联 合 国 A/HRC/34/60

大 会

Distr.: General
6 September 2017
Chinese
Original: English

人权理事会
第三十四届会议
2017 年 2 月 27 日至 3 月 24 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根据人权理事会第 28/16 号决议编写的这份报告，从国家和国际视角着重审视了政府的监控活动。特别报告员详细阐述了国际法律框架的特点及其解释。他还介绍了最近的事态发展和趋势，并就如何研究这些发展和趋势，以及它们与享有隐私权和其他相互关联的人权如何相互作用等，作了叙述。因此，特别报告员概述了第一批更有利于隐私的监督政府的监控的方法。最后，特别报告员报告了他在本报告所述期内的活动。

* 本文件迟交是为了收入最新资料。

隐私权问题特别报告员的报告

目录

一. 导言

1. 根据人权理事会第 28/16 号决议，隐私权问题特别报告员每年向理事会和大会提出报告。本报告是他向理事会提交的第二份报告。特别报告员在上一份报告中概述了一项十点行动计划和一项战略，通过“专题行动流”活动来处理与其任务有关的当今某些关键问题。由于隐私权尤其受到数字时代发展的挑战，特别报告员希望，通过这些举措有助于提高实现尊重、保护和隐私权的水平。

2. 特别报告员最近发表了一份题为“筹划中的专题报告和协商呼吁”的声明，其中介绍了目前和今后报告中将要处理的问题，并列出了提交报告的时间表。[1] 该声明应被视为向所有愿意参与本授权任务的国家的所有利益攸关方发出长期邀请。任何人如愿意贡献见解，或以其他方式参与提到的任何举措，不妨与特别报告员或其团队联系，最好通过电子邮件(srprivacy@ohchr.org)联系，特别报告员本人或其团队将会尽快作出回应。

3. 如以上摘要所述，特别报告员在本报告中重点讨论采取更有利于隐私的方式监督政府监控的初步方法。他在任期内已经开展了一些涵盖该主题的活动，并将继续这样做。特别报告员为了完成上一份报告(A/HRC/31/64)中概述的，特别是监控领域的任务，投入了大量精力组织 2016 年 10 月 11 日至 12 日在布加勒斯特举行的国际情报监督论坛。与其共同主办的单位有：罗马尼亚议会参众两院监督国家情报局联合委员会，参众两院监督外交情报机构活动特别委员会和参众两议院涉及国防、治安和国家安全的各委员会；协作单位有：马耳他大学信息政策和治理系和荷兰格罗宁根大学安全、技术和电子隐私研究小组。这次活动就可以理解的有限目标而论，非常成功。[2] 因此，特别报告员打算继续每年共同主办这一论坛。2017 年，计划于 11 月 20 日至 21 日在布鲁塞尔举行这一论坛，该论坛将主要与比利时数据保护机构──隐私委员会共同主办。该论坛的目的是使特别报告员能够汲取世界各地建立的众多监督机构取得的实际经验和业务洞见，以利履行其职责。这将使特别报告员能够更好地理解和反思力图有效监督安全和情报部门的活动及其对隐私影响的现实情况。第一届论坛汇聚了来自 20 个国家 26 个机构近 70 名代表。其中包括独立监督机关、议会委员会、民间社会的一些成员，甚至还有一个监督法庭。特别报告员认为，对情报活动更为深思熟虑和资源更充足的监督，是诸多有助于改善全球隐私权保护的补充举措之一。有人认为这是保护隐私具体措施中最有希望的途径。这仍有待观察。希望这一系列年度论坛有助于查明和分享良好做法，最终有助于加强大批会员国的监督机制。还希望监督机制能够在详细而严格的国内法中具有坚实的基础，这些法律规定民主社会必要的相称措施，并在同一法律中规定恰当的保障措施。法律还应该通过资源充足和独立的主管监督机关，加强对执法机构和安全和情报部门的有效监督。特别报告员

[1] 该声明可查阅以下网站：www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx and www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/.

[2] 论坛的目标是，在一个值得信赖的框架内，就监督机制是否充分开展公开坦率的辩论；现有和预期的监控措施可能会对隐私产生的负面影响；有目标的监控和大规模监控的区别；这类措施与民主社会是否相称；以及这类措施的成本效益和总体效力。

希望根据年度论坛的讨论情况提出建议，针对新技术所带来的挑战，确保促进和保护隐私，以便完成其任务。

4. 关于监控，特别报告员不仅注重监督机制，而且还尽可能在全世界范围内侧重涉及监控使用或滥用的新的法律草案和报告。特别报告员还尽可能在全世界范围内监测有关使用或滥用监控的新的法律草案和报告。因此，在正式请求进行国别访问时，与监控有关的活动是其主要考虑之一。这一点特别体现在他对以下国家即将成行的访问挑选上：美国(2017 年 6 月 19 日至 24 日)，法国(请求从 2017 年 11 月 13 日至 17 日)，大不列颠及北爱尔兰联合王国(请求于 2017 年晚些时候，有可能从 12 月 11 日至 17 日)，德国(请求从 2018 年 1 月 29 日至 2 月 2 日)和大韩民国(请求从 2018 年 7 月 3 日至 15 日)。这些国家有强大的民主传统，特别报告员期望它们在确定监控与基本人权，特别是隐私领域的最佳做法和保障措施方面发挥带头作用。此外，过去几年，它们在监控领域，无论是在应用监控技术还是在新的立法方面，均特别活跃。特别报告员每次访问时，都要求会见情报机构和监督当局以及负责执法机构和安全和情报部门的部长们。

5. 此外，为了避免无效劳动，并以最大限度发挥协同作用为目标，特别报告员密切跟踪其他平行举措的进程和结果，例如欧盟支持的隐私、财产和互联网治理替代管理方案(MAPPING)，其目的在于对互联网最近在门类众多的经济、社会、法律和道德方面的发展及其对个人和整个社会的后果，形成某种全面“成熟”的理解。在人权理事会确立特别报告员的授权任务一年前，也是在他担任该职 18 个月之前，替代手段项目于 2014 年启动。它发起了利益攸关方内容丰富的讨论，其中包括创建一项对监控予以约束的国际法律文书。这类讨论将持续到 2018 年 2 月底。特别报告员打算跟踪这些讨论的结果，然后打算在 2018 年 3 月至 7 月期间，就这种国际法律文书的可取性和可行性表明立场。他可能会在 2018 年 10 月提交大会的报告中提出自己的立场，可能会再次提出相关的建议，针对新技术带来的挑战，确保促进和保护隐私，以具体履行其授权任务。

