联合国 A/HRC/41/35

大会

Distr.: General
28 May 2019
Chinese
Original: English

人权理事会
第四十一届会议
2019年6月24日至7月12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

监控与人权

促进和保护意见和表达自由权特别报告员的报告*

概要

事实已经证明，对个人——通常是记者、活动人士、反对派人士、批评人士和其他行使表达自由权者——的监控会造成任意拘留，有时会引发酷刑，甚至可能导致法外处决。然而，面向明显奉行压制政策的国家政府的出口和技术转让却管制薄弱，此类监控活动更是愈演愈烈。在本报告中，特别报告员首先提出了目标监控的问题，这从人权法赋予各个国家的义务及公司的相关责任即可看出。然后，他针对私营监控行业内的监管、问责制和透明度提出了一个法律和政策框架。最后，他呼吁加大力度监管监控的出口，限制监控的使用，并呼吁立即暂停私营监控行业工具的全球销售和转让，直至制订严格的人权保障措施来监管此类活动并保证政府和非国家行为体使用这类工具的方式合法为止。

* 本报告逾期提交，以反映最新动态。

GE.19-08652 (C) 040619 270619
1908652

请回收

目录

一. 导言

1. 大会曾谴责非法或任意监控和截获通信为干涉基本人权的“高度侵入性行为”(见大会第 68/167 号和第 71/199 号决议)。然而，非法监控并未得到明显遏制，仍在继续进行。为本报告提交的资料详细列举了政府利用私营公司开发、销售和支持的监控软件的一个又一个案例。事实已经证明，对特定个人──通常是记者、活动人士、反对派人士、批评人士和其他行使表达自由权者──的监控会造成任意拘留，有时会引发酷刑，甚至可能导致法外处决。然而，面向明显奉行压制政策的国家政府的技术转让却管制薄弱，此类监控活动更是愈演愈烈。这个市场迷雾重重；实际上，我们对这一问题的了解主要依靠非政府研究人员的数字法证工作以及民间社会组织和媒体的执着报道。

2. 这个问题岌岌可危，特别报告员在本报告结论中不仅呼吁加大力度监管监控的出口，限制监控的使用，而且呼吁立即暂停私营监控行业工具的全球销售和转让，直至制订严格的人权保障措施来监管此类活动并保证政府和非国家行为体使用此类工具的方式合法为止。

3. 特别报告员针对私营监控行业内的监管、透明度和问责制提出了一个法律和政策框架。他首先提出了问题，强调问题的焦点在于目标监控，而不考虑大规模拦截、收集和保留私人数据(通常称为“大规模监控”)的问题。然后，他强调了人权法赋予各个国家的义务以及各公司的相关责任。在第四部分中，他提出了一个框架，根据现有国际人权纳入对意见和表达自由权的保护，从而完善现有法律和政策。最后，他向主要行为体提出了建议。

4. 本报告的编写工作得益于各国提交的 11 份资料和民间社会提交的 33 份资料。2018 年 12 月，人权事务高级专员办事处在曼谷组织了为期两天的专家磋商。本报告增编概述了在磋商期间提出的意见和举行的会谈。[1]

二. 政府与私营监控行业

5. 我们生活在一个数字监控工具唾手可得、易于滥用却难以发现的时代。2013 年，前任务负责人弗兰克·拉·吕在其开拓性的监控问题报告中指出，薄弱的监管环境为任意和非法侵犯隐私权及意见和表达自由权提供了沃土(A/HRC/23/40，第 3 段)。次年，人权事务高级专员在其关于“数字时代的隐私权”的首次报告中得出结论认为，许多国家的做法表明，这方面缺乏充分的国家立法及(或)执法不力，程序性保障薄弱，且监管无效，所有这些因素导致非法数字监控未被追究责任(A/HRC/27/37，第 47 段)。

6. 有些国家在其自身机构和部门内部开发目标监控工具，另一些国家则改用现有的“现成”犯罪软件产品，还有一些国家可能在国际监控市场上购买先进的商业间谍软件。[2] 在本报告中，特别报告员最关切的是最后一类工具。数字监控不

[1] 我谨此特别感谢 Amos Toh、Desiree Murray、Cristina Butoiu、Matthew Marcoly 和加利福尼亚大学欧文分校法学院国际司法所的 Kyoolee Park 为编写本报告及其增编提供了帮助。

[2] 公民实验室，《社区面临风险：对民间社会的数字威胁》(多伦多，多伦多大学蒙克全球事务学院，2014 年)，执行摘要，第 8-11 页。

再是那些有资源以内部工具为基础开展大规模目标监控的国家的专属。私营行业已然介入，却不受监管，近乎有罪不罚。隐私国际的数据显示，2016 年有超过 500 家公司在开发、营销和向政府采购方出售此类产品。[3]

本报告考虑的监控类型

7. 在本报告中，特别报告员主要关切的是让行为体能够秘密获得数字通信、工作产品、浏览数据、研究、地点历史和个人线上和线下活动的技术。下文介绍了主要的目标监控技术和实践。

计算机干扰

8. 监控技术让侵入者能够访问个人计算机或网络。这种干扰的范围相当大。[4] 例如，2017 年，美利坚合众国上诉法院审理了外国政府资助在美国境内实施监控的案件。[5] 该案涉及一名出生在埃塞俄比亚而居住在马里兰州的美国公民，他一直向埃塞俄比亚移民社区成员提供技术援助。最初是埃塞俄比亚政府特工向一名活动人士发了一份文件，用一种侵入性恶意软件感染了他的电脑。软件程序名为 FinSpy，系由一家德英公司——Gamma 集团销售。[6] 据称，FinSpy 记录了这名男子及其家人的因特网视频通话、电子邮件和其他通信，手段包括记录他的键盘敲击日志，然后将数据发回位于埃塞俄比亚的服务器。[7]

黑客攻击移动设备

9. 私营监控产品还具有直接攻击移动设备的功能。NSO 集团的“飞马”间谍软件就是典型的例子，据称该软件在墨西哥投入了侵入性使用。从 2015 年开始，许多举报腐败和毒品交易的个人在其移动设备上收到了短信或链接，其中一些来自看似合法的来源，这表明发送者对目标的了解非常详细。收到短信的有记者、政治人物、联合国调查人员、人权倡导者和其他人士。加拿大研究与宣传组织——公民实验室发现，那些链接给接收设备装上了“飞马”间谍软件，从而可以对目标进行远程监控。公民实验室确定已有 45 个国家将“飞马”软件用作针对个人的监控工具，其中包括巴林、沙特阿拉伯、多哥、大不列颠及北爱尔兰联合王国和美国。[8]

