联 合 国 A/HRC/32/38

大 会

Distr.: General
11 May 2016
Chinese
Original: English

人权理事会
第三十二届会议
议程项目 3
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

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。本报告是一系列数字时代互相交织的国家监管、私营部门和表达自由问题的系列研究的开始。在报告中，特别报告员审查了与表达自由和适用于私营部门的原则有关的法律框架，查明了涉及表达自由的信息与通信技术部门主要参与者，并提出了他将在任期内探讨的法律和政策问题。

* 本报告逾期提交，以反映最新动态。

GE.16-07644 (C) 070616 080616
1607644

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. 在数字时代，私营部门的作用似乎无处不在且日益增长，成为历史上最大规模的信息获取途径扩展的驱动力量。私营公司拥有大量供公众发表言论的社会媒体论坛。聚集全球知识和编制索引及设计影响网络可见信息演算规则的主要平台都是私人努力的结果。移动技术基础设施(数十亿人籍此进行通信和接入互联网)有赖于私人投资、维护并由私人所有。执法和情报工作的工具往往来自私营监控和数据处理行业的产品。私营公司设计、制造并往往维护储存最重要的个人数据的设备或服务——包括财务和保健信息以及电子邮件、短信、搜索历史、照片和视频。

2. 在当代行使见解和表达自由在很大程度上要归功于私营产业，后者作为信息门户及表达的中介，对数字空间拥有着巨大的影响力。在数字环境中，提出有关可适用的法律以及私人权威和公共规范的范围等重要问题不可避免。这些私人行为者是否应该承担与公共当局相同的责任？其责任应源于人权法、服务条款、合同安排，还是其他规定？公司行为者和国家之间的关系应如何构建？在受到压力，要求以干涉表达自由的方式开展业务时，私人行为者应采取何种步骤？拒绝进入市场还是撤出市场？告知客户此种压力？随着世界越来越深入地迈入数字空间，“物联网”即将来临，提供指导对于确保促进、保护和享有权利至关重要。

3. 本报告有几个目的。[1] 首先，它力求确认对数字时代表达自由有深切影响的私人行为者的类别。第二，它指出了与私营部门对见解和表达自由的保护以及公共当局确保保护表达自由空间的责任有关的问题。第三，它列出了似乎最需要规范性指导的一些领域。将通过专题报告、国家访问和公司访问以及与各国政府、工商部门和民间社会的沟通和协商处理和加强这些领域。简言之，本报告是特别报告员即将提交的旨在为私营行为者在数字时代保护和促进表达自由提供指导的多份报告中的第一份。

4. 公开的投入和协商进程为编写本报告提供了协助。2015 年 12 月 3 日，特别报告员呼吁各方为报告提供投入。自公布之日起，特别报告员收到了由各国 [2] 提交的 15 份材料和由各组织 [3] 提交的 15 份材料，这些材料均可在特别报告员

[1] 特别报告员谨此感谢其法律顾问 Amos Toh 以及他在加利福尼亚大学欧文分校法学院的学生为编写本报告提供的协助。

[2] 亚美尼亚、萨尔瓦多、爱沙尼亚、希腊、约旦、科威特、毛里求斯、墨西哥、荷兰、秘鲁、摩尔多瓦共和国、罗马尼亚、斯洛伐克、土耳其和美利坚合众国。

[3] 第十九条：国际反对新闻检查中心；进步通讯协会；民主与技术中心；技术与社会中心；新德里国家法律大学通信治理中心；丹麦人权学会；数字权利组织；欧洲数字权利组织；网上自由联盟网上隐私和透明度工作组；全球网络倡议；人权与企业研究所；国际非盈利法中心；因特网学会；韩国进步网—Jinbonet；隐私国际；数字权利排名；新美国组织。

的网站上查阅。[4] 特别报告员还从磋商中获益良多。2016 年 1 月 25 日和 26 日，他在加利福尼亚大学欧文分校法学院与来自民间社会的 25 名成员举行了一次会议，并于 2016 年 2 月 29 日在日内瓦联合国人权事务高级专员办事处与 20 名来自私营部门和民间社会的个人举行了另一次会议。会议概要也可在特别报告员网站查阅。

二. 数字时代的表达自由、国家和私营部门

5. 这份调查分析报告从一个基本问题出发：信息和通信技术部门对促进和保护见解和表达自由应负有多大责任？讨论这一问题需要首先概述国际人权法(根据该法，各国有义务促进和保护表达自由)以及阐述私营部门人权责任的原则。

A. 国际法律框架

6. 《公民权利和政治权利国际公约》和《世界人权宣言》的第十九条都保护人人有权持有主张而不受干涉，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。强调个人在网上和网下享有同样的权利已成为惯例。前任任务负责人着重指出，对网上信息权的限制数量和形式越来越多(见 A/HRC/17/27)，并说明了扩大的数字监控对表达自由的影响(见 A/HRC/23/40)。2015 年，特别报告员强调了加密和匿名在保护和促进表达自由方面所发挥的重要作用(见 A/HRC/29/32)。在联合声明中，特别报告员和区域对口机构强调了关于中间商责任、接入、内容限制等问题以及其他有关网络表达自由的重要议题。

7. 《公民权利和政治权利国际公约》第十九条第 3 款允许限制表达自由(但根据第十九条第 1 款，不能限制意见自由)。根据第十九条第 3 款，要具备合法性，限制必须由法律规定并为尊重他人的权利或名誉或保障国家安全或公共秩序，或公共卫生或道德所必需。限制必须足够明确，而且公之于众，以限制当局的酌处权和向个人提供充分的指导(见人权事务委员会关于第十九条：见解自由和表达自由的第 34 号一般性意见(2011 年))。限制要成为必要，必须不只是有用的、合理的或可取的。[5] 还得到公认的是，必要性要求评估相称性(见 A/HRC/29/32)。相称性要求证明限制措施是可用来实现保护职能的诸种手段中侵犯性最小的一个；必须与要保护的利益相称(见第 34 号一般性意见)。如果限制不符合第十九条第 3 款的标准，个人可享有《公约》第二条第 3 款规定的获得有效补救的权利。

8. 个人在网上还享有一系列其他权利，如隐私、宗教信仰、结社及和平集会、教育、文化和免受歧视等方面的权利。国家既有避免侵犯权利的消极义务，也有

[4] 可查阅 www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx。

[5] 欧洲人权法院，第 6538/74 号申请，星期日时报诉联合王国(1979 年 4 月 26 日)，第 59 段。

确保享有这些权利的积极义务。这些积极义务可能要求公共当局采取步骤，保护个人不受私人当事方行动的影响。[6]