6. 特别报告员还与其他实体或个人进行了接触和合作，这些实体或个人正在采取主动行动，为国际协调的情报监督制定一个完整一致的框架。特别报告员过去 18 个月的紧张工作，已经在全球与热衷制定某种文书的权力机构建立了卓有成效的工作关系或改善了关系，此种文书将阐明外国信号情报职能行为的共同标准。这些都是值得欢迎的事态发展，但距离取得成果仍有距离，很可能难以在现任任务负责人任期内实现。然而，这是重要的第一步，特别报告员将继续竭尽全力促进和推动这类举措。

7. 特别报告员在本报告中有意重点关注政府的监控。对于其他领域的活动，他提到提交大会的第一份报告(A/71/368, 第 7 至 17 段)中概述和描述的专题行动流。必须强调的是，故意将安全和监控问题与企业掌握的个人资料和其他专题，如大数据和公开数据分开。后者在隐私权方面有本身的具体挑战和问题。目前正在分别处理这些问题，直至以“联合方式”汇集在一起之前先暂时这样，继续通过特别报告员设立的不同平行举措加以处理。出于这些原因，特别报告员在本报告中将重点关注代表某个国家或按照其命令进行的监控活动。

8. 与此同时，其他专题行动流的工作仍在继续，并将在适当时候予以介绍，希望能按照上文第 2 段所述的时间表进行。特别是大数据和公开数据工作组正在编写第一份报告，并在 2017 年 7 月的一次协商会议上讨论。协商的结果预计将成

为 2017 年特别报告给大会的年度报告的主要重点。此外，继 2016 年 7 月在纽约举行的关于隐私、人格和信息流通这一主题的研讨会取得成功之后，特别报告员已经开始筹备第二次研讨会，其重点是中东和北非。计划于 2017 年 5 月 22-23 日在突尼斯举行，由特别报告员和突尼斯数据保护机构与民间社会组织密切合作共同主办。第三次研讨会也开始筹备，重点特别关注亚洲。计划于 2017 年 9 月 29-30 日在中国香港举行。如果任何政府、民间组织、公司、数据保护机构、学术机构或个人有兴趣参与或支持这些举措，应与特别报告员尽快联系。[3]

9. 特别报告员借此机会赞扬法国、德国、大韩民国、联合王国和美国政府即时积极答应他进行正式国家访问的请求，也对其他一些国家缺乏回应表示惋惜。令人遗憾，这恰恰是一些国家司空见惯的现实，但有必要及时提醒公众注意政府抵制接受国家访问的请求。特别报告员不希望点明某些政府，但对他的请求予以回应或缺乏回应，有助于将那些空谈人权的政府与那些愿意以公正态度参与改善隐私保护的政府区分开来。

10. 在谈到本报告的主要重点之前，特别报告员认为有必要紧急关注一些国家令人担忧的做法，即利用隐私法扼杀新闻调查。这可以通过以下情况加以说明：据称，隐私权和数据保护权被行政和国家自治机构荒谬解释，力图封杀历史文献资料，从而阻挠接触 30-40 年前甚至 120 年前的文献，这显然违反言论自由权。进一步的指称还包括在隐私受到威胁时，负责保护隐私权的相关机构令人担忧地保持沉默，而且当局明显企图以数据保护为由封杀公共信息。特别报告员与有关当局建立了良好的关系，并开始研究这类指称，但尚未就其真实性作出最后决定。应该说，这不并是他所了解到的第一次和唯一指称国家政府以隐私为借口，回避将公共利益信息在公共域公开。该领域可能成为一个单独报告的主题，这里特别提到邀请所有人，特别是民间社会组织，向特别报告员报告这种例子，以便作出详细调查。

11. 特别报告员欢迎巴西等国的举动，从而加入通过国内隐私法和数据保护法的国家行列，并鼓励它们满足，例如《关于在自动处理个人数据方面保护个人的公约》所载的最低标准。

二. 最近的事态发展和令人担忧的政府监控趋势

A. 政府监控与数字时代隐私权的现状

12. 目前关于政府监控的对话受到爱德华·斯诺登和支持他的人们的激发。尽管从国家角度来看，这是有争议的，但必须承认，斯诺登先生就某些国家安全部门的实际做法向公众提供的信息引发了关于数字时代隐私意味着什么和应当意味着什么的必要辩论。斯诺登在接受《卫报》采访时一句被引用的名言：“我不想生活在一个我所做所说的一切都被记录下来的世界里”，导致了许多重要的举措和行动。[4]

[3] 通过电子邮件联系，请使用以下地址：srprivacy@ohchr.org, 或特别报告员网页所列任何其他地址，www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx。

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

13. 联合国以多种方式对关于政府监控的辩论做出了贡献。大会在第 69/166 号决议中，呼吁各国设立或维护现有独立、有效、资源适足且公正的国内司法、行政和(或)议会监督机制，能够确保本国的通信监控、通信截取和个人数据收集具备适当的透明度并接受问责。欧洲人权法院等区域人权法院也作出判决，确立了各国政府在制定监控手段和实施时须遵守的明确和有约束力的要求。[5]

