必要和相称

适用人权于通信监控的国际原则

鸣谢

《国家通讯监控应遵守之国际人权原则》由世界各地的隐私权保护组织和专家共同撰写，包括但不限于 Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India, Comisión Colombiana de Juristas, Electronic Frontier Foundation, European Digital Rights, Reporter Without Borders, Fundación Karisma, Open Net Korea, Open Rights Group, Privacy International 以及 Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic。此外，我们亦感谢将各相关组织联系在一起的 IP Justice, SHARE Foundation - SHARE Defense, IFEX Network 和 Instituto NUPEF。

访问 **necessaryandproportionate.org/text**获取更多信息

历史背景

2012年10月布鲁塞尔会议期间，40多位隐私和安全领域的专家参与起草了《原则》。

经过2012年12月在里约热内卢举行的第二次会议等初步广泛磋商，在Access, EFF 和 Privacy International 领导的共同起草过程中，《原则》采纳了 世界各国人权和数字信息权专家的专业意见。《原则》的最初版本于2013年7月10日完成，并于2013年9月在位于日内瓦的联合国人权理事会发布。鉴于这一巨大的成功和全球400多个组织对该《原则》的广泛采纳，为了保障其在不同法律制度下得到一致的解释和应用，我们有必要对《原则》的语言进行一些具体的、主要是表面的措辞上的修改。在201 3年3月至2013年5月举行的新一轮磋商中，我们辨别并修改了这些措辞问题，并对《原则》做出了相应的修订。这些修改并不影响《原则》的效用和目的。这一版本是历经这些程序的最终成果，是《原则》的权威版本。

适用人权于通信监控的国际原则

最终版本 二零一四年五月*

随着协助政府实施通信监控的技术不断进步，政府已无法确保通信监控相关的法律、规定、活动、权力和执行机构对国际人权法和标准的遵守。这一文件旨在厘清国际人权法如何适用于当前的数字环境，尤其在通信监控技术和手段不断增多和变化的背景下。这些原则可以为公民社会团体、产业、政府及其他相关方面提 供一个框架以评估当前已实施的或正在提议中的监控法律和行为是否符合人权。这些原则是与公民社会团体、产业、和专攻通信监控法律、政策和技术的国际专家所 进行的全球性的磋商的结果。

前言

隐私是一项基本人权，对民主社会的存续十分必要。隐私是人格尊严的基本要素，对隐私的保障有助于巩固诸如言论和信息自由、结社自由等其他权利，受到国际人权法的认可。[1] 通信监控是对隐私权等人权的干预。因此，只有当其被明确法律授权，是达到合法目的的必要手段，并且干预程度与目的相当的时候，通信监控才具有正当性。[2]

在互联网被公众广泛使用之前，完善的法律原则及监控通信本身的运作成本限制了政府的通信监控行为。近几十年来，运行通信监控的门槛降低，且新科技时代法规原则的应用也变得模糊。由于个人通信或电子设备使用产生的信息和数字通信内容呈现爆发式增长、储存和挖掘大量数据的成本缩减、以及个人资料透过第三方服务供应商提供，都使得政府实施的通信监控达到了前所未有的规模。[3] 同时，由于现存人权法概念落后于政府日新月异的通信监控技术和手段，因此政府能从不同审查技术获取、合并及组织信息，或提高对于可用信息的敏感度。

政府试图获取的通信内容和元数据的频率大幅增加，却缺乏足够的监管。[4] 从通信元数据可能获知个人的生活概貌，包括医疗情况、政治和宗教观点、参与的组织、来往的对象、兴趣等等。元数据披露的信息的细致程度相当于、甚至远高于可被识别的通信内容本身。[5] 即使使得个人生活极可能受侵犯并对政治或其他团体造成寒蝉效应，法律法规、权力或执行机构通常只给予通信元数据较低级别的保护，也没有加强对政府采用元数据的限制。

适用范围

《原则》及其《前言》部分具有整体性和自参性，即在阅读和理解每一条原则和前言时应考虑一个更大的背景框架，那就是二者共同完成一个目标：保证所有与通信监控相关的法律、政策和行为遵守国际人权法则和标准，并充分保护诸如隐私权和言论自由等个体人权。因此，为了使各国政府切实履行他们在通信监控问题上的国际人权义务，政府必须遵守以下各条原则。

