以及与公共政策领导人、执法界、情报界和民间社会组织进行的讨论显示，避免形成监控社会的解决方案的一个重要组成部分是一项在国家和国际法律中都可以用的标准。

107. 特别报告员铭记人权理事会和大会在隐私权方面持有的关切，与“替代管理方案”项目合作举办了利益攸关方磋商活动。磋商活动始于 2015 年的华盛顿特区。于 2016 年在马耳他和纽约举办了研讨会。在一份文件当中记录了与会人员的想法、立场和建议。该文件以一份非常粗糙的法律文书草案形式呈现，可用于广泛的目的，不管是作为指导原则也好，还是作为国家监控法的范本也好，甚或是作为诸如有关监控问题的多边国际条约等硬法也好。

108. 在“国际情报监督论坛”内获得的支持鼓舞下，特别报告员和“替代管理方案”项目进一步就国际法中新的法律措施举办了联合磋商活动──上述国际法中新的法律措施旨在应日益增多的监控行为而增进对隐私的保护，与此同时也为在全球范围对监控做法进行切实监督提供一个共同基础。

2. 由专家组予以完善

109. 继 2017 年 2 月在美国迈阿密与“隐私、产权和因特网治理替代管理方案”项目第 4 组一揽子工作下的“因特网治理与监控工作组”召开联合会议后，于 2017 年 3 月推出了修订草案。

110. 缔结法律文书的想法获得了积极的反响，在此鼓舞下，特别报告员和“替代管理方案”项目 2017 年间在全世界范围内开展了广泛的磋商。一个由来自民间社会、“替代管理方案”项目以及大的因特网公司的专家组成的工作组 2017 年 5 月在马耳他、2017 年 9 月在巴黎就法律文书草案和监控问题召开了研讨会，约有 50 位专家与会。 在巴黎举办活动后，随即于 2017 年 9 月 15 日在法国里昂的国际刑事警察组织(国际刑警组织)总部与执法从业人员进行了磋商。

111. 2017 年 11 月 20 日和 21 日在布鲁塞尔举办的国际情报监督论坛上，分发了巴黎和里昂会议的成果以及法律文书的修订草案。这使情报监督主管部门和情报从业人员得以就法律文书草案、设立国际仲裁小组这一想法以及数据访问方面的国际保证发表评论意见。

112. 通过上述磋商活动和其他举措，形成了一份足够成熟的文本，可供于 2018 年间进行更广泛的公开磋商。于 2018 年 1 月在网上发布了法律文书草案，当时适逢 2018 年 1 月 17 日至 19 日在罗马举办的第一次公开讨论活动。

113. 有关政府主导的监控活动与隐私问题的法律文书现有草案包含一般原则及其基本要求，涵盖适用、范围、权利、系统和数据、多方利益攸关方协作以及跨境访问个人数据的机制(见本报告附录 7)。

3. 因特网治理领域内缔结政府监控问题国际法律文书的初步备选方案

114. 毋庸置疑，国际社会亟待采取紧急行动，通过就网络空间的隐私与监控问题制定一套明确、全面的法律框架，在国家一级和国家之间落实对隐私权的尊重，从而切实遵守和执行《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条。国际人权法提供了较高层面的隐私权保护普遍性规则，但其细致程度不够，无法形成在若干适用的情境中(包括国家监控和域外监控情境)提供充分保护所必不可少的全面法律框架。世界多数区域缺少诸如欧洲和北美洲过去 40 年间所创建的那种强制执行机制。由此可见，大幅度增强细致性、明确性和全面性，并针对网络空间日常发生的侵犯隐私权情事大幅度增加保障措施和补救措施，将对国际法律框架有所裨益。“魔鬼就在细节当中”。

115. 很多人对法律文书草案的愿景和全面性表示赞赏。重要的利益攸关方鼓励继续对之加以完善。特别报告员与“替代管理方案”项目近期(2018 年 1 月 18 日至 19 日)在罗马联合组织的磋商活动提出了若干重要的考虑意见：

(a) 迄今所做的工作发现了一些问题，也确定了网络空间监控方面可用的标准和可行的补救措施，应作为一个工具公开发布，以推动就该主题进行思考和展开讨论，并为目前正在考虑出台旨在确保对情报活动进行切实监督的法律法规和制度安排的成员国提供一个草案范本；

