联 合 国 A/HRC/13/37

大 会

Distr.: General
28 December 2009
Chinese
Original: English

人权理事会
第十三届会议
议程项目 3
增进和保护所有人权、公民权利、政治权利、
经济权利、社会权利和文化权利，包括发展权

在打击恐怖主义的同时促进和保护人权和基本自由问题特别报告员马丁·谢宁的报告

摘要

本报告第一章历数了特别报告员在 2009 年 8 月 1 日至 12 月 15 日期间开展的各项主要活动。第二章为报告正文，着重阐述了特别报告员在打击恐怖主义的同时保护隐私权方面关注的若干问题，其中 A 节突出强调了隐私权和数据保护的重要意义。

《公民权利和政治权利国际公约》第十七条体现出相当大的灵活性，允许对于隐私权施加必要、合法且适度的限制。特别报告员在 B 节中指出，可以认为《公约》第十七条包含适度限制原则。为此，特别报告员呼吁各国证实为某一特定目标对《公约》第十七条施加限制属于合法行为，并呼吁人权事务委员会针对第十七条提出新的一般性意见。

特别报告员在 C 节中着重指出，隐私权在打击恐怖主义的斗争中受到损害。在没有充分法律保障的情况下采用监视权和新技术，就会导致这种损害。各国在同第三国及私营部门进行合作时没有扩展现行保障机制，从而危及到对于隐私权的保护。这些做法不仅致使隐私权受到侵犯，还影响到按法律程序审判的权利和行动自由，这一点在边境地区尤其突出，而且可能禁锢结社自由和言论自由。

各国如不制订严格的法律保障措施，没有方法来判断干预措施是否必要、适度及合理，在尽量减少新政策对于隐私权的影响问题上就会陷入无所适从的境地。在 D 节中，特别报告员依据世界各国的决策、判例、政策审查和良好做法，提出了若干法律保障措施。

本报告最后一章针对国内立法机构、国内行政机构以及联合国等众多主要行动方提出建议，以期在打击恐怖主义的同时增进对于隐私权的保护。

目录

一. 导言

1. 依据大会第 63/185 号决议和人权理事会第 10/15 号决议，在打击恐怖主义的同时促进和保护人权和基本自由问题特别报告员向人权理事会提交本报告。报告正文历数了特别报告员在 2009 年 8 月 1 日至 12 月 15 日期间开展的各项活动，并分多个专题，重点阐述了在反恐背景下作为一项人权的隐私权。本报告增编分别载有来文报告(A/HRC/13/37/Add.1)和 2009 年 4 月 17 日至 21 日前往埃及开展实地调查的报告(A/HRC/13/37/Add.2)。

2. 关于即将开展的国别访问，特别报告员希望在提交本报告之前出访突尼斯。特别报告员建议将访问日期定在 2010 年 1 月末至 2 月初，并等待突尼斯政府做出答复。特别报告员还希望在 2010 年对智利和秘鲁开展正式访问。此外，阿尔及利亚、马来西亚、巴基斯坦、菲律宾和泰国也发出了访问邀请，但特别报告员尚未成行。

二. 特别报告员开展的活动

3. 2009 年 9 月 18 日至 19 日，特别报告员在位于佛罗伦萨的欧洲大学研究所召开专家组会议，探讨与特别报告员任务有关的各项专题。[1] 在此次会议期间，威尼斯委员会和欧洲委员会犯罪问题小组委员会联合发起了一场公众运动，名为“打击恐怖主义：对司法机构的挑战”。埃博学术大学人权研究所作为此次运动的出资方之一，通过具体项目支持特别报告员的工作。

4. 2009 年 9 月 29 日至 30 日，特别报告员会同其他相关任务负责人，出席了在日内瓦举行的秘密羁押问题全球协同研究非正式磋商(A/HRC/13/42)。此外，特别报告员还就已经开展和计划开展的国别访问，分别会见了埃及和突尼斯常驻代表团。

5. 2009 年 10 月 2 日至 3 日，特别报告员出席了名为“恐怖主义、安全和人权：政策变革时机”的威尔顿庄园会议，并作为小组成员，参与讨论了国际组织在打击恐怖主义和保护人权方面的作用。

6. 2009 年 10 月 4 日，特别报告员在西班牙毕尔巴鄂市巴斯克地区大学法学院的开学典礼上发表主旨讲话。

7. 2009 年 10 月 12 日至 14 日，特别报告员出席了在维也纳召开的两次会议——反恐联络点国际研讨会和反恐执行工作队务虚会。这次研讨会由多个会员国以及联合国毒品和犯罪问题办公室联合主办，反恐执行工作队办事处和反恐怖主义执行局(反恐执行局)给予密切配合。与会者在此次论坛上探讨如何将各国反恐联络

[1] 特别报告员感谢专家组成员、Gus Hosein 博士及其研究助理 Mathias Vermeulen，以及欧洲大学研究所博士生研讨会与会者协助撰写本报告。

点组织起来，建立更为发达的网络，并且充分发挥这些联络点作为国家、区域和全球反恐前沿的作用，从而将全球和各国的反恐工作进一步紧密结合起来。反恐执行工作队务虚会着重研究今后将如何扩大并加强会员国、联合国系统、区域组织和其他组织以及民间社会的合作伙伴关系，共同执行《联合国全球反恐战略》。[2]

8. 2009 年 10 月 20 日，特别报告员出席了在布鲁塞尔召开的“通过公平、公开程序加强联合国定向制裁”会议，此次会议的主办方是比利时联邦外交、对外贸易与发展合作部。

9. 2009 年 10 月 26 日至 28 日，特别报告员前往纽约，向大会第三委员会递交报告，[3] 这份报告着重阐述了反恐措施的性别影响问题。特别报告员同安全理事会下设的制裁基地组织/塔利班委员会举行正式会晤，并会见了反恐怖主义执行局(反恐执行局)主任。特别报告员作为小组成员，出席了名为“将两性平等观点纳入反恐和国家安全”的会外会议，此次会议的主办方是纽约大学法学院人权和全球正义中心。特别报告员还会见了多个非政府组织，并召开新闻发布会。

10. 2009 年 10 月 29 日，特别报告员在哥伦比亚特区华盛顿会见了美国国务院负责民主、人权和劳工事务的助理国务卿和其他官员，讨论新一届政府当前及今后的法律发展走向、特别报告员在 2007 年出访美利坚合众国的后续工作，[4] 以及在反恐背景下涉及国际人道主义法和人权法的一般性问题。

三. 隐私权

A. 载入各国宪法和国际人权条约的隐私权

11. 隐私权是一项基本人权，假定个人理应享有自主发展、互动和安享自由的领域，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。[5] 隐私权有两个方面。国际人权文书着重强调隐私权的消极面，禁止任意干涉个人隐私、家庭、住宅和通信；[6] 另一方面，某些区域及国内文书则包含了隐私权的积极面，主张人人有权确保自己的私生活、家庭生活、