这些原则适用于国家境内外所进行的监控，也适用于基于执法、保护国家安全、收集情报、及其他政府功能等各种目的的监控行

为。这些原则既适用于政府尊重和保障个体人权的义务，也适用于其保护个体人权不受包括企业在内的非国家行为体侵害的义务。[6] 企业承担着尊重个人隐私及其他人权的责任，尤其鉴于其在设计、发展和普及通信技术，启用和提供通信手段，以及协助某些政府监控活动上所扮演的关键角色。[7] 尽管如此，这些原则所阐述的仍然是政府进行通信监控时所涉及到的责任和义务。

变化中的技术与定义

“通信监控”在现代环境中涵盖对包括、反映、源自或涉及个人在过去、现在、未来通信的信息所进行的监视、窃听、收集、获取、分析、使用、保存、保留、干扰、访问或其他类似的行为。

“通信”包括通过数字媒介传递的活动、互动和交易，例如通信的内容、通信各方的身份、定位追踪、以及包含IP地址、通信时间与时长、和通信过程中所使用的通信设备身份识别码在内的信息。

“受保护信息”是指包括、反映、源自或涉及个人通信，且目前不向一般大众公开但容易被一般大众获取的信息。传统上，对通信监控的侵入性评估通常基于形式主义的人为划分。现有法律框架对“内容”或“非内容”，“用户资料”或“元数据”，已储存信息或正在传输的信息、自家持有的信息或由第三方服务供应商持有的信息等做出了区分。[87] 但是，这些区分方法已经不再适合用于衡量通信监控对个体私生活和组织的侵入程度。虽然基于通信内容揭露敏感信息的能力，对于其需要受到大量法律保护这一事实早已达成共识，但现在显而易见的是，诸如元数据等源自通信的其他非内容信息可能揭露比内容本身更多的个人信息，因此后者需要相同程度的保护。现今，任何一种信息，不管是其本身还是与其他信息一起被分析，都可能揭露一个人的身份、行为、组织、身体或医疗情况、种族、肤色、性取向、国籍或观点，或勾勒出一个人在一段时间内的地理位置、行动或人际互动等情况[9]，抑或是包括游行或其他政治活动在内的某个既定地点上所有人的情况。因此，所有的“受保护信息”都应该在法律上受到最高级别的保护。

在评估政府通信监控侵入性时，我们必须既要考量监控导致“受保护信息”被披露的可能性，也要考虑政府搜集信息的目的。任何通信监控都是对人权的干预，因此国际人权法对其适用。受保护信

息的揭露可造成一个人遭受调查、歧视或人权侵害。可能泄露受保护信息的通信监控不仅将构成对个人隐私权的严重侵犯，还有损其享有的其他基本人权，包括言论自由、结社自由、和参政自由。这是因为这些权利的行使要求人们能够在通信时不受政府监控所产生的寒蝉效应影响。因此，对于每个具体案例，审视每次所收集信息的性质和可能用途都是必要的。

在采用新的通信监控技术或扩展现有手段的使用范围时，政府必须在搜集信息之前先确认可能获得的信息是否属于“受保护信息”，并且应该服从司法部门或其他民主监督机制的审查。在衡量通信监控所获取的信息是否达到“受保护信息”的级别时，监控的形式、范围和持续时间都是相关因素。由于通信监控所使用的广撒网型或系统性的监视或者入侵手段所能揭露的私密信息远超过其收集的各单一信息本身，原本针对非受保护信息的监控的侵入性可能因此升高，以至于非受保护信息也需要受到与“受保护信息”同等的全面保护。[10]

对政府是否可以进行涉及“受保护信息”的通信监控之决定必须符合下列原则。

十三项原则

十三项原则

合法性

任何对人权的限制都必须由法律规定。若没有现行的、公之于众的、清晰度和准确性均符合标准的——即能充分保证个人被事先通知并了解其实行——之法案，政府不得采取或执行侵犯这些权利的措施。鉴于技术变化之快，限制人权的法律必须通过有民主参与的立法序及定期审查。

合法目的

法律只能允许特定的政府权力机构进行符合民主社会所必需的重要法定权益的，即具有合法目的的通信监控。任何措施在贯彻过程中不得因种族、肤色、性别、语言、宗教、政治或其他观念、国籍或社会出身、财产、出生或其他身份而具有歧视性。

