联 合 国 A/HRC/28/39

大 会

Distr.: General
19 December 2014
Chinese
Original: English

人权理事会
第二十八届会议
议程项目 2 和 3
需要理事会注意的人权状况
联合国人权事务高级专员的年度报告以及
高级专员办事处和秘书长的报告

增进和保护所有人权——公民权利、政治权利、
经济、社会和文化权利，包括发展权

人权理事会关于数字时代隐私权的小组讨论会纪要

联合国人权事务高级专员办事处的报告

摘要

本报告是根据人权理事会第 25/117 号决定提交的。报告概述了人权理事会第二十七届会议期间于 2014 年 9 月 12 日就数字时代隐私权问题举行的小组讨论会的情况。按照人权理事会的要求，小组讨论会研究了在国内和域外监控、截取数字通讯及收集个人数据(包括大规模采用此类做法)的背景下，增进和保护数字时代的私隐权问题，并查明挑战和发现最佳做法，同时考虑到联合国人权事务高级专员提交的报告。

GE.14-24707 (C) 190115 200115
1424707

目录

一. 导言

1. 人权理事会依照第 25/117 号决议，于 2014 年 9 月 12 日举行了一场关于数字时代的隐私权的小组讨论会。讨论会考虑了联合国人权事务高级专员提交人权理事会第二十七届会议的报告(A/HRC/27/37)提出的问题。

2. 按照人权理事会的要求，小组讨论会研究了在国内和域外监控，截取数字通讯及收集个人数据(包括大规模采用此类做法)的背景下，增进和保护数字时代的私隐权问题，并查明挑战和发现最佳做法，同时考虑到人权高专的报告。

3. 小组讨论会由人权理事会主席担任主席，由诺丁汉大学副教授 Marko Milanovic 主持。联合国人权事务副高级专员致开幕词。小组成员包括：美洲人权委员会表达自由问题特别报告员 Catalina Botero、哥伦比亚法学院路易斯·亨金人权和宪法权利教授 Sarah Cleveland、法国电信企业社会责任问题副主任(电信工业对话前主席)Yves Nissim、国际隐私机构法律总监 Carly Nyst。

4. 人权理事会在第 25/117 号决定中，请人权高专办在理事会第二十八届会议上提交一份小组讨论的简要报告。本报告就是依照该请求提交的。

二. 联合国人权事务副高级专员的开幕词

5. 副高专指出，数字通信技术在极短的时间内便为人类互动的方式带来了革命。对数百万人来说，数字时代是一个解放的时代，它也许是世界有史以来最伟大的解放运动。她举例说，在为 2015 年后可持续发展目标制定框架而举行的开放对话和磋商中，有逾百万人以数字形式参加，该框架呼吁充分纳入人权。她强调，人权维护者、活动家、民主声音、少数群体和其他人现在能够通过数字平台沟通，并可以此前难以想象的方式加入到全球辩论中来。

6. 副高专还指出，这些数字平台在监视、截取和数据收集面前非常脆弱。随着关于利用这一脆弱性的政策和做法在全世界被曝光，人们对此深表担忧。她补充道，监控活动会为人权带来极为现实的影响，这包括隐私权、表达和见解自由权、集会自由权、家庭生活和健康权等。尤其是，通过数字监控收集的信息被用于针对异见者；也有可靠报告表明，被用于收集信息的数字技术导致了酷刑和其他形式的虐待。

7. 副高专回顾称，在第 68/167 号决议中，大会要求人权高专呈交一份报告，阐述“在国内和域外监控和(或)截取数字通讯及收集个人数据、包括大规模采用此类做法的背景下，增进和保护数字时代的私隐权问题”。报告已提交人权理事会第二十七届会议。报告以专家磋商和深入研究为基础，对国家和国际立法及判例进行审查，并编汇了来自广泛来源的信息，包括一份对利益攸关方的问卷的回复。

8. 报告明确指出，国际人权法为增进和保护隐私权提供了一个强有力且普遍的框架，包括在国内和域外监控、截取数字通信以及收集个人数据等方面。然而，许多国家的做法暴露出国家法规和执法缺失，程序保障薄弱，有效监管不足。所有问题都在某种程度上导致了任意或非法侵害隐私权行为的广泛有罪不罚现象。

9. 副高专回顾称，人权高专的报告审查了国际人权法对隐私问题的规定，包括网上通信中“干涉隐私”的含义，该背景下“任意和非法”干预的定义、保护谁的权利和在哪里保护等问题。例如，关于干涉隐私的构成要素问题，收集通信数据显然能全面知悉个人行为、社会关系、私人偏好和身份，其范围甚至超过读取某人邮件所获得的信息。无论数据随后是否被查阅或使用，对通信数据的收集和截取都可能因此构成侵犯隐私权行为。就是由于存在对电子邮件通信和其他形式数字表达的大规模监控方案，才对隐私权造成了侵害；国家有责任表明其干预既不是非法的，也不是任意的。