[2] 见大会第 60/288 号决议。

[3] A/64/211。

[4] 见 A/HRC/6/17/Add.3。

[5] Lester 爵士和 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。

[6] 见《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)、《保护所有移徙工人及其家庭成员权利国际公约》(第 14 条)，以及《儿童权利公约》(第 16 条)。

住宅和通信得到尊重，[7] 有权确保自己的尊严、人格完整和名誉获得承认和尊重。[8] 并非所有国家的宪法都将隐私权作为一项权利单独列出来，但几乎所有国家都承认隐私权的重要意义。在某些国家，人们对于事关背信泄密和干涉人身自由、言论自由及按法律程序审判权利的普通法进行引申，提出了隐私权。在其他国家，隐私权具有宗教意义。从这个意义上讲，隐私权不仅是一项基本人权，更是支撑其他各项人权的基础，是民主社会之本。

12. 随着信息技术的发展，国家开办档案存储设施的能力得以增强。应用强大的计算机技术，人们能够用以前不敢想象的方式来收集、储存和分享个人资料。国际社会制订了国际核心数据保护原则，包括如下各项义务：以公平的方式依法获取个人信息；限制个人信息的使用范围，仅限于最初规定的用途；确保信息处理工作进行得充分、适宜、适度；确保信息的准确性；保证信息安全；不再需要这些信息时予以删除；以及，保证个人有权查阅本人的信息并要求做出改正。[9] 人权事务委员会第 16 号一般性意见明确指出，上述各项原则均属于保护隐私权的范畴，[10] 但数据保护则作为一项单独的人权或基本权利。某些国家甚至将数据保护确定为一项宪法权利，从而突显出这项权利对于民主社会的重要意义。葡萄牙 1976 年《宪法》第 35 条对此做出详细规定，就是相关最佳做法的例证。

13. 隐私权不是一项不受任何限制的绝对权利。一旦个人受到安全机构的正式调查或清查，安全机构之间为反恐目的可以相互交换个人资料，这势必会影响到隐私权。在这种情况下，国家有权依法限制受到国际人权法保护的隐私权。但反恐并不是一张无敌王牌，干涉隐私权的做法不会因打上反恐的标记而自动变得合法化。每一项干涉行动都需要经过严格评估。

B. 适度限制隐私权

14. 在关于隐私权的问题上，《公民权利和政治权利国际公约》第十七条是具有法律约束力的最重要的国际条约规定。165 个国家批准了《公约》，另有六个国家签署了《公约》。[11] 《公约》第四条允许全体缔约国采取措施，克减本

[7] 见《欧洲保护人权与基本自由公约》(第 8 条)以及《开罗伊斯兰人权宣言》(A/45/421-S/21797，第 18 条)，1990 年 8 月 5 日。

[8] 《非洲人权和人民权利宪章》(第 11 条)，另见非洲联盟《非洲表达自由原则宣言》(第 4.3 条)和《美洲人的权利和义务宣言》(第 5 条)。

[9] 见欧洲委员会《关于在个人数据自动处理方面保护个人的公约》(第 108 号)，1981 年；经济合作与发展组织《关于保护隐私和个人数据越界数据流动的指导原则》(1980 年)；以及，《电脑个人资料档案的管理准则》(大会第 45/95 号决议和 E/CN.4/1990/72)。

[10] 人权事务委员会关于尊重隐私、家庭、住宅和通信以及保护荣誉和名誉的权利（第十七条）的第 16 (1988)号一般性意见。

[11] 截至 2009 年 11 月 16 日。在签署《公约》之后尚未批准的六个国家是：中国、古巴、几内亚比绍、瑙鲁、巴拿马和圣马力诺。

《公约》的某些规定，其中包括第十七条。只有当紧急状态威胁到国家存亡安危时，方可采取这种做法，并且必须满足多项条件。[12] 《公约》于 1976 年生效，在此后的 30 多年间，仅有不到 10 个缔约国因恐怖行动或恐怖威胁而宣布进入紧急状态，[13] 其中四个国家在紧急状态下试图克减《公约》第十七条，[14] 另有八个国家宣布克减第十七条，但没有明确说明国家因恐怖主义而进入紧急状态。[15] 但相关通知大多措辞笼统，没有依据《公约》第四条的规定说明在紧急状态期间必须采取哪些具体措施来克减第十七条。[16] 总的说来，因恐怖主义而试图克减《公约》第十七条的缔约国均未遵守《公约》第四条的所有各项规定。此外，仅有一个国家因当前的国际恐怖主义威胁(与 2001 年“9 • 11”事件有关)而宣布克减在《公约》下承担的义务。[17] 对《公约》第十七条提出保留的情况大致相似。国际法通常允许各国对于人权条约提出保留意见，条件是这些保留意见不得有悖条约的目标和宗旨，[18] 仅有一个缔约国对《公约》第十七条提出保留。[19]

15. 由此可见，各国仅在极个别情况下采用公认的国际法机制和《公约》，单方面废止隐私权。有关国家虽然提交了关于克减《公约》第十七条的通知，但这些通知措辞笼统，没有说明克减的实际措施和具体形式。特别报告员认为，各国的上述做法表明，各国普遍认为《公约》第十七条规定的框架具有相当大的灵活性，可以在可允许范围内对于隐私权施加必要、合法且适度的限制，包括在应对恐怖主义状态下。特别报告员支持这种观点。《公约》第十七条允许缔约国对于本条款所载的各项权利施加限制和制约，其中包括隐私权。从这个意义上讲，人权事务委员会作为负责解释《公约》条款和督促缔约国履行条约义务的条约机构，应对此类限制和制约进行监督。行使这项监督职能的主要机制是《公约》第四十条规定的法定报告程序，对于《公约第一任择议定书》的 113 个批准国来说，则是个人申诉程序。

[12] 关于常设条约监督机构对于克减的范围及后果的意见，见人权事务委员会第 29 (2001)号一般性意见。

[13] 阿塞拜疆、智利、哥伦比亚、萨尔瓦多、以色列、尼泊尔、秘鲁、俄罗斯联邦以及联合王国。

[14] 哥伦比亚、萨尔瓦多、尼泊尔和俄罗斯联邦。

[15] 阿根廷、亚美尼亚、厄瓜多尔、尼加拉瓜、巴拿马、塞尔维亚和黑山、斯里兰卡以及委内瑞拉玻利瓦尔共和国。某些情况确实与恐怖主义有关，但关于进入紧急状态的通知没有提及恐怖主义。

[16] 例如，多个拉丁美洲国家在试图克减在《公民权利和政治权利国际公约》下承担的义务时，仅仅通知将“暂停执行”《公约》的部分条款。第 29 号一般性意见指出，这样做不符合《公约》第四条的要求。