必要性

有关监控的法律、法规、活动、权力或执行机构必须限制在监控对达到某一合法目的具有严格且突出的必要性的情况下。只有当监控是达到某一合法目的之唯一手段，或者监控在有多种可行方式的情况下，是触犯人权可能性最低的手段时，才能被执行。政府始终有责任确保和维持这一正当性。

适当性

任何经法律授权的通信监控必须适于完成其认定的、具体的合法目标。

比例原则

通信监控必须被视作一项干预人权、威胁民主社会之基、具高度侵入性的行为。在做出通信监控的决定时，必须考虑所获取信息的敏感性以及其侵害人权和其他相关利益的严重性。

这就要求：在最低限度上，政府进行以执法、保护国家安全或收集情报为目的的通信监控之前，必须向主管司法机构报备并确保以下几点成立：

1. 一项严重的犯罪或对合法目标的具体威胁已经发生或即将发生的可能性高； 而且,
2. 这一严重犯罪或对合法目标的具体威胁的相关证据和材料可通过收集受保护信息获取的可能性高；而且,
3. 其他侵入性较小的手段已经用尽或者无济于事，故通信监控是可行手段中侵入性最小的；而且，
4. 仅限于获取与严重犯罪或对合法目标的具体威胁相关和提供实质性证据的信息；而且，
5. 所采集信息的所有多余部分不得被保留，必须当即销毁或归还；而且
6. 唯有指定的执行机构能够获取信息，且必须依照被授权的使用目的和时长来采用这些信息；而且
7. 所要求进行的监控活动和所提议的监控手段不损害隐私权或基本自由的核心精神。

主管司法机构

有关通信监控的决定必须由公正独立的主管司法机构做出。该机构必须：

1. 区别且独立于进行通信监控的机构;
2. 熟知与通信监控合法性、所使用的技术和人权相关的事宜，且有能力针对其做出裁决；以及
3. 有足够的资源供其行使被分配的职能。

正当法律程序

正当法律程序要求政府保证任何涉及干预人权的法律程序都能明文列举、执行一致并且公之于众，以此尊重和保障个人

人权。尤其在关乎其人权的决定时，每个人都有权利在合理的时间内，在依法建立的独立、有法律权威和公正的法庭上进行公平公开的听证，[11] 除非有危及性命的紧急情况发生。在这样的情况下，必须在事后合理可行的时间内寻求追溯性授权。只因有潜逃或证据被销毁的风险并不不足以作为追溯性授权之理由。

告知当事人

通信被监控的当事人应该被告知通信监控获得授权的裁决，并给予足够的时间和信息以使他们能够对决定提出质疑或寻求其他补救措施，他们还应该有权获取使该监控获得授权的支撑材料。唯有下列情况可以延迟通知：

1. 若告知，通信监控被授权的目的会遭到严重损害，或者会有危及性命的迫切风险；以及

2. 延迟告知一举经过了主管司法机构的批准；以及

3. 一旦主管司法机构裁定危机已经解除，必须立刻通知当事人。

政府有义务告知当事人，但是通信服务供应商享有在自愿或被要求的情况下告知通信监控当事人的自由。

透明度

政府应该将通信监控法律、规定、活动、权力或执行机构的用途和范围透明化。在最低限度上，他们应该公布被允许和被拒绝的监控要求的汇总信息，以及服务供应商和调查机构二者所提出的监控要求的类型、目的、以及受影响的人数的分类信息。

政府应该提供足够的信息给当事人，使其能够完全了解授权通信监控法律的范围、性质和应用。政府不得干预服务供应商公开其在评估和配合政府通信监控要求时的操作程序、遵守该程序、以及公布政府通信监控要求记录等行为。

公众监督

政府应该建立独立的监督机制以确保通信监控的透明度和问责。[12] 监督机制应具有以下权力：有权获取所有可能与政府行为有关的信息，包括在适当的情况下获取秘密或机密信息；评估政府是否依法使用其被法律授权的职能；评估政府有无履行其透明化的义务，完整地和准确地公布关于通信审查手段和权利之使用情况和范围的信息；发布关于通信监控的定期报告和其他信息；以及对这些行为的合法性，包括其对《原则》的遵守程度，做出公开决定。即使现已有政府其他部门履行监督职责，也必须额外设立独立的监督机制。

