联合国 A/HRC/35/22

大会

Distr.: General
30 March 2017
Chinese
Original: English

人权理事会
第三十五届会议
2017 年 6 月 6 日至 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

促进和保护意见和表达自由权问题特别报告员的报告

秘书处的说明

秘书处谨此向人权理事会转交促进和保护意见和表达自由权问题特别报告员大卫·凯伊根据理事会第 25/2 号决议编写的报告。在提交理事会的前两份报告中，特别报告员重点讨论了数字时代的意见和表达自由问题，详述加密和匿名工具如何为行使表达自由权提供必要的保护(A/HRC/29/32)，并分析了信息和通信技术部门影响表达自由的方式(A/HRC/32/38)。他将在本报告中阐述提供互联网和电信服务的私人行为者发挥的作用。他首先审查了国家保护和促进网上表达自由的义务，然后评估了数字接入行业的作用，最后提出了一套原则，可用于为私营部门尊重人权的步骤提供指导。

GE.17-05047 (C) 180417 210417
1705047

促进和保护意见和表达自由权问题特别报告员的报告

目录

一. 导 言

1. 各国越来越多地依赖数字接入行业控制、限制或监测网上言论。当当局试图阻止用户使用网站、社交媒体或整个互联网时，常常要求互联网服务供应商予以协助。供应商对便利互联网信息进入一国或一国内部的互联网交换点进行干扰。他们获取私人通信和由电信服务供应商掌握的其他个人数据。如今，许多这类服务为私人所有或经营。无论受到抗议、获得默许还是主动参与，他们往往是国家审查和监测的重要一环。政府对私人行为者提出的要求以及这些行为者的反应可能导致信息交流陷于瘫痪；限制记者安全调查的能力；威慑举报人和人权维护者。私营部门也可能自发地限制表达自由。他们可能为换取付费或其他商业利益而给予某些互联网内容或应用优先权，改变用户接受网络信息的方式。提供过滤服务的公司可能影响其用户获得的内容范围。

2. 国家和私人行为者都可能影响表达自由。国家有保护表达自由的明确义务，但私人行为者对用户有何义务？他们应如何尊重表达自由？他们采取了哪些步骤，用于评估和处理他们对政府行动和政策的反应对表达自由及隐私的影响？他们应当与顾客分享多少有关国家提出的要求和请求的信息？当这些私人行为者直接卷入侵权事件或与这类事件有牵连时，应当为利益可能受到损害的个人或广大公众提供怎样的补救措施？

3. 提供数据接入可能性的私人行为者可发挥调解作用，促进使行使表达自由。可以肯定的是，大多数审查和监控是由国家驱动的，但是，正因为国家经常但并非总是依赖供应商采取行动进行审查，我们作为用户——数字时代卓越进步的受益者——也应当理解这些行为者之间如何互动、他们的互动及独立行动对我们产生何种影响，以及供应商有哪些遵守基本权利的责任。

4. 本报告是从 2016 年开始对信息和通信技术部门进行分析(见 A/HRC/32/38)[1]，经过一年多的研究和协商形成的成果。自开始征集资料以来，[2] 特别报告员共收到来自国家的 25 份资料；来自公司的 3 份资料；来自民间社会、学术界和其他机构的 22 份资料；和一份保密资料。此外，特别报告员于 2016 年 7 月在伦敦召集了一次头脑风暴会议，由“第 19 条”主持；他还于 2016 年 10 月在美利坚合众国康涅狄格州大学人权学院召集了一次专家会议；于 2016 年 12 月在墨西哥瓜达拉哈拉与美洲人权委员会表达自由问题特别报告员举行了一次区域磋商；并于 2017 年 2 月在贝鲁特举行了一次区域磋商。[3]

[1] 感谢任务负责人法律顾问、加州大学欧文分校法学院福特基金会研究员 Amos Toh 提供的专家研究和分析，以及加州大学欧文分校国际司法诊所的法学学生协调实质性和重要的研究工作。

[2] 见 https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/。

[3] 提交的资料可在有关此任务的网站上查阅。举行磋商的情况概述和编写本报告期间收到的投入列入一份补充附件，也可在该网站上查阅。

二. 国家保护和促进网上表达自由的义务

5. 国际人权法规定，人人有权持有主张，不受干涉，有权通过自己选择的任何媒介寻求、接受和传递各种消息和思想，不论国界(见《世界人权宣言》第十九条；《公民权利和政治权利国际公约》第十九条)。人权理事会和大会重申，表达自由和其他权利在网上同样适用(见理事会第 26/13 和第 32/13 号决议；大会第 68/167 号决议；及 A/HRC/32/38)。人权事务委员会、前任务负责人和特别报告员审查了国家在《公约》第十九条之下的义务。简而言之，国家不得干涉或以任何方式限制持有主张(见《公约》第十九条第 1 款；A/HRC/29/32, 第 19 段)。《公约》第十九条第 3 款规定，国家对表达自由的限制只应由法律规定或为下列条件所必须：尊重他人的权利或名誉；保障国家安全或公共秩序，或公共卫生或道德(见人权事务委员会第 34(2011)号一般性意见；A/71/373；及 A/HRC/29/32)。

6. 国家还有义务采取步骤，保护个人的人权免受私人行为者的不正当干涉(见《公约》第二条第 2 款；及人权事务委员会第 31(2004)号一般性意见)。人权法保护个人的权利免受国家侵犯以及免受私人或私营实体侵犯(见第 31 号一般性意见，第 8 段)。[4] 人权理事会 2011 年核准的《工商企业与人权指导原则：实施联合国“保护、尊重和补救”框架》解释指出，国家需要采取适当步骤，防止、调查、惩治和补救私人行为者的侵权行为(见 A/HRC/17/31, 附件，原则 1)。这类步骤包括制定和执行司法、立法、行政、教育或其他适当措施，要求或帮助企业尊重表达自由，并在发生私营部门侵权的情况下提供有效补救(见第 31 号一般性意见，第 7 段；及 A/HRC/17/31, 附件，原则 3 和 25)。

7. 以下列举的政府行动往往未能满足人权法标准。此外，当政府干涉数字接入行业时普遍缺乏透明度。缺乏透明度的情况包括法律含糊不清，为当局提供过度的自由裁量权，以及法律限制第三方披露有关政府获取用户数据和下达禁止公开评论令的情况。缺乏透明度破坏了法治，影响公众对此部门的了解。[5]

A. 关闭互联网和电信服务

8. 关闭互联网和电信服务指的是以违反人权法的方式，故意阻止或扰乱在网上获得或发布信息(见 A/HRC/32/13,第 10 段)。[6] 政府通常在运营网络或为网络畅通提供便利的私人行为者的协助下关闭或命令关闭这类服务。私人机构对网络基础设施进行的大规模袭击，如分散式阻断服务攻击也可能发挥关闭服务的效力。虽然关闭服务常常与整个网络中断有关，但在移动通信、网站或社交媒体及短信应用接入受到封锁、限速或“实际无法使用”时也可能发生。[7] 关闭服务可能影

[4] 另见非洲人权和人民权利委员会，关于生命权的第 3(2015)号一般性意见，第 38 段；见美洲人权法院，“Vel ásquez Rodr guez”案，1988 年 7 月 29 日的判决，第 172 段；及欧洲人权法院，Özel 及其他人诉土耳其，2015 年 11 月 17 日的判决，第 170 段。

[5] 自由在线联盟，工作组 3 的报告：网上隐私和透明度，2015 年 11 月。

[6] 根据立即普及组织的记录，2015 年发生了 15 次关闭网络的情况，2016 年发生了 56 次。第一次记录的关闭网络事件 2005 年 2 月发生在尼泊尔。