[17] 联合王国，2001 年 12 月 18 日。克减范围不包括第十七条，并在 2005 年 3 月 15 日恢复执行《公约》。

[18] 关于常设条约监督机构对于对《公民权利和政治权利国际公约》及其《任择议定书》提出保留的意见，见人权事务委员会第 24 (2004)号一般性意见。

[19] 列支敦士登对于外国人家庭生活得到尊重的权利的适用范围始终持有保留。

16. 《公约》第十七条禁止“任意或非法干涉”任何人的私生活、家庭、住宅或通信，同时禁止“非法攻击”任何人的荣誉和名誉。这就与第十二条第 3 款、第十八条第 3 款、第十九条第 3 款、第二十一条和第二十二条第 2 款等多项条款的提法产生抵触。这些条款都明确提出了适度限制原则。其中，第二十一条和第二十二条第 3 款对于这项原则的阐述最为详尽，包括如下三点内容：(a) 限制必须遵守国内法律规定；(b) 限制必须出于民主社会的需要；以及 (c) 限制必须符合包含限制条款的各项规定提出的合法目的。

17. 特别报告员认为，虽然措辞有所不同，但应该认为《公约》第十七条同样包含上述适度限制原则。依据第十七条，违反法律规定的限制属于“非法”，不必要或不符合合法目的的限制属于“任意”干涉受到第十七条保护的隐私权。因此，对于隐私权和《公约》第十七条的其他内容施加限制，应遵循适度限制原则，参见人权事务委员会第 27 (1999)号一般性意见的规定。这项一般性意见针对的是同样包含限制条款的《公约》第十二条(行动自由)。此外，第 27 号一般性意见还表明了人权事务委员会对于适度限制受《公约》保护的各项权利的看法。这项一般性意见指出，适度限制原则包含以下要素：

(a) 限制必须由法律做出规定(第 11 至 12 段)。

(b) 人权的基本内容不受限制(第 13 段)。

(c) 限制必须是民主社会所必需的(第 11 段)。

(d) 实施限制时的酌处权必须受到制约(第 13 段)。

(e) 适度限制不仅应符合合法目的，而且应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，必须有利于实现保护功能，必须是实现预期目标的各项手段当中侵犯性最低的一种，而且必须与受到保护的利益相称(第 14 至 15 段)。

(g) 任何限制均不得违背《公约》保障的其他各项权利(第 18 段)。[20]

18. 特别报告员认为，上述观点以及关于“非法”和“任意”概念的阐述同样适用于《公约》第十七条。第十七条同明文规定限制原则的《公约》其他条款相比，两者在行文上的区别在于前者没有列出合法目标的完整详尽清单。特别报告员呼吁各国设法证实，为某一特定目标对《公约》第十七条施加限制属于合法行为，并呼吁人权事务委员会继续监督缔约国采取的各项措施，包括审议定期报告和个人申诉。

19. 特别报告员认为，人权事务委员会应针对《公约》第十七条制订并通过新的一般性意见，取代现行的第 16 (1988)号一般性意见。当前的这项一般性意见非

[20] 见人权事务委员会第 27 (1999)号一般性意见。

常简短，没有反映出人权事务委员会在该项一般性意见通过后的 20 多年内采取的大部分做法。但上文依据此后出台的第 27 号一般性意见列举出的适当限制条款的部分内容，在 1988 年已经提出。[21] 此后，人权事务委员会根据《任择议定书》形成判例法，强调要干涉《公约》第十七条保障的各项权利，必须逐步满足如下多项条件——必须由法律做出规定，必须符合《公约》的条款、宗旨和目标，以及在具体情况下必须做到合情合理。[22] 此外，人权事务委员会在判断是否违反《公约》第十七条时，采用合法目标、必要性和相称性等标准。[23]

C. 反恐政策对于隐私权的损害

20. 各国在审视当前反恐政策时，往往指出在保护隐私的同时必须考虑到两个新的发展趋势。首先，各国认为防范和调查恐怖行为的国家能力同强化监视权密切相关。为此，2001 年 9 月 11 日事件以来的大部分反恐立法活动都着重扩大政府的监视权。其次，各国认为恐怖主义遍及全球，对恐怖分子的搜索必然需要跨越国境，同时需要得到可能掌握大量个人资料、为确认和监视恐怖嫌犯提供丰富资料的第三方的协助。此前没有制订宪法或法律保障的国家可以在几乎不受限制的情况下迅速扩大监视权。在业已制订宪法和法律保障的国家，政府没有将本国同第三国及私营行动方之间的合作纳入相关保障范围，或是将监视系统置于国家宪法管辖权之外，从而威胁到对隐私权的保护。

1. 日益强大的监视权

21. 监视的对象包括具体个人和广大公众。针对具体目标，法律系统可以授权并开展监视，通过秘密行动和秘密监视，确认不法行为；搜集关于某人的资料，确认其违法；以及定点监视某人，提出法律诉讼。特别报告员此前曾明确表示，各国可以采用定点监视措施，条件是由法官发布授权令，说明合理根据或正当理由，并在此基础上针对具体案件进行干预。关于某人的行为必须具备事实依据，说明有理由怀疑其可能正在筹划发动恐怖袭击。[24] 纵观全球，情报机构和执法机构越来越多地通过拦截通讯的方式，开展通讯监视。针对恐怖威胁，各国纷纷采取措施扩大监视权，这类政策呈现出惊人的相似性。大多数政策依靠现有技术或新技术，例如能够确定移动电话地理位置的“窃听器”和追踪技术，能够向政府通报因特网协议语音用户私人通话内容的技术，[25] 以及能够在嫌犯的电脑上

[21] 见人权事务委员会第 16 (1988)号一般性意见，特别是阐述《公民权利和政治权利国际公约》第十七条中任意干涉及非法干涉概念的第 3 段和第 4 段。

[22] 见 Van Hulst 诉荷兰，第 903/1999 号来文，2004 年。

[23] 见 Madafferi 诉澳大利亚，第 1011/2001 号来文，2004 年；以及 M.G.诉德国，第 1482/2006 号来文，2008 年。

[24] A/HRC/10/3，第 30 段。

[25] D.O’Brien，《中国 Skype 用户向窃听者泄露机密通讯》，电子前沿基金会，2008 年 10 月 2 日。

安装间谍软件、以便实现远程访问的技术。[26] 某些国家的安全部门甚至建议禁止使用“智能手机”等较难拦截的通讯技术。[27] 特别报告员还关切地注意到在未经司法授权的情况下跟踪跨境通讯的问题。[28]

22. 在反恐的名义下，各国利用可能侵犯个人隐私权的多项技术，对广大公众进行身份确认、扫描和跟踪。对于地点和较大规模群体的监视，其授权和监督往往不足。以下各项行为触犯、超越、甚至违反人权标准：开展拦截和盘查；制订名单和建立数据库；增强对于金融、通讯和旅行数据的监视；利用面部识别技术确认潜在嫌犯；以及建立大型数据库，判断是否存在可疑活动，确认是否需要对个人进行深入审查。更先进的技术同样得到应用，例如收集生物特征，采用能够穿透衣物的人体扫描仪。[29] 由于身体特征和生物特征被集中输入数据库，由此可能给人们的生活造成永久性侵害。

