联 合 国 A/HRC/23/40

大 会

Distr.: General
17 April 2013
Chinese
Original: English

人权理事会
第二十三届会议
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

增进和保护见解和言论自由权问题特别报告员弗兰克·拉·吕的报告*

概要

本报告根据人权理事会第 16/4 号决议提交，分析了国家通信监测对行使隐私权和见解和言论自由权等人权的影响。考虑到通信领域重大技术进步的影响，报告强调迫切需要进一步研究新的监控模式并按照人权标准修订规范这些做法的国内法律。

* 迟交。

目录

一. 导言

1. 本报告分析国家监控通信对行使隐私权和见解和言论自由权等人权的影响。考虑到通信领域重大技术进步的影响，报告强调迫切需要进一步研究新的监控模式并按照人权标准修订规范这些做法的国内法律。

2. 技术创新增加了通信和保护自由言论和见解的可能性，使匿名、快速的信息共享和跨文化对话成为可能。技术变革同时还增加了国家对个人的私人通信进行监控和干预的机会。

3. 对国家安全和刑事活动的关切可能成为使用通信监控技术的例外理由。但是，关于什么构成必要、合法和适度国家通信监控的国内法律往往不够充分或不存在。不完善的国内法律框架成为任意和非法侵犯通信隐私权的温床，并因此威胁到对见解和言论自由权的保护。

4. 在此前的报告(A/HRC/17/27 和 A/66/290)中，特别报告员分析了互联网在扩大个人行使见解和言论自由权的可能性方面前所未有的影响。他对各国为防止或限制网络信息流通而采取的多种措施表示关切，并着重指出互联网领域隐私权保护不足。

5. 本报告以以往的分析为基础，旨在查明新的通信监控方法和模式给人权包括隐私权以及见解和言论自由权造成的影响。

6. 本报告采用以下术语描述最常用的通信监控模式：

(a) 通信监控：监测、截取、收集、保存和保留通信网络上传播、传递或生成的信息；

(b) 通信数据：个人通信信息(发出或收到的电子邮件和短信、往来电话通话、社交网络信息和贴子)、身份、网络账户、地址、访问过的网站、图书和阅读、观看或听过的其他材料、进行过的搜索、使用过的资源、互动(通信的来源和目的地、进行互动的人、朋友、家人、熟人)以及个人的时间和位置，包括与他人的近距离关系)；

(c) 互联网过滤：自动或手动监测互联网内容(包括网站、博客和在线媒体源以及电子邮件)，以限制或压制特定文字、图像、网站、网络、协议、服务或活动。

二. 特别报告员的活动

7. 在报告所述期间，特别报告员参加了多次国际和国家活动，这些活动涉及他以往报告中讨论的一些问题，如互联网的言论自由、防止仇恨言论以及保护记者。他特别关注促进保护记者的国家举措；在这方面，他参加了关于巴西、哥伦

比亚、洪都拉斯和墨西哥所开展的举措的会议。它还参加了 2012 年 11 月在维也纳举行的“记者安全和有罪不罚问题联合国机构间会议”。

8. 他向联合国大会提交的上一份报告的重点是防止仇恨言论和煽动仇恨行为。[1] 特别报告员和防止种族灭绝问题特别顾问于 2013 年 2 月大会期间联合组织的会外活动也讨论了同一问题。当月，他在“关于禁止构成煽动歧视、敌意或暴力的鼓吹民族、种族或宗教仇恨言论的拉巴特行动计划”在日内瓦启动时以及在越南举行的联合国不同文明联盟第五届全球论坛上进一步论述了这些问题。

9. 特别报告员 2012 年 8 月 7 至 14 日对洪都拉斯进行了访问。他此次访问的调查结果和建议载于本报告增编(A/HRC/20/40/Add.1)。印度尼西亚政府曾邀请他于 2013 年 1 月访问该国。遗憾的是，该国政府请求推迟访问，新的访问日期尚未确认。

10. 为了编写本报告，特别报告员修订了有关研究报告并咨询了通信监控相关事项方面的专家。2012 年 12 月，他参加了电子前沿基金会组织的电子监控和人权研讨会。2013 年 2 月，他为编写本报告组织了一次专家磋商会，与之并行召开的还有联合国教育、科学及文化组织(教科文组织)在巴黎举办的“信息社会世界峰会+10 会议”，他也参加了该次会议的开幕全体小组讨论。

三. 监控技术的演变

11. 技术创新增加了通信和言论自由的可能性，使匿名、快速的信息共享和跨文化对话成为可能。同时，技术变革还为国家对个人私人生活进行监控和干预提供了新的机会。

12. 从截取最早的远程通信形式开始，各国设法截取或监测个人的私人通信以服务于执法和国家安全利益。从通信中可以揭示最私人和私密的信息，包括个人或团体过去或将来的行动。通信是一种宝贵的证据来源，国家可利用它防止或起诉严重罪行或预先阻止潜在的国家安全紧急情况。

13. 整个二十世纪的技术创新改变了通信监控的性质和影响。人们的通信方式和通信频率显著增加。固定电话系统向移动通信的过渡以及通信服务成本不断下降使得电话使用大幅增长。互联网的问世催生了一些无成本或价格非常实惠的新工具和应用程序。这些进步实现了更强的连通性，促进了世界范围内信息和思想的流动，还增加了经济增长和社会变革的机会。

14. 在信息和通信技术发展的同时，各国设法监测私人通信的方式也有所发展。与电话广泛使用伴随而来的是窃听技术的使用，将窃听器放在电话线上即可听到私人电话交谈。随着十九世纪 90 年代光纤和数字交换机取代模拟电话网

[1] A/67/357。

络，各国重新设计网络技术，加入了截取能力(“后门”)以允许国家监控，可以对现代化电话网络进行远程接入和控制。

15. 技术的动态特性不仅改变了监控方式，还改变了监测的“内容”。互联网在为通信和信息共享创造了各种机会的同时，还促使了大量个人创造的和与个人有关的交易数据的生成。这种被称为通信数据或元数据的信息包括个人的私人信息，他们所在位置和在线活动，运行记录以及他们发送或接受的电子邮件或信息的相关信息。通信数据可以储存、获取和搜索，国家当局获取和使用这些数据基本上不受管制。分析这种数据有很强的揭示性和侵入性，特别是合并和汇总的数据。因此，各国越来越多地利用通信数据为执法和国家安全调查提供支助。各国还正在强制保存和保留通信数据，以便进行历史监控。

