联合国 A/71/368

大 会

Distr.: General
30 August 2016
Chinese
Original: English

第七十一届会议

临时议程* 项目 69 (b)

促进和保护人权：人权问题，包括增进人权和基本自由切实享受的各种途径

隐私权**

秘书长的说明

秘书长谨向大会转递移隐私权问题特别报告员 Joseph A. Cannataci 先生依照大会第 68/167 号决议和人权理事会第 28/16 号决议规定提交的报告。

* A/71/150。

** 在最后限期之后才提交本报告的原因是为了反映最新情况。

请回收

隐私权问题特别报告员的报告

摘要

本报告是隐私权问题特别报告员向大会提交的第一份报告。本报告的撰写，距离特别报告员在 2015 年 8 月 1 日就任仅有一年多的时间，距离特别报告员在 2016 年 3 月 9 日向人权理事会提交其首份报告正好五个月的时间。在这之前，特别报告员一直着力于确定若干专题。他与多个利益攸关方大量协商的结果表明，这些专题是数字时代隐私保护的关键工作领域。

在此后的五个月里，特别报告员确定了他的首批共计五个优先事项，如本报告所述，并且在这些方面同步开始工作。这些优先事项被称为专题行动流(TAS)，涉及大数据和开放数据；安全和监控；健康数据；由公司处理的个人数据；“更好地理解隐私”。特别报告员选择的方法是，考虑设立一支由经验丰富、无报酬的志愿人员组成的专题行动流工作组(TASk force)，有些人称之为工作队(WP)。五个专题行动流各设一支工作队，协助特别报告员研究并起草一份专题研究报告，这些专题研究报告将成为 2017-2018 年期间提交人权理事会或大会的一份报告的主题。

特别报告员热切希望，每个专题行动流工作组或工作队都能最大限度实现地域分布广泛性、文化和族裔多样性、利益攸关方代表性和性别平衡。因此，举例来说，大数据和开放数据专题行动流工作组由澳大利亚维多利亚州隐私和数据保护专员 David Watts 担任组长，而健康数据专题行动流工作组由美利坚合众国德克萨斯州奥斯汀市戴尔医学院学习卫生系统主任 Steve Steffensen 担任组长。编写本报告时，特别报告员仍在为一些专题行动流工作组招募组长和组员。每支专题行动流工作组的确切人员构成将于适当的时候宣布，可能会在 2017 年 3 月之前。预期各专题行动流工作组将召集会议，并酌情组织公开、半公开和闭门活动，以收集证据和确定战略备选方案，在特定活动部门中改进隐私保障和补救措施。

因此，安全和监控专题行动流工作组组织的首项活动就是设立国际情报监督论坛(IIOF2016)。该论坛将于 2016 年 10 月在布加勒斯特举行会议，预计将有数十个监督机构和议会委员会参加。这次活动将帮助集体确定情报收集过程中隐私和表达自由面临的挑战，找出能提供更好保障和补救措施的最佳做法。同时，“更好地理解隐私”专题行动流工作组已经于 2016 年 7 月 19 日和 20 日在纽约组织了首次活动。按照计划，在五个优先事项中，这一专题行动流工作组将最后提交报告，时间肯定不会早于 2018 年，因为预期需在非洲、亚洲、澳大利亚、欧洲和南美洲等区域开展其他一些协商活动。该专题行动流工作组已开始收集有关各项概念的证据，如隐私与人格自由发展这一首要基本权利的关系。预期该工作组的活动将成为一个持续进程，与特别报告员设立的所有其他专题行动流工作组分享信息并借鉴经验。

这五个专题行动流工作组使工作有了专题重点，同时，特别报告员也在继续监测几十个国家的情况，并已开始实行非正式国家访问方案，在每次访问期间都与尽可能多的利益攸关方进行最大程度的互动。2016 年 3 月至 8 月的五个月间，特别报告员参加了多次活动，有时为期长达一周。这些活动所在的 11 个国家相距遥远、非常多样，包括澳大利亚、奥地利、丹麦、法国、德国、意大利、拉脱维亚、荷兰、新西兰、瑞士和美国。预计今后几个月中，特别报告员将对法国、印度尼西亚、以色列、摩洛哥、北爱尔兰(大不列颠和北爱尔兰联合王国)、撒哈拉以南非洲、南美洲、西班牙和美国进行正式和非正式的国家和地区访问。紧张工作方案的开展得到了各国政府、隐私和数据保护专员、人权机构、非政府组织和大学的直接协助。