[3] 隐私国际资料，第 1 页。

[4] 见，例如，Ronald J. Deibert，《黑色代码：网络空间战内幕》(多伦多，Signal，2013 年)，第 186-190 页。

[5] Doe 诉埃塞俄比亚联邦民主共和国，851 F.3d 7 (华盛顿特区巡回法院，2017 年)。

[6] 有关 FinSpy 宣传资料，见维基解密，“间谍档案：远程监控和传播解决方案——FINSPY”。

[7] 有关指控的详细资料，见《第一次修改的起诉书：Doe 诉埃塞俄比亚联邦民主共和国》(2014 年 7 月 18 日)。

[8] 见 Bill Marczak 等人，“捉迷藏：跟踪 NSO 集团‘飞马’间谍软件在 45 个国家的运行”，公民实验室，2018 年 9 月 18 日。

社会工程

10. 上述多项技术都采用了引诱目标不经意地在其设备上下载恶意软件的策略。举例来说，含有恶意链接的电子邮件要么冒充目标的联系人，要么欺骗目标，使其相信自己点击的是与工作、宣传或个人事务相关的善意链接。例如，研究人员将携带“飞马”间谍软件的 WhatsApp 消息发送给大赦国际的一名工作人员，敦促他报道一场抗议活动，其中包括据称会载有更多信息的链接。[9] 点击这个链接，即很可能在其移动设备上下载该间谍软件。

网络监控

11. 一些技术通过网络工作，以便能进行目标监控。例如，俄罗斯行动调查活动系统便涉及在电信网络上安装一个装置，以便能够拦截通信。该系统系由私人制造和销售，在俄罗斯联邦以及更远的中亚地区广泛使用。例如，Protei 公司生产的设备可确保该系统的技术(如窃听和因特网拦截工具)可以在乌兹别克斯坦和哈萨克斯坦等国运行。[10]

面部识别与情感识别

12. 面部识别技术努力捕捉和检测一个人的面部特征，以便可以根据往往构成非法歧视基础的族裔、种族、原国籍、性别和其他特征对其进行分析。[11] 情感识别试图从一个人的面部表情推断其感觉、情绪或意图，依据的是高度可疑的分类系统。[12] 证明这些技术全面侵入的环境可能没有其他比中国更合适的了。有可信报道显示，中国政府利用面部识别技术和全国各地的监控摄像头，“专门根据维吾尔族人的外貌来监控他们，记录他们的来往行踪，以便进行搜索和审查”。[13] 政府部署的大部分技术似乎均由国有和私营企业在国内生产。[14]

国际移动用户识别码采集器(黄貂鱼)

13. 国际移动用户识别码采集器模仿附近的发射塔来拦截由个人通信设备传输的通信和位置数据。这种采集器在世界各地通常得到执法部门和情报机构广泛使用。联合王国一家私营公司涉嫌向菲律宾出售此类采集器和其他间谍软件。许多人担心的是，政府广受诟病的禁毒战会采用这些工具来跟踪和监测吸毒者。[15]

---

[9] 见 Bill Marczak、John Scott-Railton 和 Ron Deibert，“NSO 集团基础设施涉及针对大赦国际和沙特异见人士”，公民实验室，2018 年 7 月 31 日。

[10] Andrei Soldatov 和 Irina Borogan，《红色网络：俄罗斯数字独裁者与新网络革命者之间的斗争》(纽约公共事务出版社，2015 年)，第 190-191 页。

[11] 见，例如，因特网实验室资料，第 6 页；因特网与社会中心资料，第 12 页。

[12] 人工智能现状研究所，《2018 年人工智能现状报告》(纽约，纽约大学，2018 年)，第 13-14 页。

[13] 见 Paul Mozur，“一个月 50 万次面部扫描：中国如何利用人工智能分析少数民族”，《纽约时报》，2019 年 4 月 14 日。

[14] 中国人权资料，第 2-3 页。另见 A/HRC/39/29，第 14 段。

[15] 见 Sofia Tomacruz，“你认为数据和通信设备安全吗？三思”，Rappler，2018 年 3 月 17 日。

深度数据包检测

14. 深度数据包检测既能监测和分析通过通信网络和因特网的流量并改变其方向，又可以用来将用户重新定向到受恶意软件感染的网站，以及阻止用户访问某些网站。据报道，土耳其电信的网络安装了这些设备，部署的目的是在土耳其和阿拉伯叙利亚共和国用户试图下载合法软件应用程序时，将其重新导向，让其下载间谍软件。[16]

公私合作

15. 在数字监控工具市场上，政府和私营部门是密切的合作伙伴，因为政府本身的各个部门和机构可能无法满足政府的要求，而私营公司具备满足这些需求的激励机制、专门知识和资源。这些公司通常在全球和区域贸易展览会上会面。那些展览会的目的就是将它们聚在一起，就像约会服务那样。[17] 在展览会上，各个公司会决定彼此是否匹配。尚不清楚这类公司是否开展任何形式的尽职调查来评估买方的人权记录。

16. 卖方意图可能合法。可能这些公司真的打算在司法或其他独立行为体授权下，由经授权的公共当局针对合法目标部署其产品，实施“合法拦截”。然而，这一点不能确定，因为这种合作从尽职调查、销售到最终用户支持的方方面面运作的监督和透明度通常都非常有限。事实上，关于私营监控行业的几乎所有公开信息都是在非政府机构和学术机构(如公民实验室)开展法证工作以及编写调查报告期间收集的。[18]

17. 所谓“漏洞市场”的运作尤其不可告人。众所周知，政府和私营行为体会从安全研究人员那里购买常用软件的安全漏洞，作为“零日漏洞”用于访问个人通信和设备。[19] 这些漏洞只要不对设备或软件制造商披露，就可作为监控的切入点。如果政府和公司不披露此类漏洞，就会让包括政府和私营部门客户在内的最终用户面临安全风险，因为这些客户通常将金融、卫生、就业或执法领域的敏感数据存储在商业开发的数据库中。迄今为止，对于政府和公司是否有责任共享其关于漏洞的信息，各方尚未达成一致，而且此类漏洞的销售尚不受监管。事实上，这一状况不仅推动了价值巨大的漏洞市场发展，还使得许多政府和公司都满怀戒备地保护自己的漏洞信息，希望将其用于侵犯性目的。[20]

---

[16] 见 Bill Marczak 等人，“网络不畅：Sandvine 的 PacketLogic 设备曾在土耳其部署政府间谍软件、将埃及用户重新定向到附属广告？”，公民实验室，2018 年 3 月 9 日。

[17] 见，例如 www.issworldtraining.com；及 Patrick Howell O’Neill，“ISS 世界：独裁和民主间谍软件巡回路演”，Cyberscoop，2017 年 6 月 20 日。

[18] 私营监控的故事也是一个关于自由、独立研究和媒体的极端重要性的故事。这类调查让调查人员也面临被监控的风险。见，例如，Raphael Satter，“卧底针对网络安全监管机构”，美联社，2019 年 1 月 26 日。

[19] 见隐私国际，“利用隐私：监控公司促进零日漏洞发展”，2018 年 2 月 7 日。

[20] 见 Sarah McKune 资料中的讨论，第 2-4 页；欧洲政策研究中心，《欧洲软件漏洞披露：技术、政策和法律挑战》(布鲁塞尔，2018 年 6 月)；Sven Herpig 和 Ari Schwartz，“全球各地漏洞股权化进程的未来”，Lawfare，2019 年 1 月 4 日。

18. 同样显而易见的是，公私合作并不仅仅止于产品销售和转让。所泄露文件显示，私营监控公司还提供售后支持。例如，据报道，2014 年，FinFisher 与政府客户签订了“年度支持合同”，提供产品技术升级和更新以及其他形式的客户支持，[21] 同时还培训如何优化其恶意软件，以破坏监控对象的数字通信、计算机设备和 Wi-Fi 网络。[22]