16. 与技术变革同步的是对通信监控态度的变化。官方窃听做法最初始于美利坚合众国，是在有限制的基础上使用的，仅勉强得到法院批准。[2] 因此，它被视为严重威胁隐私权，其使用必须仅限于侦查和起诉最严重的罪行。但是，久而久之，各国扩大了它们进行监控的权力，降低了门槛并增加了进行这种监控的正当理由。

17. 在很多国家，现行立法和做法没有受到审查，也没有进行更新以应对数字时代通信监控的威胁和挑战。例如，法律引进了传统的检查书信概念，允许检查个人电脑和其他信息和通信技术，而未考虑到这些设备的广泛用途和对个人权利的影响。同时，监管全球通信监控和共享安排的法律并不存在，其结果是出现了超出任何独立机关监督范围的各种特别做法。现在，在很多国家中，大量公共机构均可出于各种目的获取通信数据，往往不经过司法授权和独立监督。此外，各国都试图采用声称具有域外法律效力的监控安排。

18. 人权机制对互联网以及通信监控和通信数据获取方面的新技术的人权影响的评估同样缓慢。扩大各国监控权力和做法给隐私权和见解和言论自由权造成的后果尚未得到人权理事会、各特别程序任务负责人或人权条约机构的全面审议。本报告试图纠正这种状况。

四. 国际人权框架

19. 《世界人权宣言》和《公民权利和政治权利国际公约》分别在第十九条中保障见解和言论自由权，申明人人持有主张而不受干涉的自由，和通过任何媒介

[2] 在对窃听进行第一次司法确认时，美国最高法院的布兰代斯法官写下了尖锐的异议，指出窃听是一种“更不易察觉且更具长远影响的侵犯隐私方式”，《宪法》无法为其提供法律依据。在令人不寒而栗的准确预测中，这位著名法学家预言说：“政府可能会在某一天研制出一些办法，不用从秘密抽屉中拿走文件，即可在法庭上复制出来，它将使家庭中发生的最私密的事情暴露于陪审团面前。心理和相关科学的发展可能会带来探索未表达的信念、想法和感情的方法”。“Olmstead 诉美国”，277 U.S. 438(1928 年)。

和不论国界寻求、接受和传递信息和思想的自由。在区域一级，保护这一权利的有《非洲人权和人民权利宪章》(第 9 条)、《美洲人权公约》(第 13 条)和《保护人权与基本自由公约》(第 10 条)。

20. 国际和区域一级均明确将隐私视为一项基本人权。隐私权被载入了《世界人权宣言》(第十二条)、《公民权利和政治权利国际公约》(第十七条)、《儿童权利公约》(第 16 条)和《保护所有移徙工人及其家庭成员权利国际公约 》(第 14 条)。在区域一级，隐私权受到《欧洲人权公约》(第 8 条)和《美洲人权公约》(第 11 条)的保护。

21. 虽然保护隐私的义务得到普遍认可，但国际人权保护机制在上述人权文书中列入隐私权时没有阐述该项权利的具体内容。这项权利内容没有明确的阐述，造成了适用和执行过程中的各种困难。[3] 由于隐私权是一项有限度的权利，这给解释私人领域的构成以及界定公共利益的构成带来了一些困难。通信和信息技术近几十年来的快速和重大变化也不可逆转地影响了我们对私人和公共领域界限的理解。

22. 隐私可被解释为一种假设，即个人理应享有一个自主发展、互动和自由的领域，一个无须同他人产生关联的“私人领地”，不受国家干预，任何人未经允许不得擅自过度干涉。[4] 隐私权还是个人确定谁掌握关于他们的信息以及如何使用这些信息的能力。

23. 为了使个人在通信中行使其隐私权，他们必须能够确保这些通信保持私人性、安全性以及(如果他们决定如此)匿名性。通信隐私指的是个人能够在社会其他成员、私人部门以及政府本身触及范围之外的空间交流信息和思想。通信安全意味着个人应该能够核实他们的通信仅送达其指定的收件人，不受干涉和改动，并且他们收到的通信也同样不受侵扰。匿名通信是互联网促成的最重要的进展之一，使个人得以自由表达意见而不必担心受到惩罚或谴责。

A. 隐私权与见解和言论自由权的相互关系

24. 隐私权常常被理解为实现言论自由权的基本要求。不当干涉个人隐私可以直接或间接限制思想的自由发展和交流。例如，限制通信匿名对各种形式暴力和虐待行为的受害者产生明显的寒蝉效应，使他们由于担心双重伤害而不愿进行举报。在这方面，《公民权利和政治权利国际公约》第十七条直接提及保护“通信”免受干涉，这一术语应被解释为包括在线和离线的一切形式的通信。[5] 正如

[3] 教科文组织，《互联网隐私和言论自由全球调查》，2012 年，第 51 页。

[4] Lester 男爵和 D. Pannick(编辑)，《人权法和实践》，伦敦，巴特沃思出版社，2004 年，第 4.82 段。

[5] 公民权利和政治权利国际公约评论，第 401 页。

特别报告员在前一份报告中指出的那样，[6] 私人通讯的权利使国家有全面的义务，确保电子邮件和其他形式的网上通讯确实传递给指定的收件人，不应受到国家机构或第三方的干涉和检查。[7]

25. 人权事务委员会在其第 16 号一般性意见(1988 年)中分析了隐私权(第十七条)的内容，根据该意见，第十七条旨在保护个人的私生活、家庭、住宅或通信不受任何非法或任意干涉，国家法律框架必须规定这种保护。这一规定提出了与保护通信隐私有关的具体义务，强调："信件应送达受信人，不得截取、启开或拆读。应禁止监查(不管是否以电子方式)、截取电话、电报和其他通讯形式、窃听和记录谈话"。[8] 该一般性意见还指出，"以电脑、资料库及其他设备收集或储存私人资料——不管是由公共当局或民间个人或机构——必须由法律加以规定"。[9] 该一般性意见通过时，信息和通信技术发展对隐私权的影响还罕为人知。

