联合国 A/69/397

大会

Distr.: General
23 September 2014
Chinese
Original: English

第六十九届会议

议程项目 68(a)

促进和保护人权：人权文书的执行情况

在反恐怖主义过程中促进和保护人权与基本自由*

秘书长的说明

秘书长谨向大会转交在反恐怖主义过程中促进和保护人权与基本自由问题特别报告员本·埃默森根据大会第 68/178 号决议和人权理事会第 15/15 号决议提交的报告。

* 迟交。

在反恐怖主义过程中促进和保护人权与基本自由问题特别报告员的报告

摘要

本报告是现任在反恐怖主义过程中促进和保护人权与基本自由问题特别报告员本·埃默森向大会提交的第四次年度报告。

本报告第二节列举了特别报告员 2013 年 12 月 17 日至 2014 年 7 月 31 日的主要活动。在第三节中，特别报告员审查了在反恐中使用大规模数字监控的问题，并考察了大规模侦听技术对《公民权利和政治权利国际公约》第 17 条规定的隐私权的影响。

一. 导言

1. 本报告由在反恐怖主义过程中促进和保护人权与基本自由问题特别报告员本·埃默森根据大会第 68/178 号决议和人权理事会第 15/15、19/19、22/8 和 25/7 号决议向大会提交。本报告列举了特别报告员 2013 年 12 月 17 日至 2014 年 7 月 31 日期间的活动。报告随后审查了在反恐中使用大规模数字监控的问题，并考察了大规模侦听技术对《公民权利和政治权利国际公约》第 17 条规定的隐私权的影响。

二. 与任务有关的活动

2. 2014 年 2 月 13 日，特别报告员作为发言者参加了在伦敦经济学院举行的题为“卡迪辩论二：联合国监察员与安全理事会制裁决策中的司法审查”的小组讨论。

3. 2014 年 2 月 23 日至 25 日，特别报告员参加了奥地利、巴西、德国、列支敦士登、墨西哥、挪威和瑞士常驻日内瓦代表团在日内瓦国际人道主义法和人权学院的协助下主办的专家研讨会，主题是“数字时代的隐私权”。

4. 2014 年 3 月 11 日，特别报告员向人权理事会第二十五届会议提交了其关于在域外致命的反恐行动，包括不对称的武装冲突中使用遥控飞机或无人驾驶飞机及其对平民的影响的报告(A/HRC/25/59)。他还与理事会就其对布基纳法索(A/HRC/25/59/Add.1)和智利(A/HCR/25/59/Add.2)的国家访问报告进行了一次互动对话。

5. 2014 年 3 月 12 日，特别报告员作为小组成员参加了关于“人权与无人驾驶飞机”议题的一次会外活动，并在人权理事会第二十五届会议期间举行了一次记者招待会。

三. 反恐与大规模数字监控

A. 导言和概述

6. 在过去十年中，各国技术能力大幅提高，从而相应提高了情报和执法机构对可疑个人和组织开展定向监控的能力。侦听通信提供了一个宝贵的信息来源，各国能够借此调查、预防和起诉恐怖主义行为和其他严重犯罪。大多数国家现在有能力侦听和监测固定电话或移动电话的通话，可确定一个人的位置，通过手机地址分析跟踪其行动，并可读取和记录其短信。定向监控也使情报和执法机构能够监测特定个人的在线活动，进入数据库和云设施，获取其中储存的信息。越来越多的国家正在使用恶意软件系统，这些系统可用来渗透个人计算机或智能手机，改变其设置，并监测其活动。加在一起，这些各种形式的监控提供了各种来源的大量数据，可以生成关于特定个人或组织的宝贵情报。

7. 这些监控技术的共同特点是，它们取决于对目标个人或组织是否有事先怀疑。在这种情况下，各国的做法几乎都是一致的，即需要某种形式(无论是司法或行政)的事先授权，一些国家还多了一个事后独立审查环节。因此在大多数国家，至少有一次机会(有时不止一次)来审查据称引起怀疑的信息，并根据特定案件的案情评估监控措施是否合法，是否适度。借助定向监控，就能够客观评估慎重考虑的监控的必要性和相称性，权衡拟议的对个人隐私的侵入程度与某项调查的预期价值。

8. 但是，技术变革的快速发展已使一些国家能够在无事先怀疑的情况下大规模截收通信和内容数据。这些国家的有关当局现在能够使用自动的“数据挖掘”算法来搜集有可能无限的通信往来。通过在作为大多数数字通信通道的光纤电缆上安装窃听装置，相关国家已能够对通信内容和元数据进行大规模监控，使情报和执法机构有机会不仅可以监测和记录本国公民的通信，而且可以监测和记录身处其他国家的个人的通信。通常强制性数据保留法律要求电信和因特网服务提供者保留通信数据供检查和分析，这进一步加强了这种能力。使用扫描软件、特征标准和特定搜索关键词使有关当局可以随后过滤大量储存信息，以确定个人和组织之间的联系模式。自动化数据挖掘算法将共同识别姓名、地点、数量和因特网协议地址联系起来，寻找相互关联、位置数据的地域交叉以及在线社交和其他关系的模式。[1]

9. 因特网普及率较高的国家因此可以获得实际上数量无限的用户的电话和电子邮件内容，并保存特定网站的因特网活动概况。所有这一切都可以在无任何对某一个人或组织的事先怀疑的情况下做到。在有关国家，几乎每一个因特网用户的通信都可能会被情报和执法机构检查。这相当于有系统地干涉通信隐私得到尊重的权利，需要相应提供令人信服的理由。

10. 从执法角度看，大规模监控技术的增加值源于一个事实，即它使得监控当局以前没有注意到的个人和组织的通信成为可能。大规模数据侦听技术对公共利益的好处据说正是因为它不需要事先怀疑。这一循环推理只有通过将国家在这一领域的做法置于《公民权利和政治权利国际公约》第 17 条规定的分析之下才能变得合理。

11. 《公约》第 17 条规定，任何干涉私人通信的行为必须由法律规定，而且必须是实现一个合理的公共政策目标的必要和适度的手段(见下文第 28 至 31 段)。预防恐怖主义显然是这种做法的一个合法目的(见下文第 33 和 34 段)，但情报机构和执法机构在这一领域的活动仍须遵守国际人权法。[2] 不作具体分析，而仅仅断言大规模监控技术可有助于制止和起诉恐怖主义行为，并不能为其使用提供充分的人权