19. 正如公司与买方紧密关联一样，各个公司与其所在国政府也是如此。一些公司在本国的出口管制制度中拥有强大的话语权，削弱了加强这些制度的努力。例如，2016 年，有可信指控表明，出于行业游说者的压力，从“欧洲联盟出口管制双重用途物品和技术清单”的拟议增列清单中删除了某些形式的监控技术。[23] 在最近关于欧洲联盟出口管制制度的谈判中，据称尽管欧洲议会已就采纳人权保障措施达成广泛一致，但最后的决定受到商业利益的影响，大范围限制了将人权保障措施纳入拟议监管改革的落实。[24]

20. 最近的报告还指出，许多具有情报和执法专业知识和经验的个人游走在政府和私营部门之间。这扇旋转门或许会让前政府专家得以为私营行为体提供支持，而此类行为体的工具则可能用于侵犯人权。[25] 路透社在 2019 年的一份报告中披露，美国国家安全局的多名前雇员跳槽到了一家私营公司，支持阿拉伯联合酋长国代号为“乌鸦项目”的信号情报计划。[26] 据称，所涉雇员利用其专业知识严密监控阿拉伯联合酋长国当局的政敌，还将美国公民作为监控对象。政府对于与私营监控行业之间这扇“旋转门”的监管顶多也不过是软弱无力，在许多(如果不是大多数的话)法律体系中很可能根本不存在。

三. 法律框架

A. 国家义务

21. 无论监测工作成功与否，监控对象的隐私权及意见和表达自由权都会受到干涉。[27] 为了彻底干涉目标的隐私权，就需要让目标对侵入企图或行为一无所知。事实上，各国政府通常寻求的就是在目标不知情的情况下实施侵入的工具。然而，将这种干涉视为对目标施加影响的全面努力的一部分则具有决定性。如果出于非法目的而实施，监控企图——以及成功的行动——可能被用来压制异议、制

[21] 见隐私国际，“从最新 FinFisher 文件了解的六件事”，2014 年 8 月 15 日。

[22] 同上。

[23] 见无国界记者组织，“国际规则：游说集团的破坏或阻碍”，2017 年 3 月 14 日。

[24] 见 Daniel Moßbrucker，“监控出口：欧盟成员国如何损害新的人权标准”，netzpolitik.org，2018 年 10 月 29 日。

[25] 见隐私国际，“换帽子：为什么南非监控行业需要审查”，2016 年 12 月 14 日；Alex Kane，“以色列如何成为了监控技术中心”，《拦截者》，2016 年 10 月 17 日。

[26] 见 Christopher Bing 和 Joel Schectman，“阿联酋的美国雇佣兵秘密黑客团队”，路透社，2019 年 1 月 30 日；Robert Chesney，“乌鸦项目：美国人员服务于外国情报机构会怎么样”，Lawfare, 2019 年 2 月 11 日；Sarah McKune 资料，第 7-8 页。

[27] 纽约大学法学院全球正义所，资料，第 6 页。

裁批评或惩罚独立报道(以及报道来源)。[28] 制裁可能并非针对目标，而是针对其联系网络。在非法监控猖獗的环境中，目标社区一旦知道或怀疑存在这种监控企图，这类企图反过来就会调节和限制其行使表达自由、结社、宗教信仰和文化等权利的能力。简而言之，通过目标监控来干涉隐私，目的是压制表达自由权的行使。

22. 没有必要复制以往特别报告员、其他任务负责人、高级专员、人权理事会、人权事务委员会等已经开展的广泛人权报告，那些报告强调了防止目标监控的人权法律框架的以下关键特点。

23. 第一，《公民权利和政治权利国际公约》和《世界人权宣言》保护每个人的隐私权、意见和表达权。这两项文书的第十九条都保障人人有权持有主张，不受干涉，以及有权不论国界，通过任何媒介寻求、接受和传递各种消息和思想。《公约》第十七条第 1 款与《宣言》第十二条相呼应，规定“任何人的私生活、家庭、住宅或通信不得加以任意或非法干涉”。

24. 在数字时代，隐私权和表达权相互关联，网上私隐是保障行使意见和表达自由的关口(A/HRC/29/32；和 A/HRC/23/40，第 24 段)。第十七条允许干涉隐私权的前提条件是：“得到公开、准确且符合《公约》要求的国内法的授权”；“有合法目的”；以及“符合必要性和相称性的标准”(A/69/397，第 30 段)。第十九条规定了一项三部分检验标准，要求限制只应由法律规定并为保护他人的权利或名誉、保障国家安全或公共秩序、或公共卫生或道德所必需。[29] 人权事务委员会强调，这些原则至少有如下含义：

(a) 法律规定/合法性：任何限制必须以充分的准确性来制订，以使个人能够相应地约束自身行为，并且必须可供公众查阅。任何限制不得过于模糊或过于宽泛，以致可以赋予官员不受约束的酌处权；[30]

(b) 必要性和相称性：国家有责任证明言论和威胁之间有直接和紧密关联，以及其力求采取的限制必须是可用来实现相同保护功能的诸种手段中侵犯性最小的一个；[31]

(c) 正当性：第十九条第 3 款为合理限制规定了具体条件。虽然国家普遍力图在国家安全基础上寻找实施限制的合理理由，尤其是目标监控的合理理由，但特别报告员认定，这个理由应该仅限适用于整个国家利益处于危险之中的情况，从而排除仅出于政府、政权或权力集团的利益实施限制(A/71/373，第 18 段)。

25. 人权事务委员会在 2017 年“关于意大利根据《公民权利和政治权利国际公约》提交的第六次定期报告的结论性意见”中落实了这些原则(CCPR/C/ITA/CO/6，第 36 段)，确定要保障隐私权，就必须针对监控、拦截和黑客行为制订有力的独立监督制度，包括通过确保司法机关在任何情况下都参与此

[28] 见人权基金会资料。

[29] 对第十九条的三部分检验标准的详细说明见人权事务委员会关于见解自由和言论自由的第 34 号一般性意见(2011 年)，第 5-9 段和第 22-36 段；A/HRC/38/35。

[30] 第 34 号一般性意见，第 25 段。

[31] 同上，第 34-35 段。

类措施的授权，以及通过向受影响者提供有效补救，包括在可能的情况下予以事后通知，告知其已处于监控之下或其数据已被窃取(同上，第 37 段)。大会第 73/179 号决议赞同这些原则，指出对数字通信的监控必须符合国际人权义务，必须依据法律框架进行，而这个框架必须可供公开查阅，且必须清晰、精确、全面而无歧视。

26. 虽然这些原则适用于所有目标监控案件，但当涉及公共利益的表达时，则具有特殊效力。目标监控创设了自我审查激励办法，直接破坏记者和人权维护者开展调查以及与信息来源建立和维持关系的能力(A/HRC/38/35/Add.2，第 53 段)。委员会强调，决不能将限制作为钳制倡导多党民主制、民主原则和人权的理由。[32] 以个人行使表达自由权为由对其进行攻击的行为即违反第十九条第 3 款。[33] 该委员会进一步指出保护记者以及从事人权状况资料收集和分析、发表人权相关报告者的重要性，其中包括法官和律师。[34] 这些保护还涵盖信息来源的保密，国际和区域人权机制(非洲、欧洲和美洲系统)也强调对此应依法予以保护(A/70/361，第 5 段)。