B. 私营部门责任框架

9. 一般而言，人权法并不直接规范私营企业的活动或责任。各种倡议向企业提供指导，以确保其遵守基本权利。人权理事会核准了《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》(见 A/HRC/17/31 和 A/HRC/17/4)。《指导原则》反映现有人权法，重申各国必须确保国家机构和在其管辖范围内的工商企业尊重人权。[7]

10. 《指导原则》提供了一个独立于国家义务或履行这些义务情况之外审议世界各地的信息和通信技术部门中私营工商企业的责任。例如，《指导原则》宣称，工商企业应承担全球责任，避免通过其本身活动造成或加剧负面人权影响，并消除已经产生的影响，并努力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，即使并非它们本身造成了此类影响。[8]

11. 根据《指导原则》，尽责使得企业能够确认、防止和缓解对人权的负面影响，并对如何消除其不利影响负责。[9] 在数字环境下，关于如何应政府要求限制内容或获得用户信息的内部决定、涉及安全与隐私的服务条款、设计和工程选择的采用以及在某一市场提供或终止服务的决定都可能对人权产生影响。

12. 作为透明度措施，《指导原则》规定，工商企业应准备就其如何消除其人权影响对外通报，尤其是在受影响利益攸关者或以受影响利益攸关者名义表示有疑虑时。[10] 联合国人权事务高级专员还敦促信息和通信公司以透明的方式披露风险和政府要求(见 A/HRC/27/37)。有意义的披露可以说明政府提出删除内容和获取客户数据请求的次数和背景、处理这类请求的程序以及对相关法律、政策和法规的解释等情况。公司透明度义务还可能包括有义务披露与服务条款的执行及私人提出的内容管制和用户数据请求有关的程序和报告。

13. 最后，尊重的义务包括在私人行为者造成或加剧了不良影响时，应重视提供补救，包括道义上的补救和赔偿及保证不再发生。[11]

---

[6] 见关于《公民权利和政治权利国际公约》缔约国的一般性法律义务的性质的第 31 号一般性意见(2004 年)。其它国际法准则可能直接适用于私人行为者的活动，如按照国际人道主义法将危害人类罪、战争罪和灭绝种族行为被定为刑事罪行。

[7] 《工商企业与人权指导原则》，第一章(A)(1)。

[8] 同上，第二章(A)(11)-(13)。

[9] 同上，第二章(A)(17)。

[10] 同上，第二章(B)(21)。

[11] 同上，第二章(B)(22)

14. 《指导原则》为确定信息和通信的私人责任提供了一个有益起点，但还有其他几个项目为该部门提出了一些原则。《全球网络倡议的表达自由和隐私问题原则》借鉴了投资者、民间社会和学术界的经验和专门知识。欧洲联盟委员会发布了《信通技术部门执行联合国工商企业与人权问题指导原则指南》。民间社会的有关倡议包括：《马尼拉中介方责任原则》按照表达自由的标准，为中间商规定了基线保护；《非洲互联网权利与自由宣言》在非洲大陆互联网政策的制定和实施过程中促进人权标准和开放原则；“数字权利排名组织企业责任指数”以遵守表达自由和隐私权规范的情况为基础，评估数字空间的一些主要私营行为者。民间社会还采取行动，以制衡参与互联网治理的其他行为者：例如，《关于互联网治理中的信息、参与和透明度的良好做法守则》力求确保以有意义的方式将相关进程公之于众、对所有利益攸关方负责并强调民主参与。

三. 私营部门的作用和公/私监管

A. 私营企业对表达自由的影响

15. 私营部门在组织、接入、充实和监管互联网方面的作用是广泛的，而且常常包括互相重叠的类别。[12]

1. 实现互联网接入

16. 虽然互联网服务提供商具体为其用户提供互联网接入，但电信服务提供商提供更广泛的服务，包括广播、电视、电话和移动通信等服务。主要的跨国公司在其原籍国和全球范围内提供这两类服务。例如，沃达丰公司是英国的一家服务提供商，在 27 个国家拥有并经营网络，并在另外 50 多个国家拥有合作伙伴网络。设在芬兰和瑞典的桑内拉电信的业务遍及整个欧亚大陆市场，俄罗斯移动电信系统公司不仅开展国内业务，而且还在亚美尼亚、土库曼斯坦和乌兹别克斯坦开展电信业务。类似这样的公司往往拥有和维护互联网和电信传输业务的一些重要的技术基础设施，包括光纤网络电缆、卫星或无线电线路。当地和区域市场的互联网服务提供商可能运作有限数量的网络，或从大型运营商租赁网络能力，以为其用户提供互联网接入。服务提供商由国家所有的情况相当常见：例如，瑞士持有瑞士电信 51%的股份，[13] 乌拉圭拥有该国的一个主要电信提供商 Antel。[14]

[12] See, for example, “Strategy panel： ICANN’s role in the Internet governance ecosystem” (23 February 2014)；R. Mackinnon and others, *Fostering Freedom Online： The Role of Internet Intermediaries* (Paris, UNESCO, 2014)；and D. A. Hope, *Protecting Human Rights in the Digital Age* (February 2011).

[13] 见 www.swisscom.ch/en/about/investors/shares/ownership-structure.html。

[14] 见 www.antel.com.uy/antel/; http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/latin-america/uruguayIntro.html。

虽然电信和互联网服务提供商目前是最常见的互联网接入服务提供商，但越来越多的混合公司的目标是提供互联网接入及其他与互联网相关服务。[15]

2. 设计和维护便利信息处理和互联网接入的硬件和操作系统

17. 硬件公司设计和制造将个人接入互联网计算机设备。然而，鉴于被广泛称为“物联网”的雪崩式连通性，当代生活的所有方面都能够进行数字连接，具备个人计算机功能的设备范围在不断扩大，不胜枚举。汽车、冰箱、电视机和手表只是如今将浏览器、讯息和其他与互联网相关功能纳入其中的“智能”装置的几个例子。

18. 此外，电信和互联网服务提供商向基础设施供应商和设备制造商购买设备和其他网络部件，包括网络实体主干。这些产品可以包括简单的路由器和转换器以及深度包检测设备、网络过滤和互联网屏蔽设备和监控监测中心。这些公司还越来越多地从事服务、咨询、培训、甚至运营。

3. 分配网络域名

19. 域名注册机构和注册商在非营利实体互联网名称与数字地址分配机构的监督下，分配和销售互联网网址(即统一的资源定位器(URLs))。目前，世界上最大的注册商拥有超过 6,100 万个域名。

4. 托管信息

20. 网站托管业务使用户能够上传并向其读者或客户的浏览器发送文件和其他材料。这些公司通常还提供数据储存、电子邮件和与客户购买的网站相关的其他服务。

5. 便利信息汇总、分享和搜索

21. 搜索引擎在搜索信息的用户和创造、汇总和发布信息的人员之间提供重要的连接。事实上，搜索引擎的演算规则决定用户看到哪些信息以及信息的优先顺序，可操控演算规则对内容进行限制或排序。然而，信息搜索功能并不是搜索引擎独有的。用户还能通过内容聚合商、专业研究业务、社交媒体平台和职业网络搜索内容。

6. 自己内容的制作和接入监管

22. 在其平台上创作内容或购买在其平台上制作的内容的公司往往拥有此类内容的版权，使其能够将内容接入货币化并进行管理。一些最有影响力的版权持有者是媒体和娱乐公司，包括新闻媒体、出版社、唱片公司和电影及电视制作室。

[15] 例如，谷歌除了其搜索、内容托管和社交网络功能外，将通过谷歌光纤服务提供无线接入服务。见 https://fiber.google.com/about/.