[1] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf。

[2] 见前任特别报告员发布的情报机构的法律和体制框架及其监督方面的良好做法汇编(A/HRC/14/46，第 9-50 段)。

法上的合理性。某事在技术上是可行的，而且有时可能取得有用的情报，这本身并不意味着它(从国际法或国内法角度上看)是合理的或合法的(见 A/HRC/27/37，第 24 段)。

12. 国际人权法要求各国为无论是对某一个人，还是大规模实施的任何干涉隐私权的行为提供明确说明的基于证据的理由。相称性的核心原则是，对受保护的人权干涉程度越大，所需理由就应越有说服力，这样才能符合《公约》的要求。严酷的事实是，对大规模监控技术的使用实际上彻底取消了因特网上的通信隐私权。这一技术使得大规模截收所有数字通信往来成为可能，导致无法在个案基础上进行相称性分析。它方便了对私人通信的入侵，而无需基于对某一特定个人或组织的怀疑的事先授权。因此，只能进行最笼统的事先审查。

13. 由于大规模监控措施没有有针对性的理由，有关国家有责任对试图大规模截收数字通信的一般做法说明理由。因此，相称性分析从微观层面(评估入侵某一个人或组织的隐私的理由)转向宏观层面(评估实行一种大规模干涉所有因特网使用者的个人和集体隐私权的制度的正当性)。干涉隐私权的规模之庞大需要规模相当的相竞的公共政策理由说明。

14. 在绝对最低程度上，第 17 条要求各国在使用大规模监控技术时，对其使用所产生的切实好处作出有意义的公开说明。没有这样的理由说明，就没有任何办法来衡量这一新出现的国家做法是否符合《公约》的要求。在这方面的相称性评估应平衡兼顾保护在线隐私的社会利益与毫无疑问的有效反恐和执法需要。确定如何达成这一平衡需要在一个国家内部和国家之间开展知情的公开辩论。国际社会必须以我们对个人与国家之间关系的集体理解，坚定地面对这一新发展。[3] 前提条件是，利用这一技术的国家对这些措施的合法性的任何评估，其方法和理由说明都必须是透明的。[4] 否则，有一种风险是，系统地干扰数字通信安全的做法将继续扩散，而不认真考虑整个放弃在线隐私权的影响。如果使用这一技术的各国隐瞒其影响，一种概念审查就将占上风，从而导致无法进行知情辩论。

15. 一些人争辩说，因特网使用者本来就对隐私不抱任何期望，必须假定他们的通信可被公司和国家实体之类进行监测。支持这一观点的人所作的经典类比是将发出不经加密的电子邮件比作邮寄明信片。不论这一比较是否有道理，它都没有回答合法性、必要性和相称性这些关键问题。《公约》要求制定国家干涉通信的明确和公开的法律的根本目的是使个人能够知道他们实际享有的隐私权的程度，

[3] 正如美国隐私和公民自由监督委员会所指出的，“允许政府例行收集整个国家的通话记录，就从根本上改变了国家与其公民之间的权力平衡”;《关于按照美国《爱国法》第 215 条实施的电话记录方案和外国情报监控法院的运作情况的报告》。

[4] 人权事务高级专员在其关于数字时代的隐私权的报告(A/HRC/27/37，第 48 段)中指出，“政府在监控政策、法律和做法方面缺乏透明度，该现象令人不安，阻碍了评估这些政策、法律和做法是否符合国际人权法及确保问责制的努力”。

并预见到在何种情况下其通信可能受到监控(见第 35-39 段)。但这一技术作为反恐和执法工具的价值在于,因特网用户假定其通信是保密的(否则就没有必要入侵其通信)。美利坚合众国和大不列颠及北爱尔兰联合王国的情报界人士在这两个国家的大规模监控方案披露之后的说法即反映了这一点，据说这一披露损害了国家安全，因为它提醒可能的恐怖分子，其通信正在受到监控。[5]

16. 对相称性的任何评估还必须充分考虑到这样一个事实，即对世界各地无数人而言，因特网已成为无处不在的通信手段。数字技术的革命也带来了我们相互联系方式的巨大变化。使用因特网的数字通信技术(包括手持设备和智能手机)已成为日常生活的一部分(见 A/HRC/27/37，第 1 段)。在全球通信的现代世界，如今任何人要想交换信息和想法，就不得不使用跨国数字通信技术。因特网往来常常要经由设在外国管辖范围内的服务器。关于用户已自愿放弃其隐私权的说法显然是没有道理的(同上，第 18 段)。国际人权法的一项一般原则是，个人只能在自愿和知情的基础上明确和毫不含糊地放弃权利的情况下方可被视为放弃了一项受保护的人权。在现代数字世界，根据《公约》第 17 条，只是利用因特网作为私人通信手段，不能令人信服地构成对隐私权的放弃。

17. 因特网不是一个纯粹的公共空间。它是多层私人以及社会和公共领域组成的。[1] 在知情的情况下使用信息被张贴在完全暴露在公共视线中的社会媒体平台的人显然没有合理的隐私权预期。明信片的类比对于通过例如推特和脸书等的公共部分传播信息或在公共网站上张贴信息是完全恰当的。但是阅读一张明信片与截收通过电子邮件发出的私人信息(不论其是否有加密)却不是一个恰当的类比。

18. 因此，假定数字通信仍然有应予尊重的法定隐私权(这不应有争议(见大会第 68/167 号决议))，采用大规模监控技术无疑会有损这一权利的本意(见下文第 51 和 52 段)。这可能不符合各国在加强受保护的人权时应采用现有最不具有侵入性的手段这一核心原则(见下文第 51 段)；这种做法排除了任何个别相称性评估(见下文第 52 段)；保密要求使任何其他形式的相称性分析变得极其困难，从而绕过了这一原则(见下文第 51 和 52 段)。实行大规模监控的各国迄今未能对其必要性提供一个详细的基于证据的公开理由说明，几乎没有国家颁布了授权其使用的明确的国内立法(见下文第 37 段)。从《公约》第 17 条的角度看，这接近于完全减损了数字通信的隐私权。出于所有这些原因，大规模数字内容和通信数据监控对公认的国际法规范构成了严重挑战。特别报告员认为，大规模监控方案的存在是对隐私权的潜在的过度干涉。[6] 简而言之，各国不加区分地收集所有通信和元数据与现有的隐私概念相抵触。通信隐私权的本质是，侵犯隐私的做法必须是例外情形，并须在个案基础上确定其正当性(见下文第 51 段)。