27. 除了不干涉隐私或限制表达的主要义务外，各国还有保护个人不受第三方干涉的义务。《公民权利和政治权利国际公约》第二条反映了各国的主要义务，规定各国有义务尊重和保证其领土内和受其管辖的所有人享有《公约》所承认的权利。[35]《公约》第十七条第 2 款规定，人人有权享受法律保护，以防止其隐私受到这种非法干涉。然而，目前尚不清楚各国是否普遍针对目标监控提供了积极的法律保护。当然，跨国监控更是如此，即使是外国实体对本国公民实施的监控亦如此。[36] 在一起指控墨西哥目标监控的案件中，美洲人权委员会表达自由问题特别报告员与促进和保护意见和表达自由权问题特别报告员对该国进行了正式联合访问，其间提出了政府使用“飞马”间谍软件的问题。他们敦促政府允许独立调查关于针对记者部署间谍软件的指控(A/HRC/38/35/Add.2，第 52-55 段)。迄今为止，尽管墨西哥提高透明度、信息获取及个人资料保护问题国家研究所要求政府披露其获得“飞马”的合同性质，但针对这些指控的调查工作尚未澄清情况。[37]

28. 人权理事会 2011 年通过的《工商企业与人权：实施联合国“保护、尊重和补救”框架指导原则》清楚表明，国家的保护义务包括采取适当步骤，防止、调查、惩治和补救第三方侵犯人权行为(A/HRC/17/31)。《指导原则》敦促国家如与工商企业签约，或立法允许工商企业提供可能影响人权享有的服务，则应实行充分监督，以履行其国际人权义务(同上，第 10 页)。

[32] 第 34 号一般性意见，第 23 段。

[33] 同上。

[34] 同上。

[35] 另见人权事务委员会，关于《公约》缔约国的一般法律义务性质的第 31 号一般性意见(2004 年)。注意，第 31 号一般性意见特别列入关于隐私权的第十七条，系作为缔约国有积极义务处理私人或私营实体活动的一个条文例子。

[36] 见 Nate Cardozo，“华盛顿特区巡回法院就网络安全问题做出了危险裁决：埃塞俄比亚可以自由地在美国人家中监控他们”，电子新领域基金会，2017 年 3 月 14 日。

[37] 见提高透明度、信息获取及个人资料保护问题国家研究所，“共和国总检察长得到结束‘飞马’案有罪不罚现象的历史机遇：Salas Suárez”，2019 年 3 月 27 日；Juan Arvizu，“Ordena Inai a PGR abrir contrato de compra de Pegasus”，《宇宙报》，2018 年 4 月 17 日。

B. 公司责任

29. 由于私营监控行业的公司均秘密运营，公众并不了解公司考虑(如果考虑的话)其产品人权影响的方式。鉴于该行业的性质及其产品不符合国际人权法的广泛用途，很难想象那些公司会切实考虑这些影响。换言之：鉴于公众对其许多客户的压制行为知之甚广，这些公司也不能当真宣称自己对这些工具的压制用途不甚了解。

30. 《指导原则》提供了一个框架，用于评估监控公司是否尊重受其产品和服务影响者的权利。具体而言，《指导原则》强调：尊重人权的政策承诺；查明、防止、减轻和考虑人权影响的尽职调查程序；与受影响群体的磋商；对人权政策有效性的不断评价；针对受影响权利持有人的有效申诉机制(A/HRC/17/31，第 15-25 段)。

31. 无论从哪个角度看，这些公司似乎都不符合这些最低基准。少数几家公司发布了客户政策，含糊其辞地表示需要尊重人权。例如，黑客团队表示，该团队“在销售产品之前会对潜在客户进行评价，以确定是否有客观证据表明黑客团队提供给客户的技术将用于方便侵犯人权或是否有这方面的可信关切”，但并未解释该团队处理这些信息的方式，甚至亦未查明其技术可能牵涉哪些方面的人权。[38] NSO 集团声称，其运营遵循一个商业道德委员会的规定，该委员会“包括来自法律和外交关系等各个学科的外部专家”，并暗示，如果其产品被“不当使用”，集团可能将工作作废。[39] 该集团在其网站上还声称，将“调查对其产品滥用的任何可信指控”，但无迹象表明所谓滥用是否包括侵犯人权。[40]

32. 简而言之，各个公司尚未披露切实行动的例子，如制订尽职调查程序，查明和避免通过其本身活动造成或加剧负面人权影响，预防或缓解经由其商业关系与其业务、产品或服务直接关联的负面人权影响(A/HRC/17/31，附件，指导原则 13)。例如，无任何公开资料表明：人权评估是销售过程尽职调查的一个常规组成部分；公司对这些评估给予决定性的重视；以及这些评估贯穿产品整个生命周期和全部售后支持合同始终。事实上，有越来越多的证据表明，该行业在助长严重侵犯人权方面发挥着核心作用，再加上该行业坚决拒绝解释其保障措施，因此难免得出这样的结论：这种自我监管缺乏实质性。

33. 欧洲委员会关于信通技术部门执行《指导原则》的指南突出强调了“设计纳入人权”的重要性。[41] 滥用监控产品的巨大风险意味着，公司应该预见到其软件的非法使用，并着手为不可避免的负面影响设计解决方案。联合王国政府采取了一项颇有希望的举措，与一家技术行业协会合作，为网络安全行业制定了一套

[38] 黑客团队，客户政策。

[39] 见 NSO 集团 2018 年 9 月 17 日声明。可查阅 https://citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf。正如公民实验室指出的那样，“NSO 集团关于商业道德委员会的说法让人想起黑客团队声称‘外部专家和法律顾问小组……会审查潜在销售’云云。这一‘外部小组’像个独立的律师事务所，黑客团队并不一定听取其建议”(Marczak 等人，“捉迷藏”)。

[40] 见 www.nsogroup.com/about。

[41] 见欧洲委员会，《信通技术部门执行联合国工商企业与人权指导原则指南》(卢森堡，2013 年)。

指导方针，其中强调了在产品开发的最初阶段“通过适当的设计修改”防止和降低人权风险的重要性。

C. 国际和国内出口管制

34. 出口管制是努力降低私营监控行业及其工具的压制性使用所造成风险的一个重要因素。然而，其效力有限。首先，有关的国际出口管制制度——有 42 个国家参加的、不具约束力的《瓦塞纳尔常规武器与双重用途物品和技术的出口管制安排》——专为减少对区域和国际安全的威胁而制订。虽然这是一个值得赞扬的必要目标，但该框架不适合处理目标监控对人权构成的威胁；实际上，这一安排缺乏能够直接处理监控工具造成的侵犯人权行为的准则或执行措施。其次，该安排以出口为重点，使其无法成为解决核心问题的完美工具，因为核心问题是：利用这些技术来针对合法表达、提出异议、提出报告和其他行使人权的例子。

35. 尽管如此，《瓦塞纳尔安排》还是推动了“保持常规武器和双重用途物品和技术转让的透明度和加强其中的责任”这些重要目标。预计参与国将对“双重用途物品和技术清单”上的所有项目实行出口管制。[42] 因此，《瓦塞纳尔安排》已经(或应该)由参与国和非参与国纳入国内法律和政策；但遗憾的是，尚无执行机制来确保将其纳入国内法或由相关国内机构予以执行。