7. 联通用户与社区

23. 公司还提供各种服务，为用户进行跨多个平台的联通，包括电子邮件、网络聊天、讨论主题、社交和专业网络。在这方面最重要的行为者包括电子邮件服务提供商、社交媒体和其他网络平台，及网上公告牌。除了这些平台，新闻网站、电子商务平台和应用商店通过评测、评论和讨论提供分享信息和想法的机会。互联网支付系统还融入了社交网络的功能。

8. 出售货物和服务并便利交易

24. 电子商务促进企业与消费者之间、企业与其他企业之间，或消费者与其他消费者之间的货物和服务销售及其他商业交易。公司提供、推动或安排这些交易以及保障这些交易所产生的大量个人信息的方式可能会涉及其客户的表达自由和隐私。

9. 收集、重新利用和销售数据

25. 上文所述的绝大多数企业收集来自用户及与用户有关的信息，而这反过来又可能被用于有针对性的广告宣传、定制现有服务、减少安全风险或关闭发表侮辱性言论的用户的账户。然而，公司还可能进行信息收集和分析交易，包括设计、定制或销售监控和信息分析技术，或提供促进执法、情报、网络安全和监控行动的咨询服务。

B. 数字时代的监管

26. 互联网上的监管生态系统广泛而多样，涉及国内、区域和国际各层面的、来自公共和私营部门、学术界及民间社会的行为者。信息和通信技术的一些方面── 例如提供电信和互联网服务── 长期以来受到国家和国际监管以及公共监督。搜索、社交媒体和监控技术销售等其他领域也越来越多地受到这种监督，其程度与这些领域对在网上行使表达自由的日益增长的作用和影响是相称的。

1. 技术标准

27. 技术标准和程序确保由互联网和电信网络组成的基础设施、网络和应用程序无缝运作。用于互联网数据流通的有形基础设施，例如网络电缆和卫星，是根据确保其顺利运作的各种技术要求设置和运转的。制定这些要求的组织包括规定电信网络互操作性标准的国际电信联盟；制定了 Wi-Fi 传输标准的专业协会── 电气和电子工程师学会；和制定移动网络的标准的私营国际移动产业协会── 全球移动通信系统协会。

28. 另一组组织为如何交流、储存、整理和展示互联网数据设立和制订技术标准。互联网工程工作队制定和维护的传输控制协议/互联网协议，确定如何通过互联网连接设备及如何在它们之间传送数据。万维网集团规定与网络内容展示和互动有关的标准，其中涉及语言内容和残疾人使用等问题。互联网名称与数字地

址分配机构制定顶级域名注册政策，包括通用域名(如.com、.org、.edu)、国家代码(.cn、.tj、.sg)以及有关具体社区或行业的域名(如.aero)。其子公司，因特网制定号码登记局，管理互联网协议地址的分配，这些地址向每个连接到互联网的设备分配独特的数字标签并以此识别设备。

29. 虽然技术标准对表达自由产生深刻影响，但联合国科学和技术促进发展委员会认为，制定标准往往没有充分考虑到人权关切。[16] 当然，感兴趣的利益攸关方和公众均可参与或观察大多数标准制定机构的工作。然而，虽然技术和设计选择可能对表达自由产生重大影响，但由于有意义的参与要求普遍具有高水平的技术专门知识，人权观点并不总是被列入讨论。[17]

2. 互联网治理和决策

30. 国际法律文书没有明确阐述各国和其他行为者应如何保持互联网自由和开放，许多法律监管也不总是适当的举措。事实上，互联网治理并不仅是专门机构或政府的管辖范围。最近，信息社会世界峰会强调了继续采取纳入政府、公司和民间社会、学术和技术利益攸关方和专门知识的治理办法的重要性(见大会第70/125 号决议)。在全球贸易中，由世界贸易组织监管的国际协定所确立的不歧视原则可能要求国家限制或以其他方式监管非中立的服务。世界知识产权组织还面临着成员国越来越多的要求，它们要求知识产权组织就使它们能够在数字环境中履行条约义务的法律框架提供咨询意见。非洲联盟、欧洲联盟委员会和美洲国家组织等区域机构想方设法确保全球互联网政策的制定和执行考虑到各自区域的法律、特点和关切。[18]

31. 一些制定技术标准的组织也具有决策职能。例如，国际电信联盟制订和协调全球电信政策。互联网名称与数字地址分配机构与各国政府、私营部门、民间社会和其他有关行为者协商，对可注册的顶级域名类型及可对这些域名主张所有权者作出政策判断。

32. 行业主导的倡议还设法应对现有法律条例没有充分阐述的互联网治理方面的挑战。例如，“版权警报系统”召集电影和唱片行业及互联网服务提供商的行

[16] 见科学和技术促进发展委员会闭会期间小组会议，“总结国际互联网公共政策问题”(2014 年 11 月)。

[17] 可以肯定的是，有几个组织已经划出专用资源将人权观点纳入技术讨论。例如，互联网名称与数字地址分配机构已就尊重人权的企业和社会责任建立了一个跨社区工作方，试图分析和理解与互联网名称与数字地址分配机构提出的企业和社会责任有关的问题和潜在解决方案，可查阅 https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN's+Corporate+and+Social+Responsibility+to+Respect+Human+Rights。一些非政府组织也在技术讨论中提出了以人权为导向的意见。例如见 Neils ten Oever,“对人权议定书考虑的研究"，可查阅 https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/。

[18] 例如见，欧洲联盟委员会，《信通技术部门指南》(以上第 14 段)；美洲人权委员会、表达自由问题特别报告员办公室，《表达自由与互联网》(2013 年)。

业协会，以期制订和实施统一的打击在线侵犯版权方针。电信行业对话将电信运营商和供应商召集在一起，处理与其部门相关的表达自由和隐私权问题。

33. 虽然许多这类倡议由私营机构管理，但它们有时也与各国合作或受到其支持。例如，大不列颠和北爱尔兰联合王国网络观察基金会向互联网服务提供商和托管平台提供“通知和清理”服务，提醒它们注意各自网络上潜在的违法内容，也为执法机构调查此类内容提供“独特数据”。