(a) 拦截和盘查权

23. 各国扩大了权限，开始实施拦截、盘查、搜查和确认个人身份，同时削弱了对于防止权力滥用的管控。这些权力在欧洲 [30] 和俄罗斯联邦 [31] 引发了人们对于种族定性和种族歧视的关注，人们担心这些权力可能造成公民与国家之间的对抗。对于隐私权施加限制原则当中的相称性要求同样引发争议，人们不禁要问，在俄罗斯联邦 [32] 或联合王国 [33] 等国的指定安全区内对所有人实施拦截和搜查，是否确属民主社会的必要。

(b) 生物鉴别技术的使用和集中身份识别系统的风险

24. 一项重要的新型身份认证政策是采用生物鉴别技术，例如面部识别、指纹对比和虹膜扫描。在某些情况下，这些技术是确认恐怖嫌犯身份的合法手段，但特别报告员极为关切地指出，某些生物特征数据不是储存在身份文件里，而是集中存入中央数据库，从而加重了资料失窃的风险，致使个人可能蒙受损失。随着

[26] 相关文章载于如下网址：http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html。

[27] S. Das Gupta 和 L. D’Monte，“黑莓安全问题危及电子商务安全”，《商业标准》，2008 年 3 月 12 日。

[28] 例如，瑞典政府关于调整国防情报行动的法案，2008 年 6 月通过，第 83 页。

[29] 见欧洲议会 2008 年 10 月 23 日关于航空安全措施和人体扫描仪对于人权、隐私、个人尊严和数据保护影响的决议。

[30] 开放社会伸张正义行动组织，《欧洲警方的种族定性做法》，2005 年 6 月。

[31] 开放社会伸张正义行动组织和法律知识基金会，《莫斯科市的种族定性做法》，2006 年 6 月。

[32] 关于打击恐怖主义的第 35 号联邦法令，2006 年。

[33] 例如，见联合王国上诉法院，R.诉市警察局长等人，2006 年。

生物特征资料的不断增加，错误率可能大幅上升。[34] 这就可能导致有人被无辜判刑，或是造成社会排斥。另一方面，不同于其他身份识别资料的是，生物特征不可撤销，一旦被恶意复制和/或用于欺诈，个人无法获得新的生物签名认证。[35] 在此有必要指出，DNA 证据同样可以伪造，不具备科学客观性。[36]

25. 集中收集生物特征数据，有可能造成冤假错案，有一个例子就很能说明问题。2004 年 3 月 11 日马德里爆炸案发生后，西班牙警方在一颗没有引爆的炸弹上提取到一枚指纹。美国联邦调查局的指纹鉴定专家称，一名律师的指纹与在犯罪现场提取的样本相吻合。此人曾在美国军中服役，国家指纹系统中因此留有他的指纹记录。此人被单独关押两周，尽管那枚指纹根本不是他的。鉴定人员没有充分复核指纹比对结果，而更糟糕的是，人们后来发现此人作为一名律师，曾经为一名被定罪的恐怖分子辩护，他的妻子是埃及移民，他本人则皈依伊斯兰教。[37]

(c) 发布秘密监视名单

26. 另一项技术是对照名单进行监视，最常见的做法是制订“禁止飞行/特定旅客”名单。此类名单被发送给航空公司和安全人员，指示他们扣留并审讯某些姓名的旅客。这些名单的使用范围如何，我们不得而知，但这些系统一旦接受公众监督，便暴露出众多错误和隐私问题，特别是在美国 [38] 和加拿大。[39] 数据完整性问题依然存在，对于这些名单必须反复审查，纠正其中的错误，身份确认过程必须做到慎之又慎。这些名单可能泄露恐怖嫌犯的姓名，需要长期保密；但另一方面，这种保密做法也引发争议，个人长期受到审查，不知道自己已经被列入名单，并且得不到有效的独立监督。这种秘密监视可能违反受到《公民权利和政治权利国际公约》第十七条保护的隐私权。

27. 在公布恐怖分子名单的情况下，则可能以另一种方式触犯《公约》第十七条。人权事务委员会认为，在缺乏正当理由的情况下将某人列入联合国 1267 委员会综合名单，违反《公约》第十七条。人权事务委员会认为，鉴于姓名和制裁

[34] 例如，见 M. Cherry 和 E. Imwinkelried，“审慎看待指纹分析和对数字技术的依赖”，《司法文论》，第 89 卷，第 6 期(2006 年)。

[35] 见 E. Kosta 等，“基于无线射频识别技术的电子护照引发的安全和隐私问题分析”，国际信息处理基金会，第 232 期(2007 年)，第 467 至 472 页。

[36] 例如，见 D. Frumkin 等，“法医 DNA 样本认证”，《国际法医学：遗传学》(2009 年 7 月 17 日)。

[37] 见美国司法部，监察长办公室，《联邦调查局 Brandon Mayfield 案件调查复审》，2006 年 1 月。

[38] 见美国司法部，《联邦调查局恐怖分子监视名单提名做法审核》，2009 年 5 月。

[39] 见加拿大隐私问题专员办事处，《加拿大运输部门旅客保护方案审核》，2009 年 11 月。

名单的标题之间可能产生消极联想，散布个人资料是对被列入名单者的荣誉和名誉的损害。[40]

28. 此外，公开及秘密监视名单违反了数据保护的基本原则。在相关个人不知情或未经其许可的情况下，用于某一目的的资料被再次用于其他目的，有时甚至与其他机构共享。错误的资料被用于决策，并据此发布旅行限制。在提不出违法犯罪证据的情况下，这些人的签证申请可能被拒绝，不准出入境，或是不准登机。

(d) 检查站和边境

29. 由于恐怖主义日益引发关切，各国采用新技术，不断强化对于人们在边境地区行动的监视、管制、干涉和管控。利用更为先进的技术和数据分享协议，各国目前可以分析航空公司提供的旅客清单和旅客预订记录，对外国游客进行综合定性，以便在恐怖分子和犯罪分子入境之前就把他们认出来。各国分析这些资料，从中发现同恐怖分子或犯罪分子相符的特征。在入境时，个人将面临进一步、有时是唐突无礼的资料采集做法。

30. 目前，很多国家都要求航空公司在出发之前提交旅客清单，并试图获取旅客姓名记录，其中包括身份资料(姓名和电话号码)、交易资料(预定日期、旅行社和行程)、航班和座位资料、金融数据(信用卡号码、发票地址)、饮食偏好以及关于居住地、医疗记录、旅行前情况和航空公司常客等各项资料。这些资料用于对旅行进行定性分析和风险评估，常用方法是查询多个跨机构执法和恐怖分子数据库及监视名单。为此，有关方面可能仅仅依据目的地国的数据库查询结果，未经适当法律程序就禁止航空公司向某人发放登机牌。