---

[5] 见 http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388 和 www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations/。

[6] 另见人权事务高级专员的意见，A/HRC/27/37，第 20 和 25 段。

19. 重新评估因特网隐私权可能有有力的反恐理由，而这些做法也的确需要进行这种重评。但是，有关国家尚未公布赞成彻底废除因特网上的隐私权的理由，这些理由也没有经过知情的审查和辩论。只有在使用大规模监控技术的国家能够具体证明这种技术的使用能够带来切实的反恐好处的情况下，恐怖主义的威胁才可以为这种技术提供一个正当理由。此外，以国家有责任保护公民不受恐怖主义的威胁来证明其正当性的措施，绝不应被用作为无关的政府职能提供更广泛的监控能力的特洛伊木马。现在有日益明显的“用途渐变”的危险，即以反恐为理由的措施也可供公共当局用于不那么重要的公共利益目的(见下文第 55 段)。在本报告中，特别报告员进一步推进其前任(A/HRC/13/37)和前促进和保护意见和表达自由权问题特别报告员(A/HRC/23/40)的工作。特别报告员认为，使用大规模侦听监控技术的国家现在有责任迅速、准确地公开作出解释，为何防止恐怖主义或其他严重罪行就有必要大规模入侵集体隐私权。

B. 近期关于各国数字监控能力性质与程度的披露

20. 2013 年 6 月 13 日，联合王国一家全国报纸发表了美国外国情报监控法院根据《爱国法》第 215 条授权的一项机密法院命令的内容。报道称，该命令要求美国最大的电信服务商之一在为期三个月的时间内每天向国家安全局提供所有“电话元数据”，并禁止该公司披露存在这样一个要求或法令。2013 年 6 月 6 日，一家美国报纸报道了另一件事，披露说国家安全局有一个称为“棱镜”的秘密数字计划。据称该计划是根据美国《外国情报监控法》第 702 条获得授权的，负责收集美国九大技术公司中央服务器上的内容数据。

21. 据这两家报纸报道，通过“棱镜”项目获取的资料可供其他情报机构使用，包括联合王国的政府通信总部。随后有披露称，另有一个称作“上游”的数据收集计划，据说负责截收经由美国服务商所拥有的光缆和基础设施传递的电话和互联网通信内容。世界上大量互联网数据流都经由实体设在美国的服务器。

22. 媒体随后又报道，国家安全局系统情报司设有一个应用程序薄弱环节处，负责收集全世界通信系统中的数据。据称，国家安全局有一个称为“量子”的互联网榨用机制，能侵入第三方计算机。据称，其采用的方法是在互联网“骨干”的关键部位秘密取得服务器的控制权(或称“所有权”)。“量子”项目能伪装成被它挑中的网站(包括像谷歌搜寻页这样的常用网站)，在未经授权情况下将遥控软件安插到那些访问“克隆”网站者的计算机和无线通信设备上(这些人当然没有理由怀疑“克隆”网站是冒牌货)。技术专家评估认为，这种方法能永久侵入用户的计算机，让它源源不断地将情报信息送到美国国家安全局。

23. 随后，美国行政和立法部门采取了一系列措施应对这些披露。在此过程中浮出的一个问题是，这些计划区别对待美国公民与非美国公民(甚至包括那些住在美国拥有属地管辖权的区域内的人)。现将关键事态进展综述如下：

(a) 2013 年 8 月 9 日，巴拉克·奥巴马总统宣布，他已请隐私与公民自由监督委员会[7] 对现行反恐措施进行审查。[8] 2013 年 8 月底，该委员会请求国家情报总监和总检察长修订情报界收集、保留和散发有关美国公民的情报的程序；[9]

(b) 2013 年 12 月 12 日，总统的审查小组发布题为“变动世界中的自由与安全”的报告，提出一系列重大改革建议。在此报告基础上，奥巴马总统于 2014 年 1 月 17 日宣布了一系列立法和行政改革建议。[10] 行政部门同时发布一项新的总统政策指示(总统政策指示第 28 号)，以加强对情报界在美国境内外开展的信号情报活动的监督工作；[11]

(c) 2014 年 1 月 23 日，隐私与公民自由监督委员会发布一份报告；在这份报告和随后的第二份报告中，委员会多数人得出结论认为，电话元数据计划不符合国内法，因为《爱国法》第 215 条不足以成为其支持依据。[12] 3 月 27 日，奥巴马总统提出一系列终止该计划的新建议。[13] 2014 年 5 月 22 日，美国众议院通过《美国自由法》，纳入了总统的一些建议；

(d) 2014 年 7 月 2 日，隐私与公民自由监督委员会发布第二份报告，详细阐述了在实践中是如何根据《外国情报监控法》第 702 条开展监控行动的。[14] 尽管报告主要关注的是这些计划是否符合美国宪法和法律规定的问题，但委员会承认，他们同时还提出了有关非美国公民所受待遇这一“重要而棘手的法律和政策问题”。[15] 委员会的观点认为，关于在一国开展的国家安全监控活动可能影响另一国居民的情况下如何适用隐私权的问题，《公民权利和政治权利国际公约》缔约国之间没有形成“定论”，并称“眼下的激烈辩论”证明了这一点。[16]

---

[7] 委员会是行政部门内的一个独立机构，有权对反恐行动进行审查和分析，确保其与保护隐私和公民自由的需要相平衡；见 www.pclob.gov/。

[8] 见 www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference。

[9] 见 www.pclob.gov/newsroom。

[10] 见 www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html。

[11] 见 www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence。

[12] “Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court”。

[13] 见 www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m。

[14] “Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA”，见 www.pclob.gov/meetings-and-events/2014meetingsevents/02-july-2014-public-meeting。