14. 特别报告员以多种方式跟踪世界各地政府监控的情况，包括与一些国家和国际民间社会组织定期接触。它们做了出色的工作，将引人关注的各种问题提请特别报告员、国家政府和全世界注意。丝毫不贬低其他组织的工作价值，特别报告员愿意提到：美国公民自由联盟、[6] 即时通行、[7] 大赦国际、[8] 进步通信协会、[9] 第 19 条、[10] 人权观察组织、[11] 国际公民自由组织网络[12] 和国际隐私权，[13] 他的任务授权使其与它们以各种方式开展合作。这些组织和其他民间社会组织的相关报告已经公布，十分有益，由于联合国对特别报告员正式报告的字数限制，不允许他在陈述中介绍有关监控的发展，例如 2016 年 11 月由隐私国际交给他的情况简报中的内容，隐私国际后将它刊载在其网站上。[14] 必须指出，特别报告员赞同国际隐私对下列国家监控方面事态发展的关切：哥伦比亚、爱沙尼亚、法国、墨西哥、摩洛哥、新西兰、波兰、俄罗斯联邦、卢旺达、南非、瑞典、前南斯拉夫的马其顿共和国、乌干达、联合王国、美利坚合众国、委内瑞拉(玻利瓦尔共和国)和津巴布韦；并且独立跟踪了这些事态发展。特别报告员谨请这些国家的政府注意隐私国际提交的材料中表达的关切，最好公开回应这些关切和(或)酌情与特别报告员直接沟通。

15. 然而，自从第 69/166 号决议通过以来，令人甚为关切的是，尽管上文第 13 段提到了这种判断，但自从特别报告员上一份报告以来，监控领域的隐私权状况并没有改善。那些做出反应的国家开始着手制定和通过关于这个问题的新法律，如果有的化，只在有限的领域有微小的改进。总的来说，这些法律匆忙起草，草率通过立法程序，使那些本不应该实施的做法合法化。

16. 2016 年 12 月 21 日，欧盟法院作了非常重要和值得欢迎的裁决，提醒欧盟成员国有义务在数字时代尊重、促进和保护隐私权和其他权利。关于要求电信供应商保留大量数据的法律义务，法院指出：“这种立法对基本权利的干涉是非常

[5] 例如，见欧洲人权法院，扎卡洛夫诉俄罗斯，2015 年 12 月 4 日判决书，可查阅：hudoc.echr.coe.int/eng？i=001-159324.

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

[7] 见 www.accessnow.org/issue/privacy/。

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

[9] 见 www.apc.org/en/pubs/research。

[10] 见 www.article19。Org/cgi-bin/search.cgi？q privacy。

[11] 见 www.hrw.org/sitesearch/surveillance。

[12] 见 www.inclo.net/。

[13] 见 www.privacyinternational.org/reports。

[14] 隐私国际，“监测和监督通信监控”，2016 年 11 月，可检索：www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html。

深远的，须考虑到是特别严重的。在没有告知订户或注册使用者的情况下保留数据的事实，可能会使当事人感到其私生活成为不断监控的对象”[15] 它还提到对行使言论自由的潜在后果。

17. 法院进一步承认，“虽然打击严重犯罪，特别是有组织犯罪和恐怖主义的效力，在很大程度上可能取决于使用现代调查技术，但是这样一个普遍关注的目标本身无法证明为了这场斗争的目的，应当认为国家立法规定全面和不加区分地保留所有通信量和位置数据是必要的”。[16] 此外，法院明确指出，保留通信量数据必须是例外，而不是规则。在有具体的迹象表明，这些数据必须保存以打击恐怖主义和严重犯罪时，必须制定限制标准，例如具体地域限制。此外，法院重申，有关人员需要保障措施和补救措施，必须建立有效的监督机制，包括制衡机制。[17]

18. 虽然隐私倡导者欢迎这一裁决可以理解，但联合王国恐怖主义立法独立审查员大卫·安德森也许对该决定的其他方面作了最有用的总结：“因此，欧洲法院的裁决是真正激进的裁决。从另一方面看，并不是每个人都会同意法院的观点，即这些权力是对“隐私权”的一种“特别严重的”干涉，或者它们“有可能使当事人觉得其私生活成为不断监视的对象”(第 100 段)。对相称性的更严格分析，会集中在这种有用的权力在多年运作中可能表现出来的任何实际损害上，并力求避免基于理论或对公众感觉的非正式预测。”[18]

19. 特别报告员长期受一种坚定致力于循证决策传统的熏陶，这就是为什么他赞同独立审查员对相称性进行更严格分析的愿望。迄今为止，特别报告员还没有(至少在联合王国)获得某些(有时是分类的)数据，这证实批量获取数据的效用既属必要，也与风险相称。事实上，特别报告员对法院的裁决表示欢迎，原因恰恰是尚未提供证据说服特别报告员约束监控法律的相称性或必要性，这些法律允许大量获取各种数据，包括元数据和内容。

20. 重要的是要注意独立审查员在这方面还提到的文化层面：

> “然而，必须承认，对这些问题的感觉在欧洲至少在一定程度上各有不同。因此：
>
> - 欧洲法院对干涉隐私的严重性的评论在导致《调查权力法案》出台的三份议会报告和专家报告中，以及通信专员(英国从事这项活动的前高级法官)关于拦截问题的定期报告中，都没有得到真正的回应
> - 但是，在东欧和德国，由于历史经验，加之遭受(直到最近)恐怖主义危害相对较少，引发了更慎重的态度。国家数据保留规则证明是有争议的，在保加利亚、罗马尼亚、德国、塞浦路斯和捷克共和国甚至被爱尔兰数字权利分支机构废止。
>
> 这可能反映了我之前描述的“欧洲法院与英国法官之间一向明显的意见分歧.....这至少归因于对警察和安全部队的不同理解，以及不同(但同样合理的)的结论，而这些结论源于 20 世纪欧洲不同地区的历史(《信任问题》2.24)”。[19]

[15] 见欧洲法院，电视 2 台 Sverige 诉瑞典邮政电信管理局，2016 年 12 月 21 日的判决书。

[16] 同上。

[17] 同上。

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

[19] 同上。

B. 挑战和令人担忧的趋势

21. 特别报告员通过与其任务相关的各种研究活动和其他有关研究项目发现，执法机构和安全情报部门的监控活动有时越来越难以相互区分。虽然一个部门的活动通常是针对在本国境内进行的监控，而另一个部门的活动则着眼于境外，但跨国数据流的性质和干扰它们所需的技术要求，在数字时代通常会导致使用相同或非常相似的设备。