[7] 立即普及组织提交的资料，第一部分，第 1 页。

响一个国家的一些城镇或地区，或影响整个国家，甚至影响多个国家，持续时间可能从几个小时到数月不等。

9. 暗中命令关闭网络或在明显没有法律依据的情况下关闭网络均违反《公约》第十九条第 3 款的要求，及限制必须“由法律规定”。乍得当局未能就 2016 年 2 月至 10 月期间一系列关闭互联网和社交媒体的做法向公众提供有意义的解释，导致这类关闭行为非法的假设。[8] 在加蓬，据称在 2016 年选举期间，约有两个星期的时间每天晚上都发生整个网络中断的情况，与政府所说这类服务不会受到干扰的承诺相悖。[9]

10. 根据措辞含糊的法律或规章规定关闭互联网也不符合合法性的要求。在塔吉克斯坦，经修订的《紧急状态法》允许政府在宣布紧急状态后在没有法院命令的情况下阻断移动服务和互联网接入。[10] 法律没有规定何时以及可出于何种目的宣布紧急状态。这一含糊性使当局能够不受限制地任意关闭互联网。在有些国家，当局依靠已过时的法律为关闭互联网寻求托词。[11] 秘密通过和执行的法律和规章也违反了合法性的要求。在美利坚合众国，国家电信协调中心已对公开发布的标准操作程序 303 进行了大量修改，该操作程序是一项行政规章，规定了“中断移动数据服务”的“详细程序”。[12] 虽然这些程序尚未被公开引用，但当局利用其逃避法律审查和公开问责的可能性与《公约》第十九条相悖。

11. 只有在实现《公约》第十九条第 3 款具体规定的目标所必须的情况下，才可对表达自由施加限制，绝不能以打压对民主权利的倡导为由限制表达自由(见人权事务委员会第 34 号一般性意见，第 23 段；及 A/71/373, 第 26 段)。但是，政府常常在示威、选举和其他涉及非常公众利益的情况下关闭网络，几乎或完全不提供任何解释。[13] 在巴林，所称 Duraz 的移动和互联网接入中断，与一名被政府取消公民权的著名宗教领袖住所外的静坐示威同时发生。[14] 据报告，委内瑞拉玻利瓦尔共和国的互联网用户在 2014 年反对政府的大量示威活动期间无法接入互联网。[15] 据记录，在以下国家的选举或示威活动期间及前后也发生了网

[8] 无国界互联网组织提交的资料，第 2 页，TCD 3/2016。

[9] 同上，GAB 1/2016。

[10] 人权高专办，“Preliminary observations by the United Nations Special Rapporteur on the right to freedom of opinion and expression, Mr. David Kaye, at the end of his visit to Tajikistan, press release (9 March 2015)。

[11] 印度，《刑事诉讼法》，第 144 节；Apar Gupta and Raman Jit Singh Chima, “The cost of internet shutdowns”, *The Indian Express* (26 October 2016)。

[12] 美利坚合众国，NCC 标准操作程序 (SOP) 303。

[13] 立即普及组织提交的资料，第一部分，第 5-7 页。

[14] 巴林人权中心，*Digital Rights Derailed in Bahrain* (2016), pp. 13-14。

[15] Danny O’Brien, “Venezuela’s Internet crackdown escalates into regional blackout”, Electronic Frontier Foundation (20 February 2014).

络中断现象：喀麦隆、[16] 冈比亚、[17] 印度、[18] 缅甸、[19] 伊朗伊斯兰共和国、[20] 乌干达[21] 和黑山。[22]

12. 不解释或不承认关闭网络，会造成网络设计旨在压制报告、批评或异见的印象。有关网络中断后发生镇压和国家许可暴力行为的报告导致有人指控国家利用黑暗时期实施或掩盖侵权行为。例如，在苏丹，抗议油价上涨的示威者在 2013 年 9 月受到一次严酷镇压，其间互联网关闭了几个小时。[23]

13. 观察者注意到，在全国统考期间，为了防止学生作弊，已有越来越多的国家采用关闭网络的做法。乌兹别克斯坦在 2014 的大学入学考试期间采用这种做法，也许是第一个使用这一理由的国家。[24] 据称，2016 年，印度、阿尔及利亚、埃塞俄比亚和伊拉克等国当局也命令在考试期间关闭网络。[25]

14. 关闭网络始终未能满足必要性的标准。必要性指的是关闭网络能够实现所称目标，但事实上这类行为往往破坏了所称目标。一些国家政府认为，为了防止恐慌和效仿行为，禁止传播有关恐怖袭击的消息(哪怕是准确报道)至关重要。[26] 但是，已经发现，保持网络联通可能减轻公众的安全顾虑，有助于恢复公共秩序。例如，在 2011 年伦敦发生社会骚乱期间，当局利用社交媒体网络指认犯罪者，发布准确消息，并开展清理活动。克什米尔警方报告了移动电话对寻找恐怖袭击期间被困人士发挥的重要作用。[27]

15. 虽然关闭网络的持续时间和地域范围可能各不相同，但通常都具有不相称性。受影响用户的紧急服务、医疗信息、移动银行、电子商务、交通、学校课程被切断、无法进行投票和对选举进行监测，无法报告重大危机和事件或进行人权调查。[28] 由于关闭网络所影响的重要活动和服务的数量，导致表达自由受到限制，其他基本权利受到干涉。

[16] 人权高专办, “UN expert urges Cameroon to restore Internet services cut off in rights violation”, press release (10 February 2017)。

[17] Deji Olukotun, “Gambia shuts down Internet on eve of elections”, 立即普及组织 (30 November 2016)。

[18] 软件自由法律中心，“Internet shutdowns in India, 2013-2016”。

[19] 自由之家，“Freedom on the Net: Myanmar” (2011)。

[20] 民主和技术中心, “Iran’s Internet throttling: unacceptable now, unacceptable then” (3 July 2013)。

[21] “第 19 条”, “Uganda: Blanket ban on social media on election day is disproportionate” press release (18 February 2016)。

[22] 全球之声，“WhatsApp and Viber blocked on election day in Montenegro” (17 October 2016)。

[23] 人权观察，“Sudan: Dozens killed during protests” (27 September 2013)。

[24] 立即普及组织提交的资料，第一部分；自由之家， “Freedom on the Net: Uzbekistan” (2016)。

[25] 立即普及组织提交的资料，第一部分。

[26] 例如，见人权高专办，“Preliminary conclusions and observations by the UN Special Rapporteur on the right to freedom of opinion and expression to his visit to Turkey, 14-18 November 2016”, press release (18 November 2016)。

[27] 人权与企业研究所，“Security v. Access: The impact of mobile network shutdowns”, case study: Telenor Pakistan (September 2015), pp. 31-32。

[28] 立即普及组织提交的资料，第一部分，第 11-14 页；及全球网络倡议提交的资料。

16. 关闭网络还影响到特定关切地带以外的地带。[29] 2015 年巴基斯坦国庆日游行之前，据称游行地点及预计没有潜在安全威胁的周边地区的移动通信网络均被切断。[30] 在教皇 2015 年访问菲律宾期间，出于安全原因关闭移动网络的地区远远超出了教皇的旅行路线。[31] 特定服务或平台中断后，政府通常以最有效、安全或使用广泛的服务或平台为目标。[32]

B. 政府获取用户数据

17. 如今的政府监控依赖私人所属网络用户的通信和相关数据。获取这类数据常常需要私人行为者的协助，但也可能在其不知情或不参与的情况下取得。与其他监控形式一样，政府获取用户数据可能干涉隐私，既可能直接也可能间接地限制思想的自由发展和交流(见 A/HRC/23/40, 第 24 段)。通过不正当手段获取个人数据使用户受到间接警告，要三思其行为，或者避免发表有争议的观点、避免交流敏感信息和行使其他可能受政府监控的表达自由权(见 A/HRC/27/37, 第 20 段)。