[15] 同上，第 98 页。

[16] 同上，第 100 页。

24. 与此同时，联合王国也开展了一项审查工作。有指控称，政府通信总部绕过联合王国法律，通过美国国家安全局“棱镜”计划获取了根据国内法无法获取的通信内容。针对这一指控，2013 年 6 月 10 日，外交大臣在议会发言表示，从美国获取的有关联合王国国民的所有数据都“受联合王国法律的有效控制和保护”，包括 1994 年《情报机构法》、1998 年《人权法》和 2000 年《调查权监管法》等法律的有关规定。[17]

25. 2013 年 6 月 21 日，媒体报道称，政府通信总部还在实施另外一个计划(“时代”)。据称，该计划的做法是将数据截收器放置在联合王国与美国之间运行的光缆上，以截收元数据信息和内容信息。联合王国议会内外的人都在问，现有立法是否给政府通信总部提供了开展这类行动的合法权利？他们是否遵守了《欧洲人权公约》第 8 条所保障的隐私权？[18] 随后的披露就集中在政府通信总部联合威胁研究情报小组所发挥的作用上。有报告称，该小组为开展秘密在线行动，采用了一种称为“大使招待会”的计算机病毒。据说这个病毒会自我加密，像“千面人”似地模仿其他互联网用户的通信。

26. 在对政府通信总部截收通信和内容数据的活动进行初步调查后，情报与安全委员会(一个对情报界负有监督责任的委员会)[19] 于 2013 年 7 月 17 日发表声明。委员会在考虑了有关政府通信总部与其海外对口部门情报交流安排方面的法律框架后认定，该机构的活动没有违反任何联合王国法律，政府通信总部遵守了 1994 年《情报机构法》赋予它的法定职责。不过，委员会还认定，鉴于 1994 年《情报机构法》、1998 年《人权法》和 2000 年《调查权监管法》之间“复杂的交互作用关系”，应当进一步开展调查，审议有关截收私人通信的现有法律框架是否充分的问题。因情报机构能力范围及情报活动给隐私权带来影响的问题引起关注，情报与安全委员会于 2013 年 10 月 17 日宣布将扩大其调查范围。[20]

27. 2014 年 4 月 8 日，欧洲联盟法院对爱尔兰数字权利案发布判决，宣布《欧洲联盟数据保留指令》违背了《欧洲联盟基本权利宪章》所保障的私人生活受尊重权和个人数据受保护权。[21] 该指令要求通信服务商保留通信数据备国家主管机构之用，以预防、调查、侦测和起诉恐怖主义等严重罪行。欧洲联盟法院认为，保留和截收通信数据对上述两项权利构成“特别严重的干涉”，认定上述指令不符合相称性原则。2014 年 7 月 10 日，联合王国政府针对这一判决提出了《数据

[17] 见 www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq。

[18] 见 www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance 和 www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm。

[19] 见 http://isc.independent.gov.uk/。

[20] 见 http://isc.independent.gov.uk/news-archive/17october2013。

[21] Court of Justice of the European Union，Judgment in Joined Cases C-293/12 and C-594/12，*Digital Rights Ireland and Seitlinger and Others*，Judgment of 8 April 2014。

保留和调查权法案》。政府称该法案(现已成为法律)作为一项措施，意在“澄清”可以为电信及互联网服务商规定何种性质、何种程度的义务。[22]

C. 大规模监控、反恐与隐私权

1. 《公民权利和政治权利国际公约》第 17 条规定的隐私权

28. 隐私权可以定义为个人应当享有一个全权自主的发展、互动和自由的领域，不受国家干预，任何其他人未经允许也不得擅自过度干涉(见 A/HRC/23/40，第 22 段； A/HRC/13/37，第 11 段)。尊重通信的隐私和安全的义务意味着个人有权在不受国家(或私人行为体)干涉的情况下相互交流信息和想法，确信唯有预定收信人才能收阅这些通信。[23] 隐私权还意味着个人有权知道谁掌握着关于自己的信息以及会如何利用这些信息。[24]

29. 《公民权利和政治权利国际公约》第 17 条是在国际层面确保隐私权的最重要的具有法律约束力的国际条约规定。该条规定“任何人的私生活、家庭、住宅或通信不得受到任意或非法干涉，他的荣誉和名声不得受到非法攻击。”它还进一步规定“人人有权享受法律保护，免受这种干涉或攻击。”其他国际人权文书也包含类似规定。区域和国家层面的法律也规定所有人的私人和家庭生活、住宅和通信有权受到尊重。

30. 不过，隐私权并不是一项绝对权利。某人一旦受到情报或执法机构的怀疑和正式调查，就可能因完全合法的反恐和执法目的而受到监控(见 A/HRC/13/37，第 13 段)。尽管《公约》第 17 条没有列出具体限制条款，列举出在何种情况下干涉隐私权可能并不违反《公约》，但普遍的理解是，这类措施在下列条件都满足的情况下是许可的：(a) 措施得到公开、准确且符合《公约》要求的国内法的授权；[25] (b) 措施有合法目的；(c) 措施符合必要性和相称性的标准。[26]

31. 世界上很大一部分互联网通信流都会在某一段上路经美国——意识到这一点促使一些国家对“棱镜”计划是否侵犯了其公民的隐私权表示关切。2013 年 12 月，大会通过了关于数字时代隐私权的第 68/167 号决议，该决议由 57 个会员

---

[22] 见 www.gov.uk/government/speeches/communications-data-and-interception。

[23] 人权事务委员会第 16 号一般性意见，第 8 段。

[24] 同上，第 10 段；见 A/HRC/23/40，第 22 段。

[25] 人权事务委员会第 16 号一般性意见，第 3 段。

[26] 见 A/HRC/27/37，第 22-25 段及所引资料；A/HRC/23/40，第 28 和 29 段；A/HRC/13/37，第 13 -17 段；关于《公民权利和政治权利国际公约》的各项限制条款和克减条款的锡拉库扎原则，E/CN.4/1985/4，附件；人权事务委员会第 16，27，29，34 和 31 号一般性意见；人权事务委员会，*Van Hulst v Netherlands*，第 903/2999 号通讯，2004 年；*Madafferi v Australia*，第 1011/2001 号通讯，2004 年；*Toonen v Australia*，第 488/1992 号通讯，第 8.3 段；*MG v Germany*，第 1482/2006 号通讯，2008 年；CCPR/C/USA/CO/4。

国共同提出，未经投票即获通过。大会在决议中申明隐私权在网上应受到保护，并促请各国审查其涉及通信监控以及截收和收集个人数据的程序、做法和立法，强调各国必须确保充分而有效地履行国际人权法为其规定的义务。