22. 越来越多的情况是，个人数据最终归入同一“桶”数据，可以为各种已知和未知的目的使用和再使用。这为诸如收集、存储、分析和最终消除数据等领域的要求提出了关键问题。作为一个具体例子，华盛顿特区乔治敦法律中心的隐私和技术科室最近进行的一项研究发现，美国成年人中每两人就有一人进入了执法部门的人脸识别网络。正如研究报告的作者所说：“我们对这些系统知之甚少。我们不知道它们如何影响隐私和公民自由。我们不知道它们如何解决准确度问题。而且我们不知道这些地方、州或联邦的任何一种系统如何影响种族和少数族裔。”[20]

23. 这些和类似的洞察，导致了几种思考。首先，跨境数据流和现代信息技术的性质，要求采取全球办法来保护和促进人权，特别是隐私权。如果信息流通仍然是全球性事务，为人类带来并将继续带来各种实质性优势，就需要有一个始终如一和值得信赖的环境。这种环境不能区别对待拥有不同民族、出身、种族、性别、年龄、能力、信仰等的人民。需要有一种核心权利和价值，受到国际社会的一贯尊重、保护和促进。

24. 其次，在虚拟空间交流信息的重要性日益增加，需要私秘、可靠和安全的方法。特别报告员已经广泛地讨论了加密等技术，特别是在提交给大会的第一份报告(见 A/71/368, 第 19 至 40 段)中。此外，其他任务负责人，例如增进和保护见解和言论自由权特别报告员，已经在这方面开展了重要和值得欢迎的工作(见 A/HRC/29/32)。

25. 如果执法机关和安全情报部门担心它们无法拦截或读取使用现代信息技术的人们彼此之间发送和接收的每一条信息，它们不应忘记我们生活的时代有数千种交流信息的渠道。人们已经开始通过数字手段分享如此多的信息，即便其中一些信息不能为国家所管控，但这并不意味着没有其他方法跟踪那些居心叵测的人。尤其是，智能手机和连接设备生成的大量元数据，通常与通信的实际内容一样，为分析人们的行为提供了充分的机会。[21] 另一方面，如果国家有可能干扰每一个信息流，甚至通过保留批量数据和诸如“快速冻结”等技术来追溯，那么隐私权就不会全面过渡到数字时代。

[20] Clare, Alvaro Bedoya 和 Jonathan Garvie Frankle,“永久的嫌犯列队：美国警察无管制的人脸识别”，2016 年 10 月，可查阅 ww.perpetuallineup.org/。

[21] 例如，见哈佛大学勃克曼互联网和社会中心报告，“莫要恐慌，就‘通往黑暗’之争取得的进展”，2016 年，可查阅：cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_ on_ Going_Dark_Debate.pdf.

26. 值得欢迎的是，有些国家和组织已经开始加大力度应对这些挑战。特别是欧洲委员会在这一领域做出了贡献，并在云计算环境执法方面提出了一项倡议。这与《网络犯罪公约》有关，旨在发展出一种新的法律工具。[22]

27. 然而，令人担忧的是，现代关于监控的法律越来越容许在没有适当授权和监督的情况下生成、获取和分析个人资料。当“首先下令、执行或终止”措施时，应当有适当的授权和监督要求。[23] 虽然“传统”方法，例如拦截电话和通信在采取措施之前经常需要司法授权，但其他技术，如收集和分析涉及互联网浏览历史协议的元数据，或源于使用智能手机的数据(位置、电话、使用应用程序，等等)受到的保障措施要弱得多。这是不合理的，因为后一类数据至少如同实际通话内容一样，揭示了某人的个人活动。因此，这些措施也必须采取适当的保障措施。

28. 虽然对侵入性措施需要司法授权通常提高隐私保护的程度，但也必须保证法官本身在个案的决策过程中独立和公正。此外，他们必须掌握必要的知识和事实以透彻考虑这类措施的要求，并了解其决定的潜在影响，特别是了解所使用的技术和使用该技术的后果。因此，各国应提供必要的培训和资源，使法官能够胜任这项复杂的任务。

29. 原则上，这一点同样适用于议会监督监控活动的专门机构。它们不仅需要有相关的信息来了解执法机关的活动和安全情报机构的活动，还需要有足够的资源来理解和消化。

30. 由于牵扯到庞大数据量，在大多数国家这难以实现。进行监控的当局应采取措施，确保对监督措施进行永久详细的审查和管控。监督，特别是如果在政治领域进行，应该能够把重点放在结构性问题上，并能够解决行动的大方向。

31. 另一个值得注意的领域是监督活动的国际性。这个现象有两个特殊的层面需要更多的关注。首先，在全球一级各国尊重以人的尊严为基础的隐私权至关重要。监控活动，无论是针对外国人还是本国国民，必须按照符合基本人权，例如隐私权的方式进行。任何无视这一事实的国家法律或国际协议都必须视为过时，与数字时代隐私和基本权利的普遍性质不相容。

三. 第一批更有利于隐私的监督政府监控的方法

A. 对方法和主题的全面概述

32. 与全球不同区域一些国家当局、民间社会和公司开展的研究与交流，特别是在 2016 年国际情报监督论坛期间，显示政府监控领域出现了若干个主题，其中包括：

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

[23] 欧洲人权法院，扎卡洛夫诉俄罗斯。

(a) 使用的术语和用语需要国际化和标准化；

(b) 需要进行保密和公开的对话，以更好地了解国家体系以及其相似之处和差异；

(c) 促进和保护基本人权与所使用的方法之间的关系；

(d) 保障和补救措施，最好是在国际一级；

(e) 问责制和透明度；

(f) 收集和讨论好的做法和不良做法；

(g) 如何构建监督政府监控问题的渐进式讨论；

(h) 回答关于如何使公众参与的问题；

(i) 需要以较少的神秘态度和更积极主动的态度来解释特勤部门和执法机关进行监控的工作；

(j) 需要更多论坛在这个问题上取得进展。

B. 讨论

33. 术语和用语的国际化和标准化旨在对诸如“监控”“大规模监控”“批量收集”“批量拦截”“大量黑客攻击”“设备干涉”等用语加以界定。英国当局已经发表了一个有用但却有争议的文件，标题为“大宗权力运作案例”，它对一部分这类术语作了令人启迪的描述。[24] 重要的是，当政府当局进行监控，民间社会和其他利益攸关方清楚地了解使用与监控有关的这类术语时实际上意味着什么。其中一些，如“大规模监控”，是载荷沉重和高度有争议的。政府当局在进行监控交流时有必要更全面和统一使用术语并了解它们。然而，司法和政治部门的监督机构、民间社会、安全领域和公司的研究人员，也应该能恰当理解和使用这类术语。