四. 法律和政策问题

34. 信息和通信技术部门的多重作用产生了一些法律和政策问题，国际人权机制应加以重视并详细阐述。

A. 内容监管

35. 在数字时代，与私人行为者有关的许多问题主要涉及内容的监管。例如，各国如何促进或要求删除、审查内容及对通过私营平台和网络寻求、接受和传递互联网内容加以不必要或不相称的限制？私营企业如何应对这些要求和其他外部压力？当私营部门制订和执行其自身的内部政策和标准以保护和促进网上权利时，这些政策和标准会如何影响个人表达自由和信息获取？

36. 在私营网络上传输和私营平台上托管的数字内容越来越多地受到国家和公司的监管。用户生成内容的总量一直在扩大—博客、短信、讨论主题、照片、视频和社交媒体上的帖子只是用户日常创建和共享内容的一小部分类型。管理此类内容所在的网络和平台的公司被称为中间商，它们可能“提供接入、托管、传输源于第三方的内容、产品和服务并编排索引”，尽管它们并不创造或产生这些内容。[19]

37. 国家要求删除内容所依据的理由往往有：诽谤、亵渎、选举相关法规、骚扰或仇恨言论、煽动、知识产权、猥亵和淫秽、招募或“赞美”恐怖分子、保护国家安全和公共安全、保护儿童和防止基于性别的攻击等。长期与表达自由相关联但在数字时代变得日益复杂的问题也引发了国家的监管，包括“被遗忘权”和多元化和多样性(例如，网络中立性)。出于法律、商业和其他原因，中间商自己规定和执行服务条款，以解决其中的许多问题。许多这些问题涉及适当平衡表达自由和其他人权(如隐私，不歧视)的问题。虽然内容监管往往是限制性的，但也

[19] MacKinnon and others, *Fostering Freedom Online*, p. 19； K. Perset, *The Economic and Social Role of Internet Intermediaries* (OECD, 2010).

可能需要传播政府授权或批准的信息，[20] 或禁止对内容和内容提供服务进行差别定价。[21]

1. 国家监管

38. 国家通过各种法律、政治和技术手段监管数字内容。令人关切的趋势包括以下各项。

法律规定不明确

39. 内容管制通常以法律、法院命令或指令或被委以管理电信和互联网有关问题职权的行政机构颁布的细则为依据。例如，中国最近修订了网络安全法，禁止个人和组织利用互联网“扰乱社会秩序”或“损害公共利益”。[22] 同样，尼日利亚正在审议的一项法案草案禁止任何人在“任何媒介”发布“恶意诋毁或煽动公众反对”任何个人、团体或政府机构的言论。[23] 此类措辞赋予当局广泛的酌处权，使其可以决定何种数字表达会侵犯其条款。因此，个人和企业很可能宁可失之过于谨慎，以免受重罚，过滤法律情况不明确的内容并开展其他方式的审查和自我审查。

过多的中间商责任

40. 各国通常要求中间商与之合作实施有关私营网络和平台的规章。例如，作为获得经营许可证的一个条件，互联网和电信服务提供商必须遵守地方法律和法规，在地方法律或其执行本身不符合人权法时，这一合理要求就会带来问题。而获得许可要求较宽松的公司，例如社交网络平台、搜索引擎和域名注册商，面临着国家破坏当地基础设施、威胁其当地雇员的安全或阻止对其平台的本地接入等威胁。

41. 私人行为者也可要求中间商限制或删除内容。例如，当私人当事方声称某人分享或使用内容的方式侵犯其版权或创造的域名侵犯其商标时，往往会导致知识产权申诉。虽然对这一申诉可以利用合理使用以及其他辩护手段，但知识产权框架可能会抑制文化和艺术的表达(见 A/HRC/28/57)。

42. 欧洲法院在“谷歌西班牙诉 Mario Costeja Gonzȧez 案”中根据《欧洲联盟数据保护指令》强迫谷歌移除显示 Gonzȧez 姓名的网页查询结果，尽管并没有

[20] See Vodafone Group Plc,“Response on issues relating to mobile network operations in Egypt” (2011).

[21] 例如，印度禁止服务提供商提供基于内容的数据服务或向其收取有差别的费用(《禁止数据服务差别费用条例》，2016 年)。

[22] 中国,《网络安全法》(2015 年)第九条。

[23] Parliament of Nigeria, A bill for an act to prohibit frivolous petitions and other matters connected therewith，sect. 3 (3).

要求清理最初发布的网页本身。[24] 该决定在欧洲以外被积极适用。[25] 该方针的范围和贯彻带来了隐私权和保护个人数据与寻求、接收和传递载有此类数据的信息之间的适当平衡的问题。

43. 人们越来越多地要求中间商根据一般法律标准评估国家要求和私人投诉的合法性，并依据此类评估移除相关内容或解除链接。例如，坦桑尼亚联合共和国 2015 年的《网络犯罪法》规定，如超级链接提供者“在收到有关当局清除或取消信息接入的命令后立即照办，即可免除该提供者对所链接信息的责任”。[26] 在版权方面，美利坚合众国《数字千年版权法》规定“在线服务和网络接入”提供商只有在接到有关侵犯行为的通知后，“迅速作出反应，清除或取消接入据称侵权或构成侵权活动的主题的材料”，才能免除对第三方内容的责任。[27] 人们批评这些通知和清理框架鼓励不合理的投诉，且未能向设法对内容监管适用对人权问题有敏感认识的公平标准的中间商提供充分的保护。

44. 另一项主要关切是，私营中间商通常不具备确定内容是否非法的能力。美洲人权委员会指出，私营行为者“没有能力根据表达自由和其他人权标准权衡权利和解读法律”。[28] 原因可能是资源有限、缺少监督和问责或是由于潜在的利益冲突。面对潜在的责任，公司可能易于过度自我审查。

法外限制

45. 国家还试图在法律范围之外限制数字内容。一些国家推动社交媒体公司和其他用户制作内容托管机构主动监测和清除内容，而不是等待政府依法提出要求。政府官员还试图说服公司通过公共论坛、活动及在私下讨论中采取“反言论”举措。各国政府也越来越多地根据平台的服务条款，将社交媒体上的内容标记为不适当内容，以促使公司删除内容或注销账户。

法外限制

46. 各国经常在私营部门的协助下屏蔽和过滤内容。互联网服务提供商可屏蔽对具体关键词、网页或整个网站的接入。关于托管内容的平台，过滤技术的类型取决于平台的性质和有关内容。域名注册商可拒绝为列入政府黑名单的公司进行注册；社交媒体公司可删除帖子或暂停账户；搜索引擎可撤销链接到非法内容的搜索结果。政府要求的或公司采用的限制方法会带来必要性和相称性两方面的问

[24] 欧洲法院(大审判庭)的判决，第 C-131/12 号案件(2014 年 5 月 13 日)。

[25] 第十九条：国际反对新闻检查中心提交的材料。

[26] 第 43(a)段。

[27] United States Code, title 17, sect. 512 (c) (1) (C).