36. 2013 年，参与国将“侵入软件”及“因特网协议”网络通信监控系统相关项目增列入“双重用途技术清单”。该清单显示，“侵入软件是为避免被‘监测工具’发现，或为破解‘保护性对策’而专门设计或修改的‘软件’”，用于从计算机或网络设备提取数据，或修改程序的“标准执行路径”，允许“按外部指令执行”。[43]

37. 有关滥用监控的详细报告表明，以《瓦塞纳尔安排》为核心的出口管制制度并未切实限制监控技术的传播及其压制性用途。欧洲议会议员加强欧洲出口法律和政策的人权保护努力陷于停顿，这证明了改革的挑战。他们的努力明确要求扩大双重用途项目和全面控制的清单，并考虑监控技术的“最终目的地国对人权的尊重”。[44] 2018 年 1 月，该提案在欧洲议会通过了一读，初步获得了对加强双重用途技术出口管制的支持。[45] 然而，自那以后，该提案已遭到至少九个成员国批评，这些国家主张削弱对人权的保护。[46] 该法案的未来尚不明朗。[47]

---

[42] 见《瓦塞纳尔安排》，“双重用途物品和技术清单及弹药清单”。

[43] 同上，第 221 段。

[44] 见欧洲委员会，“欧洲议会和理事会建立欧盟双重用途物品(改造)出口、转让、中介、技术援助和转运管制制度的条例提案”，2016 年 9 月 28 日；Lucie Krahulcova，“欧洲议会奋力加强监控交易规则”，Access Now，2017 年 12 月 8 日。

[45] 有关上述条例提案的立法历史概览，见 EUR-Lex，Doc.52016PC0616。

[46] 塞浦路斯、捷克、爱沙尼亚、芬兰、爱尔兰、意大利、波兰、瑞典和联合王国代表团，“促进通过经完善的欧盟出口管制条例第 428/2009 号、推动在全世界促进人权和国际人道主义法的网络监控管制”，WK 5755/2018 INIT(2018 年 5 月 15 日)；Access Now，“欧盟：各国推动放宽向侵犯人权者出口监控技术的规则”，2018 年 6 月 11 日。

[47] 见 Catherine Stupp，“九个国家联合反对欧盟对监控软件的出口管制”，Euractiv，2018 年 6 月 11 日；Moßbrucker，“监控出口”。

38. 在国内层面，出口管制的强制执行情况各不相同，甚至在《瓦塞纳尔安排》参与国之间也是如此。例如，美国尚未通过 2013 年“侵入软件”及因“特网协议”网络通信监控系统相关的增列项目。[48] 但是，美国商务部正对现行框架进行广泛审查，且已接受委托，制订一个机构间进程，根据 2018 年《出口管制改革法案》针对“新兴”技术和“基础”技术制订新的管制措施。[49] 以色列是一个非参与国，已通过了《瓦塞纳尔安排》所管制双重用途物品的出口管制措施，但这些管制措施的执行尚处于保密之中。[50]

D. 缺乏对目标监控的补救

39. 作为一个国家尊重和确保享有人权义务的一部分，《公民权利和政治权利国际公约》第二条第 3 款(甲)项规定有义务向侵权行为受害者提供有效补救。第二条第 3 款(乙)项规定，对这种侵权行为的索赔主张必须由合格的司法、行政或立法当局或由国家法律制度规定的任何其他合格当局断定。人权事务委员会强调，执法和检察当局应通过独立和公正的机构迅速、彻底和有效地调查关于侵犯权利的指控。[51] 提供有效补救办法的义务还包括有义务通过开展尽职调查来防止、惩治、调查或补救私人或私营实体这种行为造成的伤害，从而保护个人不受私营部门实体侵权行为的伤害。[52]

40. 目标监控受害者争取让所受伤害得到承认都几乎毫无胜算，更不用说对这种伤害的补救了。正如欧洲人权法院和人权事务高级专员所解释，尽管即使在保密情况下，仅仅是监控威胁，加上缺乏补救，即可能构成对隐私的干涉，但情况却仍然如此。[53]

41. 针对制造和销售工具的私营监控公司以及部署这些工具的政府寻求补救的诉讼程序尚不确定。案由和补救的缺乏引发了对于就侵犯人权行为向公司追究责任的可能性的严重关切。至少有八个国家的据称受害者已对私营监控公司或政府提起了诉讼或正式投诉。[54] 然而，诉讼和正式投诉获胜的障碍相当大，包括缺乏司法监督、补救、案由、强制执行和数据保存。

42. 在某些案件中，民间社会组织要求政府调查非法监控，但这些要求经常遭到拒绝。在联合王国，隐私国际向联合王国国家打击犯罪局提起了针对 Gamma 集团的刑事诉讼，诉称该公司的子公司 FinFisher 向巴林政府出售监控技术并提供

[48] 隐私国际资料，第 5 页。

[49] John S. McCain，《2019 财政年度国防授权法案》，第 115-232 (2018)号公法。

[50] 见“以色列—美国出口管制”，export.gov，2018 年 7 月 20 日。另见下文第 43 段。

[51] 第 31 号一般性意见，第 15 段。

[52] 同上，第 8 段。

[53] 欧洲人权法院，Roman Zakharov 诉俄罗斯(第 47143/06 号诉请书)，2015 年 12 月 4 日判决，第 171 段；A/HRC/27/37，第 20 段。

[54] 见 Siena Anstis,“针对目标数字监控和数字监控行业的诉讼及其他正式投诉”，公民实验室，2018 年 12 月 12 日。

援助的行为违反了多项国内法律。[55] 欧洲宪法权利和人权中心及隐私国际还在德国慕尼黑提起了刑事诉讼，要求对该公司展开调查，但公诉机关拒绝了这一请求。[56] 即使各国展开调查以确定政府监控是否违反了人权准则或国家法律，调查也可能具有任意性，或毫无章法。

43. 似乎还没有诉讼替代办法可以根据国际人权法提供补救。例如，在大赦国际一名工作人员成为据称与“飞马”有关的可疑 WhatsApp 消息的目标后，该组织致函以色列国防部，要求吊销 NSO 集团的出口许可证。[57] 该国国防出口管制局对此致函回应，称其不提供有关发放出口许可证政策的信息，也不提供有关实际许可证本身的任何信息。[58] 该局未证实或否认存在出口许可证，但指出“以色列(国防部)就政府客户向 NSO 集团发放的出口许可证符合国际义务”。[59] 事实证明，现有的重大障碍就是缺乏区域和国际压力，以及以国家安全为由的保密政策。