目录

		页次
一.	导言	5
	A. 起步	5
	B. 初步反馈和后续举措	5
二.	特别报告员开展的主要活动	5
	A. 为特别报告员任务提供资源	5
	B. 规划和启动与任务相关的多项活动	7
	C. 参与多项活动	10
三.	重要进展和实质性问题，2016 年 3 月至 7 月	12
	A. 沉默权(不证己罪)：是否可以迫使智能手机作证，抑或这可能严重侵犯隐私？	12
	B. 数据保留、大规模监控和更多的加密	16
	C. 进一步认识隐私与人格的关系	20
四.	结论	20

一. 导言

A. 起步

1. 本报告于 2016 年 8 月 9 日当日或前后提交联合国，以供 2016 年 10 月大会会议之前进行翻译。提交报告前约 18 个月时，人权理事会在其第 28/16 号决议中首次设立了有关隐私权的任务，现任者则是在提交报告前一年时就任。目前，特别报告员确认，迄今采取的举措已收到大量反馈，其中大部分为积极反馈。本报告将概述特别报告员的努力迄今取得的进展，以及今后一段时间活动的主要关注点。

B. 初步反馈和后续举措

2. 2016 年 3 月提交给人权理事会的首份报告中提出了一项十点行动计划(见 A/HRC/31/64，第 46 段)。该十点行动计划收到了非常积极的反馈。因此，特别报告员将继续就这些问题开展工作，力求在任务期间与所有利益攸关方合作取得具体成果。

3. 开始执行任务以来的 12 个月中积累的经验以及对该领域事态发展的监测表明，与其他问题相比，某些问题需要更加迅速果断的反应。由此，确定了首批五个优先事项。特别报告员计划采取适当行动，在单独的专题报告中介绍这些优先领域的调查结果。

二. 特别报告员开展的主要活动

A. 为特别报告员任务提供资源

4. 没有军队，就无法赢得战斗。由于这是一项新任务，特别报告员面临着一个没有现成团队的行政处境，不得不投入大量时间在联合国之外为任务寻求资源。即使联合国提供的资源在质和量方面皆为完美——事实情况并非如此——若不能在联合国提供的资源之外取得大量资源，特别报告员的工作将无法妥善进行。监测超过 190 个国家的隐私立法和监控活动，这一工作需要数十名工作人员。会见民间组织，了解其关切的问题，以及不断与公司、执法部门、情报机构和政策制定者互动，也需要投入大量时间和人力。在下述五个专题行动流方面组织协商活动，也需要大量人力。目前，此种人力几乎都不来自于联合国，其中一项重要原因是，所需要的工作人员必须拥有领域专业知识，为隐私领域的专家。简言之，目前，协助开展此项任务工作的工作人员其经费有约 90% 和执行任务产生的差旅费用有约 80%必须从联合国以外的来源获得。此外，由于系统内的重大行政障碍，难以专注于任务的实质性部分。

5. 在资源方面，若要说联合国人权事务高级专员办事处(人权高专办)为特别报告员任务提供的支持差强人意，未免过于轻描淡写。正如一句拉丁语格言所说 contra factum non argumentum est(意即“事实面前无可辩驳”)，让事实说话：

(a) 特别报告员需要和希望的，不是一般事务官员，而是拥有隐私领域专业知识的工作人员：这种专业知识只能通过正规培训、资历和直接经验获得。特别报告员向人权高专办特别程序高级管理层提出了这一点，而在 2016 年 2 月，也确实发出了一个专业职等(P-3)人权干事职位的申请呼吁，其中提出优先考虑具有隐私领域资历和经验的申请人。特别报告员获悉，收到了 349 份申请，但这些申请的内容却从未得到考虑。特别报告员从未看到这些申请，但却从一些非政府组织处得知，这些组织知道一些申请人拥有隐私方面博士学位并且在隐私相关领域有多年工作经验；

(b) 这之后，负责特别报告员任务的人权高专办高级管理人员完全无视公开呼吁收到的申请，在 2016 年 8 月 4 日告知特别报告员，已从“内部候选人名册”中为特别报告员任务负责人任命了一名常设人权干事。这名人权干事不具备隐私领域的正规培训或资历，没有隐私方面的深入经验/知识，对于隐私事务只有肤浅的经验。8 月 8 日，特别报告员正式致函人权理事会主席，要求主席进行干预，将他本人与这一征聘过程完全脱离干系，并表达了他对于该过程及其结果公正性的深度保留意见。