31. 出于各种原因加强对于移民和游客的监督，给保护隐私带来诸多困难。第三方迫于无奈，向各国提供旅客资料，否则可能被禁止降落，或是被处以罚款，但隐私保障措施未必符合国内隐私保护法的要求。此外，外国人在这些国家未必能够在平等基础上获得司法补救措施，他们在出入境时的权利往往受到严重制约。美国政府对于旅客随身携带的笔记本电脑进行开机检查的政策就很能说明问题。在美国境内检查笔记本电脑必须符合宪法规定的适当法律程序，但国土安全部在未经司法授权的情况下依然批准开机检查旅客的笔记本电脑。[41]

32. 最后一点，各国目前要求获得更多的资料。个人如拒绝透露相关信息，可能被禁止入境；各国可能会坚持要求对方提供资料，但不保证这一要求属于法定权限。此外，为某一目的收集的资料正在用于其他目的。例如，欧洲联盟设立欧洲指纹鉴定系统，本意是利用指纹鉴定技术来管理寻求庇护者和非法移民的申请资料，但目前有人提出扩大这一系统的职能，协助有关方面防止、查明、调查恐

[40] 见人权事务委员会，第 1472/2006 号来文，第 10.12 至 10.13 段。

[41] 见国土安全部，《评估利用电子设备进行边境搜查对于隐私的影响》，2009 年 8 月 25 日。

怖犯罪和其他严重罪行。欧洲数据保护监督员质疑这些建议是否侵犯隐私权以及是否合法。[42]

2. 监视对其他权利的影响

33. 监视制度作为一项反恐措施，给其他各项基本人权造成了严重的不利影响。隐私不仅是一项权利，而且是支撑其他权利的基础；没有隐私，就不能充分享有其他各项权利。必要的隐私为个人和群体提供空间，供他们进行思考，发展关系。言论自由、结社自由和行动自由等其他权利都需要个人保有隐私，才能获得充分发展。此外，监视还造成冤假错案，打破适当法律程序，导致无辜者被逮捕。

34. 很多国家的通讯用户正在受到监听，目的是查明他们的通话对象和对方所在地点。2006 年，人们发现德国联邦情报局利用监听通讯和在新闻编辑部里安插间谍等手段，非法监视新闻记者。[43] 2009 年，人们发现哥伦比亚安全部七年来一直在非法监视媒体从业人员、人权工作者、政府官员、法官及其家人。[44] 很多国家的因特网用户必须登记真实身份，他们的会话将被保留下来，供有关当局今后使用。例如，孟加拉国在 2007 年要求因特网服务提供商将用户的身份、密码和使用情况等资料送交有关部门。这些部门随后走访了部分用户，搜查他们的电脑和联系名单。[45] 2004 年政治会议期间，美国联邦调查局的反恐部门负责监视和平人士的活动。[46] 这些监视措施给用户造成极为不利的影响，致使他们不敢访问网站，不敢表达自己的观点，也不敢同其他人联系，因为担心对方会受到惩处。[47] 持不同意见者受到的冲击尤其严重，其中某些人可能因此不敢行使自己的民主权利，放弃抗议政府政策。

35. 除监视权之外，多部反恐法都要求个人事先披露资料，规定官员有权要求对方提供资料用于开展调查。为此，特别报告员此前曾对美国使用“国家安全许可证”表示关切。[48] 某些国家进一步扩大了这项权力，要求披露新闻采访收集

---

[42] 见欧洲数据保护监督员对于执法机构利用欧洲指纹鉴定系统一事发表的讲话，2009 年 10 月 8 日。

[43] 德国之声，“德国在爆出丑闻之后停止监视记者”，2006 年 5 月 15 日。

[44] 见《周报》，2009 年 2 月 21 日。

[45] 见“电子孟加拉国”网站，“孟加拉国因特网用户遭到镇压”，2007 年 10 月 3 日(译自英国广播公司的报道)。

[46] 见美国公民自由联盟，“美国公民自由联盟揭露联邦调查局监视知名和平人士”，2006 年 10 月 25 日。

[47] 见 D. S. Sidhu，“政府监视方案对于美籍穆斯林因特网使用情况的不利影响”，《马里兰大学种族、宗教、性别和阶层法学学报》，第 7 卷(2007 年)，第 375 页。

[48] A/HRC/6/17/Add.3，第 51 段。

到的资料。乌干达 2002 年《反恐法案》规定，假如依据“特定正当理由”认为相关资料在反恐调查方面具有“重大价值”，则允许有关部门窃听新闻媒体的电话并实施搜查。[49] 特别报告员强调指出，必须满足如下各项条件，披露新闻记者秘密资料的正当利益才能高于拒绝披露相关资料的公共利益：证明确实迫切需要披露资料；事态严重，情势紧急；以及，为满足迫切的社会需求，有理由必须披露资料。[50]

36. 此外，监视行动还威胁到结社自由和集会自由。人们在行使这些自由时往往需要召开秘密会议和秘密通信往来，以便组织起来对抗政府或其他当权者。扩大监视权有时会形成某种“职能扩张”，警方或情报部门将某些人划定为恐怖分子，以便对其实施只有针对恐怖主义才能采用的监视权。美国马里兰州警方在纽约和丹佛市的政治会议召开之前，便将环保分子及和平示威人士列入恐怖分子监视名单。[51] 在联合王国，有关部门往往动用监视摄像机拍摄记录政治抗议活动，并将图像存入数据库。[52] 不久前在联合王国进行的一次民意调查发现，有三分之一的居民出于对隐私的担心，不愿参加抗议活动。[53]

37. 监视对于行动自由同样可能产生深远的影响。秘密监视名单的出现，过度的数据收集和数据分享，强行实施有侵权之嫌的扫描，以及生物特征鉴别，所有这些都给人们的行动造成了更多障碍。正如上文所述，对于国内及国际旅行者的信息收集工作显著加强，这些资料通常由多个部门共享，用于制订监视名单，从而给旅行设置新的障碍。安全部门利用从多种渠道获得的、可信度不一的资料，开展定性分析，制订监视名单，个人不了解资料来源，无法询问这些资料是否属实，更没有权力质疑外国机构据此得出的结论。将来自多个数据库的各类不同数据拼凑起来，可能导致数据挖掘算法，将无辜者视为威胁。[54] 假如国家禁止个人离境，必须出示限制行动自由的依据，否则便有侵犯《公民权利和政治权利国际公约》第十二条之嫌。[55]

38. 监视措施造成的最严重的后果是可能导致冤假错案和扰乱正当的法律程序。由于监视工作是秘密进行的，而某些国家的法律制度要求个人必须证明确实

[49] 《反恐法案》，附件三，第 8 段。

[50] 另见欧洲委员会部长理事会向成员国发出的关于新闻记者有权拒绝泄露消息来源的第 R7 (2000)号建议，以及安大略省高等法院，O’Neill 诉加拿大(司法部长)，2006 年，第 163 段。