(b) 现有草案涵盖了数量广泛的问题。保留草案的现有形式具有战略上和战术上的优势，但将草案缩减成两项或两项以上范围更有限、篇幅更短小的文书，可能有助于使其获得通过；

(c) 需就使文书广为接受并具有可持续性所需的短期和较长期时间范围制定战略；

(d) 对联合国系统内过去制定法律文书的情况进行的审视显示：

(一) 就法律文书建立国际共识是一个漫长的过程；

(二) 个体成员国、区域集团以及跨区域联盟均可在通过法律文书方面发挥关键作用；

(三) 民间社会组织在推动通过国际法律文书方面有着至关重要的作用；

(四) 即便是最值得称道的倡议最初也面临着阻力。

(e) 无论特别报告员开展哪些工作，“隐私、产权和因特网治理替代管理方案”项目均将于 2018 年 4 月 30 日前独立于特别报告员的工作之外将现有法律文书作为其“因特网治理政策简报和路线图”的部分内容提交欧洲联盟委员会，并最终将其提交欧洲议会和欧盟理事会。欧洲联盟有可能是最适合最终在全球层面支持监控与隐私问题法律文书的区域群组；

(f) 初步讨论显示，拉丁美洲和非洲有可能对法律文书草案具有更浓厚的兴趣，但这一点尚待进一步探讨和发展；

(g) 参与连续开展的磋商活动的利益攸关方所提供的反馈显示：

(一) 欧洲刑警组织和国际刑警组织等区域和全球执法界已对法律文书草案的诸多条款表现出浓厚的兴趣，尽管它们也表示，在其圈子内进一步开展细致的磋商还需要大量时间(二到三年)；

(二) 律师协会联盟以及为活动人士的隐私相关案件进行辩护的律师强烈支持法律文书草案，包括支持所提议的机制，例如数据访问方面的国际保证机制；

(三) 企业界表示对该法律文书草案具有浓厚兴趣，尤其是在该草案体现“改革政府监控”联盟所公开支持的原则情况下；[29]

(四) 情报界表示，有些国家具备先进的法律法规，其内容有 90%与现有的法律文书草案相符。还需就定向监控的定义和大面积监控的限定适用范围开展更多工作，以使草案条文更实用、更适当；

(五) 民间社会的关切集中在该进程的时机、一些国家利用这个文本淡化保护的可能性以及具体措辞等问题上；

(六) 欧洲区域正在等待欧洲联盟法院和欧洲人权法院的某些案件出结果。预计上述结果将于 2018 年底或 2019 年出炉。上述结果有可能增强欧洲各群组对法律文书草案的兴趣，但这些以及其他考量因素目前正阻碍着达成共识的进程。这种情况在 2019 年或 2021 年前可能不会缓解。

4. 专门针对监控问题的建议

116. 人权理事会应审议附录 7 的内容，以便发现问题，并确定最终有望考虑纳入将来缔结的隐私与监控问题国际法律文书的一些解决方案。

117. 有兴趣对照附录 7 所列内容出台实质性增强补救措施和解决方案的法律文书的成员国应与特别报告员联系，以便进一步探讨在国家、区域和国际各级推进这些原则的备选方案。

118. 鉴于上文所概述的时机方面的考量，特别报告员提议，若妥当且及时的话，于 2021 年 3 月向人权理事会汇报并提出更多建议。

[29] 见 www.reformgovernmentsurveillance.com。

C. 特别报告员个别致函的资格

119. 戴维·魏斯布罗特讲述了第一位专题特别报告员(即决处决或任意处决问题特别报告员)在某个案件中呼吁一个国家注意时的经历。相关国家的政府对该特别报告员函件的答复是质疑他发出此种呼吁的资格。[30]

120. 即决处决或任意处决问题特别报告员致函人权委员会，表示该问题值得进一步审视，而他将感谢委员会可能就此提供的任何指导。[31] 在那件事上，人权委员会不仅在随后的年度届会上延长了即决处决或任意处决问题特别报告员的任务，而且可以看到，正如挪威代表所表述的那样，人权委员会得出结论认为，此类案件属特别报告员任务范围内，应纳入今后的报告(挪威是相关决议的主要提案国)。[32]