10. 报告在谈及“任意”或“非法”侵害隐私时指出，国家对电子通信数据的监控若根据法律进行，则可能成为一种合法的执法措施。但国家必须表明该监控针对具体风险的必要性和相称性。强制留存第三方数据，即电话公司和网络服务供应商被要求储存其客户通信的元数据，以供执法和情报机构随后使用，这既非必要也不相称。

11. 报告强调，副高专回顾称国家有义务确保个人隐私受到法律保护，免遭非法或任意干预。所有形式的通信监控必须以向公众公开的法律为基础，且该法律必须与有关国家的宪法机制和国际人权法保持一致。秘密规则和对法律的秘密解读，即便是由法官作出的，也不符合法律应明确且公开的原则。凡是赋予安全和情报机关等行政机构过大的酌情裁定权的，都不成其为法律或规则。

12. 副高专还提到了对域外监控和截取数字通信问题的担忧。报告总结了人权事务委员会和国际法院在确定国家何时可以行使管辖权方面的工作，指出无论国家何时行使权力或有效控制，都应履行其人权义务。假如国家行使权力或有效控制，对数字通信基础设施进行监控，则无论在哪里进行，都应履行国家的人权义务。这应包括直接窃听或侵入通信基础设施，以及国家对实际控制数据的第三方行使监管管辖权等等内容。

13. 报告回顾：国际人权法还明确规定了非歧视原则，各国必须采取措施确保任何干预隐私行为符合合法性、相称性和必要性的原则，无论通信受到监控的人的种族、国籍、地区或其他地位如何。

14. 报告还提到，在法律和实践中保护隐私权，程序保障和有效监督是至关重要的。缺乏有效监督助长了在数字环境中对任意或非法侵犯隐私权行为的有罪不罚。缺乏独立监督的内部保障在遏制非法或任意监控措施方面明显缺乏有效性。适当的保障必须包含独立的民间监督和政府各部门的参与，以确保法律的有效保护。国家在法律上有义务以司法、立法或行政形式，通过公开且开放的程序，对通过数字监控侵犯隐私的行为作出有效的补救。

15. 最后，副高专提到私营部门的作用，高级专员的报告也讨论了这一问题。政府愈加依赖企业来开展和协助数字监控。在某些情况下，企业提供用户数据，可能有其合法理由。但当该要求侵犯人权法时，或信息以违反人权法的方式被使用时，这些企业就可能成为人权侵害活动的同谋。人权理事会于 2011 年 6 月 16 日在第 17/4 号决议中核可的《工商业和人权指导原则》为预防和处理工商业活动对人权的不利影响提供了一个全球标准。《原则》明确表示，保护人权的责任适用于企业全球业务的始终，无论其用户所处地点如何，且无论国家是否履行了其自身的人权义务。许多企业对这些问题的认识明显不足。

16. 副高专最后指出，政府在已经采取的、可能影响到隐私权的措施方面缺乏透明度，常常使克服差距和行使问责制的努力极为艰难。她在结尾时说，随着有关这些措施的信息公之于众，明显需要进行进一步的探讨和深入分析。

三. 小组成员的发言

17. 在回答主持人的问题时，小组成员起初的发言关注与隐私权的国际法框架相关的问题，包括程序性保障、有效监督、获得补救的权利以及商业部门的作用。

18. 国际隐私机构法律总监突出了隐私权在任何民主社会中的重要性，并强调了隐私同人的尊严的联系。她指出，隐私权是其他权利的一个基本前提和保障，因为它使个人得以发展能够自由表达的思想和想法，得以选择信奉哪个宗教、支持哪个党派。Nyst 女士解释说，隐私权首先出现在国际法中是《世界人权宣言》；《宣言》的准备工作表明，当时的起草人不仅清楚有必要把隐私权纳入进来，也清楚通信隐私权非常重要。

19. Nyst 女士指出，日常发生的许多普通行为之一是“通信”，例如发送电子邮件或短信、进入银行账户、在互联网上搜索资料，或获取政府服务。任何数字通信都需要私人数据绕行全世界，经过许多私营公司的电缆之后才到达目的地。技术对隐私构成的挑战，是确保国家履行尊重、实现和保护隐私权的义务，私营部门的责任在数字时代意义重大。她指出，法律框架已经存在，因为隐私权已经载入多数国际和地区人权条约和许多国家的宪法，这些文件如何适用需要得到新的理解。