(c) 截至编写本报告时，在 12 个月内，前后共有三名人权干事分配给特别报告员，在任一时间段内仅有一名，且包括现任在内的前后三人均为临时工作人员。有一次，由于合同问题，人权干事整整一个日历月都未能工作。这些人权干事中，没有一人具备隐私方面的正规培训或资历或是处理隐私的经验，虽说最近(2016 年 7 月)为任务分配的人权干事在表达自由这一方面拥有一些处理隐私的有限经验，而且可能会任职时间长些。不论分配来的人权干事如何和蔼可亲、在其他人权领域如何知识渊博，在这种情况下都难以实现和保持连续性和效率；

(d) 2016 年 8 月 4 日，特别报告员获悉，除了上文(b)分段提到的常设人权干事将于 2016 年 9 月 1 日开始全职为特别报告员工作之外，还可能在 9 月或之后招聘一名半职的 P-3 职等工作人员和一名半职的一般事务职等工作人员(行政助理)。鉴于迄今看到的效率，我们并不抱太大希望；

(e) 效率是如此低下，以至于 2015 年第四季度联合国差旅费用还有部分没有报销，而特别报告员这样的官员是没有薪酬的。

6. 上段较详细(但远非全面无遗)地概述了人权高专办所提供支持的不足，以免大会和人权理事会错误地认为，人权高专办提供了非常高效或慷慨的支持，特别报告员得以开展工作。我不希望在今后的报告中再提到这个话题。如果今后不再听到特别报告员谈及此问题，大会或理事会应当认为，情况并没有出现值得专门评论的改善。另一方面，这不是要推卸责任：上面几段所述的情况，是否由极端低效、亟待改革的系统和/或一群自私自利、热衷于维护自身的舒适安排而不愿为特别报告员提供妥善执行任务所需高质足量支持的国际公务员造成，我将留待即

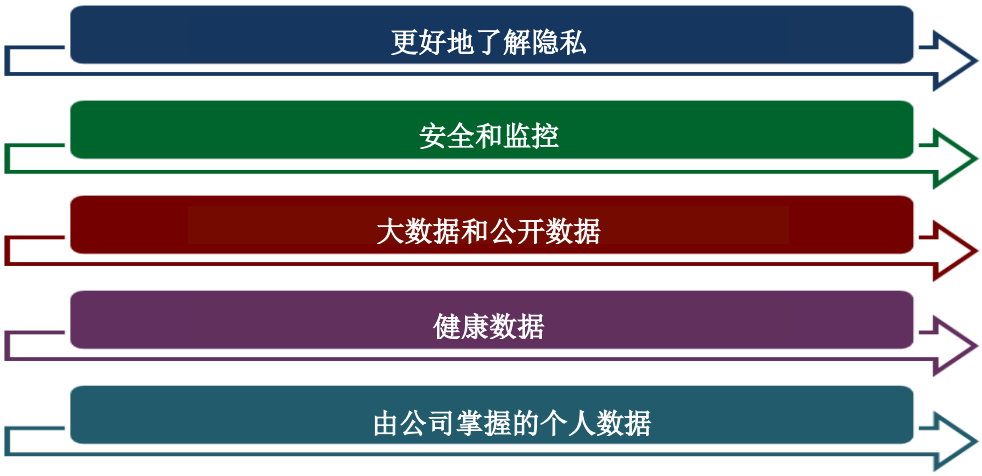
将上任的秘书长来决定，但愿新任秘书长拥有改革思想。如果你代表的国家或组织真正相信这一任务及其重要性，希望提供帮助，请直接联系特别报告员，以探讨提供进一步支持的可选方案。

B. 规划和启动与任务相关的多项活动

7. 虽然存在上文所述的行政和资源问题，特别报告员和他的团队在致力于此事业的许多民间社会行为体和其他利益攸关方的支持下，还是成功启动了多项活动。这些活动可大致分为对各国活动的持续监测和专题行动流，进一步概述如下。

8. 联合国几十个会员国内新监控活动、监控授权法律以及隐私法律的发展情况，仍然是特别报告员持续性重要监测活动的一部分，每天都在进行。这就需要审查每项新采用的技术和每项新提出的法律，并调查相关个人或民间团体向任务负责人提出的诸多申诉。这一监测活动是证据收集过程的重要组成部分，该过程提供的信息能帮助特别报告员选择对哪些国家进行正式和非正式访问。

9. 除了非常耗时的国别活动之外，还为专题优先事项投入了很多注意力和精力。2016 年 3 月提交人权理事会的报告中介绍的十点计划，其中的某些领域需要立即关注并同时采取行动。已认真确定这些领域，并将以专题行动流(TAS)的形式处理。[1] 在目前的第一个活动阶段设立了五个专题行动流，各对应下列优先事项之一：大数据和开放数据；安全和监控；健康数据；由公司处理的个人数据；“更好地理解隐私”。希望各行动流在自我发展的同时与其他专题行动流进行互动，使特别报告员能够在某个特定专题行动流相关调查和辩论成熟时编写一份专题报告。