121. 本特别报告员也有同样的感觉，因为在 2017 年间，他就一些问题提请成员国注意的资格曾在两个不同情况中遭到质疑。向成员国和其他利益攸关方发函是所有特别程序任务负责人核心活动的一个固有组成部分。这一有着详实记录可考且规范完善的程序使所有任务负责人得以通过信函(包括紧急呼吁和指称函)等手段，直接就其任务范围内的侵犯人权指称向各国政府及其他利益攸关方进行干预。[33]

122. 特别报告员就未经授权拍照一事(见上文第 84 段)进行干预的决定符合设立本任务的人权理事会决议。该决议明确要求各国及时对特别报告员的紧急呼吁及其他函件作出答复。

三. 结论

123. 特别报告员在促进和保护隐私方面采用了其他特别报告员通常利用的手段，包括向相关国家发出紧急呼吁和指称函、就个人申诉采取后续行动、出席会议以及进行正式或非正式的国别访问。

124. 特别报告员还开发了几种创新手段来履行自己的任务，包括：年度“国际情报监督论坛”；一年两度就隐私、个性与信息流动举办的区域活动(已在北美洲、中东和北非以及亚洲举办，接下来将在拉丁美洲举办)；有关大数据和开放数据、健康数据以及隐私与个性的专题行动系列工作队，以针对围绕隐私的诸多问题提供一种更为广泛的全球性的处理方法。

125. 特别报告员认识到监控是隐私权享有方面面临的一个严重威胁，共同主导了国际上为起草一项旨在对网络空间的监控行为进行规范的内容全面的国际法律框架而付出的努力，从而也向前推进了网络和平的前景。

---

[30] David Weissbrodt, “The three ‘Theme’ Special Rapporteurs of the UN Commission on Human Rights”, *American Journal of International Law*, vol. 80, No. 3 (July 1986), pp. 685–699。

[31] E/CN.4/1986/21，第 100 页。

[32] 经济及社会理事会第 1986/36 号决议。

[33] 人权理事会特别程序，见 www.ohchr.org/EN/HRBodies/SP/Pages/Welcomepage.aspx。

126. 特别程序构成人权理事会落实人权规范和制定标准的一项重要机制。[34] 进一步就采用政府主导的监控制定国际标准，将使国际社会得以对此类技术和做法的运用进行指导和评估。在“国际情报监督论坛”上对良好做法和最佳做法的标准进行定期审查。

127. 特别报告员认为，对网络空间监控行为进行规范的法律文书对现行网络法律中的欧洲委员会《网络犯罪公约》等其他文书起到补充作用，可针对因特网上的隐私提供具体的保障(A/HRC/34/60 和 A/72/540)，与此同时也可以解决网络空间的司法管辖权等长期存在的问题。迄今开展的工作非常成功，非常令人鼓舞，但法律文书的实际形式和内容获得的支持依然不够一致，无法建议人权理事会立即对现有文件进行审议。不过，随着不断的努力，随着时间的推进，可在较近的将来(例如，可能甚至是 2021 年前)将这样一份可行的文书提交理事会。

128. 特别程序任务负责人是独立专家，也是保护人权的一项重要机制。各成员国必须完全接受其函件和问询并与之合作，停止质疑其建设性批评的合法性。

四. 向人权理事会提出的建议

129. 人权理事会应注意到：特别报告员通过各专题行动系列，在本任务各个方面所取得的成就；上述成就与特别报告员提交理事会的第一份报告当中所载计划的一致性；下一步举措，包括针对儿童隐私问题增设一个专题的提议；未来专题行动系列报告的提交时间表。

130. 理事会应注意到：就政府主导的监控制定国际标准方面取得的进展；创造性地成功创立了“国际情报监督论坛”；有意在中期之内起草一项可供联合国审议，以便最终可能由会员国以及其他相关利益攸关方予以完善的文书。

131. 理事会应建议大会：在坚定不移地努力就因特网制定一项更为全面的法律框架过程中，协同隐私问题特别报告员，为旨在探讨网络空间的隐私与安全和国家行为的交集点的所有联合国努力注入新的活力。