34. 由于监控具有国际性，因此有必要在保密和可信的国际舞台上谈论这个问题。加强进行监控的国家当局之间的对话非常重要。此外，在进行这种讨论时，民间社会的专家必须能够提供他们的意见并分享他们的关切。

35. 至关重要的是，基本人权，特别是隐私权、言论自由权和获得信息权，仍然是评估任何类型和种类的政府监控措施的核心。虽然保护生命权和人身安全是人类生存的一个基本先决条件，但必须铭记，人权没有严格的等级。它们通常是相辅相成的。换言之，这就意味着有必要广泛宣传所有权利，而不必特别关注其中的一两个。

36. 一项权利的价值与其划定的界限和执法机制所允许的范围相一致。这在政府监控方面至关重要，因为需要跨界保障措施和跨境补救办法。正如已经提到的那样，需要执行和提升司法协助。如果没有可能实现一种共同的全球办法，并且尚未将它被排除在外，则需要更多的区域和跨区域举措。

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

37. 需要明确进行监控的政府组织内部的问责制和透明度结构。还需要明确为什么要收集一组特定的数据，分析的目的是什么以及哪些目的不合法。执行这些机制首先需要嵌入进行监控的当局，而且在界定了适当的法律要求之后，需要明确遵守由谁问责。

38. 在这一尝试中收集好的做法和不良做法的例子会有帮助。例如，一些情报监督机构成立了专家咨询机构，其中有可信赖的外部专家，由他们为具体问题提供咨询。此外，对行动作出评估和反思它们对促进和保护基本人权的影响至关重要。作为第三个例子，进行监控的当局成员必须接受培训，不要对技术过分信赖，明白技术最终应当帮助人类而不是驱动人类作出决策。

39. 如果内部问责制和透明度机制失效，则需要有其他制衡机制。各国需要有能力发现和评估有权进行监控的机构存在的结构性问题。在一些国家，议会委员会履行这些职能。然而，监督当局往往缺乏这一领域的知识、资源和(或)接触相关的信息。如果有的话，这也同样适用于司法监督机制。

40. 此外，斯诺登的揭露及其后果清楚地表明，政府当局迫切需要对其工作给予解释。通过事后通知被监控者可能部分做到这一点。一旦可以安全完成，应该通知被监控者并解释此种行动的后果。被监控者还应有权更改或删除不相关的个人信息，只要不再需要这些信息从事任何正在进行或将要进行的调查即可，而且收集和使用这些信息应得到过适当的授权。

41. 此外，公众需要对那些实施监控的机构的运作重拾信任。安全显然是每个人的合理关切。因此，公众虽然没有必要详细了解每一项操作的特点和应用，但必须提供信息，以便掌握保护公众所采取行动的总体情况。乘客预订机票不需要知道飞机如何驾驶，但是如果乘客不信任飞机运营和安全系统的整体能力和安全性，就不会支付机票费用。