[1] 关于这一问题的更多信息，可查阅：Joseph Cannataci 在 2016 年 6 月 3 日发表的博客文章“Parallel streams of action (TAS) for the mandate of the United Nations Special Rapporteur for privacy and the first set of priorities”。可查阅：https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/。

10. 特别报告员选择的方法是，考虑设立一支由经验丰富、无报酬的志愿人员组成的专题行动流工作组(TASk force)，有些人将之称为工作队(WP)。五个专题行动流各设一支工作队，协助特别报告员开展研究并起草一份专题研究报告，这些专题研究报告将成为 2017-2018 年期间提交人权理事会或大会的报告的主题。

11. 次级研究结果，特别是 2016 年 3 月至 7 月访问澳大利亚、奥地利、丹麦、法国、德国、意大利、拉脱维亚、荷兰、新西兰、瑞士和美利坚合众国期间进行的多次利益攸关方会议和事实调查活动的结果证明，将大数据和开放数据列为优先事项是正确的。因此，于 2016 年 5 月成立了大数据和开放数据专题行动流工作组，澳大利亚维多利亚州隐私和数据保护专员 David Watts 接受特别报告员的邀请成为工作组组长。6 月份开始制定工作队工作目标的粗略纲要，并开始招募首批组员。2016 年 7 月 20 日，Watts 先生和特别报告员在纽约共同组织了一次活动。在此活动上，Watts 先生和特别报告员介绍了首份拟议工作大纲，请各界人士提出评论意见，并邀请志愿者加入工作队。自那之后，已收到来自巴西、加拿大、法国、塞内加尔和美国的志愿专家报名。预计将在 2016 年 10 月底之前公布该专题行动流工作组的人员构成、首份目标纲要和职权范围。该专题行动流工作组还从愿意帮助对技术解决方法进行压力测试的独立组织寻求帮助。在大数据分析能够利用开放数据源进行三角测量的背景下，据说这些解决方法能够成功地去除个人数据识别，并防止再次识别。

12. 安全和监控将是特别报告员高度关注的优先事项，这一点毫无疑问。此领域非常复杂，涉及执法机构以及安全和情报部门的利益，与一些大公司的活动相交叉。这就意味着，需要首先将要处理的问题拆分为一些较小的子集，把确定和强化隐私保障和补救措施作为贯穿始终的重点。特别报告员在此部门采取的第一项重大举措就是设立国际情报监督论坛(IIOF2016)。该论坛将于 2016 年 10 月在布加勒斯特举行会议，预计将有数十个监督机构、议会委员会和情报部门参加。这次活动将帮助集体确定情报收集过程中隐私和表达自由方面面临的挑战，找出能提供更好保障和补救措施的最佳做法。2016 年 3 月至 7 月，特别报告员为组织国际情报监督论坛做了大量筹备工作，来自联合国各主要会员国的反馈非常令人鼓舞，一些国家已经确认将参加此次会议。如果此次会议能够取得成功，今后可定期举行论坛会议，不断为特别报告员的报告、建议和其他倡议提供意见和建议。特别报告员借此机会公开感谢参与这项工作的诸多联合国会员国，特别要感谢罗马尼亚参议院和议会的四个情报监督委员会接受他的邀请共同主办这一活动。还要感谢欧洲联盟基本权利机构以各种方式支持这一活动。同时，由公司处理的个人数据专题行动流工作组也在推进监控方面的工作(见下文)。此领域的其他举措和工作将在今后公布。

13. 特别报告员与利益攸关方的不断互动和深入研究结果已经证实，在世界范围内，大量健康数据的产生、处理、出售和再出售都在持续增长。在少数引领潮流

的国家，这一情况已成为制度化的业务模式，而且，由于越来越多的消费者开始使用可穿戴设备、智能手机应用和其他便携技术，具有潜在敏感性的健康和生活数据被持续收集和发送，加剧了上述情况。此外，由于人工智能技术的发展，一些国家尝试利用现有医疗记录来改善诊断能力，这也可能成为一个日益令人关切的问题。另一方面，显而易见的是，健康数据的使用可能带来一些益处，比如医学研究的进步。一些独立的市场研究也表明，患者对于个人数据可能被滥用越来越感到关切。为了以有条理的方式推进关于健康数据部门的工作，特别报告员在与此领域主要非政府组织进行了一段时间的协商之后，高兴地宣布，来自美国德克萨斯大学戴尔医院的 Steve Steffenson 博士接受邀请，担任被称为医疗工作组(MedITAS)的工作队组长。正在招募该工作队的其他组员，工作队的职权范围已经初步划定，预计将在 2016 年第四季度初该专题行动流工作组开始运作后进一步拟定并通过。