32. 大会在同一决议中还请联合国人权事务高级专员办事处向人权理事会和大会提交一份报告，说明在国内及域外监控和/或截收数字通信以及收集个人数据(包括大规模开展这项工作)情形下保护和增进隐私权的问题。高级专员在 2014 年 6 月 30 日发表的报告(A/HRC/27/37)第 47 段中作出结论认为，国际人权法为促进和保护隐私权提供了明确、普遍的框架，这也涵盖国内和域外监控、截收数字通信和收集个人数据等情形。不过她又指出，许多国家的做法表明缺乏充分的国家立法和/或执法、程序性保护薄弱、监督不利，致使任意或非法干涉隐私权的行为得不到惩罚。高级专员强调，数字监测行动的性质和程度还在渐渐浮出水面，但她表示关切，“政府在监控政策、法律和做法方面缺乏透明度，该现象令人不安，阻碍了评估这些政策、法律和做法是否符合国际人权法及确保问责制的努力。”(同上，第 48 段)她呼吁各国审查其国内法律和做法，确保充分遵守国际人权法，并酌情加以修订。她还呼吁国际社会对这些问题开展进一步的深入研究(同上，第 49 和 51 段)。

2. 以反恐作为正当目的

33. 与其他一些受《公约》保护的有条件权利不同，第 17 条没有详尽罗列能够成为干涉隐私权合理依据的正当公共政策目标。不过，就第 17 条而言，预防、制止和调查恐怖主义行为显然是一个正当目的。恐怖主义会破坏社群稳定，危害社会和经济发展，割裂国家的领土完整，破坏国际和平与安全。根据《公约》第 6 条，各国有保护其公民及处于其管辖范围内的其他人免遭恐怖主义行为的积极义务。该义务的一个方面就是有责任建立有效的机制，在恐怖主义威胁具体实施之前就发现潜在威胁。各国依靠情报和执法机构对有关信息进行收集和分析来履行这一职责(见 A/HRC/20/14，第 21 段)。

34. 据称，各国加强对互联网所有通信流的监控能力对反恐工作尤其重要，因为互联网通信在资助和实施国际恐怖主义行动方面发挥着重要作用，因为恐怖组织利用互联网招兵买马，而且若不利用互联网监控，则情报工作的局限性可能会妨碍提前发现那些参与规划和煽动恐怖行为的人。由于恐怖主义是一项全球活动，故而搜索恐怖分子的行动就必须跨越国界。因此，预防和制止恐怖主义是至高无上的公益义务，可在原则上构成大规模监控互联网的有说服力的正当理由。

3. 大规模监控与法律定性要求

35. 《公约》第 17 条明确规定，人人都有权受法律保护，使其隐私免遭非法或任意干涉。这就 引出了“法律定性”要求，即须满足三个限制条件：(a) 所采取的措施必须有一定的国内法依据；(b) 国内法本身必须符合法治和《公约》的要求；(c) 国内法有关规定必须公开、清晰、准确。如果有关国内立法不满足可及

性、具体性和可预见性等核心要求，[27] 或如果国内法因其他缘故不满足必要性和相称性标准，则就第 17 条而言，国内法所授权的干涉可能是“非法”和/或“任意”的。[28] 因此，国内法必须纳入有关条款，确保针对具体、正当的目的授予侵入性监控权力(见 A/HRC/13/37，第 60 段；A/HRC/27/37，第 28 段)，并提供有效保障，防止滥用。[29] 此外，适用法律或已发布的有约束力的指南还必须具备合理的清晰度，以约束执行中的酌处权。[30]

36. 可及性不仅要求公布国内法，还要求国内法满足清晰和准确的标准，足以使那些受其影响的人预见到在何种情形下会实施侵入性监控，从而规范自己的行为。人权事务委员会在其关于隐私权问题的第 16 号一般性意见第 8 段中强调，授权干涉私人通信的立法“必须详细准确地说明在何种情形下允许采用这种干涉措施”。在本报告所述大规模监控计划出现之前，对上述规定的一向理解是国内立法必须写明：在何种条件下、可经由何种程序授权实施干涉；其通信可被截收的人员的类别；监控措施的时限；使用和储存所收集数据的程序。[29] 欧洲人权法院也强调必须就这一问题制定明确详细的规则。[31]

37. 大规模监控计划对《公约》第 17 条提出的合法性要求构成重大挑战。大规模侦听计划在运转过程中对受监控者的类别和监控时长不加限制，因此立法中无法写明这些条件。关于大规模监控的详细法律和行政框架往往仍属机密，公众对这些截获数据是如何被处理利用的依然所知甚少。迄今很少有国家颁布基本立法，明确授权这类方案。相反，用于处理较初级监控形式的过时的国内法不加修订就被适用到新的数字技术上来，无法反映一些国家现在监控能力骤增的现状。事实上，有人认为，某些国家“故意对越来越敏感的信息适用相对陈旧和薄弱的保障制度”(见 A/HRC/13/37，第 57 段)。

38. 特别报告员认为，各国迫切需要修订管制现代监控形式的国家法律，以确保其做法符合国际人权法的规定。必须更新关于截收通信问题的国内法，使之体现出现代数字监控形式的特点。较之现有国内立法颁布之时所设想的监控形式，现代数字监控的范围要大得多，对私人空间的刺探要深入得多。在缺乏明确而应时的立法的环境中，任意干涉隐私权的现象就得不到相应保障机制的制约。在此情

---

[27] 人权事务委员会第 16 号一般性意见，第 3 段。

[28] 同上，第 8 段。

[29] CCPR/C/USA/CO/4，第 22 段；*Malone v United Kingdom*，第 8691/79 号申请书，1984 年 8 月 2 日判决，第 67 和 68 段；*Weber and Saravia v Germany*，第 54934/00 号申请书，2006 年 6 月 29 日判决。

[30] A/HRC/27/37，第 29 段；关于《公民权利和政治权利国际公约》的各项限制条款和克减条款的锡拉库扎原则(见 E/CN.4/1985/4，附件)，第 16 段和 18 段。

[31] *Weber and Saravia v Germany*，第 54934/00 号申请书，2006 年 6 月 29 日判决；*Uzun v Germany* (2012) 54 EHRR 121，第 35 段。