五. 辅助文件导引

132. 鉴于篇幅有限，下列文件发布在特别报告员的网站上：

- 附录 1: 隐私权问题特别报告员的任务

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix1.docx

- 附录 2: 格雷厄姆·格林利夫，“数据隐私法 2017:120 个国家的数据隐私法，包括印度尼西亚和土耳其”

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix2.docx

[34] Weissbrodt，“The three ‘Theme’ Special Rapporteurs”。

- 附录 3: 隐私权问题特别报告员的函件

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix3.docx

- 附录 4: 大数据和开放数据专题行动系列工作队的中期报告和初步建议

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix4.docx

- 附录 5: 为 2015-2017 年间的国际事件作出的贡献

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix5.docx

- 附录 6: 在美国政府诉微软公司一事中向美国最高法院提交的“法庭之友”材料

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix6.pdf

- 附录 7: 关于政府主导的监控活动的法律文书草案

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix7.docx

- 附录 8: 鸣谢

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReport Appendix8.docx

Annex

Paper presented at Expert workshop on the right to privacy in the digital age

Office of the High Commissioner for Human Rights

Geneva, 19–20 February 2018

1. Privacy is a fundamental human right recognized as such under international law. It is also a universal right, one which should be enjoyed everywhere by everybody, as such it should be respected everywhere by everybody, by States as well as by non-State actors, irrespective of the ethnicity, nationality, gender, religious, philosophical or political beliefs of any given individual or any other status. The recognition of the universal right to privacy is part of the set of fundamental norms established in the development of human rights law since World War II.

2. Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. These contexts may be as diverse as medical and health, insurance, statistics, national security, finance, police, social security, education and many others. Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context and an identification of safeguards that protect it, and remedies available to citizens which may be specific to that context. The devil, literally, is in the detail, and privacy requires very detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular context as well as the remedies that a citizen may resort to if his or her privacy is breached in that context. The importance of this level of detail is even greater in the case of privacy since there exists no universally accepted definition of privacy. In other words, people across the world have agreed that the right to privacy exists and that everybody is entitled to such a right but they have not spelt out precisely what the right is or what it entitles a person to in a wide variety of circumstances. This fact has both advantages and disadvantages: too narrow a definition of privacy would restrict its ability to be protected as circumstances and privacy-threats change and also as we develop our understanding of what constitutes privacy-infringing behaviour in a number of changing or new contexts.

3. The rules and remedies provided for at national law come together with those established under international law to constitute the international legal framework available for the protection of privacy. Those at the national level are most often to be found in an amalgam of principal and subsidiary legislation complemented by the case law of that particular country. The courts of all countries and especially those with constitutional competences interpret the extent — and occasionally the limits — of the right to privacy in accordance with their understanding of that country's constitution, the national law on privacy — if it exists — as well as, often enough, the precepts of international law on the subject. Very importantly, over the past forty years we have witnessed a huge growth in the impact of international law on national law in the sphere of privacy protection. We have seen the concerted development of international law at the regional level, most notably in Europe, which has then guided the development of national law and practices in diverse contexts where privacy may be threatened.

4. Moreover, privacy is not an absolute right. It is a qualified right. There exist a small number of very special occasions when limitations to the right to privacy may be introduced subject to a number of special measures which are normally best spelt out under international law as well as necessarily having a clear legal basis in domestic law. Some of these will be explored below in the context of security. The way that the right to privacy is qualified needs to be spelt out in great detail in a given context. If limitations to the right to privacy are not adequately defined the gaps in privacy protection will increase.

5. An additional but essential overall consideration is that constantly developing technologies pose important challenges for the protection of privacy: these technologies may reveal the most intimate behaviour, wishes, preferences and indeed the very thoughts of individuals in ways that previously were not possible. Smartphones, credit cards and the Internet are three good examples of the types of technology that bring significant new challenges to the protection of privacy.