26. 人权事务委员会在其关于言论自由的第 34 号一般性意见(2011 年)中指出，缔约国应考虑信息和通信技术的发展能够在多大程度显著改变全球通信业务。委员会还呼吁缔约国采取一切必要步骤，促进这些新媒体的独立。该一般性意见还分析了保护隐私和言论自由之间的关系，并建议缔约国尊重言论自由权包括不披露信息来源的有限新闻特权这一点。[10]

27. 隐私权和言论自由权之间还存在冲突，例如，当通过媒体传播被认为是隐私的信息时。在这种意义上，第十九条第 3 款规定了为保护他人权利对言论和信息自由权的一些限制。但是，与对言论自由权所有可允许的限制一样(见以下)，相称原则必须得到严格遵守，否则言论自由有受到损害的危险。特别是在政治领域，并不是对政客良好声誉的每次攻击都需要得到准许，否则言论和信息自由的重要意义将被剥夺，[11] 无法在政治见解形成过程中倡导透明度并打击腐败。区域一级的国际判例显示，在隐私和言论自由出现冲突的情况下，应参考所报道事项的整体公共利益。[12]

---

[6] A/HRC/17/23。

[7] 公民权利和政治权利国际公约评述，第 401 页。

[8] 公民权利和政治权利中心(《公民权利和政治权利公约》)第 16 号一般性意见(一般性意见)，第 8 页。

[9] 同上，第 10 页。

[10] 《公民权利和政治权利国际公约》第 34 号一般性意见。

[11] 曼弗雷德·诺瓦克，《联合国公民权利和政治权利国际公约：公约评述》(1993 年)，第 462 页。

[12] 教科文组织，《互联网隐私和言论自由全球调查》，2012 年，第 53 和 99 页。

B. 对隐私和言论自由的可允许的限制

28. 《公民权利和政治权利国际公约》第十七条的框架通过可允许的限制对隐私权进行必要、合法和适度的限制。与说明可允许的限制原则的因素的第十九条第 3 款相反，[13] 第十七条的表述中并未包含限制条款。虽然存在这些措辞差异，但普遍认为《公约》第十七条也应被理解为包含人权理事会其他各项一般性意见中阐述的可允许的限制原则的因素。[14]

29. 在这方面，特别报告员持有的立场是，隐私权应遵守在第 27 号一般性意见中阐述迁徙自由权可允许的限制原则。[15] 该意见中表述的原则除其他外，包括以下因素：

(a) 任何限制必须在法律上加以规定(第 11-12 段)；

(b) 不得限制各项人权最根本的内容(第 13 段)；

(c) 限制一定要是民主社会所必需的(第 11 段)；

(d) 实施限制的裁量权须加以限制(第 13 段)；

(e) 要成为可允许的限制，仅实现各项合法目的中的一项是不够的。它必须是实现合法目的所必需的(第 14 段)；

(f) 限制措施必须符合相称原则，它们必须适合于实现保护功能，必须是可用来实现预期结果的诸种手段中侵入性最小的一种，并且必须与要保护的利益相称(第 14-15 段)。

C. 国际人权保护机制近期做过的审议

30. 在以前的报告中，特别报告员评估了互联网对实现见解和言论自由权的影响(A/HRC/17/27 和 A/66/290)。他指出，虽然互联网用户在互联网上享有相对的匿名，但国家和私人行为者能够获取监测和收集个人通信和活动的信息的新技术。这种技术可能会侵犯互联网用户的隐私权，从而破坏人们对互联网的信任和网上安全并阻碍信息和思想的网上自由流动。特别报告员敦促各国根据人权标准实行有效的隐私和数据保护法，并采取一些适当措施确保个人能够在网上匿名表达自己的意见。[16]

[13] 第十二条第 3 款、第十八条第 3 款、第二十一条、第二十二条第 2 款分别列出了迁徙自由和选择住所自由权、思想、良心和宗教自由权、和平集会权和结社自由权可允许的限制清单。

[14] 同上。

[15] 另见《公民权利和政治权利公约》第 34 号一般性评论。

[16] A/HRC/17/27, 第 22 段。

31. 其他特别程序任务负责人论述了干涉隐私权问题。反恐中注意增进与保护人权和基本自由问题特别报告员研究了以打击恐怖主义为借口对隐私权产生不良影响的监控做法和技术的发展。[17] 特别报告员强调，这些措施不仅致使隐私权受到侵犯，还影响到正当程序权和行动迁徙权、结社自由权和言论自由权。特别报告员敦促各国政府依据国际人权标准，详细说明本国的监控政策如何恪守相称性和必要性原则，以及采取哪些措施防止权力滥用。特别报告员还呼吁各国采用全面的数据保护和隐私法并设立强有力的独立监督机构，授权其审查侵入性监控技术的应用和个人信息的处理过程。它还呼吁专门为研究和开发隐私增强技术投入资源。

32. 其他的人权保护机制最近也关注了通信监控对保护隐私权和言论自由权的影响。例如，人权事务委员会对国家监测互联网使用并阻止访问一些网站[18] 表示关切，并建议审查授予行政部门监控电子通信的广泛权力的立法。[19] 普遍定期审议也列入了有关建议，例如关于确保有关互联网和其他新通信技术的法律遵守国际人权义务的建议。[20]

五. 通信监控的模式

33. 使各国能够侵入个人私生活的现代化监控技术和安排有模糊私人和公共领域界限的危险。它们助长了侵入性和任意性的个人监测，而个人甚至可能不知道其已遭到这种监控，更不用说进行质疑了。技术进步意味着国家进行监控的效力不再受到规模或持续时间的限制。技术和数据存储成本的不断下降使进行监控的资金和实际阻碍因素不复存在。因此，国家进行实时、侵入性、定点和大规模监控的能力比以往任何时候都强。

A. 定点通信监控

34. 各国拥有一些不同的技巧和技术，可对特定个人的私人通信进行通信监控。实时截取能力使各国能够收听并记录使用固定电话或移动电话的任何个人的电话通话，其所使用的国家监控截取能力是所有通信网络都必须植入其系统的。[21] 个人的位置可以被查明，它们的短信可以被读取和记录。将窃听器安装在与某地