况下，为确保合法性和相称性，就必须制订明确而详细的法律。这也是一种不可或缺的手段，让每个人能预见到自己的通信会不会、在何种情况下会受到监控。

39. 公共立法过程使政府有机会向公众说明大规模监控措施的正当性。公开辩论能让公众体谅在隐私与安全之间保持的平衡(同上，第 56 段)。透明的立法过程还应当发现数字通信系统中的内在薄弱环节，让用户能做出知情的选择。这不仅是《公约》第 17 条法律确定性要求的一个关键要素，也是让公众有效参与关乎国家和国际公益问题的辩论的一个宝贵手段(见 A/HRC/27/37，第 29 段；A/HRC/14/46)。特别报告员认为，在数字社区整体隐私权受到系统干涉的情况下，基本立法必须至少对监控授权进行详细而明确的规定，才能满足合法性原则。

40. 适成对照的是，已有国家通过下放立法权(由行政部门根据授权立法)的方式使大规模监控的秘密法律框架得以通过，抑制了立法及司法机构和公众对这种新权力的使用进行仔细审查的能力(见 A/HRC/13/37，第 54 段)。这类规定不符合《公约》第 17 条的法律定性要求，因为对公众不具备足够的可及性(见 CCPR/C/USA/CO/4)。尽管可能有正当的公益理由对具体技术和业务数据保守秘密，但这不能成为不向公众交代一个国家互联网刺探活动的一般性质和程度的理由。没有这类信息，就无法评估这些措施的合法性、必要性和相称性。因此，各国在大规模通信监控的使用及其范围方面应当保持透明(见 A/HRC/23/40，第 91 段)。

4. 域外大规模监控方案

41. 某些国家的技术能力使其可以对其管辖范围之外的个人间通信进行大规模监控，因此，实施了具有域外效力的监控安排。其中一些监控活动是在有关国家境内实际进行的，因此牵扯到《公约》规定的属地管辖权原则。这不仅涉及国家人员将数据截收器安装在途径其管辖地区的光纤电缆的情况，也涉及一国对实际控制数据的电信或因特网服务提供商行使监管权的情况(A/HRC/27/37，第 34 段)。在这两种情况下，无论那些隐私受到干涉的人是否实际居住在服务提供商所在国，这些人的人权都必须受到保护。法律规定一国境内或法律管辖范围内的服务提供商有义务强制保留数据的情况也是一样。即使当各国侵入完全是其领土管辖范围外的基础设施时，有关当局仍然受《公约》规定的国家义务的约束(同上，第 32-35 段以及其中提到的资料来源)。

42. 域外监控活动给适用《公约》第 17 条的“法律定性”要求构成独特挑战。关于截收外部(国际)通信的国内法律提供的保护往往比保护纯粹国内通信的类似规定少。[32] 更令人关切的是，一些国家(包括美国)继续允许对国民和非国民实行

[32] 高级专员在其关于数字时代隐私问题的报告中提到了若干此类规定：美国的外国情报监控法第 1881(a)条、联合王国 2000 年调查权监管法第 8(4)条、新西兰 2003 年政府安全局法第 15A 条、澳大利亚情报机构法第 9 条以及加拿大国防法第 273.64(1)条(见 A/HRC/27/37 第 35 段，脚注 30)。

不对称的保护机制。这一待遇差别影响所有数字通信，因为信息往往是通过设在其他法域的服务器传输的。不过，这对云计算普及的影响尤其大。[33]

43. 任何形式的差别待遇都不符合《公约》第 26 条的不歧视原则，这项原则也是相称性概念中所固有的。[34] 此外，开展大规模监控方案截收其他法域内个人的通信让人严重质疑关于干涉隐私权的法律的可及性和可预见性，而且个人无法知道，他们可能会受到外国监控或他们的通信内容会在外国法域被截收。特别报告员认为，国家在法律上有义务给予国民和非国民及其管辖范围内外的人同样的保护。

5. 情报机构之间的国际合作

44. 对国际情报交流安排也有类似关切。现在还没有法律规范国家间的信息交流协定，这给情报机构订立不受任何独立机构监管的秘密双边和多边安排留出了余地(见 A/HRC/13/37)。个人通信资料可能会在没有任何公开的法律框架保护和没有适当(或任何)保障的情况下被外国情报机构使用。经过广泛协商，人权事务高级专员最近发现的可信证据表明，一些国家政府一直通过隐私保障薄弱的法域进行数据收集和分析工作(见 A/HRC/27/37，第 30 段)。这种做法使受影响者无法预见监控机制的运作，因此不符合《公约》第 17 条的规定。

6. 保障和监督

45. 第 17 条提供的一个核心保护是秘密监控系统必须由适当的程序性保障监管，以防滥用。[29] 这些保障措施的形式可以多种多样，但通常包括独立的事先批准和(或)随后的独立审查。最佳做法是应有行政、立法和司法机构的参与以及民间的独立监督(见 A/HRC/27/37)。没有适当的保障措施会导致对任意或非法侵犯因特网隐私权缺乏问责(同上)。

46. 开展有定向监控方案的许多国家都规定了事先司法授权。虽然符合国际标准的司法参与是一项重要保障，但有证据表明，在一些法域，此类审查的程度和效力被限定为司法服从行政(同上，第 38 段)。在联合王国等其他国家，政府部长无需事先司法授权便可对特定目标发布截收令。据说这样做的理由是，部长们按照民主方式对选民负责。接下来行政部门使用这些权力要接受一个独立的通信侦听专员的审查，个人也可以向有权在非公开审理中审议保密信息的司法机构——调查权法庭提起诉讼。

---

[33] European Parliament Directorate General for Internal Policies and Casper Bowden，“The US surveillance programmes and their impact on EU citizens' fundamental rights”，2013 年。

[34] 人权事务委员会还强调，“必须采取措施确保对隐私权的任何干预都要符合合法性、相称性和必要性的原则，不管通信受到直接监控的个人的国籍或所在地点如何”，CCPR/C/USA/CO/4 第 22(a)段。