44. 隐私国际还向经济合作与发展组织(经合组织)德国和联合王国国家联络点投诉了 Gamma 和 Trovicor，指控其参与了巴林政府对政敌的目标监控。[60] 针对 Trovicor 的投诉要求德国国家联络点“查明该公司向巴林出口监控产品是否违反了《经合组织跨国企业准则》，因为巴林当局将这些产品用于了侵犯人权活动，包括逮捕、拘留政敌和持不同政见者以及对其施以酷刑”。[61] 但是，该国家联络点驳回了投诉，理由是无充分证据表明 Trovicor 在巴林开展业务。在向联合王国国家联络点提出的几乎相同的投诉中，多个民间社会组织针对 Gamma 提起了类似的侵犯人权指控。[62] 该国国家联络点受理了投诉，并于 2013 年 6 月发布了初步评估报告，报告称：“虽然双方均未就 Gamma 向巴林供货提供直接证据，但所提供的证据表明，该公司的产品可能被用于对付巴林的活动人士。(国家联络点)认为，这证实该公司在履行开展适当尽职调查和应对影响的义务方面存在问题。”[63]

[55] 见隐私国际，“代表巴林活动人士向国家打击网络犯罪机构提起的刑事诉讼”，2014 年 10 月 13 日。还在以色列和塞浦路斯针对 NSO 集团提起了法律诉讼：见 David D. Kirkpatrick 和 Azam Ahmed，“为给客户留下深刻印象而窃听王子、高级官员和记者”，《纽约时报》，2018 年 8 月 31 日。

[56] 见欧洲宪法权利和人权中心，“FinFisher：未对德英软件公司展开调查”，2014 年 12 月 12 日。

[57] 隐私国际资料，第 8 页。

[58] 同上。

[59] 同上。

[60] 该组织网站显示，国家联络点的主要作用是“通过开展宣传活动，处理询问，并帮助解决在特定情况下可能因未遵守准则而引起的问题，从而进一步提高准则的有效性”。

[61] 见隐私国际，“经合组织投诉：Trovicor 向巴林出口监控技术”，2013 年 2 月 1 日。

[62] 见隐私国际，“经合组织德国国家联络点不愿调查德国公司在巴林侵犯人权事件中扮演的角色”，2013 年 12 月 20 日。

[63] 联合王国商业、创新和技能部，“《经合组织跨国企业准则》联合王国国家联络点的初步评估：隐私国际等对 Gamma 国际英国有限公司的投诉，2013 年 6 月”(伦敦，2013 年)，第 25 段。

45. 虽然国家联络点的最后报告根据人权标准提出了若干建议，但无证据表明 Gamma 执行了这些建议，抑或承认该报告。[64]

四. 保护基本权利免遭目标监控的框架

46. 如果说目标监控技术的控制和使用综合系统已崩溃，其实并不准确。因为几乎不存在这样的系统。虽然人权法对使用监控工具作出了明确限制，但各国依然在开展非法监控，并不担心法律后果。人权法律框架已经就位，但尚无实施限制的框架。情况如此紧急，各个国家必须将这些技术仅限于合法使用，并须接受最严格的监督和授权，而且各国必须规定私营部门参与监控工具市场(从研发到市场营销、销售、转让和维护)的前提条件：人权尽职调查和遵守人权规范的记录。

47. 前任务负责人坚持认为，考虑到监控技术助长蓄意侵犯人权行为的功能，各国必须采取措施防止这些技术商业化，要特别留意其研究、开发、交易、出口和使用(A/HRC/23/40，第 97 段)。今天，这一呼吁仍然意义重大。在本节中，特别报告员审查了一个框架的主要内容，该框架旨在保护个人避免成为干涉人权享有的监控技术应用目标。本报告所提议的步骤需要以下各方采取行动并予以实施：国家——作为这些技术的用户和出口国；公司——按照《工商企业与人权指导原则》；国家和公司——与民间社会合作；以及人权理事会。

A. 暂停出口和使用目标监控技术

48. 私营公司创造、转让监控技术及提供服务的方式令人不安，而各国购买和使用这些技术的方式也同样令人不安。有可信指控显示，各个公司将其工具出售给政府，而政府则利用这些工具来针对记者、活动人士、反对派人士以及在民主社会发挥关键作用的其他人。其中一些公司驳斥了这些指控，辩称它们不允许将其产品用于非法目的，具备多种机制来评估对“敏感”最终用户的销售，而且遵守有关出口管制的国家法律。各个公司可能会认真处理就以监控为基础的压制和侵犯人权行为对其提出的共谋指控。然而，如果私营公司不接受公开披露和问责程序，则没有具体理由相信其说法。指控的严重程度要求在公司关系和程序方面保持透明度，更不用说下文所述的一系列其他步骤了。

49. 执行本报告所述步骤将需要时间。在此期间，许许多多的记者、活动人士、人权维护者和政府批评人士将任由政府摆布，政府则借助一系列高度侵入性的监控工具而胆大妄为。因此，至关重要的是，公司应立即停止出售和转让此类技术，停止为这些技术提供支持，直到有令人信服的证据表明其已采取了有关尽职调查、透明度和问责制的充分措施(如下所述)，来防止或减少使用这些技术实施侵犯人权行为。政府也应该立即暂停颁发监控技术的出口许可证，直至有令人信服的证据表明，可以从技术上将这些技术的使用仅限于符合人权标准的合法目的，或者这些技术仅出口到其使用须经授权的国家——由独立和公正的司法机构

[64] 见 Amitpal Singh，“经合组织认为 Gamma 国际存在侵犯人权行动”，公民实验室，2015 年 3 月 3 日；“《经合组织跨国企业准则》联合王国国家联络点——隐私国际与 Gamma 国际英国有限公司：审查投诉后的最后陈述”，2014 年 12 月。

根据正当程序及合法性、必要性和正当性的标准授权。然而，目前有越来越多的证据表明，私人开发的监控工具正用于明显的非法目的，这为暂停这些转让提供了充分理由。

B. 各国政府作为监控技术用户的义务

1. 根据国际人权法义务加强限制监控的国家法律

50. 作为首要步骤，部署监控工具的各国政府必须确保按照符合国际人权法所要求标准的国内法律框架进行部署。法律只应授权对最严重的刑事罪行实施监控。为了符合这些标准，各国法律必须：

(a) 强调人人享有不受非法或任意干涉其隐私的权利，并享有不受干涉持有意见的权利，以及不分国界而通过任何媒介寻求、接受和传递信息和思想的权利；

(b) 要求任何管辖监控的立法必须载于精确、可公开查阅的法律中，并且仅在必要和适当时适用，以实现《公民权利和政治权利国际公约》第十九条第 3 款所列合法目标之一；

(c) 确保仅根据国际人权法，并经合格的独立和公正司法机构授权后，才在对监控时间、方式、地点和范围作出一切适当限制的情况下，批准对特定人员实施监控行动；

(d) 考虑到目标监控技术相关侵权的极端风险，要求经授权使用这些技术时必须遵守保存详细记录的要求。仅按照正规、有文件证明的法律程序并在签发相关使用指令后，才批准监控请求。只要不严重损害监控目的，便应尽快将授权监控决定通知监控对象。[65]

51. 各国普遍对寻求接触记者工作的刑事调查规定了严苛的举证责任(A/70/361，第 24 段)。监控技术往往用于针对那些在促进民主价值观方面发挥重要作用的人。特别报告员认识到，有些国家可能认为，在某些情况下，例如，记者可利用其职业做掩护而从事严重刑事犯罪。据他的经验，这些说法几乎无一例外是谬论或言过其辞。政府经常利用这类指控来破坏新闻调查和不同意见，或将记者作为监控对象，即便他们并非合法刑事调查目标，也同样监控，这对新闻自由造成了不成比例的影响。在这方面，法律默认立场应是禁止对媒体个人使用数字监控工具。当然，这并不意味着记者可以免于其他形式的合法法律程序，包括非数字监控。原因很简单，在使用数字监控这种侵入性技术的环境下，对涉及其他新闻工作的各个领域的合法刑事调查有可能侵犯权利或“泄露”资料。这种可能性确实存在，即使并非不可遏止，也的确难以遏止。也正是这种可能性很可能会阻止记者们调查最敏感的问题，更不用说让消息来源和举报人愿意站出来了。