[28] 美洲人权委员会，《表达自由和互联网》，第 47-48 页。

题，这取决于所援引的删除理由的合法性及可能删除合法或受保护的表达的风险。

47. 国家监管方面的不明确性，加之中间商须承担责任义务繁重，可能造成过度过滤。即使有效地颁布和实施内容监管，用户仍可能受到不必要的接入限制。例如，一个司法辖区中的内容过滤可能会影响到其他司法辖区用户的数字表达。虽然公司可能设置将过滤只适用于某一特定司法辖区或区域，但在一些情况下，过滤设置会被传递到该平台的其他网络或地区。例如，2013 年经国家授权，由印度 Airtel 公司执行的过滤导致其在阿曼的伙伴 Omantel 拥有的多个网络受到了同样的内容限制。[29]

网络和服务关闭

48. 服务关闭和相关限制是特别有害的内容监管执行手段。这些措施往往以国家安全、维持公共秩序或防止公共骚乱为理由。2015 年，特别报告员与欧洲安全与合作组织、美洲国家组织和非洲人权和人民权利委员会的代表一道谴责互联网“锁死开关”，认为“锁死开关”为非法。[30] 仅在一年中，就有报道称在孟加拉国、巴西、布隆迪、刚果民主共和国、印度和巴基斯坦发生了关闭情况。[31] 特别报告员证实，在其 2016 年 3 月正式访问塔吉克斯坦时，该国发生了电信服务提供商和服务被关闭的情况。[32]

非中立网络

49. 除避免对数字接入进行不必要和不相称的限制之外，各国还有义务确保互联网的自由和开放。网络中立性是一项原则，要求对所有互联网数据、内容和服务平等对待，而不加以不当的区别对待。然而，互联网服务提供商可能采用技术，加速或以其他方式帮助某些内容和服务的接入，同时延缓其他内容或服务的接入(这种做法也被称为“节流”)。互联网服务提供商和内容托管平台之间开展了越来越多的合作，提供接入后者提供的在线内容或服务免费无线数据(也被称为提供“零费用”服务)，这种做法引起了争议。虽然这类措施有损于网络中立性原则，但在真正缺少互联网接入的地区是否可以允许这一做法仍然是一个有争议的问题。

50. 国家对这一领域的监管既零散又不确定。有几个国家承认网络中立性的普遍重要性。例如，罗马尼亚表示，该国“赞成所有旨在保障全体人民以有意义的

[29] Citizen Lab, “Routing gone wild：documenting upstream filtering in Oman via India”(2012).

[30] 关于表达自由和应对对冲突局势问题的联合宣言(2015 年)。

[31] 人权与企业研究所提交的材料。

[32] 联合国见解和表达自由权问题特别报告员大卫·凯伊先生在结束对塔吉克斯坦访问时提出的初步意见(2016 年 3 月 9 日)。

方式接入网上信息的举措”。[33] 提供了具体法律保护的国家更少。[34] 2016 年初，印度电信监管机构发布了一项规章，禁止服务提供商提供或收取“向消费者提供或收取的基于内容的有差别的数据服务费用”。[35] 巴西、智利、荷兰和美国等国家已经在法律和政策中采用了某种形式的网络中立。

2. 内部政策和做法

51. 中间商的政策和规则可能对表达自由产生重大影响。虽然服务条款是监管的主要源头，但设计和工程选择也可能影响内容提供。

服务条款

52. 服务条款是个人接入平台通常必须接受的条件，它往往载有对可分享内容的限制。这些限制是根据当地法律和法规制定的，并反映了类似的禁止规定，包括禁止骚扰、仇恨言论、宣传犯罪活动、无端暴力行为和直接威胁的规定。[36] 服务条款往往制订得较为笼统，以致可能很难以合理的确定性预测哪些内容可能会受到限制。服务条款执行方面的不一致也引起了公共关注。一些人认为，世界上最受欢迎的平台未能充分满足弱势群体的需要和利益；例如，有人谴责这些平台“在与技术相关的暴力侵害妇女行为成为公共关系问题之前，不愿直接处理该问题”。[37] 同时，人们批评这些平台过度热衷于审查各种合法但(或许令有些受众)“感到不舒服的”表达。[38] 公司缺少关于内容为何被移除或账户为何被注销问题的申诉程序或沟通不力加剧了这些问题。服务条款要求个人用实名登记或提供证明使用假名合理的证据，也可能不当地制约封闭社会中的弱势群体或民间社会行为者使用网上平台实现表达、结社或倡议。

53. 各国还越来越多地依靠服务条款删除它们认为不能接受的内容。在反恐中注意促进与保护人权问题特别报告员指出，一些国家已经建立的内容删除机制往往试图删除合法但可能被视为极端主义的内容(见 A/HRC/31/65)。例如，联合王国的反恐网络传送部专门负责删除“具有暴力极端主义或恐怖主义性质的”网上内容，包括通过“利用网站的内容标识机制报告违反该网站[服务条款]的内容”。[39] 这种做法增加了各国依靠私营服务条款绕过反对内容限制的人权或国内法准则的可能性。

---

[33] 罗马尼亚政府提交的材料。

[34] Mackinnon and others, *Fostering Freedom Online*, p. 80.

[35] Prohibition of Discriminatory Tariffs for Data Services Regulations， 2016.