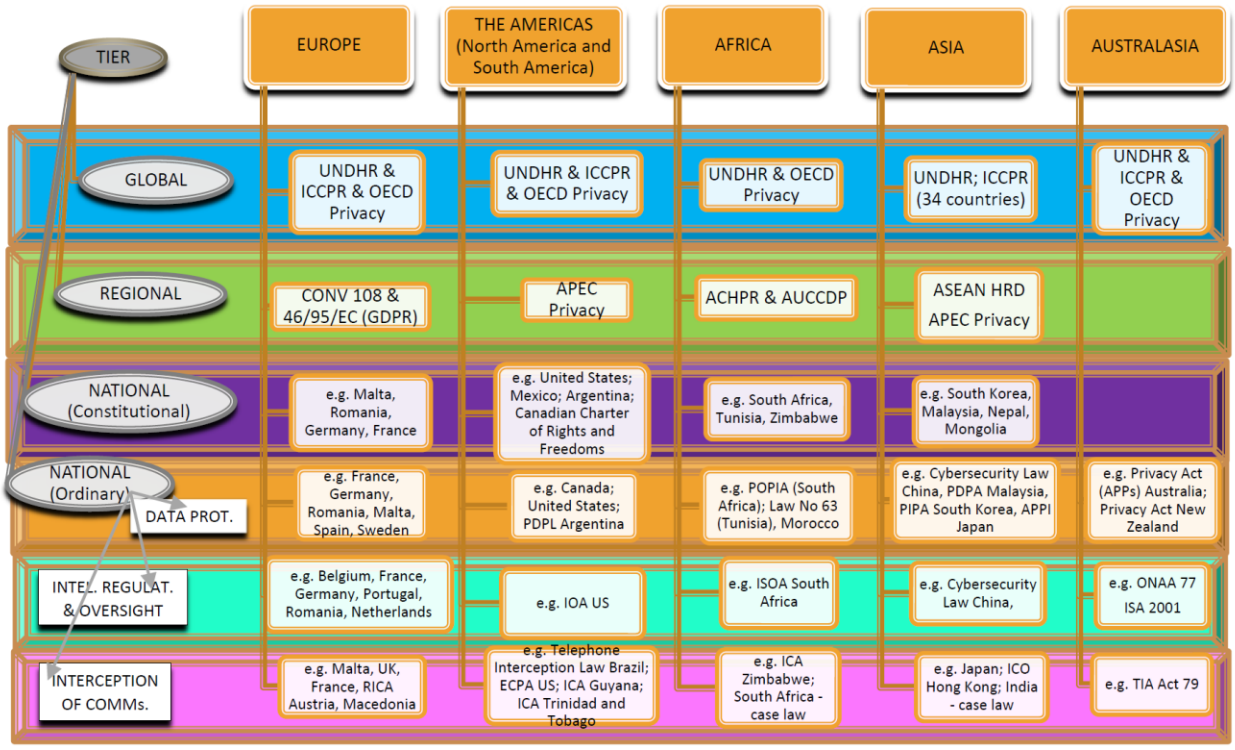
6. When dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that "whatever is protected off-line is protected on-line". That is a hopelessly inadequate approach to the protection of privacy in 2018. International law such as Art. 12 UDHR and Art 17 ICPPR only provides an answer to the question "Why?" as in "Why should we protect privacy" i.e. because we have agreed that it is a universal fundamental human right. They however do not provide answers to the questions: When? Which? What? How? Who? When should privacy be protected? How should privacy be protected? Which are the privacy-relevant safeguards to be created in a particular context? Which new contexts pose the greatest risks to privacy? What should be done to protect privacy in given circumstances? Which are the remedies most appropriate and possible in those cases where, despite all the safeguards provided, a breach of privacy still occurs? Who has special duties and obligations in the case of privacy protection, in which circumstances, what measures are the minimum to discharge these obligations and how should such persons be held accountable? The answers to these and other questions can only be found if the international and national legal framework is detailed enough.