索取用户数据

18. 含糊的法律和规章违反合法性的要求(见 A/HRC/23/40,第 50 段)。例如，马来西亚的《通信和多媒体法》允许当局命令披露有关“发生任何公共紧急事件或涉及公共安全”的“任何通信或通信种类”。该法没有界定引发公共紧急时间的条件，国王的证明即可被视为“这一点的确证”。[33] 在卡塔尔，执法机构享有在发生国家安全或紧急事件时要求服务商提供客户通信资料的宽泛权利。[34] 这些条款使当局有权仅以国家安全为由索取用户数据。因此，用户无法合理准确地预测他们的通信和相关数据在哪些情况下可能被披露给当局。

19. 只有在收到司法当局的命令，证明为实现某合法目的所必须且符合相称性的情况下，服务商才应被迫披露数据。加拿大《刑法》要求执法机构向法官提交索取数据的申请，由法官批准披露刑事调查所需电话记录。[35] 在葡萄牙，当局必须取得司法命令才可强迫披露通信数据。[36] 然而，国内法常常免除向司法机构请求批准使用用户数据的程序。在孟加拉国，当局以国家安全和公共秩序为由获取电信用户的通信数据，只需获得行政机构批准。[37]

---

[29] 人权与企业研究所，“Security v. Access: The impact of mobile network shutdowns”, case study: Telenor Pakistan (September 2015), p. 20。

[30] 同上，第 27-28 页。

[31] Deniz Duru Aydin, “Five excuses governments (ab)use to justify Internet shutdowns” 立即普及组织 (6 October 2016).

[32] “第 19 条”提交的资料，第 2 页。

[33] 马来西亚，《电信和多媒体法》 (1998)，第 266 节。

[34] 卡塔尔，2006 年第 34 号《法令法》。

[35] 见加拿大提交的资料，第 6 页。

[36] 葡萄牙,《刑事诉讼法》，第 187-190 条。

[37] 孟加拉国,《电信监管法》(2001)，第 97 节 (Ka)。

20. 要求私人行为者创建供政府使用的大型用户数据库的法律引发了对必要性和相称性的关切。在哈萨克斯坦，服务商必须将电话号码、电子邮件和互联网协议地址及计费信息保存两年。[38] 俄罗斯联邦要求私人行为者将所有顾客的通话和短信息内容保存六个月，将相关的通信元数据保存三年。[39] 这两个国家还要求在本地保存这些数据。[40] 在移动电话为主要通信手段的国家，强制 SIM 卡登记的法律实际上要求大多数人口披露可识别的个人信息(见 A/HRC/29/32,第 51 段)。强制保留大量用户数据与既定的正当程序标准(如：对错失行为提出个别怀疑的必要性)相悖。

破坏加密

21. 自从特别报告员撰写关于使用加密和匿名的问题的报告(A/HRC/29/32)以来，不必要和不相称地破坏加密的措施在全球愈演愈烈，威胁并破坏用户的表达自由和数据安全。例如，在大不列颠及北爱尔兰联合王国，2016 年的《调查权法》允许国务大臣发布“技术能力通知”，要求供应商取消对通信的“电子保护”——这一做法可能导致强迫“开后门”，或限制或削弱加密。[41] 各国尚未提供充足的证据证明这类脆弱性是保护国家安全和公共秩序方面侵扰性最低的手段，尤其是在可供各国使用的其他调查工具的广度和深度的背景下(同上，第 39 段)。

直接接入

22. 直接接入互联网和电信网络使当局能够在有限的法律监督或问责制背景下截获和监测通信。技术进步提高了执法机构和情报机构在网络运营商不参与和不知情的情况下直接接入网络的能力。[42] 在前南斯拉夫的马其顿共和国 2014 年大选期间，据称情报当局直接接入了该国的主要电信网络，截获了 20,000 多人，包括政治家、活动分子、政府官员和记者的通信内容。许多目标人员还收到了一份自己的电话通话文本。[43] 在印度，当局似乎正在发展一个中央监测系统方案，该方案能够“无需电信服务供应商人工干预，在安全网络上以电子方式提供政府机构要求的目标号码”。[44] 这类活动似乎并未经法律规定，因此即缺乏司法授权，也没有外部监督。此外，这类活动对网络基础设施的安全和完整性构成的风险也引起了对相称性的关切。

[38] 哈萨克斯坦，政府第 1593 号决议(2011 年 12 月 23 日)。

[39] 人权高专办，2016 年 7 月 28 日致俄罗斯联邦政府的信函 (OL RUS 7/2016)。

[40] “第 19 条”提交的资料，第 5 页。

[41] 大不列颠及北爱尔兰联合王国,《调查权法》(2016)，第 253 条；及人权高专办，2015 年 12 月 22 日致联合王国政府的信函 (AL GBR 4/2015)。

[42] 隐私国际提交的资料；及电信行业对话提交的资料，第 3 页。

[43] 隐私国际，“Macedonia: Society On Tap” (23 March 2016)。

[44] 立即普及组织提交的资料，第二部分，第 4 页。

C. 网络中立

23. 网络中立指的是所有互联网数据应得到平等对待、不受不正当干涉的原则，该原则倡导尽可能广泛地获得信息。[45] 在数字时代，只有在各种互联网内容和应用的传播不受非国家行为者(包括供应商)的不正当歧视和干涉的情况下，在不同信息来源之间进行选择的自由才是有意义的。国家促进表达自由的积极义务是网络中立的重要原因，旨在促进尽可能广泛地、不受歧视地获取信息。

付费优先

24. 根据付费优先计划，供应商为某些付费或提供其他商业利益者的某些类型互联网内容提供优先于其他内容的待遇。这类计划实际上为负担得起额外费用的内容供应商提供了互联网快行道，为其他人提供慢行道。[46] 这种将数据分等级的做法影响到用户的选择。用户在使用慢行道获得互联网内容和应用时遇到费用高昂或服务质量低劣等问题。同时，他们被迫使用他们并不知情或没有提供投入、但优先显示的内容。

25. 若干国家禁止付费优先的做法。例如，较早实行网络中立的国家之一荷兰禁止供应商“根据通过这类服务提供或使用的服务和应用确定接入互联网服务的费率”。[47] 美国联邦通信委员会 2015 年的《开放互联网令》禁止“宽带供应商网络管理者直接或间接允许某些内容优先于其他内容……从而换取第三方的(金钱或其他)好处，或使某一附属实体获益”。[48]

零费率

26. 零费率指的是对使用某一特定应用或服务相关互联网数据不收取费用但对其他服务或应用进行计费的做法。零费率安排从数据计划免除某一用户账户中某些互联网服务费，到无需购买数据计划，对某些服务提供免费接入等。[49] 尽管形式多种多样，但因为零费率安排对接入某些内容给予优惠，可能导致计费数据的费用上升。对于勉强可负担计费数据的用户而言，他们最后可能只能依赖零费率服务，导致在获取信息和公共参与方面可能已被边缘化的社区在获取信息方面受到限制。

27. 零费率安排也许为用户提供可能在其他情况下完全不提供的有限接入互联网服务。[50] 然而，用户也许仍无法实现更广泛的互联网接入，导致他们困在永

[45] Luca Belli submission; and Article 19 submission, pp. 7-8.

[46] Dawn C. Nunziato and Arturo J. Carrillo, “The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States”, Georgetown Journal of International Affairs: International Engagement on Cyber V: Securing Critical Infrastructure (2 October 2015), p. 103.