[17] A/HRC/13/37。

[18] CCPR/C/IRN/CO/3。

[19] CCPR/C/SWE/CO/6。

[20] A/HRC/14/10。

[21] 例如，见 1994 年《美国执法通信援助法》(美国)；1997 年《电信法》，第十五章(澳大利亚)；2000 年《调查权力规范法》，第 12-14 章(联合王国)；2004 年《电信(截取能力)法》。

或某人有关的互联网网线上，国家当局还可以监测个人的网上活动，包括他或她访问的网站。

35. 个人电子邮件和信息的存储内容，以及其他相关通信数据可以从互联网公司和服务提供商那里获得。欧洲标准制定机构欧洲电信标准协会强制要求云提供商[22] 将“合法截获能力”植入云技术中，以便国家当局直接获取这些提供商存储的内容，包括电子邮件、信息和语音邮件，这一举措令人关切。[23]

36. 各国可以通过各种方式追踪特定移动电话的行踪，查明指定区域内携带移动电话的所有个人，并截取他们的通话和短信。一些国家利用名为国际移动用户识别码捕捉器的无线移动监测设备，它可以临时(如在抗议或游行中)或永久(例如机场和其他边境通道)安装在任意地点。这些捕捉器模拟移动电话发射塔发出和回应移动电话信号，以探取特定区域内每一部移动电话独有的客户识别模块(SIM)卡号。

37. 各国还在越来越多地获取可以用来侵入个人电脑、移动电话和其他数字设备的软件。[24] 攻击性侵入软件，包括所谓的“木马”(也被称为间谍软件或恶意软件)，可被用来打开设备的麦克风或摄像头，跟踪在设备上进行的活动，并获取、更改或删除设备上存储的任何信息。这种软件使国家能够完全控制被侵入设备，并且它几乎是无法察觉的。

B. 大众通信监控

38. 随着允许对信息进行广泛截取、监测和分析的各种技术激增，进行大规模监控的成本和后勤障碍继续快速减少。现在，一些国家有能力追踪和记录全国范围内互联网和电话通信。大部分数字通信信息通过光纤电缆流动，在电缆上安置窃听器，并运用文字、声音和语音识别，各国可以基本实现对电信和在线通信的完全控制。例如，在阿拉伯之春发生之前，埃及和利比亚政府据报道使用了这样的系统。[25]

39. 在很多国家，强制性数据保留为大规模收集可随后进行过滤和分析的通信数据提供了便利。各种技术使国家可以扫描电话通话和短信以发现某些文字、语音或短语的使用，或过滤互联网活动以确定个人访问某些网站或使用具体在线资源的时间。“黑匣子”可以用来检查互联网上的数据流，以过滤并解析与在线活

[22] 云提供商提供联网在线数据存储业务。

[23] 欧洲电信标准协会技术报告草案 101 567 VO.0.5 (2012-14)，技术报告草案：合法拦截；云/虚拟服务。

[24] Toby Mendel、Andrew Puddephatt、Ben Wagner、Dixi Hawtin 和 Natalia Torres, 互联网隐私和言论自由全球调查，《教科文组织互联网自由丛书》(2012 年)，第 41 页。

[25] 欧洲议会对外政策司政策处，阿拉伯之春后：欧洲外交政策处理人权和互联网问题的新途径(2012 年)，第 9-10 页。

动有关的所有信息。这种称为“深度数据包检查”的方法使国家不仅能够获取个人访问网站的简单信息，还能分析所访问网站的内容。例如，据报道，中东和北非地区最近面临民众起义的国家使用了深度数据包检查。[26]

40. 各国现在经常使用的另一工具是社交监测。各国拥有实际能力，可以监测社交网站、博客和媒体渠道的活动，以查明联系和关系、意见和关联、甚至是位置。各国还可以将极为发达的数据挖掘技术应用于公开信息或第三方服务提供商提供的通信数据。在更基础的层面上，各国还掌握了获取脸谱网等社交网站的用户名和密码的技术方法。[27]

C. 通信数据获取

41. 除了截取和跟踪个人通信的内容，各国还可能设法获取第三方服务提供商和互联网公司拥有的通信数据。因为私营部门收集了越来越多的暴露个人日常生活敏感信息的各种信息，并且个人和企业选择将语音邮件、电子邮件和文件等通信内容存储于第三方服务提供商，获取通信数据成为了国家日益倚重的监控手法。

42. 包括大型互联网公司在内的第三方服务提供商收集的通信数据可被国家用来勾勒有关个人的全面轮廓。即便是看似无害的通信交易记录，当全部获取并分析时，也可以建立个人私生活的轮廓，包括医疗状况、政治和宗教观点和/或派别、互动和兴趣，透露出的详细信息与从通信内容本身可觉察出的一样多，或甚至更多。[28] 通过合并关于关系、位置、身份和活动的信息，各国能够追踪个人在不同区域的行踪及其活动，从他们旅游的地方到他们学习的地方，他们阅读的内容或与之交流的个人。

43. 各国获取通信数据的实例正在快速增加。在谷歌报告它收到的要求获取通信数据的次数的三年中，这种要求几乎翻了一番，从 2009 年最后六个月的 12,539 次增加到 2012 年最后六个月的 21,389 次。[29] 在联合王国，执法当局有权自行批准其关于通信信息的要求，每年报告的这类要求达到 500,000 次。[30] 在大韩民国，该国人口约为 5,000 万，每年关于通信数据的要求约为 3,700 万次。[31]

[26] Mendel 等人，前引，第 43 页。

[27] 欧洲议会，前引，第 6 页。

[28] Alberto Escudero-Pascual 和 Gus Hosein, “质疑合法获取交通数据”，《计算机协会的通信》，第 47 卷，问题 3, 2004 年 3 月，第 77-82 页。

[29] 见 http://www.google.com/transparencyreport/userdatarequests/。

[30] 见 http://www.intelligencecommissioners.com/docs/0496.pdf。

[31] 2012 年 10 月 23 日，《今日货币》引用韩国通信委员会为进行 2013 年年度国家审计向 Yoo Seung-Hui 议员披露的信息，http://www.mt.co.kr/view/mtview.php？type=1&no=2012102309430241764&outlink=1。