20. 美洲人权委员会表达自由问题特别报告员提到，互联网创造了自由表达、通信和信息交换的机遇。她指出，同时，捕获、存储和管理大量数据也已更为容易。信息，不论是内容数据还是元数据，极可能透露出个人或社群私生活中最私密的方面。她指出，法律框架没有跟上数字时代技术发展的步伐；并强调，需要结合表达自由、隐私权和其他相关人权，规范信息的收集和分析。

21. Botero 女士进一步指出，监控政策可能对人权造成广泛影响。她提到监控直接或间接地影响到表达自由权，直接影响在于言论自由权因监控而无法匿名行使，间接影响在于单单由于监控的存在，就会引起“寒蝉效应”、灌输恐惧和禁

镉，并使个人谨言慎行。她解释称，由于表达自由权是一项纲领性的权利，侵犯该权利可能导致对其他权利的侵犯，包括对结社自由、集会自由、宗教自由和健康权的侵犯。由于监控活动对整个人权架构构成潜在影响，因而国家需要修订法律以限制监控方案，其中应包含遵守必要性和相称性原则，以及适当的监测机制。Botero 女士解释称，由于互联网是一个特殊且独特的通信媒介，能使人们自由、多元和民主地行使表达自由权，因此互联网的治理是一件意义尤其重要的事。她指出，为了确保所有相关观点均得到妥善考虑，国家必须确保与互联网治理相关的所有行为方平等参与，并在国家和国际层面巩固增强官方、学界、民间社会、科技界和私营部门间的合作。

22. 哥伦比亚法学院路易斯·亨金人权和宪法权利教授说，所有人，不论其处所或国籍，都受到人的尊严所普适和固有的人权的保护。她指出，国家的监控做法有时对公民和非公民加以区分。Cleveland 女士就此强调，人权事务委员会认可，《公民权利和政治权利国际公约》第二条规定的不歧视原则对公民和非公民均予保护。[1] 因此，公民和非公民的隐私均不受非法或任意干涉。她还指出，国家常常在自己的领土上进行监控，以压制表达自由和结社自由，或惩罚记者、异见人士和其他政府批评人士。根据《公民权利和政治权利国际公约》第十七条，国家有义务尊重和确保在其境内或受其管辖的所有人的隐私权。

23. Cleveland 女士强调，《公民权利和政治权利国际公约》中的保护适用于在其他方面受一国管辖的人，这是国际法院[2] 和人权事务委员会[3] 所承认的。这也是能将《公民权利和政治权利国际公约》的文本与其内容、目标和目的最好地统合起来的解读。人权事务委员会早就认识到，一国不可通过在境外从事本国国内禁止从事的行动来逃避其国际人权义务。Cleveland 女士解释说，网络活动超越领土，在数字监控中，国家可能会对人或领土进行最少的实际控制，在某一地点的活动可能会影响到另一地点的某一个人。她强调说，这种行为可能需要国家承担人权义务。最后，她指出，隐私权适用于非公民和身处境外的国民，这并不意味着监控活动本身总是非法的。为符合正当的国家安全和执法利益而对隐私权实行的任何限制，都必须，同时充分考虑国际人权法规定的要求；尤其是，限制不得是任意的或非法的。

24. 主持人 Milanovic 先生提到私营部门的作用时指出，私营公司为自身目的而汇总数据，也可能不得不参与政府的计划。他重点提到政府与私营电信公司的关系，提出私营公司应如何回应政府要求的问题。法国电信企业社会责任问题副主任指出，电信公司可能收到各种各样的要求，去收集或保存有关客户的信息，或

[1] 见人权事务委员会关于不歧视的第 18 号一般性意见(1989 年)。

[2] 见国际法院，《在巴勒斯坦被占领土修建隔离墙的法律后果，咨询意见》，《2004 年国际法院案例汇编》，第 136 页；和《刚果境内的武装活动(刚果民主共和国诉乌干达)判决》，《2005 年国际法院案例汇编》，第 168 页。

[3] 见人权事务委员会关于《公约》缔约国的一般法律义务的性质的第 31 号一般性意见(2004 年)。

使其网络“待命窃听”；与此相关的问题在阿拉伯之春期间变得更加鲜明。电信公司收到政府的要求，有时是在枪口下，这些要求可能影响其客户的言论自由权和隐私权。这使得这些公司成立了电信业表达自由和隐私对话组织，以联合解决电信部门中与表达自由和隐私权相关的问题。[4] 对话组织于 2013 年 3 月 12 日发布了一套共 10 条的指导原则，这套原则受到了《工商业与人权：实施联合国“保护、尊重和补救”框架指导原则》的影响。对话组织发布的原则探讨了与电信业相关的隐私和表达自由问题，具体探索了政府保护人权的义务和电信公司尊重人权的责任之间的相互作用和界限。