[47] 荷兰,《电信法》,第 7.4a (3)条。

[48] 美利坚合众国，联邦通信委员会， Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 18. This Order, possibly under threat at the time of writing the present report, remains a useful template for net neutrality regulation。

[49] Erik Stallman and R. Stanley Adams, IV, “Zero Rating: A framework for assessing benefits and harms”, Center for Democracy and Technology (January 2016).

[50] Ibid., pp. 4 and 11.

久地被围墙围起来的网上花园里。[51] 关于有限接入最终会发展成熟为全面联通的假设尚有待进一步研究，这可能取决于用户行为、市场条件、人权状况和监管环境等诸多因素。[52]

28. 这些相互竞争的考虑因素导致监管方式的不同。在印度，公众对脸书免费基础服务的关切最终导致对“基于内容对提供给顾客或向其收费的数据服务导致产生歧视性费率”的任何安排的禁止令。[53] 智利、挪威、荷兰、芬兰、冰岛、爱沙尼亚、拉脱维亚、立陶宛、 马耳他和日本都对零费率施加限制。[54] 反之，美国和后来的欧洲电子通信监管机构采取了逐案分析的方针。[55] 采取逐案分析方针的国家应进行认真审查，如有必要，应否决以下安排：基于内容决定零费率；以付费为零费率的条件；或在一类或相似应用当中使某些应用的接入享有优先权(如对某些音乐下载服务而非所有音乐下载服务实施零费率)等。此外，各国应要求企业认真披露网络流量管理做法。例如，智利要求互联网供应商披露互联网接入速度、价格或国内接入与国际接入的速度差异，以及相关的服务保障。[56]

三. 数字接入服务商和表达自由

29. 虽然国家尊重和保护表达自由的职责已充分确立，但创办、运营和维持数字接入的私人行为者也在这方面发挥重要作用。

A. 电信和互联网服务供应商

30. 电信供应商和互联网服务供应商(在本报告中合称“供应商”)提供各种服务。他们主要运营组成互联网的一系列网络并销售接入服务，同时也使用户能够通过移动服务和传统的电话线路交流和分享信息(见 A/HRC/32/38, 第 16 段)。虽然许多地区的供应商仍然为国有企业，但现在已出现越来越多由私人创办和管理的企业。该行业覆盖多个国家的趋势也越来越明显：世界上一些最大的供应商常常通过与国内公司或其子公司合作的方式，在多个国家和地区运营网络。

31. 作为大量信息网络的守门员，供应商面临大量来自政府的压力，被迫接受审查和监控活动。为了在一个国家运营网络，他们必须投资于大量物质和商业基础设施，包括网络设备和人员。这类运营商通常受当地法律和与国家签署的协定

[51] Barbara van Schewick, “Network neutrality and zero-rating”, submission to the 美国 Federal Communications Commission (19 February 2014), p. 7.

[52] Erik Stallman and R. Stanley Adams, IV, “Zero Rating: A framework for assessing benefits and harms” (January 2016), p. 15.

[53] 印度，电信监管当局，“TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016”, press release (8 February 2016)。

[54] Emily Hong, “A zero sum game? What you should know about zero-rating”, *New America Weekly*, Edition 109 (4 February 2016).

[55] 美国，联邦通信委员会，Protecting and Promoting the Open Internet, FCC 15-24 (12 March 2015), para. 21; and BEREC, Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (August 2016) (BoR (16) 127)。

[56] 智利, Ley No. 20.453, art. 24 H (D)。

规定的其他许可证要求的约束。除法律压力以外，供应商还面临法外威胁，如在不守约的情况下，其工作人员和基础设施安全受到的威胁。[57]

32. 虽然一些供应商试图抵抗审查和监控要求，但仍有许多供应商不加严肃质疑即为政府提供协助。据称，虽然法律未提出要求，但美国最大的供应商之一创造了一个“超级搜索引擎”，帮助执法机构获取客户通话。[58] 经济合作与发展组织收到的一份申诉指出，联合王国主要的供应商允许该国情报机构接入其网络和获取客户数据的范围远远超出当时法律要求的范围。[59]

33. 越来越多的供应商正在与媒体和其他所提供内容威胁到网络中立的公司建立安排，也正在大力游说对网络中立标准大打折扣。例如，正当欧洲监管机构制定网络中立准则时，该地区 17 家主要的供应商发布了“5G 宣言”，警告说，“指示性过强”的准则将延迟其对下一代移动互联网连接——即对 5G 的投资。[60]

B. 互联网交换点

34. 互联网交换点能够使一个国家或区域内部不同供应商管理的网络互相交流互联网内容。[61] 这种互联方式使地方或区域互联网内容无需使用漫长的国际迂回线路，从而提高了互联网联通的速度和效率。互联网交换点可能由互联网基础设施公司设立，作为更广泛成套服务的一部分卖给供应商，或作为非盈利或自愿机构运营。[62]

35. 互联网交换点处理的大量内容可能是政府要求过滤或截获的互联网内容。越来越多涉及互联网交换点的审查和监控事件表明，即使其确切作用尚不清楚，但这类交换点是主要的接入瓶颈。例如，接入 YouTube 于 2013 年在巴基斯坦受阻的形式表明，该平台是被互联网交换点而非互联网服务供应商过滤的，使用了一种称为“数据包注入”的方法。[63] 根据在厄瓜多尔运营的一家多国互联网服务供应商泄露的内部备忘录，用户在 2014 年 3 月无法接入谷歌和 YouTube, 因为厄瓜多尔的私人互联网供应商协会(运营该国两个主要的互联网交换点)“在该国政府要求下阻拦接入某些互联网网站”。[64] 披露的有关美国国家安全局进行大规模监视的信息引起技术专家的关切，即该机构利用美国的互联网交换点，截

[57] 电信行业对话提交的资料，第 10 页。

[58] Dave Maass and Aaron Mackey, “Law enforcement’s secret ‘super search engine’ amasses trillions of phone records for decades”, Electronic Frontier Foundation (29 November 2016).

[59] 隐私国际，“OECD complaint against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3, and Interoute”。

[60] “第 19 条”提交的资料，第 9 页。

[61] 见 www.bgp4.as/internet-exchanges/。

[62] Jason Gerson and Patrick Ryan, “A primer on Internet exchange points for policymakers and non-engineers” *Social Science Research Network* (12 August 2012), p. 10.

[63] Zubair Nabi, “The anatomy of web censorship in Pakistan” (2013), p. 4.

[64] Katitza Rodriguez, “Leaked documents confirm Ecuador’s Internet censorship machine”, Electronic Frontier Foundation (14 April 2016).

获大量国内和外国互联网内容。[65] 2016 年 9 月，位于德国的世界最大互联网交换点对该国情报机构的法律命令提出质疑，该命令要求交换点监测通过其枢纽中转的国际通信内容。[66]

C. 内容提供网

36. 内容提供网络是以战略方式分布在世界各地的服务器网络，旨在有效提供网页和其他互联网内容。大型内容制作者依靠内容提供网尽快向用户提供内容。[67] 内容提供网储存由这些平台提供的内容，针对用户索取内容的要求，将内容从该平台服务器发送至网络内部离用户最近的服务器。[68] 此过程加快提供内容的速度，对所在位置离平台服务器较远的用户而言更是如此。内容提供网被视为对抗网站阻截行为的有效保障；以管理某特定网站或平台的服务器为目标的审查措施不会影响内容提供网向用户提供相同内容的拷贝。[69] 内容提供网还是对抗网络中断的重要舷墙。快速接入的需要为其提供了动力，激励其大量投资于能够抵制分散式阻断服务和其他恶意攻击的基础设施和服务。[70]

37. 内容提供网的抗审查性也使它们成为受到不相称地限制表达自由的目标。在埃及，“新阿拉伯”网站 2016 年 8 月受到封锁，接入一些与该网站无隶属关系但共用相同内容提供网的其他网站同时受阻，导致研究者认为当局以该网站作为攻击目标。[71] 在中国，据报告，一个全国滤网封锁了为该国一些大型网站提供内容的 EdgeCast 内容提供网。[72]

38. 因为内容提供网处理来自各种网站和平台的用户提出的互联网内容请求，所以更容易受到政府监控。例如，据报告，容纳世界最大内容提供网的亚马逊云服务[73] 2016 年收到政府获取数据的要求是前一年的一倍以上。[74] 研究者还认

[65] Andrew Clement and Jonathan Obar, “Canadian Internet ‘boomerang’ traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges”, in *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Michael Geist, ed. (University of Ottawa Press, 2015).