四. 特别报告员的活动

42. 隐私权问题特别报告员作为其任务授权一部分，报告了进行的主要公开或半公开活动。本报告涵盖 2016 年 7 月至 2017 年 2 月初的活动，其中包括：

(a) 2016 年 8 月 3 日在德国慕尼黑华为德国研究中心举办的欧洲隐私保护创新研讨会；

(b) 2016 年 9 月 9 日在法国斯特拉斯堡欧洲委员会举行的主题为“互联网自由：欧洲民主安全的不变因素”会议上任主旨发言者；

(c) 2016 年 9 月 19 日至 20 日在德国达姆施塔特举行的欧洲生物识别协会研究项目会议上任生物识别与隐私专题小组主席；

(d) 2016 年 9 月 27 日在布鲁塞尔举行的欧盟委员会移民和内政事务总局 2020 年愿景保护与安全咨询小组会议；

(e) 2016 年 10 月 11 日至 12 日在布加勒斯特举行的国际情报监督论坛任特别报告员；

(f) 2016 年 10 月 13 日至 14 日在布加勒斯特举行的知识社会中的情报问题会议上任主旨发言者和小组讨论主席；

(g) 2016 年 10 月 18 日至 22 日在摩洛哥马拉喀什举行的第 38 届数据保护和隐私专员国际会议上任主旨发言者；

(h) 制图项目 2016 年 10 月 31 日至 11 月 2 日在布拉格举行的第二届年度大会；

(i) 2016 年 11 月 25 日至 26 日在捷克布尔诺举行的网络空间会议上任主旨发言者；

(j) 2016 年 11 月 30 日至 12 月 2 日在墨西哥曼萨尼约举行的亚太隐私权威机构论坛上任主旨发言者；

(k) 2016 年 12 月 7 日在都柏林举行的爱尔兰公民自由委员会监控专题讨论会上任主旨发言者和小组讨论成员；

(l) 2016 年 12 月 8 日在联合王国贝尔法斯特举行的北爱尔兰人权委员会年度报告会上任主旨发言者；

(m) 2016 年 12 月 12 日至 14 日在突尼斯举行的关于隐私、个性与信息自由流通第二次研讨会筹备会议；

(n) 2017 年 1 月 25 日至 27 日在布鲁塞尔举行的人工智能与隐私，计算机，隐私和数据保护第十届国际会议上任小组讨论成员；

(o) 2017 年 2 月 1 日至 2 日在马德里举行的第九届西班牙信息安全隐私论坛上任隐私与安全问题主旨发言者。

五. 结论和建议

43. 在现阶段，特别报告员谨基于临时结论提出五项不同的建议。它们涉及：

(a) 为什么民粹主义和隐私不利于安全；

(b) 各国如何通过更好地监督情报搜集加强隐私保护；

(c) 谁应该享有隐私权，即所有人，随处随地——隐私权的普遍性在这方面具有特殊意义；

(d) 如何通过国内和国际法的发展更好地保护隐私权；

(e) 国际法的某些发展，特别是有关监督法律文书的发展，由于可从更广泛的讨论中受益，可能很快就会处于成熟阶段。

为什么民粹主义和隐私不利于安全

44. 更准确地说，这一节的标题或许应该是民粹主义、隐私与安全。从 2015 年到 2017 年期间，尤其是但不仅仅限于欧洲，出现了一种日益增长的沉溺于“政治姿态”的趋势。换言之，过去 18 个月中看到政治家们希望让人们看到正在对安全立法权力采取某些行动，带有隐私侵入性，或将现有做法合法化，却没有以任何方式表明，这是一种适度或确实有效的对付恐怖主义问题的途径。

45. 所采纳的新的法律以恐惧心理为基础：尽管过分，但可以理解选民面对恐怖主义威胁所怀有的恐惧。恐惧的程度妨碍了选民客观评估拟议措施的有效性。

46. 对于法国、德国、联合王国和美国新监控法律带来的一些极具隐私侵入性的措施，很少或根本没有证据能说服特别报告员相信它们的有效性或相称性。就象最近美国移民禁令的审案法官一样，特别报告员必须寻求法律规定的措施相称性的证据。[25] 如同法官明确询问 2001 年以来，作为移民禁令对象国的国民从事了多少恐怖主义行为一样，特别报告员必须要问，假使更多的钱花费在开展有目标的监控和渗透所需要的人力资源上，假使更少的精力花费在电子监控上，这样做难道不是更相称吗？更不用说更具成本效益和隐私侵入性更低了。其实绝大多数恐怖袭击是由当局已经了解的嫌疑人实施的。

47. 越来越多的证据表明，各国掌握的情报，包括通过大规模获取或大规模监控收集的情报，越来越容易遭到敌对政府或有组织犯罪的黑客攻击。从来没有证明收集这些数据所产生的风险与批量获取所导致风险的降低成正比。

48. 此外，滥用批量获取所收集的数据仍然是一个主要令人关切的问题。并非旨在中伤即将上任的美国政府，人权观察的一位高级研究人员在这方面表达的关切值得在此引述：“在美国，尽管 2015 年进行了有限的改革，但国家安全局每天仍旧对数百万人进行拉网式信息筛查。现在世界上最先进的监控器的钥匙已经交给了.....一位候选人，他威胁要监禁政治对手，登记和禁止穆斯林，驱逐数百万移民，并恐吓自由新闻”[26] 虽然美国现有的制衡机制，或者行政本身的道德标准，可能有希望推动国家摆脱这种风险的实现，但特别报告员在这里指出，一旦存在由大规模监控或批量获取产生的数据集，而且肆无忌惮的新政府在世界任何地方上台，避免滥用这些数据的潜能首先是排除其收集。

49. 因此，特别报告员建议各国不要打恐惧牌，而是通过相称和有效的措施，不是通过过分不成比例侵犯隐私的法律来提高安全性。引用威斯敏斯特大主教文森特·尼科尔斯的话说：“我不相信运用恐惧能够最好地实施任何形式的领导。真正的政治领袖不打恐惧牌。”[27]

各国如何通过更好地监督情报搜集加强隐私保护

50. 2016 年国际情报监督论坛(情报监督论坛)表明，关于如何以加强隐私保护的方式管理情报监督的讨论是一个复杂的过程，需要大量的时间、资源、偶尔的文化变革、政治意愿和信任。找出和进一步发展最佳实践并没有捷径可走。

51. 特别报告员的建议是一个简单而重要的建议：联合国所有会员国都应该参与特别报告员在 2016 年国际情报监督论坛上发起的对情报监督的深入讨论，这一讨论将在 2017 年举办的下一届论坛上继续进行。各国政府应鼓励监督机构和情报机构参加论坛，并为它们的参加提供便利。

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

[26] Cynthia M.Wong,“民粹时代的监控”，人权观察社，2017 年 2 月，可查阅：www.hrw.org/news/ 2017/02/07/surveillance-age-populism。

[27] 文森特·尼科尔斯大主教在英国广播公司第 4 套节目上的谈话，“威斯特敏斯特时间”，2017 年 2 月 5 日。

谁应该享有隐私权？

52. 特别报告员建议各国做好准备，确保在国内和国际上使隐私作为一项真正的普遍权利得到尊重，特别是在互联网上开展的监控方面，隐私不是一项依赖口袋里的护照的权利。

53. 这项建议需要一些空间来发展，并在这里仅用(纯粹是出于空间的原因)美国判例法和立法变化的例子来加以说明。首先应当明确的是，无论在这里对美国的何种建议，在类似情况下同样适用于联合国所有会员国。

54. 2017 年 2 月 6 日，美国众议院做了一件非常值得称赞的事，特别报告员长期以来一直在等待它。众议院一致通过了《电子邮件隐私法》，该法堵塞了美国法律的一个缺口，即要求提供司法授权，才准许访问存储在云盘或其他地方的 6 个月以上的电子邮件。这是特别报告员衷心欢迎的一个事态发展，而且他相信也是参议院可以接受的，它使上次于 2016 年 4 月尝试过的进程脱轨。的确，特别报告员请参议院抓住这一历史性的机会，并进一步显示美国对全世界人权的承诺，同时厘清了一些政府有意无意地宣扬的仇外谬论，即只有“讨厌的外国人”来“给我们找麻烦”，因此他们不配享有法律尊重的基本人权。