D. 互联网过滤和审查

44. 技术进步不仅助长了特定情况下的通信截取和获取，还使各国能够广泛地、甚至在全国范围内过滤在线活动。在很多国家，互联网过滤是在维持社会和谐或消除仇恨言论的幌子下进行的，但实际上是用于消除异议、批评或激进主义。

45. 以上提到的过滤技术为监测网络活动提供了便利，使国家能够发现被禁止的图像、文字、网址或其他内容，并进行审查或更改。各国可使用这类技术发现具体词汇和短语的使用，以审查或控制其使用，或查明使用它们的个人。据报道，在互联网普及率较高的国家，互联网过滤使审查网络内容和通信成为可能，并为监视人权维护者和活动者提供了便利。[32]

46. 除了便利过滤和审查的技术之外，很多国家还进行人工互联网过滤，为此设立了网络警察和检查员，以人工方式监测网站、社交网络、博客和其他形式媒体的内容。在一些国家，“网络警察部队”负责检查和控制互联网、搜索网站和网站内的重要节点(特别是在线论坛)，一旦含有政府不许可的内容(包括对国家领导层的批评)，即封锁或关闭这些网站。这种监督负担被转移到私营中介机构，例如搜索引擎和社交网络平台，有关法律将违禁内容的责任从最初发表言论者扩大到所有中介机构。

E. 对匿名的限制

47. 互联网的出现促成的最重要的进步之一是使人能够匿名使用和传播信息并在不暴露身份的情况下安全通信。最初，这是可能做到的，因为那时互联网没有“身份层”；起初，人们不可能知道具体信函、电子邮件地址、甚至具体电脑后的使用者。但是，各国逐渐以安全和执法为名消除了匿名通信的机会。在很多国家，个人在网吧必须进行实名登记，其在公用电脑上的交易必须记录。购买 SIM 卡或移动电话设备、访问某些主要网站或在媒体网站或博客上发表评论也越来越多地需要进行身份验证和注册。

48. 匿名限制措施使得获取或传播违禁内容的个人更容易被查明身份，从而为国家通信监控提供了便利，使这些个人更容易遭到其他形式的国家监控。

49. 从这种意义上说，匿名限制措施具有寒蝉效应，阻止自由表达信息和思想。这些措施还会导致个人在事实上被排除在重要社会领域之外，损害他们的言论和信息权利，并加剧社会不平等。此外，匿名限制措施允许私营部门收集并汇编大量数据，给企业行为者保护这些数据的隐私性和安全性带来巨大的负担和责任。

[32] 欧洲议会对外政策司政策处，阿拉伯之春后：欧洲外交政策处理人权和互联网问题的新途径(2012 年)，第 12 页。

六. 对国家法律标准的关切

50. 一般而言，立法没有跟上技术变革的步伐。在多数国家，处理现代通信监控环境的法律标准要么不存在，要么不充分。因此，各国日益设法在旧的法律框架范围内为使用新技术进行辩护，不承认它们现在拥有的扩展能力远远超出了这些框架的设想。在很多国家，这意味着含糊的宽泛意义上的法律条款被援引来批准和许可严重侵入性技术的使用。在明确授权这类技术和手段并界定其使用范围的法律不存在的情况下，个人无法预见其运用，甚至毫不知情。同时，国家不断通过新的法律，扩大国家安全例外情况的范围，使不受监督和独立审查的侵入性监控技术得以合法化。

51. 法律标准不完备增加了个人人权(包括隐私权和言论自由权)受侵犯的风险。它还给某些个人群体带来了负面影响，例如，某些政党的党员、工会会员或民族、族裔和语言少数群体更可能受到国家的通信监控。在没有强有力的法律保护情况下，记者、人权维护者和政治活动者面临着遭到任意监控活动的风险。

52. 有很多资料证明，很多国家对人权维护者进行监控。在这样的情况下，人权维护者和政治活动者报告说有人监测他们的电话通话和电子邮件，并追踪他们的行踪。由于记者依赖网上通信，因此他们也特别容易成为通信监控的目标。为了从包括举报人等机密来源得到和追查信息，记者必须能够做到通信隐私、安全和匿名。在监控普遍存在且不受正当法律程序或司法监督限制的环境下，保护消息源的假定无以为继。如果不认真和公开记录监控的运用情况，也没有已知的避免滥用的制衡机制，即便小范围、不透明、不记录地运用监控也可能产生寒蝉效应。

53. 以下各小节列出了对一些法律的共同关切，这些法律允许国家在可能危及言论自由权和隐私权的情况下进行通信监控。

A. 司法监督不足

54. 传统上，通信监控需要得到司法机关的批准，然而，这一要求正在被日渐弱化或消除。在一些国家，一名政府部长、其代表或一个委员会即可批准截取通信。例如，在联合王国，截取通信由国务大臣批准；[33] 在津巴布韦，截取通信由交通通信部长批准。[34] 逐渐地，广泛且不加区分的通信监控也能够获得批准，而无需执法当局逐案确立监控的事实依据。

55. 很多国家在法院发出截取令后不再需要执法机关返回法庭接受监督。例如，2012 年《肯尼亚防止恐怖主义法》规定，可以无期限地进行通信截取，而

[33] 第五章，2000 年《调查权力规范法》。

[34] 第五章，2006 年《截取通信法》。

不要求执法机关向法院进行报告或请求延期。一些国家对截取令的执行设置了时限，但允许司法当局多次无限地延长该指令。

56. 即便在依法规定需要司法授权的情况下，往往这种授权实际上是对执法请求的任意批准。在执法需要确立的必要门槛较低的情况下尤为如此。例如，2010 年《乌干达截取通信规范法》仅要求执法当局证明存在允许进行截取的“合理”理由。在这种情况下，考虑到监控导致调查、歧视和人权受侵犯，确定监控必要性的举证责任是极低的。在其他国家，一系列复杂的法律批准在各种不同情况下获取或截取通信。例如，在印度尼西亚，《精神药品法》、《麻醉药品法》、《电子信息与交易法》、《电信法》和《腐败法》均包含通信监控部分。在联合王国，根据 2000 年《调查权力规范法》，200 多个机构、警察部门和监狱当局有权获取通信数据。因此，个人很难预计他们可能在何时遭到哪个国家机关的监控。