25. 关于挑战，Nissim 先生强调，电信公司在诸多国家拥有许多实地工作人员，他们的安全和安保是一个绝对优先事项，这是第五条指导原则认可的。[5] 他还指出，虽然参与电信业对话的公司想要维护人权，特别是表达自由和隐私权，但必须记住的是，他们与政府订有许可证协议，受到国家法律法规的约束。电信公司需要保护在所在国的员工，因而必需在必要时能与东道国政府进行对话。他指出，有三个紧要事项需要解决。第一，政府不得要求或获准直接进入电信网络。第二，政府向电信公司提出要求的过程必需清晰、透明。第三，虽然电信公司愿意保持所收到的要求的透明度，但透明首先是政府的责任。

26. Botero 女士在谈到合法限制隐私权和表达自由的条件时解释称，任何限制都必须事先由立法确立。这些法律必须准确界定国家得以从事影响隐私权的活动的原因和条件，如截取个人的通信、收集通信数据或对其进行监控或监视。法律不得模糊不清，在解释时不得给予行政机关以宽泛的酌情决定权。法律还必须提供有关监控措施的性质、范围和期限的保障。对隐私权的限制还必须拥有合法目的。就监控而言，国家最有可能依赖的理由是国家安全和打击犯罪。任何限制必须是相称的且严格必要的。这意味着，必须清楚地确立实施限制的需要是真实且迫不得已的，而且其他任何限制性较弱的措施均无法实现这一目标。任何情况下，只有当受保护的利益面临的风险在狭义上大于维护隐私权和表达自由权的一般利益时，方可对这两项权利进行限制。Botero 女士还指出，当受保护的权利涉及某人私生活最私密的方面时，这种标准必须更为严格。为了确保保护合法性、相称性和必要性原则，关于采取限制隐私权和其他权利的监控活动的决定必须得到独立的司法机关的授权。

27. 关于相称性，Cleveland 女士指出，措施应与所涉利益(即国家采取这项措施的利益与个人的隐私利益)的重要程度相称。她解释称，个人的隐私利益越是重大，该措施必须越是严格具体。她提到欧洲人权法院的判例说，在逐案决定哪些措施对实现某项国家利益有必要且相称方面，这些判例为国家提供了借鉴的合理空间，尤其是在国家安全领域。Cleveland 女士还指出，为确保监控制度得到妥

[4] 电信工业对话现由七家运营商和两家销售商构成。见 www.telecomindustrydialogue.org。

[5] 第五条原则是：“公司员工如身处风险之中，应随时努力确保其安全和自由”。

善运用，国家实施程序性保障意义重大。她指出，必需要有法律保障来界定该制度，还要有监督和事后补救措施来确保该制度不被滥用。

28. Milanovic 先生指出，国家经常把对通信内容的收集同对通信数据(即元数据)的收集区分开来；前者比后者受到更强有力的保障。他提出这种区分是否影响到数字通信的问题。Nyst 女士指出，必须毫不含糊地摒弃这些区分，因为它们反映出对当今通信性质的理解已经过时，法律没有因此而更新。她指出，这些区分可追溯到一个信封与信封中的内容确实有所不同的年代；然而看看数字通信，所谓的信封(即元数据)包含着非常敏感、有价值和大量的信息。例如，可从元数据中得到信息，分析后便可获得关于个人政治或宗教信仰的情报。她提到斯坦福大学做的一项研究，表明可从元数据中获取医疗、财务和法律信息。她强调，因此急需重新评估这种区分，这也是人权高专的报告所指出的。Nyst 女士注意到几个国家取得的进展，它们已认识到需要加大对元数据的保护。她还指出，欧洲法院近期废除了完全数据保留法[6]；她最后说，现在的趋势是加大对元数据的保护。然而，Nyst 女士强调，需要进一步指导国内法如何效仿。

29. Nissim 先生从运营商的角度说，电信公司经常出于技术原因把追踪电话等数据保留下来，以确保服务和网络质量。但是他指出，政府要求电信公司把这些信息保留更长时间或提供访问许可时，这些信息就可能被不当利用。他补充说，对政府的任何访问都应进行立法。Nissim 还指出，当信息达到“大数据”级别时，如果它是匿名的，便可以非常积极的方式加以利用，如用于城市规划、交通、通信等。

四. 讨论概要

30. 互动讨论期间，阿尔及利亚、澳大利亚、比利时、加拿大、中国、古巴(代表类似观点国家组)、厄瓜多尔、欧洲联盟、爱沙尼亚、法国、德国(代表奥地利、巴西、德国、列支敦士登、墨西哥、荷兰、挪威和瑞士)、印度、印度尼西亚、爱尔兰、意大利、马来西亚、巴基斯坦(代表伊斯兰合作组织)、罗马尼亚、俄罗斯联邦、塞拉利昂、斯洛文尼亚、阿拉伯联合酋长国、大不列颠及北爱尔兰联合王国、美利坚合众国、委内瑞拉玻利瓦尔共和国的代表团，以及联合国教育、科学及文化组织(教科文组织)分别发言。由于时间不足，智利、缅甸和乌拉圭未能发言。其发言副本张贴在人权理事会外网上。