55. 这不只是美国制定法律的一些过失。例如，德国政府最近犯了一个同样的过错，它通过了一项法律，将德国人和欧盟公民分成一类，而将其他人分成另一类(见 A/71/368, 第 35-36 段)。当然，人们可以纯粹根据逻辑来否定这种法律：如果看一看在欧洲发生的绝大多数恐怖袭击，它们不是由外国人干的，而主要是由持有欧盟身份证或护照的欧盟公民干的。同样，美国最近发生的恐怖袭击似乎也是类似的情况。那么为什么要迎合那种谬误认为歧视那些不属于立法者管辖权的公民合乎逻辑且明智呢？如果各国政府真诚希望防止和减少恐怖主义，逻辑表明，它们应处理这一问题的根源，如激进行为。投资于更多的措施，打击激进化和拨出更多资源，用于有针对性的长期监控和卧底渗透似乎比沉迷于政治姿态要有效得多。试图通过将大量无用、极其昂贵和完全不相称(侵害如此多的人的隐私权和其他权利)的措施合法化，以便在安全问题上显得很强硬，显然不是政府该走的路。

56. 特别报告员非常恭敬地表示，如果美国的法律能与欧洲最近在以下案例中阐述的原则保持一致，将更为明智和有效，并为世界其他国家树立榜样，即欧洲人权法院审理扎卡洛夫诉俄罗斯一案，以及欧洲法院审理瑞典电视 2 台 Sverige AB 诉瑞典邮政和电信局一案，即进行有针对性的监控的关键要求是合理怀疑，而非公民身份。如果安全和情报部门或执法机构可以证明有合理的怀疑，不论嫌疑人持有什么样的护照，都可以批准司法许可发出逮捕令。关键考虑因素是风险，而且应该保持风险管理。如果一个人显然构成风险，那么此人应该在任何地方都受到监控，而不论其护照身份如何。不论持有什么样的护照，不合理的搜查和扣押适用同样的保障措施──在这种情况下是司法令──也同样适用。《世界人权宣言》非常正确地阐述，并非只有美国公民才有隐私权。相反，它指出，人人有权享有法律保护不受这种干涉或攻击(见第十二条)，特别报告员认为，这也包括美国的法律。因此，美国的立法者在这里有机会为世界各地的其他国家树立榜样，恪守《世界宣言》的文字和精神，并采取具体步骤，通过朝正确方向修改《电子邮件隐私法》，使美国法律真正尊重隐私权的普遍性，其中一些内容概述如下。

57. 如果隐私如同免于酷刑或其他权利一样，是一项基本人权，那么它也是一项普遍权利，这意味着世界各地的每个人都有隐私权，无论他或她在哪里，不论其持有的护照如何，也不论其肤色、信仰、种族、政治哲学或性取向如何。这就是特别报告员所称的美国参议院也应作证的真相。美国政府多次设法惩罚其他国家侵犯人权的行为，经常带头划出红线和拟定制裁措施，以提高遵守的机会。美国参议院通过把美国公民的隐私保障扩大到全世界所有公民，在消除美国公民与他国公民之间区别的同时，将对隐私基本人权的普遍性和立法中的排外趋势给予明智的一击。这样做也将符合欧盟和欧洲委员会的隐私和数据保护法律，不区分公民与非公民的隐私权。

如何通过国内和国际法的发展更好地保护隐私权

58. 鉴于先前的建议主要涉及在国内法中保护隐私普遍性的可能性，以下几段思考通过国际法补充国内措施的可能性。

59. 《美国电子邮件隐私法》目前的措辞引起的另一个关键问题是，法律加强的保障措施是否也适用于无论在何处持有的数据，无论是在美国或是在其他地方。为说明这一问题，有必要引用微软的案例，它质疑美国对其在美国境外持有的数据的全球搜查令。[28] 人们可以很容易理解微软对允许美国查看其在美国境外所持有的数据表现出的勉强态度。这不仅会对其在世界范围内的竞争力产生潜在的负面影响，而且在决定如何处理来自世界各国政府的各种数据请求时，也成为一个特别棘手的问题。这不单单只是微软面临的问题。谷歌、脸书、苹果和推特(仅举几例)等大多数主要来自美国的行业技术巨头，每年都面临着数千个来自世界各地政府的数据访问请求。

60. 如果美国国会希望从这方面找出一种合理的办法，更不用说提供一个从基本人权角度来看合理的解决方案，而不是使美国公司处于商业劣势地位的解决方案，应该认识到答案不完全在于国内法。还必须认识到，这个特殊法律领域并没有得到得力的服务，如司法协助等已有几十年的历史。国会应认识到，虽然《网络犯罪公约》在一些领域取得了相当大的进展，但尚未成功地使个人数据跨界转移和象一些人所希望的那样，快捷、毫无问题地获得调查所需要的数据。这种相对失败的主要原因之一是，它过分依赖十九世纪主权民族国家的观念，而不是顺应二十一世纪互联网跨越国界的现实。虽然这可能是一个很好的例子，说明“婴儿迈步”可以取得什么成果，虽然已经取得了一些成功，包括识别和编纂计算机和互联网犯罪，但《公约》没有及时规定适用于互联网时代犯罪侦查、调查和防范需要的个人资料的跨界流通。之所以没有这样做的一个主要可能的原因是，它没有采取额外步骤建立一个机制，例如一个负责授权国际获取数据的国际机构，并且受权这样做。

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

61. 如同其他形式的国际法规定设立机构，负责诸如海洋法、空间法、核武器、化学武器等不同领域建立信任和实施适当的保障一样，《网络犯罪公约》可以同样的方式与其他多边条约(包括为此目的而设立的新的多边条约)并驾齐驱，有可能扩大到设立一个国际权威机构，能够授予等同于国际监控令，或可在网络空间执行的国际数据访问令。签署此种新条约或附加议定书的国家，可贡献专门的独立法官形成一个小组，成为条约签署国的一个可在世界各地执行相关司法令的一站式服务供应商。以此种方式，再回顾 2016 年 7 月微软案决定的例子，像微软、谷歌、脸书、亚马逊、苹果和其他在国际数据运营中心的技术巨头，不必担心任何国家超越界限，而只需面对根据明确的国际法以合理怀疑为理由发布国际数据访问令。同样，世界各地的公民也可以放心，他们的隐私权，更不用说其他权利，譬如言论自由和结社自由，均可得到不偏不倚和普遍的恰当保障。倘若真的希望隐私权具有普遍性，那么就有理由认为，通过建立具有国际性和普遍性的机制，即可以在世界范围内实施相同的标准和保障措施。