57. 在很多国家，通信服务提供商被迫改造其基础设施以允许直接监控，因而消除了司法监督的机会。例如，2012 年，哥伦比亚司法部以及信息技术和通信部发布了一项指令，要求电信服务提供商建立基础设施，允许司法警察在没有总检察长命令的情况下获取通信。[35] 上述 2010 年《乌干达截取通信规范法》(第 3 条)规定设立一个监测中心，并强制要求电信提供商确保将截取的通信传送至监测中心(第 8 条第 1 款(f)项)。印度政府拟设立一个中央监测系统，将所有通信发送至中央政府，使安全机构能够避开与服务提供商的互动。[36] 这些安排使通信监控脱离司法授权领域，允许不受监管的秘密监控，使政府摆脱了任何透明度和问责制要求。

B. 国家安全例外情况

58. 含糊不明的“国家安全”概念在很多国家已成为了截取和获取通信的理由。例如，在印度，2008 年《信息技术法》除其他外，允许为了“印度的主权、完整或国防、与外国的友好关系、公共秩序和调查犯罪行为”截取通信(第 69 条)。

59. 在很多情况下，国家情报机关还享有司法授权要求的广泛例外情况。例如，在美国，《外国情报监控法》授权国家安全局无需司法授权既可截取下述情况下的通信：通信的一方在美国境外，另一方有理由被认为是国家认定的恐怖组织的成员。德国的法律允许国家情报部门出于保护自由民主秩序、国家的存在和安全的目的在没有搜查令的情况下对国内外通信进行自动化监听。[37] 在瑞典，

[35] 司法部以及信息技术和通信部第 1704 号指令。基于 2004 年《刑事诉讼法》。

[36] 通信部。印度政府。2011-2012 年度报告，第 58 页，http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf。

[37] G-10 法。

《防卫行动信号情报法》授权瑞典情报部门在没有搜查令或法院指令的情况下截取所有瑞典境内的电话和互联网信息。在坦桑尼亚联合共和国，1996 年《情报和安全事务法》允许该国情报部门只要有合理理由认为某人或机构对国家安全构成危险或危险源或威胁，即可开展调查并调查任何人或机构。

60. 以含糊不明的国家安全概念为依据大规模限制人权的享受，这是令人严重关切的情况。[38] 这一概念定义广泛，因此易被国家操纵，成为针对人权维护者、记者或活动分子等弱势群体采取行动的借口。它还许可调查和执法活动采用常常不必要的保密做法，破坏了透明和问责原则。

C. 不受监管的通信数据获取

61. 获取国内通信服务提供商掌握的通信数据常常是立法强制要求的，或是签发执照的一个条件。因此，各国普遍可以无限获取通信数据而不受监督或监管。例如，巴西 2012 年反洗钱法授权警察无须获得法院指令即可从互联网和通信提供商获取注册信息。[39] 在国际一级，通信数据的获取由《司法协助条约》规范。但是，这方面的合作还常常是基于服务提供商或互联网公司的自愿遵从而违法进行的。因此，很多国家可以在不经独立授权且仅有有限监督的情况下获取通信数据。

D. 法外监控

62. 以上列出的一些监控能力超出了现有法律框架，但依然被各国广泛采用。木马等进攻性侵入软件或大规模截取能力构成了对传统监控概念的严重挑战，以致于它们无法与关于监控和获取私人信息的现行法律保持一致。它们不仅是进行监控的新方法，还是新的监控形式。从人权角度来看，这类技术的使用极为令人不安。例如，木马不仅使国家能够连接设备，还能无意或故意地更改设备中的信息。这种做法威胁到的不仅是隐私权，还有在法律诉讼中使用这种证据的程序公正权。大规模截取技术消除了相称性的考量，允许不加区分的监控。它使国家能够监测特定国家或区域的所有通信行为，而不用为每次截取获得授权。

63. 各国政府往往不承认使用这类技术进行监控，或辩解说这类技术是在现行监控立法范围之内合法使用的。显然很多国家都掌握着木马技术等进攻性侵入软件，但除了德国之外，没有任何一个国家对其使用的法律依据进行过公开辩论。在那次辩论后，北莱茵－威斯特法伦州于 2006 年通过了一项立法，授权“秘密访问信息技术系统”(§ 5.2 第 11 号，《北莱茵－威斯特法伦宪法保护法》)，据

[38] 人权理事会关于反恐的各项决议。

[39] 巴西联邦法 12683/2012, 第 17-B 款。可查阅 http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm。

认为这种做法为技术渗透，其实施办法是安装间谍程序或利用系统的安全漏洞。德国联邦宪法法院于 2008 年 2 月废除了该法，裁决这种措施不符合人权，除非它们得到司法授权和审查，并仅用于极其重要的合法权益可能面临实际危险的情况。[40]

E. 监控法律的域外适用

64. 为了应对数据跨国流动增加以及通信大部分都存储于外国第三方服务提供商的情况，一些国家已开始通过各项法律，授权它们进行域外监控或截取外国辖区的通信。这种做法引起了严重关切，它涉及实施域外侵犯人权行为，并且个人无法知晓他们可能受到外国监控，无法质疑外国监控的决定或寻求补救措施。例如，在南非，《一般情报法修正案》允许对南非境外或经过南非的外国通信进行监控。[41] 2012 年 10 月，荷兰司法与安全部向荷兰国会提出了立法修正案，拟允许警察侵入荷兰境内外的电脑和移动电话以安装间谍软件以及搜索和销毁数据。[42] 2012 年 12 月，巴基斯坦国民议会通过了 2012 年《公平审判法》，其中第 31 款规定了在外国辖区执行监控授权令。当月晚些时候，美国更新了 2008 年《外国情报监控修正案法》，扩大了政府对美国境外的非美籍人士进行监控的权力(§1881a)，包括任何利用设在美国的云服务主机的通信(如谷歌和其他大型互联网公司)。[43] 还是在 2012 年，欧洲电信标准协会设计了欧洲各国政府截取外国基于云的服务的标准草案。[44] 这些事态发展显示了监控权力超越国家边界这一令人忧虑的趋势，增加了国家执法和安全机构达成合作协议规避国内法律限制的风险。