31. 下列非政府组织的代表也发了言：美国公民自由联盟(与人权观察联合发言)、第十九条协会、进步通信协会，以及韩国联合国人权政策中心。

[6] 见欧洲法院 2014 年 4 月 8 日对合并案件 C-293/12 和 C-594/12 所作判决。

A. 关于数字时代的隐私权的一般评论

32. 许多代表团强调：高级专员就数字时代的隐私权问题提交的报告质量很高，对当前的讨论来说是一个重要的里程碑。许多代表团还表示赞赏联合国人权事务高级专员办事处(人权高专办)和其他机构在法律和实践中保障隐私权方面所开展的工作。

33. 许多代表团欢迎这一小组讨论会；考虑到技术进步已领先于人们对其人权影响的理解，这一话题恰逢其时，讨论非常必要。与会者还指出，人权理事会就此问题举行的讨论会，以及因特网治理论坛等其他论坛举行的讨论会非常重要。

34. 有一个代表团指出，全世界的互联网用户接近 30 亿人，一个自由、安全的互联网对全球各地的人而言都是重中之重。2015 年后可持续发展目标和《2011-2020 十年期支援最不发达国家行动纲领》(A/CONF.219/3/Rev.1)预见，到 2020 年，人人均应有机会接入互联网。

35. 大多数发言表明，正如联合国高级专员已在报告中着重指出的那样，技术创新已经对表达自由产生了积极影响，为全球性的辩论创造了便利，并促进了民主参与。发言指出，数字通信可以作为促进享有人权的工具，已经推动了人类文明的进步，已经为通信、知识和商业带来了新的机遇。隐私对一个自由、公平和开放的社会是必不可少的，人们可以自由表达言论，而无需害怕受到压制或拘留。

36. 然而，大多数代表团指出，同样的技术平台也增强了国家和非国家行为方开展监控、截取和大规模数据收集的能力。一些代表团说，这些平台不但容易受到大规模监控，而且实际上为监控提供了便利。一个非政府组织指出，当网上隐私受到威胁时，互联网上的信任就消失了，剥夺了所有人的安全、匿名和秘密通信的自由，包括记者、博客撰写人和人权维护者在内，对表达自由造成了“寒蝉效应”。另一个非政府组织强调，对所有人而言，尤其是对生活在高压政权下的人而言，通信安全对维护个人自由、人身安全和政治权利至关重要。

37. 有人指出，一些国家的国家权力由于其信息技术基础设施而出现指数级增长。一些代表团着重提出，全世界的电子通信中的很大部分经过有限几个国家，从而为截获私人通信提供了机会。一些国家已经开发出一些技术，允许其访问全球互联网的很多内容、通话记录、个人电子通讯录和大量其他数字通信内容。有人还提到，有报告称某些政府在发生全球性事件时对通信进行监控。几位发言者回顾称，在监控、截获和收集个人数据的问题上，应永远尊重国家主权。

38. 其他代表团指出，一些政府利用网络技术控制其公民的趋势愈演愈烈，这侵犯了他们的表达自由权和获取信息权。有人指出，政治活动人士和宗教少数群体成员被列为目标、被拘留，有时被杀害。一个非政府组织指出，网上监控的效果经常在网下就可以感受到，是限制公民空间的全球趋势的一部分。合法抗议运动受到国家和私人行为方的监视，从而削弱了和平行动和相关权利，尤其是表达自由权和集会权。

39. 多数代表团重申，人们在网下享有的各种权利也应在网上受到保护，这是大会第 68/167 号决议和人权理事会第 20/8 和第 26/13 号决议确定的。

40. 大多数代表团认为，隐私权是自由表达自身观点的一个前提，是民主社会中的基本权利之一。许多代表团指出，除隐私权外，监控还影响到其他权利，特别是表达和言论自由，以及集会和结社自由。有人进一步指出，隐私和表达自由是“相互联系和互相依存的”(见 A/HRC/23/40, 第 79 段)，他们使其他基本权利和可持续发展成为可能并为其创造便利。为了说明这一点，两个非政府组织指出，大规模电子监控可能对记者和律师的工作造成具体危害，损害表达自由、结社自由和获得律师协助的权利。[7] 一个代表团提到试图使媒体沉默的一些做法。另一个非政府组织提到，有的博客撰写人面临恐怖主义指控，部分原因仅在于他们为了保证其隐私而把通信加密、参与数字安全培训。