2. 建立监控技术的公众核准和监督机制

52. 政府使用监控技术的司法授权必不可少，但还不够。购买这些技术还应受到切实的公众监督、商议和控制。近年来，由于美国执法机构对监控技术的使用激

[65] 见“必要性和适当性：在通信监控中适用人权的国际原则”(2014 年 5 月)。

增，一些社区设立了民间控制委员会来监管这些技术的使用和购买。例如，加利福尼亚州奥克兰市通过了一项法令，对监控技术的购买做出了若干规定，各国可以效仿。[66] 其中包括：

(a) 有关部门根据国家人权义务执行核准程序；

(b) 通过正规程序发布购买公告，以及就此类购买所涉人权影响以及有关技术是否会有效实现预期目的等问题进行公众咨询；

(c) 定期公开报告此类核准、购买和使用。

53. 特别是在购买执法工具方面赋予国家以下各级机关一定自主权的国家，应鼓励和加强社区对此类购买的控制。鉴于公众明显有意维护广泛使用的商业软件的隐私和安全，还应授权公共监督机制制订有关漏洞储存和相关利用途径开发的政策。

3. 为受害者提供国内法律补救工具

54. 由于上述原因，非法或任意监控的对象很难对政府提出索赔主张。其中有一些结构性障碍，例如许多法律体系均无法用于对政府行为体提出索赔主张。当立法机关和法院过分尊重眼前国家安全和执法利益时，也可能禁止这些索赔主张。有些索赔主张可能难以实现，因为要证明存在监控，或将监控归咎于国家行为体或者甚至归咎于特定国家机构，使其成为诉讼对象，既困难又费钱。被监控个人目标通常不知道自己已被监控——或者即便他们知道，也可能超出了追诉时效。[67] 换言之，索赔人在据称非法监控引起的国内法律索赔中的获胜几率微乎其微。

55. 严肃对待滥用监控技术的国家应采取步骤，使个人能够对国家和非国家行为体提出索赔主张。对许多国家而言，这必然包括确保有关管辖权、证据、及时性和其他基本门槛条件的规则适合在数字时代适用。例如，这些规则应确保法院能够接受技术专家的法证分析作为证据，并予以分析。国家立法还应确立针对私营实体的案由，其中应考虑到公司所有权的变化(称为“处置”或“改造”)，这往往使受害者追究责任和寻求补救的努力复杂化。[68] 同时还应考虑替代补救形式，例如成立真相委员会，让数字监控协助的严重侵犯人权行为受害者能够作证，并审查公司是否共谋参与这些侵犯人权行为。

56. 与此同时，目标监控并不总是局限于领土范围之内。如果国家越境进行目标监控，受此类监控的个人可能很难对侵权国提出指控。这些案件中也可能出现与国内索赔相同的一些举证责任和其他负担。此外，正如在上文所述的 Doe 一案中，法院可能不愿受理针对外国主权的诉讼。虽然这类诉讼的规则各不相同，但各国应解释主权豁免的准则，以确保其法院可以受理针对外国政府的诉讼。

[66] 见加利福尼亚北部美国公民自由联盟，“奥克兰成为最新一个收回地方执法部门采用监控技术的地方控制权的城市”，2018 年 5 月 2 日。

[67] 见 Roman Zakharov 诉俄罗斯。

[68] Access Now 资料，第 8 页。

C. 许可监控技术出口的政府义务

57. 《瓦塞纳尔安排》并非对监控技术出口管制的最终决定；管制清单的执行取决于国家的执行情况。该安排亦未包括所有主要出口国的参与：以色列是监控技术市场的主要参与者，自称“完全遵守”该安排，但至今仍未成为参与国。[69] 该安排还只是一个有限的框架，因为尽管安排有着涉及区域和国际和平与安全的重要目标，却未针对人权问题。即便如此，鉴于该安排确立了期望得到广泛执行和遵守的标准，参与国应利用这一宝贵论坛，对监控技术的转让施加基于权利的限制。

58. 为了加强该安排在制订全球出口标准方面发挥作用，如果有一个人权工作组可提出和审议将人权问题纳入技术转让的出口标准，将对参与国大有裨益。但是，该安排无论是采用这样一个工作组，还是采用其他机制，都应制订一个框架，根据此框架，任何技术的许可都将以国家人权审查和公司是否遵守下文讨论的《工商企业与人权指导原则》为条件。正如隐私国际所指出的那样，在“出口物品用于侵犯人权的风险巨大，目的地尚无管辖监控物品使用的法律框架，或者针对其使用的法律框架不符合国际人权法律或标准”的情况下，参与国以及其他出口国政府都应该拒绝颁发许可。[70] 为确保在出口许可证因此被拒绝时遵守规定，应将相关监控技术纳入现有的制裁制度。[71]

59. 虽然这些标准将是对《瓦塞纳尔安排》的宝贵补充，但公众或具体民间社会组织监测其执行情况的能力将取决于在国家和国际一级加强透明度的义务。该安排本身应通过为许可标准、许可授权、修改或拒绝决定、滥用监控技术的事件或模式及相关侵犯人权行为以及数字漏洞处理方面的政府间信息共享和公共信息披露制订明确、可执行的指导方针，从而加强这方面透明度。国家出口法律还应为出口许可决定的公开记录和开放供查阅划拨充足资源，授权有关政府机构在处理出口许可证申请时征求公众意见并展开多利益攸关方磋商。最后，各国还应为安保研究建立安全港，免除对加密项目的出口管制限制。[72]

D. 公司执行《工商企业与人权指导原则》的情况

60. 鉴于监控技术被滥用的风险巨大，应根据国内法禁止颁发出口许可证，除非公司定期证明其在设计、销售、转让这类技术或为其提供支持方面严格履行了《指导原则》规定的责任。这将有效地把《指导原则》确立为公司进入监控市场的前提条件。特别报告员在以往报告中解释了信息和通信技术部门应如何履行其尊重人权的责任(A/HRC/35/22，第 45-75 页)。私营监控公司为履行这些职责，至少必须制订下列各项：[73]