F. 强制性数据保留

65. 一些国家为了存储更多它们获取的通信数据通过了强制性的数据保留法，要求互联网和电信服务提供商(统称为“通信服务提供商”)持续收集并保存通信内容和用户网上活动的信息。这些法律使国家能够汇编个人的电子邮件和信息、位置、与亲友的互动等历史记录。

---

[40] 资料为德文，联邦宪法法院，1 BvR 370/07 vom 27.2.2008, 第(1-67 段)，http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html。

[41] 第 1 部分 c 项，综合情报法修正案，可查阅：http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf。

[42] 见 http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware。

[43] 见欧洲议会内部政策司政策处 C：公民权利和宪法事务，在云端打击犯罪和保护隐私：研究报告，2012 年。

[44] 欧洲电信标准协会技术报告草案 101 567 合法截取，第 1.0 卷(2012-5)；云/虚拟服务。可查阅 www.3gpp.org。

66. 为了向用户提供服务，通信服务提供商为用户的设备或网络提供了一个互联网协议(IP)地址[45]，该地址定期变更。IP 地址的信息可被用来查明个人的身份和位置并跟踪他们的网上活动。强制性数据保留法强迫通信服务提供商在特定时限内保存其 IP 地址分配情况，这使国家更有能力要求通信服务提供商根据具体日期和时间的给定 IP 地址确定个人身份。一些国家还正在设法迫使第三方服务提供商收集和保留它们通常不收集的信息。

67. 国家数据保存法律具有侵害性且代价较大，还威胁着隐私权和言论自由权。强制性数据保留法迫使通信服务提供商建立大型数据库，记录个人之间通过电话或互联网的通信、交流持续时间、用户的位置等信息并保存这些信息(有时长达数年)，从而极大地扩大了国家监控的范围，也因而扩大了侵犯人权的范围。通信信息数据库容易遭到偷窃、欺诈使用和意外披露。

G. 身份披露法律

68. 在很多国家，法律要求个人在网吧提供身份证明。在个人电脑拥有率低且个人严重依赖公用电脑的国家，这种法律特别成问题。例如，在印度，2011 年《信息技术(网吧指导方针)规则》要求网吧业主获取网吧客户的身份证件，其记录必须保存至少一年(第 4(2)项规则)。网吧必须保存包含登陆和退出系统的时间以及电脑终端标识等信息的运行登记簿，保存期最少为一年(第 5(1)和 5(2)项规则)；存储并备份任何用户每次接入或登陆的运行记录至少一年(第 5(4)项规则)。

69. 很多国家还要求个人在网上使用真实姓名，并需要提供官方身份证明以确定其身份。在大韩民国，2007 年通过的《信息通信法》要求用户只有在进行实名注册后才能访问日访问量超过 100,000 次的网站，声称这是为了减少网上欺凌和仇恨言论。宪法法院最近废除了该法，依据是它限制了言论自由并破坏了民主。[46] 中国最近通过了《关于加强网络信息保护的决定》，要求互联网和电信提供商在用户注册互联网接入、固定电话或移动电话服务时收集其个人信息。为用户提供信息发布服务的服务提供商须能够将网名与真实身份联系起来。实名注册要求更便于当局查明网络评论者的身份或将移动设备的使用与具体个人进行绑定，消除匿名言论。[47]

70. 防止通信匿名的另一项举措是逐渐通过各项政策，要求用户使用真实姓名或政府发放的身份证件注册 SIM 卡。在 48 个非洲国家，法律要求个人在激活预付费 SIM 卡前向其网络提供商注册个人信息，据报道，这些法律便利了用户信

[45] IP 地址是识别接入互联网的所有电脑或其他设备的唯一数字代码。

[46] 宪法法院决定 2010Hun-Ma47(“实名”决定)，2012 年 8 月 23 日，法院决定的正式概要可查阅 http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp，仅提供韩文。

[47] “中国将加强互联网信息保护”http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm。

息大型数据库的建立，消除了匿名通信的可能性，使定位跟踪成为可能，还简化了通信监控。[48] 在缺乏数据保护立法的情况下，政府部门可以共享 SIM 卡用户的信息，并将其与其他私人和公共数据库进行对应，使国家能够建立每个公民的全面概况。如果个人注册时无法或不愿意提供身份证件，他们将面临无法使用移动电话服务(这种移动电话服务不仅能进行通信还能使用金融服务)的风险。

H. 对加密的限制以及主要的披露法律

71. 限制使用加密等用来保护通信的隐私增强工具的法律也破坏了通信的安全性和匿名性。很多国家已通过了法律，强制要求个人在得到命令后进行解密。2002 年《南非截取通信和获取通信相关信息规章法》要求任何掌握破解秘钥者协助破解。[49] 类似的法律也存在于芬兰(1987/450 号《强制措施法》第 4 条(4)款(a)项)、比利时(2000 年 11 月 28 日《计算机犯罪法》第 9 条和澳大利亚(2001 年《网络犯罪法》第 12 和第 28 条)。

七. 私营部门的作用和责任

72. 实现动态的新通信形式的重要技术发展主要产生于私营部门。从这种意义上说，我们交流、接受和传递信息方式的很多变革都是基于企业行为者的研究和创新。

73. 私营部门还在通过多种方式助长国家对个人的监控方面发挥了重要作用。企业行为者不得不响应要求，使数字网络和通信基础设施的设计允许国家侵入。这种要求最初于二十世纪 90 年代被各国所采用，正在成为对所有通信服务提供商的强制性要求。各国越来越多地通过立法，要求通信服务提供商允许国家直接获取通信数据或改造基础设施为新形式的国家侵入提供便利。

74. 通过以特定方式开发和使用新技术和通信工具，企业行为者还主动采取措施为国家监控通信提供便利。这种合作最简单的表现形式是关于企业行为者如何收集和处理信息的决定，它使企业行为者成为大规模的个人信息库，国家可以在需要时使用。企业行为者采用了相应的规格，允许国家进入和侵入，收集过度的揭示性信息，或限制可能不利于企业和政府获取信息的加密或其他技术的使用。私营部门还常常未能采用隐私增强技术，或以不够先进和安全的方式采用这种技术。