[36] 例如见：脸书服务条款第三(7)节；推特服务条款；YouTube 社区准则；和 Reddit。

[37] 见 https://ourinternet-files.s3.amazonaws.com/publications/no24_web_2.pdf。

[38] 见 onlinecensorship.org。

[39] 全国警察总监委员会，反恐网络传送部；民主与技术中心提交的材料。

54. 大量的申诉和中间商机构日常标注的内容本身就使私营机构的审查工作复杂化。大型平台也可将内容节制外包，进一步扩大内容节制人员和内部决策之间的距离，并加剧执行中的不一致之处。在各个不同市场中运营的中间商机构不可避免地面临“复杂的价值判断”、具有文化敏感性和多样性的问题以及 “涉及法律冲突的困难决定”。[40]

设计和工程选择

55. 中间商组织、分类和排列内容的方式影响用户在其平台上接入和看到的信息。例如，平台运用演算规则预测用户偏好并以此指导个人可能看到的广告、他们的社交媒体聚合的安排方式以及查询结果的出现顺序。[41] 其他自我管理措施，如支持反恐或反骚扰信息的“反言论”倡议，[42] 也影响着用户对与敏感问题有关的互联网内容可能的消费和处理方式。如何协调设计和工程选择所带来的表达自由方面的关切与私营实体按照自己的选择设计和定制其平台的自由这一问题仍尚无定论。

B. 监控和数字安全

56. 国家监控和公司收集和保留数据提出了大量与表达自由有关的问题。例如，各国如何与私营部门合作开展监控活动，以及这种合作如何影响表达自由？当私营行为者发现国家秘密接入其网络或平台上传输或储存的互联网和电信数据时，它们有哪些责任？私营部门在保护网上安全和匿名性方面有哪些责任？

57. 无论是国家或还是私人行为者都在越来越多地对私营网络和平台上传输或储存的数字通信和数据进行监控和其他形式的干预。不必要和不相称的监控可能破坏网上安全和信息与想法的获取(见 A/HRC/23/40)。监控可能对普通公民的网上表达产生寒蝉效应，他们可能因担心被不断追踪而自我审查。监控对广泛的弱势群体的表达自由造成的影响更大，这些群体包括种族、宗教、族裔、性别和性少数群体，某些政党的党员、民间社会、人权维护者、记者、律师等专业人员和工会会员，暴力和虐待行为的受害者以及儿童(见 A/HRC/29/32)。国家的监控能力可能取决于工商企业与国家合作或抵制此种监控的程度。

[40] Emily Taylor, *The Privatization of Human Rights： Illusions of Consent, Automation and Neutrality*， GCIG Paper No. 24 (2016).

[41] 技术与社会中心和数字权利排名提交的材料。

[42] See, for example, Home Affairs Committee, Oral testimony of Anthony House， Google Europe, Middle East and Africa (2 February 2016).

1. 关于提供客户数据的要求

58. 由于互联网服务提供商、社交网络平台、搜索引擎、云服务提供商和其他公司传输或积累数量巨大的客户数据，政府根据当地法律和法规提出提供用户信息的要求数量也开始增加。多个主要的互联网公司报告称此类要求有所增加。[43] 其中许多要求是执法和情报机构发出的。国家对这些要求的监督各不相同，包括事前司法授权、[44] 高级别行政批准 [45] 以及完全不予监督。许可证协议和法律可能会限制私营部门抵制这些要求或强制问责的能力。甚至内容托管平台(在其运营的某些司法辖区没有实体办事处)也可能面临服务被整体屏蔽及子公司雇员受到恐吓的情况。尽管如此，信息和通信技术行业各领域的公司在与国家的关系中都能够建立和行使不同程度的影响力，抵制或减轻滥用法律造成的损害。有效的抵制战略包括：将人权保障纳入许可证协议和有关的其他合同；对政府的要求进行限制性解读；与政府官员谈判此类要求的范围；对过于宽泛的要求或法律进行司法质疑；向受影响的个人、媒体或公众提供有关信息；并中止在某特定市场的服务、退出或决定不进入。

2. 销售监控和审查设备

59. 私营部门供应硬件、软件和其他技术，使各国能够拦截、储存或分析通信和其他信息。基础设施供应商、硬件制造商和软件开发商可以为国家设计或定制产品，或供应两用设备和技术，各国随后可按自己的需求调整。互联网和电信服务提供者也可以向这些公司购买设备或软件，安装在其网络组件上，以便遵守其运营国家法定的拦截协议。国家可以依赖这些产品和服务来定位、骚扰或恐吓弱势群体成员。

3. 秘密监控

60. 各国还可以秘密接入服务提供商和内容平台的技术基础设施，以拦截范围广泛的各种信息，包括通信、用户账户信息以及电话和互联网记录。有报道称，有国家在向消费者提供计算机硬件的过程中篡改这些硬件、以恶意软件非法潜入私人网络和平台、非法侵入具体装置并利用其他数字安全漏洞。如果企业接到了关于这种监控的通知，就可能出现有关其人权责任的问题，如通知客户或通过安全措施减轻这种损害。向政府出售实施秘密监控技术设备和服务的公司可能因其销售而被卷入侵犯人权问题。

[43] 见谷歌、脸书、Dropbox、推特和微软最近的透明度报告。

[44] Sweden, Act on Signal Surveillance for Defense Intelligence Activities, sect. 4 (3).

[45] Australia, Telecommunications (Interception and Access) Act 1979, sect. 9 (1).

4. 法律互助条约和数据本地化

61. 有必要注意，监控受到关于提供私营部门所掌握信息的其他要求的影响。例如，无法跟上跨边界数据要求的法律互助条约制度可能会驱使各国诉诸具有侵扰性的域外监控措施。要求公司保留客户数据或将此类数据储存在地方数据中心的法律还可能会鼓励此种监控。

5. 加密和匿名

62. 自从特别报告员提出加密和匿名对保护见解和表达自由的重要性的报告以来，政府加大了向公司施加的压力，要求公司降低其客户的数字设备、通信和信息安全性。包括硬件制造商以及电子邮件服务商和短信服务商在内的各私营实体正在采取措施，开发和运用加强用户的安全性、匿名性和隐私的技术。这些措施包括对数字通信端对端加密、磁盘加密和及时的弥补安全漏洞的软件更新。对此，各国正在努力强制公司，为了国家利益在其产品和服务中的制造技术漏洞或加以利用。例如，美国联邦调查局向联邦法院申请强迫苹果公司制作软件，为在恐怖主义调查中接入嫌疑人的 iPhone 手机提供便利。2016 年 3 月 1 日提交英国国会的《调查权力法案》将许可情报部门申请授权令，要求私营实体“确保干预任何设备以获取通信[……]设备数据和其他信息”。[46]

C. 透明度

63. 透明度可以帮助确保互联网监管的主体能够有意义地预测其法律义务，并酌情对此提出质疑。在遵守这些标准方面的差距会威胁到个人知晓其网络表达自由所受限制以及在权利受到侵犯时寻求适当补救的能力。国家和私营部门中都会出现透明度问题，例如公私伙伴关系、私营部门参与贸易谈判以及数字军备竞赛。

64. 尽管有许多改革尝试，政府的要求仍缺乏透明度。虽然在关于政府提出用户信息要求的透明度报告方面有所改进，但是对政府要求限制或清除内容的数量和性质方面的可用信息则少得多。[47] 甚至这些统计数字是否保留也不清楚。国家对私人披露相关信息施加的限制会成为提高公司透明度的一个主要障碍。一些国家禁止披露关于政府提出删除内容或接入用户数据要求的信息。例如，印度禁止网络中间商披露关于屏蔽互联网内容接入的政府命令的细节以及中间商为响应该命令所采取的任何行动。[48] 英国《调查权力法案》将禁止电信服务提供商披

[46] Investigatory Powers Bill (2015)，Cl. 88 (2).