通信和系统的完整性

为了保障通信系统的完整性、安全性和私密性，和基于对以政府之名妨碍安全往往会殃及其它这一现实的认识，政府不得强迫服务供应商或硬件软件贩售商在自家系统内安装监控或监视功能，或者收集和保留仅用于国家监控目的的特定信息。政府决不能要求服务供应商提前保留或收集数据。个人有匿名表达自我的权利，因此，政府应该避免强迫实行通信用户进行实名制。[13]

维护国际合作

为应对信息流、通信技术和服务的变化，政府可能需要寻求国外服务供应商和其他国家政府的协助。相应地，各国政府间签订的司法互助协定和其他条约都应确保，若两国或多国皆有适用于通信监控的法律，则应以对个人提供保护标准最高的一方之法律为准。政府寻求执法协助的目的，应采取“双重犯罪原则”。各国不得利用司法互助协定和他国获取“受保护信息”的请求为由，规避国内法律对通信监控的限制。司法互助协定和其他条约应该明确载录、对公众公开、并保证程序的公平性。

防止非法获取信息

政府必须立法将公共或私营行为体的非法通信监控行为定为犯罪。该法律对罪犯的民事和刑事处罚、对举报人的保护以及为受影响的个人提供的申诉途径都应该是充分而重大的。法律应规定，任何通过与这些原则相悖的方式所获取的信息均不得被

视作证据，或在任何诉讼中被考虑，连由这些信息衍生出证据也不例外。政府还应该制定法律规定，通信监控所获得的材料在被用于授权目的之后，不得被保留，应当被销毁或者退还给当事人。

*《原则》的详细制定过程始于2012年10月于布鲁塞尔举行的，由40多位隐私权和安全专家出席的会议。经过2012年12月在里约热内卢举行的第二次会议等初步广泛磋商，在Access, EFF 和 Privacy International 的领导的共同起草过程中，《原则》采纳了世界各国人权和数字信息权专家的专业意见。《原则》的最初版本于2013年7月10日完成，并于2013年9月在位于日内瓦的联合国人权理事会发布。鉴于这一巨大的成功和全球400多个组织对该《原则》的广泛采纳，为了保障其在不同法律制度下得到一致的解释和应用，我们有必要对《原则》的语言进行一些具体的、主要是表面的措辞上的修改。在2013年3月至2013年5月举行的新一轮磋商中，我们辨别并修改了这些措辞问题，并对《原则》做出了相应的修订。这些修改并不影响《原则》的效用和目的。这一版本是历经这些程序的最终成果，也是《原则》的权威版本。

尾注

1 《世界人权宣言》第十二条、《联合国移徙工人条约》第十四条、《联合国儿童权利公约》第十六条、《公民及政治权利国际公约》第十七条；区域性公约如《非洲儿童权利与福利宪章》第十条、《美洲人权公约》第十一条、《关于非洲言论自由原则的宣言》第四条、《美洲人的权利和义务宣言》第五条、《阿拉伯人权宪章》第二十一条、《东盟人权宣言》第二十一条、《欧洲保障人权和根本自由公约》第八条；《约翰内斯堡关于国家安全、言论自由和获取信息自由原则》和《关于言论自由和平等的卡姆登原则》。

2 《世界人权宣言》第二十九条；联合国人权委员会按照《公民及政治权利国际公约》第四十条第四款通过的一般性意见第二十七号，1999年11月2日CCPR/C/21/Rev.1/Add.9; 也可参见马丁·施凯宁（Martin Scheinin）《在反恐的同时促进和保护人权和基本自由问题特别报告员报告》，2009年A/HRC/17/34；也参见弗兰克·拉吕（Frank La Rue）《特别报告员向人权理事会提交的关于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的报告》，2013年A.HRC/23/40EN。

3 通信元数据可包括关于我们身份（用户信息、通信设备的信息），互动（通信的起点和终端，尤其是那些数据可披露所访问的网站、阅读的书籍和其他材料、相来往的人、朋友、家人、熟人、搜索的信息和使用过的资源），和地点（什么时间在什么地方，与其他人的距离）的信息。总而言之，元数据提供了观察现代生活的近乎每一个行为、我们的心理状态、兴趣、意图和最隐秘的想

法的一个窗口。

4 例如，单单在英国每年就有将近50万获取通信元数据的请求。目前，英国的执法机构能够自我授权，即自行批准他们从服务供应商那里获得信息的请求。同时，谷歌透明度报告的数据显示，仅在美国，获取用户信息的请求就由2010年的8888起上升到2011年的12271起。在韩国，每年有大约600万获取用户或发帖者信息的请 求，而且在2011年到2012年间，每年有3000万针对其他形式通信元数据的请求