[48] Kevin P. Donovan 和 Aaron K. Martin, “非洲 SIM 注册的兴起：移动、身份、监测和阻力”，信息系统和创新小组工作文件系列，第 186 号，伦敦政治经济学院(20012)

[49] 第 29 条，2002 年《南非截取通信和获取通信相关信息规章法》。可查阅：http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf。

75. 在最严重的情况下，私营部门违反现行法律标准共谋开发能够进行大规模侵入性监控的技术。[50] 企业部门造就了一个专注于监控技术交流的全球产业。这种技术常常被售往一些很可能将其用来侵犯人权(特别是人权维护者、记者和其他弱势群体的人权)的国家。这一产业基本不受监管，因为各国无法跟上技术和政治发展的步伐。

76. 各国的人权义务要求它们不仅应尊重并促进言论自由权和隐私权，还应保护个人免受企业行为者实施的侵犯人权行为。此外，国家如与企业行为者签约，或立法允许工商企业提供可能影响享有人权的服务，则应行使充分监督，以履行其国际人权义务。[51] 这方面的人权义务适用于企业行为者在国外经营的情况。[52]

77. 各国必须确保私营部门能够独立地以增进个人人权的方式履行其职能。同时，不应允许企业行为者参与侵犯人权的活动，并且各国有责任在这方面对公司进行问责。

八. 结论和建议

78. 各种通信技术取得了很大发展，改变了各国进行通信监控的方式。因此，各国必须调整其对通信监控的理解和监管并改变其做法以确保尊重和保护个人人权。

79. 各国如果不尊重、保护和增进个人隐私权，就无法确保他们能够自由寻求和获取信息或表达意见。隐私和言论自由是相互联系和互相依存的；侵犯其中一项权利就可能是侵犯另一项权利的起因或后果。如果没有确保通信隐私、安全和匿名的适当立法和法律标准，就无法使记者、人权维护者和举报人等人确信他们的通信不会受到国家检查。

80. 为了履行人权义务，各国必须确保言论自由权和隐私权是其通信监控框架的核心。为此，特别报告员建议如下：

A. 更新并加强法律和法律标准

81. 通信监控应被视为具有高度侵入性的行为，可能会妨碍言论自由权和隐私权，威胁民主社会的基础。立法必须规定国家对通信的监控只能在最特殊的情况下进行，并仅在独立司法当局监督下进行。法律中应包括一些明确保障，涵盖可

[50] 私营部门设计并被利比亚、巴林、阿拉伯叙利亚共和国、埃及和突尼斯所采用的监测技术实例，可参阅欧洲议会对外政策司政策处，阿拉伯之春后：欧洲外交政策处理人权和互联网问题的新途径(2012 年)，第 9-10 页。

[51] 工商业与人权：实施联合国“保护、尊重和补救”框架指导原则，第 5 条原则。

[52] 人权事务委员会，结论性意见，德国，2012 年 12 月。

能采取措施的性质、范围和持续时间，命令进行监控的理由，授权、执行和监督这些行动的主管当局，以及国内法规定的补救办法。

82. 个人应拥有被告知他们受到通信监控或国家获取其通信数据的合法权利。虽然认识到提前或即时的通知可能会损害监控的有效性，但应在监控完成后立即通知个人，并使他们有可能在事后就通信监控措施的运用寻求补救。

83. 法律框架必须确保通信监控措施：

(a) 由法律规定，符合明确和准确标准，足已确保使用这些措施时个人得到提前通知并可以预知；

(b) 为实现合法目的而绝对和明确必要的；

(c) 遵守相称原则，在可使用或未用尽侵入性较小的技术之前不予使用。

84. 各国应对公共或私人行为者实施的非法监控进行定罪。这些法律不得被用来针对举报人或其他试图揭露侵犯人权行为的个人，也不应妨碍公民对政府行动的合理监督。

85. 私营部门向国家提供通信数据的行为应得到充分监管，以确保无论何时均优先考虑个人人权。只有在其他可用的侵入性较小的技术被用尽的情况下方可使用国内企业行为者掌握的通信数据。

86. 向国家提供通信数据的做法应受到法院或监督机制等独立当局的监测。在国际一级，各国应通过《司法互助条约》，监管获取外国企业行为者所掌握通信数据的行为。

87. 非法采用的监控技术和做法必须受到立法管制。其法外使用破坏了基本的民主原则，并有可能产生有害的政治和社会影响。

B. 便利私人、安全和匿名的通信

88. 各国应避免强制将用户身份证件作为进行通信(包括在线服务、网吧或移动电话通信)的先决条件。

89. 个人应能够自由使用任何他们所选择的技术来防护其通信。各国不应干涉加密技术的使用，或强迫提供加密秘钥。

90. 各国不应仅出于监控目的保留或要求保留特定信息。

C. 增加公众获取信息的渠道，提高对威胁隐私因素的了解和认识

91. 各国应在通信监控技术和权力的使用和范围方面完全透明。它们至少应公布关于批准和拒绝的要求次数的资料，将要求按服务提供商、调查和目的进行分列。

92. 各国应向个人提供充分信息，使他们完全理解许可通信监控的法律的范围、性质和适用。各国应使服务提供商能够公布它们处理国家通信监控所采用的程序，遵守这些程序并公布国家通信监控的记录。

93. 各国应设立能够确保国家通信监控的独立性和问责制的独立监督机制。

94. 国家应提高公众对新通信技术使用的认识，以帮助个人适当评估、管理和减轻通信所涉的风险，并就此做出知情决定。

D. 监管监控技术的商业化

95. 各国应确保企业行为者提供通信服务时收集的通信数据受到最高标准的数据保护。

96. 各国不得强迫私营部门实施危及通信服务隐私性、安全性和匿名性的措施，包括不得要求为国家监控目的而建设截取能力或禁止使用加密办法。

97. 各国必须采取措施防止监控技术的商业化，考虑到这些技术助长蓄意侵犯人权行为的能力，要特别注意这些技术的研究、开发、交易、出口和使用。

E. 进一步评估有关国际人权义务

98. 鉴于技术进步，很有必要增强对保护隐私权的国际认识。人权事务委员会应发布一份新的关于隐私权的一般性意见，取代第 16 号一般性意见(1988 年)。

99. 各人权机制应进一步评估开发和提供监控技术的私人行为者的义务。