[69] 见《瓦塞纳尔安排》，“IL — 以色列网络安全出口管制政策”(PowerPoint 演示稿)，2016 年 6 月。

[70] 隐私国际资料，第 8 页。

[71] 同上，第 3-4 段。

[72] 同上，第 5 段。

[73] 其中许多标准来自民间社会的资料，可参见本报告增编和特别报告员网站。

(a) 客户政策：明确确认公司有责任在其整个经营过程中尊重表达自由、隐私和相关人权，客户遵守国际人权法是批准和订立销售、转让或支持合同的条件；

(b) 人权尽职调查程序(如人权影响评估)：在公司从事影响表达自由和隐私的活动时启动，如监控产品和服务的设计、销售、转让和服务；

(c) 内部政策和标准合同条款：明确、具体禁止违反国际人权法的产品定制、目标、服务或援助；

(d) 内部流程：确保设计和工程选择纳入人权保障，例如探查滥用并在滥用时触发终止开关的标记系统；

(e) 定期审计方案和人权核查程序：确保其产品和服务的使用符合国际人权法，包括承诺公开披露这些审计和核查程序的主要结果；

(f) 通知程序：迅速向有关政府监督机构(如国家人权机构)或政府间机构(如特别程序投诉机制)报告其工具的滥用情况；

(g) 透明度报告：披露其产品的潜在用途和功能，以及所提供售后支持的类型、滥用事件，以及向执法、情报或其他政府机构或其代理人销售的数量和类型数据；

(h) 与受影响权利持有人、民间社会团体和数字权利组织的定期磋商：讨论其产品和服务的持续或潜在影响以及防止或减轻这些影响所需的人权保障措施，特别关注那些面临以监控为基础的歧视或压制风险的群体，如少数种族、少数民族和传统边缘化群体；

(i) 申诉机制：使个人能够就公司产品和服务协助的侵犯人权行为提出申诉，并对这些申诉提供独立评估和切实的后续行动；

(j) 补救机制：使投诉人能够在独立核实投诉的情况下酌情寻求赔偿、道歉和其他形式的补救。

E. 共同监管举措

61. 这里所述国家和公司的方法可能不足以解决目标监控的全球问题，其本身还缺乏若干重要方面的投入──民间社会行为体的投入，不论是活动人士、技术人员、学者、受害者，还是同属上述一个以上类别的人。涉及国家、工商企业和民间社会行为体切实参与的共同监管治理可为私营监控行业的人权问责制提供一份蓝图。具体而言，为在私营安保行业公司之间灌输问责制和监督而制订的共同监管举措具有指导意义。与私营监控公司一样，私营保安公司所承担的风险与其对国家职能的内在参与有关，尤其是在国家安全领域。因此，对私营保安公司的共同监管需要努力教育公司了解人权关切，并鼓励多利益攸关方参与(基于民间社会包容性审计和监测过程的认证)，这一点也可供私营监控行业借鉴。

62. 私营保安公司的监管环境有两个方面值得在私营监控公司背景下考虑。《蒙特勒文件──武装冲突期间各国关于私营军事和安保服务公司营业的相关国

际法律义务和良好惯例》提出了这种情况下的良好国家做法建议。[74] 这份文件虽然不具约束力，但载列了私营保安公司的现有国际法义务，以最佳做法形式向缔约国、领土国和所属国提出了建议。其公开披露和尽职调查原则早于《指导原则》提出，反映了其中规定的责任。

63. 《私营安保服务提供商国际行为守则》可能也是一种适当模式。该守则的制订得到了民间社会、私营行业和瑞士政府的支持，是少数几种让私营保安公司参与的方法之一。私营安保服务提供商国际行为守则协会是一项多利益攸关方倡议，有各个国家、私营保安公司和民间社会组织的代表参加。这一不具约束力的守则旨在补充监测和监督规定，阐明公司的国际法义务，并建立协会的责任制框架结构。该协会包括大会和理事会。大会由利益攸关方群体代表参加；而理事会则由从三个利益攸关方群体代表选出的 12 名成员组成。值得注意的是，公司的成员资格取决于对守则的遵守，包括协会的认证、审计和核查过程。

64. 如《协会章程》所述，守则的核心思想是促进负责任地利用私营安保服务以及尊重国际人权法。守则本身既概括了国家和私营保安公司及其他私营安保服务提供商的一般承诺，又载列了以下各个领域的具体行为原则，包括：使用武力、拘留、逮捕人、酷刑和其他惩罚、基于性别的暴力、人口贩运、奴役和强迫劳动、歧视、私营安保人员的身份识别和登记。[75]

F. 联合国对监控活动的最新关注

65. 人权理事会为切实发挥效力而设立了若干工作组，其任务是处理关于执行国际人权准则的关键主题。人权理事会或其特别程序可考虑设立一种新的机制，关注个别任务负责人可能无法保持关注和评价的特殊案件。新的工作组、交叉授权工作队或授权行动计划可以专门特别关注针对国家监控干涉基本人权的指控——这涉及人权法的许多领域，从而涉及特别程序的许多任务。

五. 建议

66. 各个国家：

(a) 各国应立即暂停出口、销售、转让、使用私人开发的监控工具，暂停为其提供服务，直至制订符合人权的保障制度为止；

(b) 购买或使用监控技术的各国(“购买国”)应确保国内法律仅允许这些技术根据目标合法性、必要性和正当性的人权标准使用，并建立法律补救机制，且此机制要符合其为监控相关侵权的受害者提供有效补救的义务；

(c) 购买国还应建立确保公众或社区核准、监督和控制监控技术购买的机制；

[74] 见瑞士联邦外交部和红十字国际委员会，《蒙特勒文件——武装冲突期间各国关于私营军事和安保服务公司营业的相关国际法律义务和良好惯例》(伯尔尼，2008 年)。

[75] 另见 Sarah McKune 资料，第 10 页。

(d) 出口或允许出口监控技术的国家(“出口国”)应确保有关政府机构在处理出口许可证申请时征求公众意见并展开多利益攸关方磋商。所有与出口许可证有关的记录都应尽可能地加以保存并供查阅。各国还应为安保研究建立安全港，免除对加密项目的出口管制限制；

(e) 出口国应加入《瓦塞纳尔安排》，并在符合国际人权法的范围内遵守其规则和标准；

(f) 《瓦塞纳尔安排》参与国应制订一个框架，在此框架下，任何技术的许可都将以国家人权审查和公司是否遵守《工商企业与人权指导原则》为条件。这种框架可以通过特别设立的人权工作组来制订。此外，还应就许可决定、监控相关侵犯人权行为和数字漏洞处理的透明度和问责制，制订明确、可执行的指导方针。

67. 各个公司：

(a) 私营监控公司应公开确认其尊重表达自由、隐私和相关人权的责任，并从产品开发的最初阶段直至整个经营过程均纳入人权尽职调查程序。这些程序应确立“设计纳入人权”、与民间社会(特别是有被监控风险的群体)定期协商以及对有人权影响的商业活动的健全透明度报告；

(b) 公司还应采取健全的保障措施，确保其产品或服务的任何使用都符合人权标准。这些保障措施包括禁止违反国际人权法的定制、目标监控、服务或其他使用的合同条款；标记、防止或减轻滥用的技术设计特征；以及人权审计和核查过程；

(c) 如果公司发现其产品和服务被滥用于侵犯人权，则应立即向有关的国内、区域或国际监督机构报告；另外还应建立有效的申诉和补救机制，使监控相关侵犯人权行为的受害者能够提出申诉并寻求补救。

68. 联合国：本组织，特别是人权理事会，应设立一个工作组或交叉授权工作队，监测借助数字监控侵犯人权行为，并就其趋势和个案提供建议。

69. 所有利益攸关方：各国、私营部门、民间社会和其他相关利益攸关方应制订共同监管举措，制订基于权利的私营监控行业行为标准，并通过独立审计及学习和政策举措实施这些标准。