[47] 网上自由联盟网上隐私和透明度工作组及电信行业对话提交的材料。

[48] India, Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009, rule 16.

露，除其他外，“政府关于保留客户通信数据的命令及其内容”。[49] 在另一些国家，法律规章模棱两可，使公司难以确定哪类信息允许披露。例如，南非禁止私人披露政府关于客户数据的要求，[50] 但不清楚同样的限制是否适用于关于删除内容的要求。[51]

65. 在私营部门，服务提供商和内容托管平台往往至少披露一些资料，说明它们在什么情况下清除内容或遵守政府索要客户数据的要求。然而，在是否以及如何解读或解释国家条例和服务条款及内部实施和强制执行程序方面存在着很大差异。无论是由于国家施加的限制还是由于内部政策决定，公司在披露有关删除内容和提供用户数据的要求的数量、频率和类型方面也存在差距。无论如何，与私人请求相比，公司更有可能披露关于政府要求的统计数字。关于其他中间商(如金融或电子商务中间商)和公司披露有关删除内容和索要客户数据要求的情况的研究要少得多。

66. 正在进行的有关公司披露最低标准和有关的最佳做法的辩论体现了在适当平衡透明度及互相抵触的价值(如个人安全与贸易保密)方面的不确定性。虽然人们越来越一致认为，公司应披露信息，说明如何解读和执行限制，但关于应如何操作的共识很少。同样，人们普遍同意量化的透明度非常重要，但却不太清楚应如何在具体情况中考虑、提出及公布这些信息。

D. 补救

67. 限制网络表达自由的情况每天都会发生，且经常涉及公司行为，无论是受法律所迫还是根据公司政策和做法(如服务条款中所显示的)。这类限制的常见例子包括非法或以其他可疑方式删除内容、限制服务和暂停账户及侵犯数据安全。

68. 根据《公民权利和政治权利国际公约》第二条第 3 款，缔约国必须保证被侵犯了公约所规定权利的人能得到有效的补救。《工商企业与人权指导原则》预计，公司应提供合理合法、可获得、可预测、公平、符合权利、透明、立足对话和参与及有持续学习来源的补救和申诉机制。[52] 然而，对于应如何在信息和通信技术背景下实施或评估这些要素，只有有限的指导。例如，被错误地从查询结果中删除的网页链接，可能需要搜索引擎恢复这些链接。然而，尚不清楚应如何设计或执行投诉或上诉机制以确保此类删除得到有效标识、评价和补救。搜索引

[49] Investigatory Powers Bill，Cl. 84 (2).

[50] South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, sect. 42 (1).

[51] South Africa, National Key Points Act 102 of 1980, sect. 10 (c).

[52] 《指导原则》，第三章 III (A) (31)。

擎的客户群高度分散，使设计问题进一步复杂化。也不清楚公司是否应提供更多的补救办法，如对删除期间的收入损失提供资金补偿，或保证不再发生。

69. 为执行服务条款，公司可能未必总设有充足的上诉程序，供认为删除内容或注销账户的决定有误或是滥用标识活动的结果的用户对这些行动进行上诉。审查公司如何沟通服务条款执行决定及如何执行上诉机制的最佳做法的进一步研究可能会有所帮助。

70. 公司补救责任的范围也存在争议。当公司过于严格地解读或执行相关国家法律时，谁来为不当删除的做法或索要数据的要求承担责任？如果一个公司的产品或服务被用来实施侵犯人权行为，何种程度的因果关系会触发提供补救的义务？当公司被指控犯有违法行为时，是否有责任进行内部调查，这些调查必须符合某些标准吗？如果某项限制涉及国界之外的个人，由哪种司法管辖权来审议补救问题是适当的？这些问题体现了在公司和国家行为相互交织的情况下，人权受害者所面临的不确定性。

71. 需要更深入地分析国家在补充或监管公司补救机制方面的适当作用。受到企业行动不利影响的消费者常常可利用民事诉讼和其他司法补救，但这些手段往往十分烦琐且费用高昂。有意义的替代办法可包括由消费者保护机构和行业监管机构设立和管理的申诉和投诉机制。一些国家还委任了内部补救或申诉机制：例如，印度要求掌握、处理或操作个人敏感数据的公司指定申诉处理员，以处理“与信息处理有关的任何不符之处和申诉”。[53]

五. 进一步专题的发展工作

72. 鉴于构成和影响行使网上见解和表达自由的私人信息和通信技术活动的范围，特别报告员将具体关切领域的国家义务和企业责任作为重点。上文提出的法律和政策问题将指导专题报告、与各国政府的交流、对国别和公司的访问、区域和专家协商以及其他工作。

73. 特别报告员的专题研究和指导包括以下优先事项：

对电信和互联网服务提供的限制

74. 各国政府越来越多地要求提供电信和互联网服务的私营实体遵守审查要求。除了网络过滤的做法外，各国强迫或迫使公司关闭网络或屏蔽全部服务。需要进一步记录和观察这一趋势。今后的工作将审查使各国政府能够执行此种限制的法律、政策和法外措施，以及此种限制的代价和后果。特别报告员还将审查公

[53] India, Information Technology Act, 2008, sect. 43 A； Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, rule 5 (9).

司在违规情况发生时，以尊重权利、减轻损害和提供补救渠道的方式应对这类措施的责任。

服务条款和社区标准所规定的内容限制

75. 私营行为者面临来自各国政府和个人的沉重压力，被要求限制被视为构成极端主义或仇恨、敌意或骚扰的表达。私营行为者自身也可以在其平台上努力促进它们所认为的文明言论、通过实名要求和其他注册政策监管接入情况或出于商业原因突出或优先某些内容。今后的工作将评估国家侵犯私人倡议的可能性、私营措施对表达自由的影响以及有关的人权义务和责任。报告将重点讨论社交媒体和搜索引擎的作用，以及不太知名的行为者(如电子商务和金融中间商)的作用。

内容托管的责任

76. 由于中间商责任制度和审查要求，中间商越来越多地因为托管的第三方内容而被追究责任。此类限制经常援引的理由包括网络安全、版权、诽谤和数据保护。进一步的研究将侧重此类理由的合法范围、附属限制的必要性以及删除第三方内容的现有框架之下缺少程序性保障措施的问题。今后的工作还将审查中间商在特定情况和区域的责任来源和模式，并力求总结出可适用的主要原则和做法，以确保中间商促进和保护表达自由的能力。