[51] 见 L. Rein 和 J.White，“受到警方监视的人多于想象”，《华盛顿邮报》，2009 年 1 月 4 日。

[52] 见 P.Lewis 和 M.Vallée，“揭露：警方设立数千名示威者数据库”，《卫报》，2009 年 3 月 6 日。

[53] 见 A.Jha 和 J.Randerson，“民意调查表明公众对于警方监视环境示威活动感到不安”，《卫报》，2009 年 8 月 25 日。

[54] 见美国国家研究委员会，《在反恐斗争中保护个人隐私：评估框架》，防范恐怖主义和其他国家目标中的技术和隐私问题委员会，2008 年 10 月。

[55] 另见人权事务委员会，B.Zoolfia 诉乌兹别克斯坦，第 1585/2007 号来文，2009 年，第 8.3 段。

存在干涉，否则不得诉诸司法，由此给申请司法审查造成困难。个人可能无法证实或证明自己确实受到监视，因此无法向法院提出申诉。在某些案件中，法院因个人无法证明自己受到监视而裁定其无权提出起诉，伤害被认定为臆想猜测。[56] 在另一些案件中，个人能够证明确实存在干涉，国家有时会动用“国家机密”特权，规避对非法监视行动的审查。[57] 特别报告员赞赏欧洲人权法院的做法，该法院规定个人无须证明自己确实受到监视。[58]

3. 拓展法律适用范围

39. 各国签订法律互助条约，目的是合作开展调查，共享某些案件的资料。[59] 此外，各国还签订协议，共享关于从事某些活动的个人的资料，例如所有出境旅客的资料以及所有跨国金融交易者的资料。情报机构之间签署更加隐秘的协议，共享数据库和情报数据。这些数据库通常在很多问题上不受国内法律的约束。即便适用国内法律，这些数据可能涉及在国内法院无法行使权利的外国公民。情报部门制订的名单不会公之于众，个人不可能知道自己正在受到监视，例如被列入恐怖嫌犯名单，也就无法申请复查。假如这份名单由多国共享，个人无从判断自己最初被列入名单的理由，也无法从此后产生的多份名单中清除自己的名字。

40. 各国不仅加强了国家间反恐合作，同时还加强了同掌握个人资料的私营第三方的合作，以便确认并监视恐怖嫌犯。某些国家的政府没有将国内隐私保障措施适用于本国同第三国及私营行动方的合作范围，从而危及到对隐私权的保护。

41. 银行、电话公司、乃至网吧等第三方目前掌握着方方面面的个人资料。获取这些资料，就可以深入了解个人的私生活。另一方面，政府机构可以通过第三方轻易获取这些资料，比将这些资料交由个人保存、存放在家中、或者由政府机构保管还要容易。例如，美国最高法院裁定，个人提供给银行或电话公司等第三方的数据是个人同这些机构“免费”共享，没有理由要求对方保护自己的隐私。[60] 假如国家没有制订为干涉个人私生活提供法律依据的宪法保障，私营部门就必须自行决定如何应对政府机构的要求。在一般情况下，私营部门普遍希望政府能够制订法律依据，要求私营部门出示相关个人资料，私营部门将由此不再承担考虑案件性质的责任。

---

[56] 见不久前结案的大赦国际等诉 John McConnell 等，美国纽约南区地区法院，2009 年 8 月 20 日。

[57] 见美国加利福尼亚北区地区法院，两圣地伊斯兰基金会等诉布什等，2009 年 5 月 1 日。

[58] 见欧洲人权法院，Klass 诉德国，1978 年 9 月 6 日，第 38 段。

[59] 见 G. Hosein，《全球调查：网络犯罪和司法管辖中的国际合作 —— 承诺与威胁》(T.M.C.阿塞尔出版社)，2006 年。

[60] 见美国最高法院，Smith 诉马里兰州，1979 年，通讯数据案件；以及，美国诉 Miller，1976 年，金融资料案件。

42. 此外，有关方面日益向第三方施加压力，要求其收集不必要的资料，并长期保留这些资料。例如，联合王国建议电信公司主动监督个人在线活动，并保留相关资料，包括社会串联活动，电信公司完全没有正当理由去收集这些资料。[61] 欧洲联盟数据保留指令[62] 同样引发了激烈的批评。2008 年，德国联邦宪法法院下令，中止执行这项指令的德国法律，宪法法院指出：“在不说明理由的情况下全盘保留关于个人的敏感数据，用于在保留数据时不可预见的政府目的，可能造成严重的威慑作用”。[63] 此外，德国研究也表明了数据保留政策的不良影响，52%的受访者表示，由于数据保留法案，他们可能不会通过电信方式同药剂师、心理医生、婚姻顾问等人取得联系。[64]

43. 为此，特别报告员关切地指出，很多国家都制订了数据保留法案，但没有出台关于获取相关资料的法律保障措施，也没有注意到新技术的发展正在逐渐模糊通讯内容和通讯数据之间的界限。宪法条文往往要求对于获取通讯内容制订保障措施，但对于交易记录文件的保护则比较少。这些资料对于调查可能弥足珍贵，但它同通讯内容一样，都属于个人敏感资料。

44. 为打击资助恐怖主义和洗钱，各国纷纷要求金融业分析金融交易，以便自动区分“正常”交易和“可疑”交易。例如，欧洲联盟在 2005 年颁布关于“防止利用金融系统洗钱和资助恐怖主义”的指令，[65] 要求金融机构恪尽职守，向金融情报机构报告可疑活动和“准异常”活动。金融情报机构如何对相关资料进行深入处理，我们不得而知，但澳大利亚[66] 和加拿大[67] 等国采用先进的数据挖掘工具，每年处理数以百万计的交易记录。

45. 外国法律同样可能要求第三方披露资料。例如，美国政府向环球银行间金融电信协会发出行政传票。这是一家比利时协会，负责协助世界各地 200 多个国家的超过 7,800 家金融机构相互发送电信指令。美国财政部进入这家协会设在美国的数据库，立时便能监督通过协会网络开展的外国金融交易，查找并确认恐怖

[61] 见联合王国隐私问题全党派议会小组,《简报：通讯数据监视建议和拦截技术现代化方案质询》, 2009 年 6 月。

[62] 欧洲议会和欧洲委员会 2006 年 3 月 15 日关于在提供公共电子信息服务或公共通讯网络过程中保留所生成或所处理的数据的第 2006/24/EC 号指令和第 2002/58/EC 号修正指令,《公报》, L 105 (2006)，第 54 至 63 页。

[63] 宪法法院第 256/08 号裁定，2008 年 3 月 11 日。

[64] 德国福尔萨研究所, Meinungen der Bunderburger zur Vorratsdatanspeicherung，2008 年 5 月 28 日。

[65] 见欧洲联盟和欧洲委员会 2005 年 10 月 26 日关于防止利用金融系统洗钱和资助恐怖主义的第 2005/60/EC 号指令,《公报》, L 309 (2005)，第 15 至 36 页。