[66] De Cix, “Information on the lawsuit against the Federal Republic of 德国” (16 September 2016).

[67] Geoff Huston, “The death of transit?”, Asia Pacific Network Information Centre (27 October 2016).

[68] Vangie Beal, “CDN – Content Delivery Network”, *Webopedia*.

[69] John Holowczak and Amir Houmansadr, “CacheBrowser: bypassing Chinese censorship without proxies using cached content” (2015).

[70] Geoff Huston, “The death of transit?”, Asia Pacific Network Information Centre (27 October 2016).

[71] Leonid Evdokimov and Vasilis Ververis, “Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?”, Open Observatory of Network Interference (27 October 2016).

[72] Joss Wright, “A quick investigation of EdgeCast CDN blocking in China”, blog, Oxford Internet Institute (18 November 2014).

[73] 撰写本报告时，亚马逊云服务提供服务的网站数量为全球最高。

[74] Amazon Information Request Report (June 2016).

为，大规模监控活动以内容提供网作为战略目标，以尽可能收集最多信息，但这些活动具体如何进行以及内容提供网的参与程度尚不清楚。[75]

D. 网络设备供应商

39. 这类供应商提供构成互联网和通信网络基础的硬件和软件。网络设备通常包括路由器、开关和接入点，使多种设备和网络能够相互联接(见 A/HRC/32/38, 第 18 段)。供应商还将其业务多样化，提供可进行无线通话的网络电话设备以及能够使智能设备相互联网的“物联网”技术。[76] 供应商极少面向消费者：他们的主要顾客是网络运营商，如政府、互联网服务供应商或内容提供网，因此，他们需根据这些运营商提出的具体技术标准，包括根据当地法律规定的标准(如执法和国家安全要求)进行网络配置。但是，供应商也可设计或调整设备和技术，以确保与私人或政府的具体要求保持一致。

40. 鉴于其业务模式，供应商必须应对其顾客面临或制造的人权挑战。在监控方面，供应商常常受制于“合法阻截”措施，这类措施要求其网络配置允许政府获取用户数据。[77] 此外，供应商可能承包建立“管理和调解系统”的工作，为网络运营商、政府当局共享截获数据提供便利，以及为处理截获数据的政府系统提供便利。[78] 如果供应商也管理其建立的网络，他们也可能负责代表运营商处理政府获取用户数据的要求。[79]

41. 网络设备的设计和多重用途技术引发了对表达自由和隐私的关切。例如，深度封包检测装置被用于无害技术目的，如网络拥堵管理，但也被用于过滤互联网内容、截获通信内容和使数据流减速。移动网络的配置可随时检测移动电话的位置，以确保可从任何地点接入移动服务，但这类监测也可用于攻击用户。[80]

42. 有证据证明，供应商可能为政府审查和监控提供支持。在美国法院一项未决案件中，思科公司被控设计、部署和帮助中国维护一个被称为“金盾工程”的监控和内部安全网。[81](思科否认这些指控。)[82] 在埃塞俄比亚，一些人权团体认为 ZTE 公司为埃塞俄比亚电信公司设计和安装了一个能够进行侵扰性监控的用户管理数据库。[83]

---

[75] See, for example, Harrison Weber, “How the NSA & FBI made Facebook the perfect mass surveillance tool”, *Venture Beat* (15 May 2014).

[76] Michael E. Raynor and Phil Wilson, “Beyond the dumb pipe: The IoT and the new role for network service providers”, Deloitte University Press (2 September 2015).

[77] 例如，见欧盟理事会 1995 年 1 月 17 日关于合法截获电信内容的决议，公报 C 329；及隐私国际提交的资料，第 2-3 页。

[78] 人权与企业研究所，“Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson” (November 2014), p. 16.

[79] Ibid., p. 17.

[80] Ibid., p. 13.

[81] 美国，District Court for the Northern District of California, San Jose Division, *Doe et al. v. Cisco Systems, Inc. et al.*, Case No. 5:11-cv-02449-EJD-PSGx (18 September 2013)。

[82] John Earnhardt, “Cisco Q&A on China and censorship” Cisco blogs (2 March 2006).

[83] 人权观察，“They know everything we do: telecom and Internet surveillance in Ethiopia ” (25 March 2014)。

E. 其他私人行为者

43. 本报告所述结论和建议适用于上述从事提供数字接入服务的任何实体。越来越多的互联网公司正在将重要的数字接入和基础设施服务纳入其一揽子服务。例如，中国最大的两家互联网公司——阿里巴巴和腾讯现在也提供内容提供网络的服务。[84] 谷歌一直在实验避开传统供应商提供无线接入的方法；2010 年，谷歌公司向一些挑选的美国城市的家庭和企业提供互联网高速连接服务。[85] 该公司还与脸书和微软合作建设海底电缆网络，使其能够无需依赖第三方设备或系统即可联通用户。[86]

44. 标准制定组织虽然不是严格意义上的“行业行为者”，但能够制定技术规范和标准，促成电信和互联网基础设施的互操作性。制定标准时忽视人权因素，可能对表达自由产生不利影响。例如，不能强制将传输层安全性作为超文本传输协议的特征，导致网络内容易受审查和监控。因此，技术界将人权尽职审查纳入制定标准的努力是向正确方向迈出的一步。[87]

四. 数字接入服务商的人权责任

45. 《工商企业与人权指导原则》承认，工商企业拥有尊重人权的责任，无论国家的义务或履行这些义务的情况如何(见 A/HRC/17/31, 附件；及 A/HRC/32/38, 第 9-10 段)。这些原则为企业的人权责任提供了最低基线，敦促企业：公开声明高级或执行官级别管理层承诺尊重人权；开展尽职审查进程，真正“查明、防止、减轻”公司所有业务实际或潜在的人权影响并“实施问责制”；对人权负面影响的补救措施进行规定并开展相关合作(见 A/HRC/17/31, 附件，原则 16-24)。

A. 背景因素

46. 《指导原则》强调，公司在履行人权责任时有必要考虑其运营环境的独特性(同上)。在数字接入行业，必须考虑一些背景因素。

接入服务商提供一项公共产品

47. 数字接入行业从事数字表达业务；其商业可行性取决于在服务商建设和运营的网络内寻求、接收和传递信息和思想的用户。因为私人拥有的网络在当代对行使表达自由权至关重要，所以这些网络的运营者也承担了重要的社会和公共职

[84] 腾讯云（内容提供网）和阿里巴巴云（内容提供网）。

[85] Klint Finley, “Google eyes blazing-fast wireless as a way into your home”, *Wired* (12 August 2016).

[86] Joon Ian Wong, “Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable”, *Quartz* (17 October 2016).