7. Over the past fifty years some countries and some inter-governmental organizations have taken the initiative to develop their legal framework with respect to privacy but others have not. As a consequence, in 2018 more than a third of United Nations Member States have no privacy laws at all[1] while most of the other 125 states have laws which cover some of the contexts where privacy may be threatened but not all. Some important threats to privacy especially those arising in the context of national security, intelligence and surveillance are inadequately regulated in most countries of the world. International law, especially in the form of some regional initiatives, helps provide a level of co-ordinated response to some privacy threats for some countries but these remain, at best, a significant minority. The result is a patchwork quilt, in many places crocheted in stitches which are far too open to keep in the warmth and which, in any case, is not large enough to cover all of the bed. This patchwork quilt can in no way be characterized as a comprehensive and sufficiently detailed legal framework through which persons anywhere and everywhere can enjoy the universal right to privacy. It is the duty of the Special Rapporteur on the right to privacy, in conformity with his mandate, to identify the lack of a comprehensive, detailed and universal legal framework as a serious obstacle to the protection of the right to privacy world-wide. The rest of this paper, for reasons of time and space, mostly focuses on the lack of an adequate legal framework in two often-related contexts: national security and the prevention, detection, investigation and prosecution of crime but this is not to say that all other contexts are well served by the international legal framework.

The current international legal framework

8. The diagram below attempts to sketch out the international legal framework for the protection of privacy which exists so far:

[1] Though this does not exclude the possibility that their constitutional courts could be seized of privacy-related matters.



9. The diagram above is intended primarily to illustrate the tiered structure of the international legal framework but limitations of space do not permit one to clearly see that the tiers in Asia and Africa contain many more gaps and vacant spaces than those in Europe and North America. These gaps are however summarized in the overview text below.

Gaps in protection from government-led surveillance.

10. The surveillance of citizen behaviour on the internet can be broadly categorized into two main types: Government-led surveillance, and, surveillance or monitoring of citizens behaviour by private corporations that track citizens browsing, purchasing and other activities on the internet.

11. This overview analysis is focused on Government-led surveillance and the gaps in protection which currently exist in the international legal framework.

12. The surveillance and/or monitoring and/or profiling of citizens by corporations will be the subject of a separate report.

What do we understand by a comprehensive legal framework?

13. A comprehensive legal framework protecting citizens' privacy in cyberspace is one which provides both safeguards and remedies for all facets of the citizens' presence in cyberspace, irrespective of the fact if the threat to privacy comes from inside that citizen's country or from outside it.

14. Tension has continued to build up in cyberspace, with the privacy of many responsible citizens being put at risk by the behaviour of State actors in the form of cyber-surveillance, cyber-espionage and elements of cyber-war.

Problem Statement

15. In cyberspace, the citizen may be surveyed in both a domestic situation by his or her own Government, or else in a transboundary/transnational situation by a Government which is not his/her own. The case studies referenced below outline a fraction of some of the ways in which a citizen in one country finds him/herself subject to infringement of their privacy by their own Government or another State actor.

16. Where a citizen is subject to surveillance by his/her own Government then the safeguards and remedies must normally be sought within domestic law. Where a citizen is subject to surveillance by a State which is not his own, obligations of both the State conducting the surveillance and the State where that person is physically located are relevant; yet a remedy becomes harder to seek, because in practice most states accord the citizens of other States a lower level of protection than that accorded to their own citizens, in breach of the prohibition of discrimination found in articles 4, and 26 of the ICCPR.

17. For individuals not to suffer interferences in their right to privacy, they firstly need to benefit from safeguards which exist within domestic law, in other words, their Government should be subject to a whole set of regulatory procedures provided for by the law of that State, and which would include precautionary measures designed to ensure that surveillance cannot be initiated until or unless, it is proven to an independent and competent authority that this surveillance is legal, necessary and proportionate to objective pursued, "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UDHR, Art. 29(2).

Summary overview of protection gaps

18. In summary: the United Nations has 193 sovereign Member States and two non-member observer States, all of them capable of having their own independent systems/structures such as domestic legislation and data protection authorities.

19. More than 33 percent of United Nations Member States, i.e. over 70 countries, have no privacy law at all.

20. Out of the remaining 125 United Nations Member States which do have one form of privacy law or another, (for an outline of these states please see article by Professor Graham Greenleaf in Appendix Two attached) less than 65 have certain key fundamental characteristics such as a truly independent data protection authority or truly strict enforceable safeguards and remedies. Thus, these laws are not homogeneous and the level of protection of privacy differs quite widely from one country to the next.

21. The types of laws mentioned in Graham Greenleaf's article are mostly those intended to cover the use of personal data by companies or state departments outside the law enforcement and national security sector. Most of them are therefore not intended to adequately and comprehensively cover the use of surveillance by intelligence agencies.