41. 一个代表团指出，个人经常不知道数据在何种程度上被使用或分享，甚至不知道在他们同意的情况下何时被收集。一些代表团提到了数据受到保护的权利和《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》及其附加议定书；并称该《公约》及其议定书是数据保护领域首部具有约束力的国际文书，是对隐私权的重大贡献。有人希望不要仅仅联想到其生活或往事的某一特定方面，这种愿望是合情合理的，但它可能与知情权冲突，也可能会导致集体记忆的扭曲，就这种情况，有一个代表团引述了所谓的“被遗忘权”。

42. 许多代表团着重指出，为了确保数字时代的隐私权得到保护，国家层面采取了多项措施。教科文组织提到以下方面的工作：数字时代的隐私和表达自由，一份关于互联网的隐私、自由和表达的出版物，关于互联网问题的一项综合研究，包括关于表达自由、隐私、获得知识和信息以及信息社会伦理等问题的一个重点。

B. 隐私权的法律保护

43. 多数代表团强调，国际法已经为隐私权提供了一个清晰框架，隐私权已被载入《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。然而，许多代表团认为，隐私权没有得到落实，需要采取保障隐私权的具体措施。一些代表团指出，单方面、未经授权地访问私人数据和广泛监控的问题需要综合解决；呼吁采取紧急措施，以制止当前的监控做法，保护个人隐私权免遭侵犯。

44. 许多代表团回顾称，对隐私权的任何限制必须基于公开、透明、清晰、综合和非歧视的法律，必须限于为维护民主社会的公共利益所必需的范围。国家对

[7] 人权观察社和美洲公民自由联盟，“监控一切的自由：美国大规模监控如何损害新闻、法律和美国民主(With liberty to monitor all: how large-scale US surveillance is harming journalism, law and American democracy)”(2014 年 7 月)。

个人的任何监控必须是相称和公正的，符合国际准则和标准，受到法治管辖，接受监督。必须有防止滥用的充分适足、有效保障。有人指出，正确界定任意或非法干涉隐私权，可能是今后几年诸多挑战中的一个。有人强调，全面监控可能相当于一种无理侵权。一个代表团指出，必须以《公约》第十七条为基础，讨论其明确规定的限制原则(合法性与任意性)。

45. 几个代表团指出，国家有一些合理的安全关切，包括对恐怖主义和网络犯罪威胁的关切。一个代表团指出，利用互联网从事犯罪或反社会活动的情况在增加。另一代表团指出，维护安全需要情报，包括反恐方面的数字通信情报；而另一代表团则指出，政府有责任保护个人，数据监控可作为执法的一个有效、合法措施。然而，与会者广泛同意，合理的安全关切应放在包括隐私权在内的国际人权法框架下予以解决。

46. 在回答一个关于政府机构间数据分享的问题时，Nyst 说，对直接收集信息和通过分享获得信息应该适用同样的监督和程序性保障。Cleveland 女士指出，人权事务委员会就此表达了关切。[8] 一国内的多个政府机构分享数据可以是合法的，前提是这些机构收集和使用这些数据的目的是相同的，以便确保遵守必要性和相称性原则，从而不侵害隐私权。

47. 一些代表团指出，互联网超越传统存在的地理边界。几个代表团回顾，正如高级专员报告所言，人权法适用于一国在其领土以外行使权力的情形，从而使国家无法通过在领土以外采取国内禁止的行为，逃避其国际人权义务，绕开国内法律。几个代表团回顾称，《公民权利和政治权利国际公约》第十七条必须与《公约》第二条一并解读，第二条规定国家义务适用于在其领土内和受其管辖的所有个人。几个代表团指出，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。尽管许多代表团强调，国家保护隐私权的责任并不止于其边界；一些代表团对宽泛地理解《公约》的境外适用表达了关切，呼吁对第十七条的境外适用问题开展深入探讨。

48. Nyst 女士回顾称，大多数监控发生在一国之内。她就出于监控目的而依据公民身份进行区分的做法指出，这些区分不仅违反不歧视原则，还是一种非常过时、不切实际的方式；因为获知数字通信发送者的国籍即便不是不可能的，也是很困难的。关于就《公约》第二条而言，国家控制电信基础设施能否构成其管辖权的问题，Cleveland 女士说，由于数字通信跨越地域，适当设想人权的境外适用是必要的，从而确保人权在网上和网下得到同样保护。她指出，境外适用有多种方法，其中多数方法的重点是认为境外管辖涉及对某人或某领土实施某种形式的有效控制；按这种方法，可以将行使对互联网基础设施的控制视为行使对领土的控制，对个人权利发生影响，而不论个人所在地点如何。