47. 在定向监控方面，无论采用哪种事先授权方法(司法或行政)，至少应有一次机会，根据案情以及通信将被截收的个人或组织的具体情况，对侵入性监控的必要性和相称性进行事先审查。大规模监控机制未提供这些机会，因为采用该机制并不取决于对个人的怀疑。因此，事先审查仅限于授权整个机制继续实施，而不是将其适用于某一特定个人。特别报告员认为，使用大规模监控技术的国家必须建立强有力的独立监督机构，并为这些机构提供适当资源，使其负责对照《公约》第 17 条的合法性、必要性和相称性要求对侵入性监控技术的使用进行事先审查(A/HRC/13/37，第 62 段)。

48. 第 17 条的另一个程序要求是应对侵入性监控措施进行事后审查。一些国家让一个独立审查员分析监控法律的适用方式和使用程度及其理由说明，以此监测这一法律的运作情况。此类审查应始终分析国家做法是否符合《公约》要求。

49. 除了这类总体审查外，各国有向据称《公约》权利受到侵犯的个人提供救济的具体义务。《公约》第 2 条第 3(b)款要求缔约国确保任何要求此种救济的人享有由国内司法、行政或立法主管当局裁定其在这方面的权利。为有效保障这一权利，国内法必须设立一个独立机制，该机制应能进行彻底、公正的审查，能获取所有有关材料，并获得有效的正当程序保证，并有权提供具有约束力的救济(包括酌情命令停止监控或销毁监控结果)(见 A/HRC/14/46；A/HRC/27/37，第 39 段)。

50. 为援引有效救济权，通常需要个人证明其为侵权行为的受害者。在秘密监控措施情况下，这项要求可能很难或根本无法满足。很少有国家制订了要求事后通知被监控嫌疑人的规定。欧洲人权法院相应放宽了对个人证明他们遭秘密监控的要求。欧洲人权法院对两种告诉进行了区分，一种是就涉嫌不符合《欧洲人权公约》要求的机制的存在提起的诉讼，另一种是就国家具体非法活动提起的诉讼。在前一种情况下，法院准备对所涉条款进行审查，[35] 而对于后一种情况，其通常要求原告证明他们一直受到非法监控的“合理可能性”。[36] 对于大规模监控机制，特别报告员认为，所有因特网用户都应有权质疑有关措施的合法性、必要性和相称性。

7. 大规模监控方案的必要性和相称性

51. 各国有义务证明，对《公约》第 17 条规定的隐私权的任何干涉都是实现一个合法目的的必要手段。这要求在采用的手段和寻求实现的目的之间必须有合理联系。还要求所选措施“在可能实现预期结果的那些方法中是造成侵扰最少的”(见 CCPR/C/21/Rev.1/Add.9；A/HRC/13/37，第 60 段)。相关的相称性原则要求对照公共机关本着公共利益进行调查所产生的具体利益平衡侵入因特网隐私权的程度。但所允许的干涉《公约》权利的程度是有限度的。正如人权事务委员会所强

[35] Klass 诉德国，(1979-80)2 EHRR 214。

[36] Halford 诉联合王国(1997)24 EHRR 523。

调的“在任何情况下，所实施或援引的限制都不得损害《公约》权利的实质”。[37] 因此，在秘密监控方面，委员会强调，允许干预通信的任何决定都必须由法定主管部门“逐案”作出。[38] 因此，任何干预隐私权行为的相称性问题都应根据具体案情加以判断。[39]

52. 这些原则没有一项不与各国使用大规模监控技术的做法相抵触。拥有运行收集和分析大量数据方案的技术能力无疑给反恐和执法调查提供了额外手段。但在评估这些方案的相称性时还必须考虑到对集体隐私权的附带损害。大规模数据收集方案似乎违背了情报机构必须选择对人权侵扰最少的措施的要求(除非有关国家能够证明，只有全面获取所有因特网通信才能免受恐怖主义和其他严重罪行的威胁)。由于在采用这些措施前根本没有机会进行单个的相称性评估，因此，这些方案似乎也损害了隐私权的实质。它们完全排除人权事务委员会认为必不可少的“逐案”分析，因此，即使这些方案有合法目的，也是依据公开的法律制度实行的，但也可能会被认为具有任意性(见 A/HRC/27/37，第 25 段)。因此，特别报告员得出结论认为，只有相关国家能够证明系统干涉世界上任何地方可能人数无限的无辜民众的因特网隐私权有正当理由，此类方案才符合《公约》第 17 条的规定。[40]

8. 强制性的保留立法及自动挖掘电信和因特网服务提供商持有的通信数据

53. 大规模监控方案并不仅限于截收通信内容。数字通信产生大量的业务数据。这些通信数据(或元数据)包括有关个人、其所在地点以及在线活动的个人信息。迫使许多国家已通过法律，迫使电信和因特网服务提供商收集和保存通信数据，供日后分析使用。这类法律通常要求服务提供商向国家当局提供因特网协议分配，使得在任何特定时间都可以识别特定的因特网协议地址。获取通信数据已成为各国一个日益宝贵的监控技术。通信数据易于存储和检索，可用于汇编个人简况，这和通信内容一样属于个人隐私(见 A/HRC/27/37，第 19 段)。通过合并和汇总从通信数据中获取的信息，就有可能确定一个人所在的地点、与谁来往以及进行的活动(见 A/HRC/23/40，第 15 段)。如无特殊保障措施，那么个人的私生活就基本上没有可以防止元数据遭仔细分析的私密空间。[1] 因此，自动化数据挖掘对隐私权尤其具有侵蚀作用。

54. 在许多国家，各种公共机构都可以在往往没有司法授权或有意义的独立监督情况下因各种各样的目的获取通信资料。例如，在联合王国，200 多个机构有权

[37] 人权事务委员会第 27 和第 31 号一般性评论。

[38] 人权事务委员会第 8 段第 16 号一般性评论。

[39] 人权事务委员会第 4 段第 16 号一般性评论，Van Hulst 诉荷兰，第 903/1999 号来文，2004 年，第 7.3 段；Toonen 诉澳大利亚，第 488/1992 号来文，第 8.3 段。

[40] 见 A/HRC/27/37，第 25 段，人权事务高级专员指出：“仅仅为了在草堆中找到某些针而采取措施是不够的；恰当的标准是比照可能遭受的危害判断所采取的措施对草堆的影响；也就是说，采取的措施是否是必要和相称的。”