22. More than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance.

23. 100 percent of existing State legislations concerning the oversight of domestic intelligence within United Nations Member States require amendment and reinforcement.

24. 75 percent of United Nations Member States have no system of detailed safeguards or remedies to which they can readily turn to for cases of surveillance upon their citizens by other states. Even where remedies for citizens exist within the courts of those States, these courts often lack jurisdiction over the surveillance behaviour of other State actors.

25. 25 percent of United Nations Member States — those within the European region encompassed by the Council of Europe, have agreed to a basic principle in the application of privacy law to state security: by agreeing to Article 9 of Convention 108 they have accepted that measures can only limit the right to privacy where these measures are provided for by law and are necessary and proportionate in a democratic society.

26. This however means that it is only the very highest principles that have been agreed to, even in European states with more developed legislation on the right to privacy and this is mostly applied in the case of domestic intelligence. The situation relating to foreign intelligence is much more fluid, elastic. What actually constitutes a necessary and proportionate measure in a democratic society then needs to be translated into very detailed legislation and this is still very much work-in-progress all across Europe. Belgium, the Netherlands and the United Kingdom are some of the European states currently reviewing

their legislation in order to improve compliance with basic principles in a detailed manner. France has done so in 2015 but intends to re-visit its legislative framework in the near future.

27. Even where legislation exists regarding the oversight of intelligence it is often largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases.

28. In the absence of more detailed regulation, several United Nations Member States have to rely on their existing legislative and judicial frameworks, often at the national constitutional or the regional level in order to develop remedies and safeguards on the hoof. This works slowly but relatively well at the European levels where the European Court of Justice and the European Court of Human Rights often have pan European reach with their judgments about surveillance and privacy.[2] This however is not a completely satisfactory solution since it is one ex post. Very preferably citizens wish to have their privacy protection provided ex ante and this, especially to protect themselves against or minimize intrusion. In order to resolve problems of jurisdiction in cyberspace, this can be only provided by detailed international law which does not yet exist in the surveillance sector, including in the European region. If the remedies are unclear and imperfect in Europe where the European Court of Human Rights has relatively worked well with over 100,000 cases decided since it was established in 1959, the situation outside Europe is even more concerning. In the Americas, the Inter-American Court of Justice established in 1979 has cross-country reach, as so has in in Africa the recently set-up (2006) African Court for Human and People's Rights. Both courts strive but struggle. The United States signed but never ratified the American Convention on Human Rights and, unlike the European human rights system, individual citizens of Member States of the Organization of American States cannot take their cases directly to the Inter-American Court, having to refer first to the Inter-American Commission on Human Rights. Likewise, only seven African states have signed the protocol empowering their regional court to receive petitions from non-governmental organizations and individuals. These limitations substantially weaken the reach of these regional courts. Moreover, in Asia or the Pacific there is no regional court to turn for infringements of privacy whether caused by domestic intelligence or foreign intelligence.

29. The United Nations Human Rights Committee plays a very important role in the protection of human rights, but once again is largely an ex post forum and cannot be expected to provide in-depth regulation and governance structures, which are the required minimum adequate legal response to questions like transborder data flows and cross-border espionage and surveillance.

[2] *The Snowden revelations – 6 June 2013 –ongoing reverberations across Europe*

The revelations over mass surveillance and other privacy –intrusive programmes carried out by the signals intelligence arms of the United Kingdom and United States intelligence communities have not really receded. They have been followed by legislative changes in both countries, sometimes imposing more constraints and safeguards, on other occasions legitimizing existing practices. The unilateral nature of transborder forays by United States and/or United Kingdom agencies into Belgium, Brazil, France, Germany and other countries led to a great deal of concern which still finds its reverberations in various fora, international and otherwise. Both countries are still struggling to find the right formula to frame their behaviour in cyberspace such that, for example, the legislative measures of the United Kingdom would be found necessary and proportionate by either the European Court of Human Rights or the European Court of Justice. The United Kingdom's intelligence services were found to be in default on several counts by the UK's own Investigatory Powers Tribunal while the United Kingdom law on bulk collection of metadata has been declared disproportionate by the European Court of Justice on the 21st December 2016. An important decision in this respect is also being expected in a case first heard by the European Court of Human Rights on 7th November 2017, Big Brother Watch and Others v. the United Kingdom (no. 58170/13), Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14) and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15).