[8] 见人权事务委员会关于隐私权的第 16 号一般性建议(1988 年)，第 10 段。

49. 有人指出，尊重隐私权的责任取决于几个不同的行为方。一些代表团强调，缺乏有效监督，助长了对非法侵犯隐私权缺乏问责的问题以及依赖内部保障而无独立的外部监督的弊端。与会者强调，需要保护受害者的权利。一个代表团指出，各国应制定独立、有效的国家监督机制，从而确保管理电子监控的规定得到妥善运用。一个非政府组织说，存在以逮捕人权维护者或查出和平集会参与者为目的而实施大规模监控的情况；这中间，法院“盖橡皮章”起到了作用，或者是电信公司通过实名核查制收集到的数据在未经法院审查的情况下就交给情报和调查机关。与会者强调，必需建立有效监督机制，重点关注受害者获得有效补救的权利，包括让独立、公正的司法机关参与进来，作为关键保障。

50. Nyst 女士在回答关于确保法律在实践中的效力和适用的程序性保障和监督机制的问题时解释，实现更广泛、更有效监督的一个根本前提是结束无处不在的保密做法。对为了提供安全而必需采取的活动，政府要提高透明度；政府不得以公众不可控的方式危害基础设施。她还指出，所有人，尤其是法官和律师，都应加强对互联网技术机制的理解，这将帮助他们加强对监控的工作机制的理解。她强调，确保任何监控得到独立、有管辖权的司法当局的授权非常重要。她补充说，个人被告知受到监控至关重要，以便能够获得纠正。她还指出，必需制定更为严苛的独立监督机制，且在技术上理解监控的工作原理，从而使审查安全机构的监控活动对人权的影响成为可能。最后，她指出，特别程序任务负责人，如果具备技术专业知识，就可以在良好做法以及人权框架为保护隐私权所需哪些努力等问题方面提供指导。Botero 补充说，在规范监控的国内标准上不存在统一做法；国家层面的一个好的做法是成立一个专家机构，以具体专注于技术和监控背景下的人权问题。她指出，监督可以通过制度、司法机关、部门间或通过监察专员实施；程序性保障应包括：采取监控措施前得到司法授权，做出监控决定的法律基础和标准应该公开。

51. Cleveland 女士提到国家有义务对侵犯隐私权行为提供有效补救的问题时指出，《公民权利和政治权利国际公约》第二条规定国家有义务给予有效补救。这是一个非常困难的问题，因为个人经常不知道自己已经受到监控，从而因无法证明受到足够伤害而缺乏起诉权。她指出，政府需要提高正在实施的监控项目的透明度，从而允许公众监督。她还指出，监控停止后，个人收到自己受到监控的通知非常重要。她进一步指出，长期规定必须足够宽厚，允许对监控项目提出有意义的挑战。在这方面，她强调，欧洲人权法院要求造成实际伤害的可能性充分即可，而无需表明实际发生了伤害。她指出，保密的司法诉讼问题重重，但某些司法检验却很重要。关键挑战是让这些诉讼尽可能地透明、有效。

52. Cleveland 女士就是否应设立审查监控措施的专门法院这一问题指出，国家需要找到一个满足透明要求和民主监督、同时允许某种程度的保密的办法。一个好的选择是设立处理机密信息的特别程序，但要设立在常规法院中。Nyst 女士就这一点补充说，虽然任命具备技术知识的特别法官有些价值；但法院在处理挑战监控的案件中给予当事方同等地位，这一点极为重要。因此，至关重要的是，不应存在秘密法庭，或对法律进行秘密解读的程序。任何法庭，如果不容许透明

和监督最大化，就不能使个人与国家间的权利失衡得到纠正，实际可能起到使非法监控措施合法化的作用。

C. 有关商业实体的具体问题

53. 几个代表团也提出了私营公司的作用问题。一些代表还指出，公司受到政府的压力，或被强迫交出数据。其他代表团指出，互联网和电信技术跨国公司一直在开发或使用其自身的监控能力，或帮助国家监控个人。Nissim 先生指出，电信公司使用的技术非常复杂，但政府接触得到。他提到诸如“深度包检测”等技术，该技术允许在通讯传播过程中对其内容进行审查，从而允许互联网服务提供商实时监测和分析用户的互联网通信。Nissim 先生指出，这一设备可被电信公司用于改善向客户提供的服务，但也可被政府用于实现监控目的，而电信公司甚至不知道监控正在发生，这在法国电信的运营过程中发生过。[9]