[87] Internet Research Task Force, “Research into human rights protocol considerations” (25 February 2017). Available at https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include_text=1. The supplementary annex analyzes the roles and responsibilities of standards developing organizations in more detail.

能。行业的决策，不论是应政府要求还是基于商业利益作出的决策，都可能直接影响表达自由和相关的人权，这类影响既可能是有利的，也可能是破坏性的。

对接入互联网的限制在全球影响表达自由

48. 该行业的人权影响常常具有全球性，甚至影响到相关企业服务范围以外的市场里的用户。例如，对美国一个互联网交换点的监控可能捕捉美国人和外国人之间的大量通信数据流，甚至完全是外国人之间的通信数据流。同样，网络设计在安全方面的脆弱性影响到所有依靠这一网络进行数字接入的用户，包括离网络很远的用户。因此，公司应查明和处理其活动对一般的表达自由产生的广泛影响，以及其活动对所运营市场当中的顾客或权利所有者的影响。有一点可以确定，他们产生影响的方式可能依公司规模、资源、所有权、结构和运营环境而不同(同上，原则 14)。例如，所有供应商应审查用户的数据请求，确保其遵守最低的规范要求，不论请求的来源如何，也不论受影响用户是谁。多国供应商可能有专门的团队负责对请求进行审查，而小型或中性供应商则可能要求其法律或公共政策团队履行该职责。

该行业易受到国家禁止表达自由的压力……

49. 《指导原则》旨在处理因国内法缺失或执行不力导致企业在问责制方面的差距。[88] 然而，热切执行国内法也有可能导致数字接入行业的人权挑战。例如，国家可能追究供应商的责任，或对他们施加压力，要求他们限制用户在其网络上发布的内容，包括依照有关仇恨言论、诽谤、网络犯罪和冒犯君主等法律施加压力。这类中间商责任为审查提供了强有力的动力：供应商可能认为，不质疑这类规章最为安全，因此对内容进行过度监控，以至于连合法内容最后也受到限制。当局骚扰、恐吓或逮捕工作人员，或试图破坏公司的网络或设备，也导致协助国家审查和监控的压力升级。[89]

但同时拥有确保尊重用户权利的独特地位

50. 该行业发挥双重作用，既是数字接入的提供者，又是国家施加限制的自然关卡，这一点正好加强了该行业作为舷墙防止政府和私人部门超越界限的重要性。例如，供应商通常最有条件抵制关闭网络或拒绝用户数据请求。内容提供网在互联网基础设施中的战略地位使其能够应对导致接入中断的恶意攻击。供应商具有独特资格，可评估其产品是否将被或正被用于便利侵犯人权，尤其是在其进行销售时的尽职审查或正在提供服务时。

[88] Yael Ronen, "Big Brother's little helpers: the right to privacy and the responsibility of Internet service providers", *Utrecht Journal of International and European Law*, vol. 31, No. 80 (February 2015), p. 76.

[89] 2014 年，中非共和国当局要求多国电信服务商 Orange 关闭网络，据报告，该要求“伴随着若不遵守则对个人实施处罚的威胁”。见电信行业对话提交的资料，第 11 页。

B. 尊重用户表达自由的责任

51. 为了履行其人权承诺，数字接入行业应至少为下列活动分配适当资源。虽然这些原则在数字接入环境下得到评估，但是它们与数字经济的其他部门，如社交媒体、商业、监控和搜索等都有相关性。

1. 尽职审查

52. 尽职审查程序使数字接入供应商能够查明、防止和减少其活动对人权产生的影响(见 A/HRC/17/31, 附件，原则 19)。虽然一刀切式的尽职审查方式既不可能也不可取，但人权影响评估可作为评估和处理表达自由及隐私权面临的风险的手段。[90] 尽职审查至少包括以下内容。

有关进行尽职审查的政策

53. 公司应制定明确和具体的标准，用于查明哪些活动影响表达自由并触发尽职审查程序。[91] 公司过去和当前的人权影响以及行业惯例可提供有用的指标。在数字接入行业，这类活动可能包括并购；进入或退出市场；政府或非政府机构要求进行内容限制或获取用户数据；施加或更改对内容的限制及隐私政策；产品在内容审核或加密通信方面的改变；为优先接入互联网内容和应用提供便利的安排；设计、销售和购买网络拦截和过滤设备和技术以及相关的培训和咨询服务等。[92] 这一并非详尽无疑的清单“要求时刻保持警惕并时常更新”，考虑新的商业领域、技术发展及运营环境的其他变化。[93]

需审查的问题

54. 尽职审查进程应至少严格审查适用的地方和国际法律和标准，包括地方法律和人权之间的潜在冲突；公司的产品和服务本身可能导致的表达自由和隐私权风险；减轻和防止这类风险的战略；公司的法律、监管或运营环境对这类战略有效性的限制；以及在公司所有运营活动中促进人权的潜力。[94]

内部程序和培训

55. 虽然公司内部专职从事业务和人权专业的人士至关重要，但尽职审查不应仅仅是这些人的责任，而应有公司内部其他相关职能部门的参与。这就需要不同业务单位(如隐私、执法部门、政府关系、遵约、风险管理、产品开发和运营等部门)与专业人员(如工程师、用户体验调查人员、销售团队和业务执行官)开展对

[90] 进行人权影响评估的大型电信供应商包括 Telia Company 和 Telefonica. 同上，第 7-8 页。

[91] 诺基亚在销售工具中内嵌了一项自动功能，可报告有潜在人权风险的销售行为，同上，第 7 页。

[92] 欧盟委员会,《信通技术部门执行联合国工商企业和人权问题指导原则的指南》(2013)，第 32-36 页。

[93] Michael A. Samway, “Business, human rights and the Internet: a framework for implementation”, in *Human Dignity and the Future of Global Institutions*, Mark P. Lagon and Anthony Clark Arend, eds. (Washington, D.C., Georgetown University Press, 2014), p. 308.

[94] Ibid., pp. 310-312, for a more comprehensive overview of relevant topic areas that due diligence processes should cover.

话与合作。[95] 就隐私而言，研究者发现，在隐私管理方面“要求高级业务部门执行官参与及承担责任”和“业务部门吸收具备隐私保护专门知识的工作人员并要求个人承担隐私方面的责任”等措施，创造了一个有利于保护隐私的环境。[96] 类似的管理做法也可确保企业尊重表达自由。对小型和中性企业而言，这些考虑因素可能要求所有业务部门参与尽职审查活动。[97]

外部专门知识

56. 由于尽职审查程序需要广阔的知识基础，所以应汲取外部、非政府机构的专门知识，包括民间社会、国际人权组织、国际和区域组织人权机制、学术界和技术界的专门知识。多利益攸关方论坛也为共同学习和相互问责提供了机会。例如，研究者认为，是否参与专门针对部门或行业的人权举措，如“全球网络倡议”和“电信行业对话”等举措，与公司在人权方面的表现一致。[98]

征求用户和受影响权利所有者的意见

57. 所有的数字接入供应商都以某种形式影响着最终用户的表达自由。因此，即使公司不直接面对消费者，也应征求最终用户的意见，作为其风险评估进程的一部分。这类征求意见活动区别于以上列举的多利益攸关方参与这种更为宽泛的做法，是一种“双向对话”，旨在“向受影响的利益攸关方(或其代表)征集具体看法或建议，并将这些看法和建议纳入公司的内部决策和执行进程”。[99] 例如，正在高风险运营环境中进行有关经营许可谈判或在设计、测试和推广零费率政策期间，可征求弱势或被边缘化个人和群体的意见。有意义的磋商还应包括定期与民间社会组织外联，这些组织可能真正代表特定群体终端用户的需求和利益，这些群体可能因其宣传，本身面临更大的压力。

持续动态评估

58. 公司应快速根据情况变化或运营环境调整尽职审查程序。例如，设计阶段结束后应继续进行风险评估，并在产品或服务的整个生命周期内定期进行这一评估，考虑技术和基础设施变化、与安全相关的脆弱性、消费者行为的改变，以及公司在其中运营的法律、政治和社会环境的变化等因素。[100]

---

[95] 欧盟委员会,《信通技术部门执行联合国工商企业和人权问题指导原则的指南》(2013)，第 36 页。

[96] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United Sates and Europe* (Cambridge, Massachusetts, MIT Press, 2015), p. 177.