[66] 见澳大利亚交易报告和分析中心,《中心 2008 至 2009 年年报》, 2009 年 10 月。

[67] 见加拿大金融交易和报告分析中心,《中心 2008 年年报》, 2008 年 9 月 11 日。

嫌犯。[68] 20 多个国家的人权组织提交诉状，指责环球银行间金融电信协会将这些资料交给美国政府，违反了本国的隐私保护法。[69]

46. 特别报告员还关切地指出，监视设备正在嵌入技术基础设施，个人和机构可能因此蒙受风险。例如，为合法拦截通讯制订标准，需要电信公司有意设置技术薄弱环节，方便国家拦截通讯。这项技术在希腊被随意滥用，神秘的第三方竟然可以监听总理和其他数十名高官政要的通讯内容。[70] 就在不久前，有报道称伊朗伊斯兰共和国政府利用这项技术监视抗议人士。[71] 要避免滥用监视技术，应记录数据读取者信息，做到有据可查，以便实施监督，防止滥用。[72]

47. 某些国家的宪法保障依然有效。例如，《加拿大权利和自由宪章》规定，假如第三方掌握的个人资料透露“个人生活方式和个人选择的具体细节”，则受到隐私保护。[73] 这就要求在保护个人尊严、人格完整及自主权的社会利益与有效执法之间谋求某种平衡。[74] 《欧洲人权公约》同样将第三方掌握的个人资料纳入隐私权的范围。《关于在个人数据自动处理方面保护个人的公约》要求公共部门和私营部门保护其手中掌握的资料，并限制同政府机构共享这些资料。维护国家安全、公共安全和国家金融利益、打击刑事犯罪、保护个人以及保护其他人的权利和自由等特殊情况除外。[75]

D. 最佳做法

48. 特别报告员关切地指出，各国目前普遍将这种监督权用于恐怖主义之外的其他问题。2001 年 9 月 11 日事件之后，有观点认为要应对当时的威胁，需要在短时期内扩大权力，为此有多部立法要求审议现行反恐法，并提出定期废止条款。这些定期废止条款和审议要求没有纳入某些决策领域，此后出台的政策也未予考虑。反恐法赋予执法机构多项调查权，而后者利用这些权力开展与恐怖主义无关的调查。另一方面，各国争先恐后地仿效其他国家制订政策，没有考虑到由此给人权造成的影响。上文提及的多项政策最初是特例，但不久之后就成为区域和国际标准。总的说来，由于得不到充分的法律保障，这些干预措施正在严重影

[68] 另见美国财政部负责恐怖主义资金追踪方案的副部长斯图亚特·利维的讲话，2006 年 6 月 23 日。

[69] 例如，见隐私国际，“银行转账资料转眼之间被送给美国政府”，2006 年 7 月 27 日。

[70] 背景资料见 V.Prevelakis 和 D.Spinellis，“雅典事件”，《电气和电子工程师学会概览》，2007 年 7 月。

[71] 参考资料见诺基亚－西门子网络，《伊朗的合法拦截能力》，2009 年 6 月 22 日。

[72] 见脚注 54。

[73] 见加拿大最高法院，R.诉 Plant，1993 年，以及 R.诉 Tessling，2004 年。

[74] R.诉 Plant。

[75] 《关于在个人数据自动处理方面保护个人的公约》第 9 条。

响到隐私权的保护。各国如不制订严格的法律保障措施，没有方法来判断干预措施是否必要、适度及合理，在尽量减少新政策对于隐私的影响问题上就会陷入无所适从的境地。特别报告员依据世界各国的决策、判例、政策审查和良好做法，提出如下若干法律保障措施。

1. 最低侵犯原则

49. 对于个人私生活的某些干预措施的侵犯性尤其严重。经过 50 年来的发展，针对财产和人身的宪法保护范围已经扩展到通讯、[76] 生平核心资料、[77] 保守秘密的权利以及信息技术系统的完整性。[78] 这些保护工作要求各国尽量采用侵犯性较低的技术，只在万不得已的情况下才能动用其他技术。联合王国议会内政委员会审议并修正了现代化数据集中监视系统构想，将其纳入数据最低化原则，这与用途说明极为接近。[79] 内政委员会建议政府“不要收集更多的个人资料，不要建立更大型的数据库。在决定是否创建大型数据库，是否分享其中的资料，以及是否听从关于加强监视力度的建议时，必须证明这样做确有必要。”特别报告员主张各国应将这项原则纳入现行及今后出台的各项政策，以便反映出政策是否必要，以及是否适度。

2. 禁止二次使用的用途说明原则

50. 数据保护法规定，为某一目的收集的资料不得再次用于其他目的，但国家安全政策和执法政策往往不受这些规定的限制。依法获取数据的通知、通用传票以及国家安全证书等豁免证书所载的保密条款可以规定某个数据库不受隐私法保护。特别报告员关切地指出，这种做法削弱了防止权力滥用的必要保障措施的功效。根据宪法和人权原则，各国有义务为反复使用资料提出法律依据。必须在人权框架内完成这项工作，而不是规定例外和豁免。在各方跨国共享资料的情况下，这一点尤其重要。此外，假如各国共享资料，必须继续适用保护和保障措施。[80]

3. 监督和限制依法获取数据授权原则

51. 监视系统必须接受有效监督，以便尽量减少伤害和滥用。在制订保障措施的情况下，这项工作通常采用独立授权的形式，通过司法授权书和/或传票程序

[76] 见美国最高法院，Katz 诉美国，1967 年。

[77] 见脚注 74。

[78] 见德国宪法法院第 370/07 号裁定，2008 年 2 月 27 日。

[79] 见联合王国议会内政委员会，《监督型社会？2007 至 2008 年届会第五次报告》，2008 年 6 月 8 日。

[80] 例如，关于旅客名单记录，见第 29 条数据保护问题工作组关于欧洲联盟和美利坚合众国交换航班旅客名单记录的相关旅客资料问题提出的第 8/2004 号意见，2004 年 9 月 30 日。

来完成，以便开展独立审查。但多项政策力图限制监督权，降低授权级别。例如，通讯拦截法对于某些通讯仅做出最低授权要求；为获取第三方掌握的资料发出秘密传票，并限制对方寻求司法保护的余地；以及，各国日益允许情报机构和执法机构自行授权获得个人资料，而此前则需要独立授权和有效报告。

52. 某些国家已经采取措施，应对保障措施受到削弱的情况。在经过多起案件之后，并根据《美国爱国者法案》提出的重新授权要求，美国再次增加了司法审查。瑞典和美国改变了通讯监听做法，以司法授权的形式在有限范围内再次规定保障措施。此外，欧洲法院也裁定，法院有必要审查国际监视名单在国内是否合法。[81]

53. 特别报告员关切地指出，由于监视做法和监视技术缺乏切实有效的独立审查，人们不禁要问，这些干涉措施是否合法(是否可以问责)以及是否必要(是否适度)。他赞赏内部隐私问题办公室、审计部门和总检查局等政府内部监督机构开展的艰苦卓绝的工作，这些部门在发现权力滥用问题上起到了关键作用。为此，特别报告员呼吁加强内部监督，作为独立授权和外部监督的补充措施。这种内外双重问责制度将确保个人可以得到有效的补救措施，同时可以切实求助于拨乱反正机制。