62. 这并非是空想。它将区别真正的民主国家和那些蓄意主要利用互联网作为社会控制手段，并在其管辖范围内保住权力的国家。正如微软公司总裁兼首席法务官最近所主张的那样，这也可能与旨在维护网络空间和平的其他举措相关。[29]

63. 目前特别报告员掌握的证据表明，一些国家，甚至是一些主要的民主国家，十分令人遗憾地以机会主义方式对待互联网，它们的执法机构，特别是安全和情报机构可以通过运作，拦截数据和侵入全球数百万台设备(智能手机、平板电脑、笔记本电脑以及服务器)。在这样做的过程中，15-25 个国家把互联网视为自己的游乐场，它们在互联网上相互争夺战利品，无休止谋求在网络战争、间谍和反间谍活动或工业间谍领域占据上风。动机清单很长，而另外大约有 175 个国家看起来无能为力，难以应对，唯有期盼网络和平能够占上风。

64. 坦率地说，极少数国家积极尝试非正式劝阻特别报告员不要在这一领域寻求解决办法，但特别报告员有责任报告，这伙人似乎是唯一不希望互联网上有国际可执行的保障措施和补救措施的人。尽管他们可能会气馁的是这不会短期内实现，但我尚未遇到过一个公民社会组织，一个公司，实际上，一个合理的执法机构或安全和情报部门不希望有更明确和普遍适用的保障措施和补救办法。

65. 只有通过载有国际法的多边协议，才能实现这种明确性，采取保障措施和补救办法的方式使其更加及时、不偏不倚和快速执行。全世界需要的不是互联网上国家资助的欺诈戏法，而是规定网络空间国家妥当行为的理性、文明的协议，这使得本报告又回到了监控主题。

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

66. 上文中提到的一些改进的国际机制在网络空间执法方面非常有用，目前由《网络犯罪公约》作出了规定。但正如其名称所表明的，联合国约有 25%的会员国加入了该公约，它只涉及刑事司法部门。不涉及以国家安全名义进行的国家安全监控。换句话说，爱德华·斯诺登所揭露的活动类型不在《公约》的范畴之内，如要令人满意地管理这类活动，就需要大大拓展《公约》的范围，否则就必须有一个单独但互补的条约，以充分涵盖网络空间监控。比起一些民主国家，如法国、德国、联合王国和美国等，正争先恐后地制定监管监控的新法律，而其中的心态似乎受到十九世纪主权国家观念的不当影响，公约方式似乎更为可取。

67. 虽然民族主义、沙文主义，乃至民粹主义，似乎正在经历历史上可能呈现出的一种周期性上升的宿命，但它们对于选票的用处，不应该与它们真正为国内和国际安全提供效率混为一谈。应该认识到，即使看政治家在国家一级的演说，绝大多数会员国对助长有组织犯罪或恐怖主义行为毫无兴趣，无论这些行为发生在何处，也不论它们是何人所为。简而言之，假使比利时的一名调查人员，去找由巴西、法国、德国、加纳、印度、英国和美国(只随机提及一些国家)等国法官组成的国际小组，应该很少担心，一旦证明有合理的怀疑，这样一个专门小组或专门为此目的成立的专门小组，不会授权获取有关某人的资料。一旦这个过程产生了国际数据准查证，那么这将大大简化在国家管辖范围内通过国际条约就这种机制达成一致的政府和公司的任务。

68. 不应该把这样一个法律文书与一个面面俱到的互联网治理条约或《日内瓦互联网公约》混为一谈。负责监督网络空间的法律文书尚未触及互联网管理的许多其他部分，尤其是《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条规定的，但常常被忽视的其他部分，即保护名誉的权利，这一权利与隐私权既相似又不同。

国际法的某些发展，特别是有关监督法律文书的发展，由于可从更广泛的讨论中受益，可能很快会处于成熟阶段

69. 因此，总而言之，规范网络空间监督的法律文书将是对《网络犯罪公约》等其他现有网络法律的一个补充步骤，并且可为互联网的隐私提供具体的保障。令人欣慰的是，就特别报告员的任务而言，由欧盟支持的一个现已存在的倡议，即隐私、财产和互联网治理替代管理方案(MAPPING 项目)目前正在探索规范网络空间监控的法律文书的备选方法。已经有了文本草案，目前正在由民间社会和一些国际大公司的专家进行讨论，预计 2017 年的某个时候，肯定于 2018 年春季之前公开。对于任何人，包括特别报告员在内，在探讨备选办法的初期阶段对这一案文或类似的案文采取立场为时尚早，但它有可能最终被证明是各国政府，尤其是包括联合国在内的政府间组织讨论的一个有用跳板。

70. 正如特别报告员准备特别是在 2018 年 3 月至 7 月之间审议这个问题一样，由议会及其选民(恰值 2017-2018 年举行选举)赋予政府的诸多行政部门积极探索恰当监督导监控的选择，并在网络空间引入隐私保护和补救措施，不失为明智之举。这不仅对全世界公民具有重大的内在价值，而且还会向那些错误地认为处理网络空间的最好方式是对互联网的大块区域或其公民在互联网上的探索行为宣示国家主权的国家、民主国家、伪民主国家和其他国家发出明确信号。人权具有普遍性，网络法的存在方式不仅要保护隐私，还要保护其他基本人权。

71. 要实现这一目标无论多困难，并不是不可能的；事实上，既可信又合理的是，相当数量的国家最终会围绕一个监督导网络空间监控和保护隐私的法律文书联合起来。这将对公民有利，对政府有益，对隐私有好处，对商业有益处。围绕新近阐明的原则和新建机制汇聚的国家数量逐渐壮大，从而达到临界质量。这是过去几个世纪以来从国际法发展中汲取的经验。在隐私、监控和网络空间方面，没有理由忽视这一经验。特别报告员的任期内可能不太会取得成果，但至少可能是最有希望开启的途径。特别报告员在任期内迄今为止目睹的一切，使他认识到，当时机到来之时，这可能是最明智的道路。这个时刻可能会比一些人想象的会早一些来临。