且基本上都被批准和执行。2012的数据可见于http://www.kcc.go.kr/user.do?mode=view&page=A02060400&dc=K02060400&boardId=1030&cp=1&boardSeq=35586。

5 可参见麻省理工学院《科技创业》（Technology Review）中对桑迪·彭特兰（Sandy Pentland）《挖掘真相》（Reality Mining）的书评，2008年，http://www2.technologyreview.com/article/409598/tr10-reality-mining/， 以及阿尔伯托·艾斯库德罗-帕斯卡尔（Alberto Escudero-Pascual）和格斯·霍森（Gus Hosein）《对非法获取互联网流量数据的质疑》（Questioning lawful access to traffic data), 载于《美国计算机学会通讯》第47卷第3期，2004年3月，77-82页。

6 《联合国增进和保护见解和言论自由权问题特别报告员报告》，弗兰克·拉吕（Frank La Rue），2011年5月16日，可见于http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf。

7 “人们向其手机服务供应商泄露他们所拨打或发送短信的电话号码，向他们的互联网服务供应商泄露他们访问的网址和有邮件往来的电子邮件地址，以及向网上零售商泄露他们所购买的书籍、杂货和药品……我认为这些因特定目的自愿披露给部分人的信息不该单单因这一原因被剥夺第四修正案的保护。”摘自2012年美国诉琼斯案（United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 957）索托马约尔法官 （Sotomayor, J.）协同意见书。

8 “短期监视一个人在公共街道上的行动符合隐私权的期许”但是“在绝大多数犯罪调查中使用GPS系统进行的较长期监视则侵犯了隐私权的期许。”摘自2012年美国诉琼斯案（United States v. Jones, 565 U.S., 132 S. Ct. 945, 964）阿里托法官（Alito, J.）协同意见书。

9 “长期监控披露出短期监控所不能的信息，如一个人反复做的事情、一般不会做的事情、和在某个团体里所做的事。每一种这类信息对一个人的披露程度都比一次性、单个的监控高。监视到一个经常去教堂、健身房、酒吧或体育比赛赌博登记的人和监视到这个人去过一次这些地方，或者一个人在一个月内没有去过这些地方一次，完全是两码事。一个人行动的连续性还可以披露出更多信息；一个女人去看一次妇科并不说明什么，但是如果这个女人在数星期之后又去了婴儿用品店，那么这个信息就有不同的意义了。* 一个人若知道他人的一举一动，则可以推断他是否每周都去教堂、是否嗜酒、是否经常在健身房锻炼、是否是一个出轨的丈夫、是否是正在服用药物的门诊病人、是否是某私人或政治团体的成员等。他不仅可以知道关于这个人的一件事，而是所有事。”摘自美国诉梅纳德案（U.S. v. Maynard, 615 F.3d 544, U.S., D.C. Circ., C.A.） 第562页；美国诉琼斯案（U.S. v. Jones, 565 U.S.__, 2012）阿里托法官（Alito, J.）协同意见书。“此外，若公开信息被系统地收集和储存在当局的文档中，则可被划

入私生活的范畴。尤其是当这些信息牵涉一个人很久之前的过去时……本法院认为，若这些信息被系统地收集和储存在政府部门的文档中则应根据《公约》的第八条第一款被划入“私生活”的范畴。”摘自罗塔鲁诉罗马尼亚案（Rotaru v. Romania, [2000] ECHR 28341/95）第43-44段。

10 “正当法律程序”一词可与“程序公平”和“自然公正”互换，并在《欧洲人权公约》第六条第一款和《美洲人权公约》第八条中有所阐述。

11 英国通信监控专员（Interception of Communications Commissioner）就是一个独立监督机制的例子。该机构所发布的一份报告中包含一些汇总数据，但并没有提供足够数据以检视信息获取请求类型、每次请求的程度、请求的目的、和对这些请求做了哪些审查。可见于 http://www.iocco-uk.info/sections.asp?sectionID=2&type=top。

12 《增进和保护见解和言论自由权问题特别报告员报告》，弗兰克·拉吕（Frank La Rue），2011年5月16日，A/HRC/17/27，第84段。