30. In order to better understand the protection needs in the privacy area, one has to take the Yahoo cases[3] cited below and ask "which ex ante safeguards should have been applied by which country in order to protect citizens in, say France, from having their Yahoo e-mail account privacy infringed and what ex post remedies are available to that same French citizen?" The answers to these questions can only be provided by a detailed international law regime which has yet to be worked out. The Human Rights Committee's interpretative advice of ICCPR's article 17 should be a last resort; it cannot be the primary mechanism designed to protect the privacy of billions of people who use the Internet on a daily basis.

[3] The following two cases are being cited for purposes of illustrating a problem area but are not here being represented as facts proving certain types of behaviour by the United States or Russian authorities. The Special Rapporteur on the right to privacy reserves the right to investigate these cases separately through Letters of Allegation and until doing so remains neutral on the accuracy or otherwise of media and governmental reports on the subject:

Case 1: Privacy of 500 million Yahoo! users infringed – 15 March 2017

Formal indictments were brought in the United States of America by the Justice Department, which announced on 15 March 2017 that the "indictments of two Russian spies and two criminal hackers in connection with the heist of 500 million Yahoo user accounts in 2014, marking the first United States criminal cyber charges ever against Russian government officials. The indictments target two members of the Russian intelligence agency FSB, and two hackers hired by the Russians. The charges include hacking, wire fraud, trade secret theft and economic espionage, according to officials."

While this case remains sub judice and therefore the evidence available has not yet had time to be exhaustively evaluated by the court in question, the nationality of the accused and the locus of the judicial proceedings are almost immaterial for the purposes of this observation. The point here is that the spread of the damage was global, possibly the largest or one of the largest intrusions in history on the private e-mail accounts of five hundred million Yahoo! users spread across the planet. If it transpires that the men indicted were not responsible after all, we are still left with the problem of the nature and scale of the attack in addition to the instability induced by public accusations made against Russia. If the guilt of the accused is eventually proved beyond reasonable doubt then the problem would be compounded by the involvement of state officials who may or may not have been acting on instructions. Either way the suspicion of their acting as agents of the Russian state is already a destabilising factor in international relations and threatening all forms of peace, above and beyond cyber-peace. The violation of the personal space of hundreds of millions of internet users has not, to date, attracted much attention but it remains a source of major concern to those involved, over and above the charges actually made in the indictment.

Case 2: Privacy of 500 million (?) Yahoo! users breached by United States agency (reported 4th October 2016)

If you're a Yahoo! e-mail user, if it's not one government hacking into your e-mail account or scanning your incoming e-mail, then it's another. Or at least un-contradicted media reports so suggest. For some time during the period 2014–2016, hundreds of millions of Yahoo! e-mail users apparently not only suffered the most massive hack in history as already mentioned above (allegedly by a combination of Russian criminal and state-connected persons) but also had their incoming mail scan-read on the orders of a United States Government agency. There are multiple causes for concern here. Firstly, all those Yahoo! users within the United States may arguably claim that such searches violated their Fourth Amendment rights under the United States constitution, although the scan-reading was carried out in terms of lower-level United States law (FISA). Secondly, it should be clear to all concerned that well more than half of those five hundred million Yahoo users are not United States citizens and would need to seek recourse elsewhere for protection of their fundamental and universal right to privacy…but where to do so is the obvious question. Even if this were ever to be considered a proportional measure – and that is a contentious point in its own right, unless there were to be an international agreement that this would constitute appropriate state behaviour in cyberspace, hundreds of millions of citizens world-wide yet again find themselves without any effective safeguards or remedies when it comes to their fundamental right to privacy.

31. Thus it should be glaringly evident from the above summary that huge gaps exist in the legal protection of privacy at both the national and international levels. Unless and until it will be possible for any citizen, anywhere, irrespective of passport held, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that "a clear and comprehensive legal framework exists". In order to create such a clear and comprehensive legal framework it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles to establish what state behaviour in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when.