依照 2000 年的《调查权监管法》查询通信数据，[41] 仅 2013 年，公共主管部门就提出了 514 608 个查询通信数据的请求。[42] 一段时间以来，法庭确认，向公共当局提供元数据构成侵犯隐私权，而欧洲联盟法院最近认定，保留与个人私生活有关的元数据和通信本身就是侵权行为[43] (准许为分析目的获取保留的元数据构成另一种不同的侵权)。[44] 在做出这一决定时，欧洲联盟法院强调，通过通信元数据“可以对数据被保留个人的私生活做出非常精准的判断”。[45]

55. 按照欧洲联盟法院采用的这一方法，无论数据之后是否被公共当局获取或分析，收集和保留数据都构成侵犯隐私权。无论是根据强制性的数据保留立法获取通信数据还是随后披露给国家当局(及国家当局进行分析)，都需要对特定个人或组织的事先怀疑。因此，特别报告员同意高级专员对强制性数据保留法律的必要性和相称性所表达的保留意见(见 A/HRC/27/37，第 26 段)。

9. 用途细分

56. 许多国家缺少“指定用途”规定，以限制为一目的收集的信息不被用于其他不相干的政府目标。因此，表面上为国家安全目的收集的数据可能会在情报机构、执法机构以及税务局、地方议会和许可证发放机构等其他国家机构间共享。[46] 国家安全和执法机构通常无需遵守限制共享个人数据的数据保护法。因此，个人可能很难预见他们可能何时、受到哪个国家机构的监控。这一“用途渐变”风险违反了《公约》第 17 条，不仅是由于相关法律缺乏可预见性，而且还因为对于一个合法目的可能必要、相称的监控措施对另一个合法目的而言可能就不具有必要性和相称性(同上，第 27 段)。因此，特别报告员赞同其前任的建议，即各国有义务根据人权原则为再次利用个人资料提供法律依据(见 A/HRC/13/37，第 50 和第 66 段)。当跨国或在国家间共享信息时，这一点尤其重要。

10. 私营部门

57. 各国日益依赖私营部门便利电子监控。这不仅限于颁布强制性数据保留法。各公司也通过设计方便大规模监控的通信基础设施直接串通采用大规模侦听技

---

[41] 有权查询数据的机构清单上有税务当局和地方政府机构，根据授权立法(行政命令)该清单还可扩大。

[42] 见 http://www.intelligencecommissioners.com/。

[43] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014, para. 34。

[44] 同上，第 35 段。

[45] 同上，第 26、27 和 37 段。

[46] 若想分析此类用途悄然发生变化在联合王国是怎样发生的，见 www.whatdotheyknow. com/request/127491/response/315758/attach/html/2/Summay%20of%20 Counsels%20advice.pdf.html。

术。国家一直要求电信和因特网服务提供商必须在技术中设计弱点，以确保方便进行窃听。人权事务高级专员称这些做法是“以自我监管与合作为幌子，赋予互联网中介以执法和准司法职责”(见 A/HRC/27/37，第 42 段)。特别报告员同意这一评价。为确保服务提供商不成为侵犯人权行为的同谋，他们应确保其行为符合人权理事会 2011 年核可的《工商业与人权指导原则》(同上，第 43-46 段)。

四. 结论和建议

58. 《公民权利和政治权利国际公约》第 17 条规定的国家义务中包括有义务尊重数字通信的隐私和安全。在原则上，这意味着个人有权在不受国家干涉的情况下彼此间交流信息和想法，并确知只有预定的接收方才能收读他们的信息。干涉这项权利的措施必须得到公开、准确并符合《公约》要求的国内法的授权。它们还必须有合法目的，并满足必要性和适当性的检验标准。

59. 预防和制止恐怖主义是一项最重要的公共利益，原则上可构成大规模监控互联网的一个有说服力的理由。但目前所开展的方案的技术覆盖面如此广泛，以至于只有相关国家能够证明系统干预世界上任何地方可能人数无限的无辜民众的因特网隐私权是适度的，才能说此类方案符合《公约》第 17 条。大规模侦听技术不加区分地侵蚀在线隐私，危害第 17 条保障的权利实质。在没有正式减损《公约》规定国家义务的情况下，这些方案对国际法的既定规范构成直接、持续的挑战。

60. 特别报告员同意人权事务高级专员的观点，即迫切需要使用这项技术的国家应修订和更新国家法律，以确保与国际人权法相一致。这不仅是第 17 条的一项要求，而且也为开展能提高公众认识，使个人能够作出知情选择的知情辩论提供了一个重要机会。当整个数字社会的隐私权都受到威胁时，只有详细、明确的主要法律才能解决问题。应对所获数据的使用实施适当限制，要求相关公共主管部门提供再次使用个人资料的法律依据。

61. 各国应设立强大、独立的监督机构，为其提供适当资源，使其负责进行预先审查，审议授权申请时不仅要对照国内法的要求，而且还要对照《公约》的必要性和相称性要求。此外，个人在在线隐私权涉嫌受到任何侵犯时，应有权寻求有效的救济。这需要有关个人能够有途径向一个独立机制提出起诉，该机制应能进行彻底、公正的审查，能获得所有有关材料，并有充分的正当程序保障。问责机制的形式可以多种多样，但必须有权命令给予有约束力的救济。各国不得规定有损有效救济权的常规要求。

62. 特别报告员同意人权事务高级专员的意见，即国家侵入其领土管辖范围以外区域的基础设施时，仍受《公约》规定的义务约束。此外，《公约》第 26 条禁止以国籍和公民身份为由予以歧视。因此，特别报告员认为，各国在法律上有义务给予国民和非国民以及其法域内外的人以同样的隐私保护。不对称的隐私保护制度显然违反了《公约》的要求。

63. 特别报告员呼吁目前采用大规模数字监控技术的所有国家参照《公约》第 17 条的要求，为系统干预在线社区的隐私权提供详细的、有据可依的公开理由说明。各国应披露其入侵互联网的性质和程度、采用的方法和理由，并应向公众详细说明这一做法带来的切实好处。

64. 特别报告员同意其前任（见 A/HRC/13/37，第 19 段）以及前增进和保护见解和言论自由权问题特别报告员（见 A/HRC/23/40，第 98 段）的观点，即人权事务委员会应就在线隐私权问题拟订和通过一项新的一般性意见，并在其中反映 1988 年通过第 16 号一般性意见以来在数字通信监控方面的新发展。