54. 许多代表团请企业和第三方提高其行为的透明度和问责制。一些代表强调，必需更深入地了解中间机构和其他商业实体如何能实现尊重人权的责任的问题，并明确应该由公众和私营部门掌握的监督权力。Nissim 先生确认，透明度是电信公司的一个关键问题，它们承受着改进透明度的巨大压力。他就此指出，他所在公司的首席执行官已经签署了一个数据保护章程，承诺公司将保护客户个人数据的安全；为客户控制他们的个人数据及其使用方式；在处理客户和用户数据的各个阶段实现透明；以及向所有客户和用户提供支持，帮助他们保护隐私、管理个人数据。然而，他指出，自章程签署以来，他的公司已经遭遇两起侵犯隐私事件；他强调，保护数据面受政府干涉一直是一个挑战。他又一次说，必须铭记，虽然几家电信公司致力于实现透明，但政府必须首先实现透明。他还回顾，电信公司受到当地法律的约束，因而规范他们运营的法律框架在各国不尽相同。他指出，现在的一个趋势是，各公司正在全面掌握其运营所在国的法律框架。他指出，在一些国家，法规允许公司提供关于政府要求、或发送给政府的数据的信息，或允许政府这样做，从而实现事后透明。在另一些国家，公司和政府都不能对公司不得不分享的措施实现透明。他指出，电信公司尝试用它们现有的手段来维护国际人权法。他指出，阿拉伯之春期间，某个政府要求他的公司向所有基本客户发送短信息。公司一开始予以拒绝，随后军人被派来重申政府的要求。他的公司按要求发送了信息，随之发送的还有在场一名军人的签字。这个消息虽然很小却很重要，可以使民间社会理解情况。

55. Nissim 先生突出指出了多利益攸关方参与的重要性。为了说明这一点，他提到他的公司面临过的另一个情形，该政府出于几个因素收回了对电信公司提出的要求，其中一个是民间社会公开了这些要求。他指出，他支持在国际层面拟定

[9] 见人权观察:“他们知道我们所作的一切：埃塞俄比亚的电信和互联网监控 (They know everything we do: telecom and Internet surveillance in Ethiopia)”(2014 年 3 月)。

一份法律文书，解决私营实体保护隐私权免受监控措施的义务的问题，示范性法律和最佳做法也将极大帮助各国政府。

D. 前进方向

56. 许多代表团强调，需要继续多利益攸关方参与。他们说，仅有国家的参与是不够的，私营实体、民间社会、科技界、企业部门、学术界和人权专家需要参与讨论。与会者还强调，人权理事会需要进一步参与进来。

57. 几个代表团请各国政府审查与通信监控、截获和收集个人信息相关的程序、做法和法规，以便使其符合二十一世纪的需求，并确保其完全符合国际人权法。其他代表团呼吁建立一个透明的国际制度，配备一个互联网治理的适足国际框架，包括保护个人数据的适当保障措施。一个代表团呼吁在这些问题上制订一项行为守则。几个代表团和非政府组织呼吁人权理事会建立隐私权问题特别报告员任务授权，因为这对给予这些问题特别、持续关注至关重要。

五. 结论

58. 小组成员得出结论，技术进步可能对现行法规构成新的挑战。在这种情况下，业已确立的法律框架，包括国际人权法，将继续适用，即便为了应对新现实而必需调整法律的适用。对于包括在境内和域外监控的背景下增进和保护隐私权的问题，国际人权法框架是清晰的。然而，必需通过适足的国家立法、更强有力的保障措施和监督，在国家层面更好地执行与隐私权相关的国际准则。

59. 小组成员注意到，制定防止侵权的法律保障措施，所有利益攸关方都参与有效监督，这两者都至关重要。独立、公正、有能力的法院必须更多参与进来，并改善其条件，以应对这些复杂的问题。此外，小组成员指出，在监控政策和法规，法律解释和法院判决着两方面，只要有的话，都必须提高其透明度。法律、法规及其解释和适用的方式必须公开。政府访问与通讯相关的数据的权力必须建立在一个清晰和透明的法律框架之上，既容许技术进步，又符合法治以及国际人权准则和标准。

60. 小组成员支持各国、区域组织和非政府组织的观点，强调说，保护、增进以及尊重隐私权要求各利益攸关方持续努力，包括政府、行业、民间社会和国际组织。他们突出了联合国独一无二的能力，可以召集所有利益攸关方，并探索保护隐私权的最有效方式；他们强调，人权理事会应通过普遍定期审议等方式继续解决这一问题，民间社会也应加大努力。人权高专办和高级专员应继续在这一问题上开展工作，特别程序必须在其适当的任务授权范围内开展努力。还必须考虑新设立一个隐私权问题特别程序任务授权，以审查现有挑战以及如何更广义地构思这一权利的问题。

61. 最后，小组成员突出了联合国和其他国际组织在推广国际法律标准上发挥的关键作用，这些标准能指导私营公司为尊重客户和其他用户的人权而采取的行为。企业期待联合国支持促进会员国在国内法中采纳这些标准。国际组织通过推动国际框架，也在支持企业随着技术进步的持续，实现尊重和保护客户隐私权的责任。是否能够起草一部示范性法律或行为守则的问题应该加以考虑。