审查和监控行业

77. 私营公司在开发、生产和转让各国政府可用于执法、情报和公共安全目的的软件和硬件方面发挥着主要作用。虽然这些工具可能具有合法的目的，但政府往往将其用于审查和不相称的监控目的。今后的工作将通过人权框架探讨这些问题并鼓励各方尽责查明使用此类技术妨碍表达自由的情况。

破坏数字安全的努力

78. 传输、储存或生成通信和其他形式用户数据的公司—特别是电信和互联网服务提供商以及内容托管平台—面临着执法和安全部门提出的越来越多的接入其客户信息的要求。今后的工作将力求查明既可以最大限度地扩大表达自由的范围又可以满足政府在国家安全和公共秩序方面的合法利益的办法。

互联网接入

79. 数十亿接入网络的个人享有获取信息和想法的机会，而人数更多的另外几十亿人因缺少连网所必要的基础设施或政治、安全、法律或社会环境而无法获得这样的机会。随着私营部门日益加大努力赋予这数十亿人接入的权能，确保这种

接入是自由、开放和安全的至关重要。今后的工作将探讨有关接入以及私营部门参与和投资以确保可负担性和可接入性的问题，特别要考虑到边缘化群体。

互联网治理

80. 信息社会世界峰会的成果表明了对互联网多利益攸关方治理的持续广泛支持。然而，现有模式面临着具体国家政策(如数据本地化)和战略(如“网络主权”)等形式的日益增长的压力。此外，还始终需要维持或增加各级治理中的人权参与(包括制订技术标准)并确保互联网治理框架和改革努力对妇女、性少数群体和其他弱势群体的需求有敏感认识。

81. 在今后的这项工作中，特别报告员将始终特别注意国家和区域一级在法律(立法、监管和司法)方面的事态发展。为此，他通知所有利益攸关方他有兴趣为今后的信息和报告收集此类材料，并鼓励有关缔约方在这项工作的整个过程中收集和提供此类材料。

六. 结论和建议

82. 信息和通信技术部门一直在迅速发展，不断升级技术，将日常生活数字化。因此，着眼于现行规范方面的差距来阐述法律和政策问题有可能无法述及刚刚出现或尚未出现的趋势。这是数字时代的一个自然特征，但即使技术迅速变化，数字环境仍将继续受到对见解和表达自由的持续威胁而无法平息下来。这些威胁包括政府通过对网上服务和基础设施进行审查来控制或企图控制信息来源；企业争取在不利于表达自由的环境中推销其产品和服务的努力；许多企业在追求商业利益的过程中无法确保促进和保护权利；以及个人往往自相矛盾的要求，即工商业实体不仅向其提供安全，还要提供便利、连通和共享。随着探讨信息和通信技术职责的项目不断推行，特别报告员期待该领域的专家──来自政府、私营部门、民间社会、技术界、学术界的专家──帮助他进行分析和提出报告，以应对技术与表达自由交叉领域当前的问题并反映数字时代的长期特征。

83. 特别报告员大力鼓励所有利益攸关方──包括国家行为者、私营部门企业以及民间社会组织和个人──积极参与制订即将开始的项目。他特别鼓励较不发达国家的利益攸关方和弱势群体就信息和通信技术部门可能对享有权利的影响及各国在干预和促进这些权利方面可以发挥的作用交流看法。

84. 虽然这一项目仍处于初步阶段，但国家和私营行为者采取步骤确保尊重见解和表达自由至关重要。这些步骤至少应包括以下各项，特别报告员随后将在整个任期内进行进一步分析。

国家

85. 国家负有保护和尊重见解和表达自由权的行使的主要责任。在信息和通信技术方面，这意味着各国不得通过法律、政策或法外手段要求或以其他方式强迫私营部门采取对表达自由进行不必要或不相称的干涉的步骤。关于撤销数字内容或获取客户信息的要求、请求和其他措施的依据必须是经正当手续颁布的法律，受到外部和独立的监督，并证明是实现《公民权利和政治权利国际公约》第十九条第 3 款中一项或多项目标的必要和相称的手段。特别是在监管私营部门的背景下，国家法律和政策必须以透明的方式通过和执行。

86. 政府还必须通过和执行法律和政策，保护私人制订和提供推动表达自由的技术措施、产品和服务。它们必须确保存在涉及互联网权利和限制的立法、决策和其他有关规范制定程序，以便向私营部门、民间社会、学术界和技术界提供有意义的投入和参与的机会。

私营部门

87. 各国向私营信息和通信技术部门施加无可否认的压力，往往导致严重限制表达自由的情况。然而，私营部门也具有独立作用，既可促进也可限制权利，人权理事会准确地认识到了这一点，于 2011 年通过了《工商企业与人权指导原则》，作为这一领域的一般性指导。对私营实体的评价应依据其所采取的促进表达自由步骤和破坏表达自由的步骤，甚至是在不尊重人权的不利环境下也应如此评价。

88. 制定和执行透明的人权评估程序是私营行为者应采取的最重要的步骤之一。私营行为者制定和执行的政策应考虑到对人权的潜在影响。这些评估应批判地审查其所参与的范围广泛的私营部门活动，如制订和执行服务条款和有关用户表达自由的社区标准，包括对这种执行工作的外包；正在开发的产品、服务和其他商业举措，包括设计和工程选择以及差别定价或接入互联网内容和服务的计划，对用户表达自由的影响；及与潜在政府客户做生意，如运营电信基础设施或转让内容管制或监控技术，对人权的影响。

89. 私营实体在其涉及表达自由和其他基本权利的政策、标准和行动中确保最大的透明度同样至关重要。应就方法、对法律义务的解释和此类评估对商业决定的重要性等方面对人权评估进行透明的审查。透明度的重要性是全方位的，包括在内容监管方面，并应包括报告关于政府提出的撤销内容的要求。

90. 除了执行政策，私营实体还应将对表达自由的承诺纳入内部决策、产品设计、业务发展、员工培训和其他相关的内部程序。特别报告员将致力于通过多种方式，包括通过访问公司，探讨政策和各种执行步骤。

国际组织和多方利益攸关方进程

91. 正如本报告所示，许多国际组织在信息和通信技术治理进程中发挥着作用。至关重要的是，这些组织应向公众提供有意义的获取由该组织和/或其成员制订或制作的有关互联网治理的政策、标准、报告和其他资料的机会，包括通过便利接入免费的网上资源和公共教育举措。更广泛而言，互联网多利益攸关方治理进程一直是支持表达自由的政策的重要驱动因素。考虑到这一点，国际组织应确保民间社会有意义地参与决策和其他标准制定进程，包括通过加大对人权问题有敏感认识的技术专家的参与。