4. 透明和诚信原则

54. 对监视系统采用保密特权，可以禁止立法机构、司法部门和公众审查国家权力。未经事先通知，个人可能受到不正当的监视，利用数据挖掘技术进行定性分析，可能做出错误判断。此外，对于监视政策没有明文规定适当限制，很难证实这些权力是否被任意滥用。

55. 透明和诚信原则要求对监视做法采取公开的态度，并进行交流。某些国家规定，必须在事后尽快通知个人在何时以及以何种方式对其进行监视。拉丁美洲国家的资料保护令宪法制度[82]以及欧洲国家的数据保护法均规定，个人有权获取并修改数据存储系统和监视系统中保存的个人资料。这些权利必须享有国际保障，确保法律制度同样保护本国公民和非公民。

56. 公开辩论和审查，是了解监视技术利弊的必要途径，以便公众能够理解监视行为的必要性与合法性。很多国家的议会和独立机构负责审查监视政策和监视程序，有时还开展立法前审查。立法中的定期废止条款和审查条款对这项工作有所助益。

[81] Yassin Abdullah Kadi 和 Al Barakaat 国际基金会诉欧洲委员会和欧洲联盟委员会，2008 年 9 月。

[82] 例如，见《巴西宪法》第 5 条(第七十一章)、《巴拉圭宪法》第 135 条和《阿根廷宪法》第 43 条。

5. 有效现代化原则

57. 目前可以更加轻易地获取更为隐秘的资料，但各国没有制订相应的保护措施。各国名义上努力实现监视权的现代化，实则有时故意采用相对陈旧和薄弱的保障措施，以便获取更为敏感的资料。[83] 某些国家意识到，有必要考虑到技术革新和政策变化可能给个人造成的不利影响，因而着手进行隐私影响评估，在设计开发新的监视技术时明确提出隐私问题，包括决策者如何看待数据最小化和纠正平反权利等上述各项原则。特别报告员认为，利用隐私影响评估等工具，有助于让公众了解监视行为，在政府机构开发制订新的反恐监视系统的同时在政府内部逐渐营造保护隐私的氛围。此外，必须制订国际标准，要求各国针对技术发展加强本国的保障措施。

四. 结论和建议

A. 结论

58. 特别报告员关切地指出，曾经的例外如今已经成为惯例。首先，各国不再将非常监视方案仅限于反恐目的，而是将手中的监督权用于所有目的。其次，监视如今已渗入决策过程。个人如今要对不必要的监视建议提出批评，必须说明为什么不可以收集更多资料，而不是由国家承担举证责任，说明为什么必须采取干涉。第三，几乎所有法律保护和保障措施的质量及成效都被削弱了。这是由于随着技术的发展，监视权变得更加强大，并且无所不在。然而最让人忧心的是，这些技术和政策正在输入其他国家，并且在这一过程中往往丧失最基本的保障。

59. 必须制订国际法律标准，防止出现上述形式的权力滥用。恪守本报告提出的各项原则，对此将有所帮助，其中包括尽可能降低监视行为的侵犯性，在行使新权力的同时规定适当的保障措施、限制、有效监督、授权、定期报告和审查，同时全面阐述由此给隐私造成的影响。广大公众和立法机构从来没有机会探讨反恐权是否必要、适度、合法。特别报告员认为，采纳新兴的良好做法将惠及各方。

B. 建议

立法会议

60. 特别报告员再次指出，对于隐私、家庭、住宅和通信权利的干涉应通过公开的法律条文进行授权，干涉行为要做到清晰明确，与安全威胁相称，并提供有效保障，防止权力滥用。假如侵犯性相对较低的调查方法能够有效侦查、预防和

[83] 见政策参与网，《联合王国政府拦截技术现代化方案简报》，2009 年 6 月。

起诉恐怖犯罪，各国务必要确保主管部门采用这种调查方法。决策机关应做出规定，对于隐私的侵犯程度越深，所需的授权级别越高。

61. 恪守关于隐私和人权保护的国际标准，应作为国内法的一项准则。为此，需要制订综合性数据保护和隐私法，确保个人能够得到明确的法律保护，防止过度收集个人资料，确保制订相应措施，保证资料准确无误，限制资料的使用、存储和分享，规定个人有权了解本人资料的用途，并且有权获取和修改本人资料，不受国籍和司法管辖权的制约。

62. 必须规定严格的独立监督授权，负责审查政策和做法，确保侵犯性监视技术的应用和个人资料的处理过程得到严密监督。为此，不得在有效监督机构的审查范围之外设立秘密监视系统，所有干涉措施一律由独立机构授权。

63. 现行和拟议的各项反恐政策必须包含隐私影响评估，审查并公布政策和技术如何确保降低隐私风险，并在决策的最初阶段就考虑到隐私问题。

64. 特别报告员建议制订更为有力的保障措施，确保各国政府之间的资料共享工作能够继续保护个人隐私。

65. 特别报告员还建议制订更为有力的规章制度，限制政府获取第三方掌握的资料，包括报告制度，尽量减少强迫第三方收集更多资料的要求，在第三方代表国家行事时，适用宪法和法律保障。

66. 特别报告员警告，应重新审视法律措辞，防止反恐权用于其他目的。在制订新的法律系统时必须限制用途说明的范围。

政府

67. 特别报告员敦促各国政府依据国际人权标准，详细说明本国的监视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。

68. 特别报告员建议公开讨论和定期汇报信息化监视方案。向立法机构和监督机构提交报告，对监视做法开展独立审查，都将有助于为今后制订和审议反恐政策提供资料。

69. 名单监视方案或定性监视方案必须包括适用于所有人的适当法律程序保障，包括纠正平反的权利。必须坚守透明原则，让个人了解本人被列入名单的原因和方式或定性分析过程，并且了解申诉机制，不得施加任何不正当的制约。

70. 鉴于数据挖掘技术的固有风险，特别报告员建议对信息化反恐方案实施严格的独立监督。特别报告员还建议各国不要为反恐目的开发和使用数据挖掘技术。

71. 鉴于滥用监视技术的风险，特别报告员建议为研究和开发隐私保护技术投入同等经费。

人权理事会

72. 特别报告员建议制订保护隐私全球能力建设方案。在世界各国不约而同地制订反恐法和国际监视标准的同时，作为制衡，必须进一步认识到应采取必要的保障措施，维护个人尊严。

73. 特别报告员敦促人权理事会制订适当程序，在现有数据保护原则的基础上，就起草全球数据保护和数据隐私宣言提出建议措施。

人权事务委员会

74. 特别报告员建议人权事务委员会针对《公民权利和政治权利国际公约》第十七条，着手起草新的一般性意见，深入阐述适当限制原则，指导各国采取适当保障措施。这项一般性意见还应适当考虑到数据保护作为《公约》第十七条所载隐私权的一项要素。