[97] 欧盟委员会,《信通技术部门执行联合国工商企业和人权问题指导原则的指南》(2013)，第 37 页。

[98] 数字权利排名组织提交的资料，第 5 页。

[99] 欧盟委员会,《信通技术部门执行联合国工商企业和人权问题指导原则的指南》(2013)，第 37-38 页。

[100] 工商业与社会责任，“Applying the Guiding Principles on Business and Human Rights to the ICT industry”, Version 2.0: Ten lessons learned, A briefing paper (September 2012), p. 9.

2. 通过设计纳入人权保障

59. 与所有重大技术发展一样，设计和工程方面的选择体现了公共政策考量因素，应以对人权的尊重为指导。例如，一项关键的 5G 技术——“网络切片”技术能够使移动供应商更有效地管理网络流量，满足物联网时代无限扩张的消费者需求。同时，因为网络还可能被“切片”，分成快行道和慢行道，所以可能为接入某些互联网应用提供优先权，导致对纯中立性产生潜在的干涉。因此，公司应确保网络设备和技术方面的创新，尤其是具备多重用途的设备和技术的设计和配置符合表达自由和隐私标准。[101]

60. 在制定促进表达自由和隐私权的措施方面，公司应发挥积极的参与作用。例如，应实施能够识别和防止分散式阻断服务攻击和黑客攻击的数字安全措施，保证在抵制恶意攻击的同时不破坏个人、组织和群体之间的合法互动。配置网络设备，尽可能减少不必要地收集用户信息(在地方法律和选路要求的前提下)，可有效地先发制止过于宽泛的数据请求，因为公司无法提供自己并不拥有的信息。[102] 虽然录入了用户信息，但对是否保留这些信息及保留多长时间施加实际限制，也可限制第三方获取个人数据和敏感数据的范围。

3. 利益攸关方参与

61. 政府、企业合作伙伴和其他利益攸关方参与人权方面的工作，可能防止或减少下游侵犯人权现象。直接与政府打交道的公司应在经营执照和销售合同中争取人权保障，如要求作出保证，在公司不知情的情况下不得接入或更改网络设备(否则可能为侵犯人权提供便利)。在诉讼期间及时干预(如在由民间社会团体或同行公司提出反对审查或监控法的案件中提供书面协助报告)，以及在立法和制定政策过程中进行以人权为导向的游说工作，都有可能促进对表达自由和隐私的法律保护。

62. 与企业合作伙伴之间的安排应促进所有各方履行自己的人权责任。具体而言，制定这类安排时应确保子公司、合资公司伙伴、供应商和分销商均遵守公司制定的表达自由和隐私政策。例如，当地方业务收到非正常审查或监控要求时，公司政策应确保将这类要求提交全球管理层审查。[103] 应向员工和合同商提供举报机制。当公司的业务关系中出现人权方面的关切问题时，公司应逐步发挥杠杆作用，以防止或减少伤害。[104]

63. 公司还可以通过合作行动促进尊重人权。这类合作包括联合外联和向同行公司进行宣传；与区域或国际机构，包括与人权机制和经济机构合作；以及参加行业协会和多利益攸关方举措等。[105] 与用户、民间社会和受影响的权利所有者

[101] “第 19 条”，“Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?” (15 September 2016)。

[102] 电子疆界基金会，“User privacy for ISPs and accidental ISPs”。

[103] 电信行业对话提交的资料，第 13 和 16 页。

[104] SHIFT, “Using leverage in business relationships to reduce human rights risks” (New York, November 2013).

[105] 电信行业对话提交的资料，第 12 页；及全球网络倡议提交的资料，第 7 页。

进行定期磋商也可调动公众对公司抵制政府跨越边界的行为予以支持。跨部门合作可加强已商定的人权最佳做法及标准的规范性力量，对政府和同行公司遵守标准施加更大压力。

4. 减轻风险战略[106]

64. 公司在处理对内容进行监管和获取用户数据的请求时，可制定一些具体政策和做法，以减轻政府限制造成的伤害。

确保限制内容和获取用户数据的请求完全合法

65. 公司必须确保所有关于内容限制和获取用户数据的请求不仅符合地方法律规定的程序和法律要求，而且符合国际上规定的正当程序标准。[107] 因为其侵犯人权的特点，所以这类请求必须得到独立和公正的法院或司法裁决机构许可。此外，公司应要求收到书面请求，其中明确解释提出请求的法律依据，并提供授权官员的姓名、头衔和签名。公司还应力求核实相关官员和政府机构是否有权提出这类请求。[108] 即使并非法律要求，公司也应履行这些程序。此外，公司应保留与提出请求者之间关于每项请求的所有通信内容，以及为执行请求登录使用用户数据的记录，前提是该记录不会造成不正当隐私风险。[109]

对政府请求和法律的范围的解释

66. 含糊和开放式的政府请求和法律框架使公司难以确定这些请求是否符合当地法律。为了减少这一不确定性，公司可制定适用于全公司的政策，要求所有业务单位，包括当地子公司以利于尊重表达自由、隐私和其他人权的方式处理法律的模糊之处。这类政策不仅基于供应商的人权责任，还基于国家遵守适用的人权法和根据地方法律(如宪法、刑法程序和数据保护法)提供相关保护的义务。

67. 在实践中，公司对请求的解释应尽可能确保减小对内容的限制，减少提供的用户数据。例如，“全球网络倡议”建议，当请求过于宽泛时，公司应寻求澄清请求的范围，并进行适当的调整。[110]

对请求和所依据的法律提出质疑

68. 公司应当在一个遵守人权、符合正当程序和法治规范的法律环境中运营。公司应探讨所有法律备选方案，对侵扰性过强的请求提出质疑，如关闭整个服务

---

[106] 本节提供的指导主要获益于电信行业对话提交的资料和全球网络倡议的“言论自由和隐私原则执行指南”。

[107] 例如，见 the Manila Principles on Intermediary Liability and the International Principles on the Application of Human Rights to Communications Surveillance, co-authored by a number of non-governmental organizations。

[108] 全球网络倡议,“执行指南”，第 5-6 页；及电信行业对话提交的资料，第 8-10 页。

[109] 电信行业对话提交的资料，第 8-9 页。

[110] Ibid.

或平台、明显针对批评或异见移除网站的做法，或广泛覆盖未具体说明用户的客户数据请求等。[111]

69. 正如任何有关启动法律程序的决策，公司需考虑一系列因素，如“潜在的有益(人权)影响、成功的可能性、案件严重程度、费用、案件的代表性，以及案件是否构成一个更主流趋势的一部分”。[112] 然而，公司应在决策进程中为人权因素分配更大的总体权重，认真评估对人权造成的潜在好处和风险。例如，公司应对比较有可能成功的过于宽泛的请求提出质疑，即使提出质疑可能导致耗用大量资源；另一方面，如果质疑可能导致不良先例或反作用力，破坏表达自由和隐私，则公司可采取其他替代办法。

5. 透明度

70. 透明度是数字接入行业需尊重的一项关键特征。应在法律允许的范围内尽最大可能披露要求企业协助或参与政府活动的信息。公司应铭记，这类信息主要由民间社会使用，以向法院提出有关侵犯人权的申诉，代表用户向国内或国际机制反映不满之处，或寻求问责制的替代办法。因此，这类披露应该定期持续进行，采用易于使用的形式，提供适当的背景信息。

71. 即使地方法律限制完全透明，公司还是应披露所有相关和可发布的信息。例如，如果公司被禁止披露一项关闭请求的来源或依据，它们依然应该定期提供更新信息，说明受影响服务的情况或是否恢复服务、公司处理问题的步骤，以及事件之后的解释。创新的透明度措施，如发布综合数据和有选择地保留信息，[113] 也可减少禁止公开评论令和其他禁止披露的法律的影响。公司应披露所有其遵守的法律，并在可能的情况下质疑任何阻止或限制其对用户和公众透明的法律或规章。[114]

72. 公司应披露其影响表达自由的政策和行动。相关的披露包括保留数据和使用数据的政策、网络管理做法，以及买卖过滤和拦截技术网站的行为。[115] 公司还应披露有关尽职审查的频率、范围和事由等信息，以及重要结论的摘要。总体而言，公司应参考越来越多研究宝贵的透明度指标的资源和其他透明度方面的最佳做法。还应就设计和执行透明度措施征求用户、民间社会和同行公司的意见。

6. 有效的补救办法

73. 虽然企业责任的某些方面近年来有所进步，但私营部门议程中似乎常常缺少补救步骤。然而，补救是企业责任的重要支柱之一，只要企业“造成或加剧了不利影响”，就应提供补救(见 A/HRC/17/31, 附件，原则 22)。国家承担对企业相关侵犯人权行为进行补救的首要责任，尤其是因其鼓动导致的侵犯人权行为，

[111] Yael Ronen, “Big Brother’s little helpers” (February 2015), p. 81.

[112] 全球网络倡议，“Implementation guidelines”。

[113] 例如，当“Telia 公司被要求中止服务时，该公司未声明这是技术问题导致的结果“，电信行业对话提交的资料，第 14 页。

[114] 电信行业对话，“Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications” (2016).

[115] 数字权利排名组织提交的资料。

如过于宽泛的内容限制、获取用户数据的非法请求及不相称的监控等。但是，未能采取适当尽职审查措施和其他保障措施的公司也可能造成或加剧这类侵权行为。在这种情况下，公司应“通过合法程序提供补救，或在补救问题上给予合作”(同上)。

74. 补救可包括资金和非资金手段(同上，原则 27)。在表达自由受到伤害的情况下，适当的补救可包括诉诸投诉机制和提供有关侵权行为的信息，以及关于不再发生的保证。[116] 对于账户被错误冻结的用户，应允许其发声，为其提供解释和不再发生的保证。[117]

75. 为了应对侵犯表达自由问题，还可改革或加强已有的政策和机制。例如，供应商可改善其内容限制政策，为内容审查团队提供培训，以减少不公平关闭网站的可能性，或过于宽泛的内容限制，如过滤等做法。还可对客户投诉机制进行更新，允许用户报告网络管理做法、商业过滤分类及他们认为属于不正当限制或不公平的其他内容限制做法。

五. 结论和建议

76. 个人依靠数字接入行使基本权利，包括意见和表达自由、生命权及一系列经济、社会和文化权利。但个人在接入方面也常常面临障碍：网络因监控被关闭。本报告主要讨论生硬地通过数字审查制造障碍，剥夺、威慑或排斥言论的问题。本报告没有处理其他严重障碍，如缺乏充分的连接基础设施、政府强加的接入高费用、性别不平等和语言障碍等，这些障碍也可能构成审查形式。[118] 因此，报告的大部分内容侧重国家的作用和义务，但各国已开始越来越多地通过私营部门进行审查。本报告不仅试图处理国家在人权法之下的限制，也讨论了私人行为者在尊重人权方面应遵守的原则。现将在上文分析当中强调的重要建议罗列如下。

各国和人权理事会

77. 人权理事会在第 32/13 号决议中明确谴责违反国际人权法、有意阻止或干扰在网上获取或传播信息的措施，吁请所有国家不要采取或停止采取这类措施。这一谴责对理事会促进网上人权至关重要，应予以补充和具体说明。有意阻止或干扰上网的行为包括关闭电信网络、移动服务、社交媒体平台等服务或使用户无法接入这些服务。本报告中列举了理事会今后的工作，即澄清适用于数字接入行业的规则，这一工作可促进网上的意见和表达自由权。

[116] 电信行业对话提交的资料，第 17 页。

[117] Peter Micek and Jeff Landale, “Forgotten pillar: the Telco remedy plan”, Access Now (May 2013), p. 6.

[118] 全球互联网治理委员会提交的资料； Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, “Situación del derecho a la libertad de opinion y expression en Cuba” (Situation of the right to freedom of opinion and expression in Cuba) (July 2016), p. 20.

78. 理事会和各国明确对隐私的干预和表达自由之间的关系也同样重要。有一点可以确定，必须根据《公民权利和政治权利国际公约》第十七条和其他人权法规范，对干涉隐私权本身的情形进行评估。但是，某些干涉，如获取用户数据的过于宽泛的请求和第三方保留这类数据，都可能在短期和长期对表达自由产生威慑作用，因此法律和政策都应避免这类干涉。各国至少应确保监控是由一个独立、公正和具备资格的司法当局授权进行，该当局应证明监控请求对于保护一项合法目标是必要和相称的。

79. 特别报告员尤其感到关切的是，有关于公司、公司雇员和设备及基础设施受到威胁和恐吓的报告。此外，理事会强调，私营部门的重要作用和为其提供保护的必要性值得思考。各国应审查获得网络接入的所有活动，以确保这些活动合法、必要、相称，尤其应关注这类活动是否对受保护合法目标的侵扰程度最低。

80. 国家对私营部门的保护作用只能到此为止。国家不应倡导私人实体以用户的意见和表达自由为代价换取经济收益。因此，国家应禁止以收费或获取其他商业利益为目的，对某些种类的互联网内容或应用给予优先权的企图。

81. 对于许多国家而言，国家的行为和企业的作用在数字时代的相互关系还是一个新鲜事物。在国际和国内层面一项有益的做法包括制定有关工商业和人权的国家行动计划，以便为所有类别数字接入行业找到查明和处理其各自人权影响的实际道路。

私人行为者

82. 数年来，数字接入部门的个人和公司已理解他们在信息和通信服务大幅度扩张方面发挥的重要作用。这个行业的成功模式应该具备扩大接入范围、效率、多样性和透明度等特征。他们应将本报告中查明的原则作为工具，用于加强他们自身在促进用户表达自由方面的作用。本着这种精神，除了高级别政策作出人权承诺以外，该行业也应当为履行这些承诺分配充分的资源，包括开展尽职审查、基于权利的设计和工程选择、利益攸关方参与、防止和减少人权风险的战略、透明度和有效补救等。同时，企业在设计和落实人权问责措施时应汲取内部和外部的专门知识，确保顾客和其他受影响的权利所有者、民间社会和人权团体提供有意义的投入。

83. 这并非意味着私营公司没有压力，它们其实也承受压力。当国家要求企业参与审查或监控时，公司应力求在法律允许的最大范围内防止或减少其参与对人权产生的不利影响。无论如何，公司应采取一切必要和合法措施，确保它们不造成、加剧或共谋侵犯人权。与企业合作伙伴之间的安排架构应确保所有各方履行自己的人权责任。公司还应寻求通过已存在的业务关系发挥杠杆作用，以防止或减轻对人权的不利影响。