14. 特别报告员继续加强在以往和正在进行的项目中与大公司达成的互动协作，特别是与欧洲联盟支持下的隐私、财产和互联网治理替代管理方案(Managing Alternatives for Privacy, Property and Internet Governance，简称 MAPPING)项目相互协作，以继续审查企业部门日益增加使用个人数据对隐私的影响。隐私、财产和互联网治理替代管理方案囊括若干轨道，在其中至少三条轨道方面，即国际法的潜力、商业模式和隐私，特别报告员不断得益于与公司的合作。预计这些轨道将进一步为任务负责人在这一领域的工作提供意见和建议，并且(在该方案项目内)制定一份政策简报和路线图，供欧洲联盟考虑。这项工作中的一部分还与政府监控活动有关。特别报告员任务负责人与隐私、财产和互联网治理替代管理方案项目将于 2017 年 2 月 15 日和 16 日共同组织一次活动，预期届时将联合与民间团体就此问题进行协商。要感谢包括微软、谷歌、脸书、苹果和雅虎在内的一些大公司，以及一直以来以非常值得欢迎的方式与特别报告员任务和隐私、财产和互联网治理替代管理方案项目进行互动的全球网络倡议(Global Network Initiative)。欢迎所有其他利益攸关方在适当的时候加入这一进程。特别报告员邀请各界人士对这一问题以及所有其他专题行动流倡议表达意向。

15. “更好地理解隐私”专题行动流工作组是特别报告员一项较长期的举措。设想的是，在五个优先事项中，这一专题行动流工作组将最后提交报告，时间肯定不会早于 2018 年，因为预期需在非洲、亚洲、澳大利亚、欧洲和南美洲等区域开展其他一些协商活动。该专题行动流工作组已开始收集有关各项概念的证据，如隐私与人格自由发展这一首要基本权利的关系。预期该工作组的活动将成为一个持续进程，与特别报告员设立的所有其他专题行动流工作组分享信息并借鉴经验。该专题行动流工作组也将非常重视隐私与表达自由、(获取)信息自由等其它基本权利的关系。早在 2015 年 9 月，就与人权观察组织进行了初步讨论。在此基础上，该专题行动流工作组于 2016 年 7 月 19 日和 20 日在纽约组织了题为“隐私、人格和信息流动”的首次活动。在两天的活动期间，能容纳 90 人的会议室

座无虚席。这一活动的举办要感谢以下组织的慷慨支持和共同努力：人权观察组织；纽约大学法学院布伦南司法中心；哥伦比亚大学全球表达自由中心；隐私、财产和互联网治理替代管理方案项目；马耳他大学信息政策和治理系；荷兰格罗宁根大学安全、技术和电子隐私研究小组(STePP)。还要感谢德国政府向任务负责人提供一部分资金，支持来自世界各地的人们参与此活动。

16. 显然，代表会议举办地(美国)的观点得到了最详尽的陈述，但是来自澳大利亚、巴西、加拿大、哥伦比亚、印度、大韩民国、中东和北非地区、欧洲[2] 和联合国教育、科学及文化组织的与会者也分享了他们的观点和见解。第一天会议的主要目的是，更好更全面地理解数字时代中隐私权作为一项普遍人权的意义，以及是否应该更加强调这项权利在促进个人发展方面的作用。第二天的重点是促进对宣传战略的理解和制定，以帮助在全球范围内更有效和有力地推进隐私权。此次活动为一系列处理同一主题的新活动开了一个头。这些活动将在各大洲举办，目的是综合关于此主题尽可能多的观点，以建立和深化对于隐私以及在数字时代如何解释隐私的更全面理解，造福全球社会。因此，虽然在亚洲举行的下一次活动已经开始筹划，特别报告员谨此邀请有意在近期支持、主办或参与此类活动的方面直接与他联系。

17. 特别报告员及其团队还建立了一个关于隐私和人格的博客，主要为了(但不仅限于)帮助开展任务工作。地址为 www.privacyandpersonality.org。

C. 参与多项活动

18. 除上述活动以外，为了落实十点行动计划中概述的隐私认识目标，特别报告员自 2016 年 3 月 3 日以来参与了数项活动，其中包括：

(a) 3 月 15 日，德国波鸿，在和平与武装冲突国际法研究所(Institute for International Law of Peace and Armed Conflict)发表主旨演讲；

(b) 3 月 18 日，巴黎，会晤法国国家信息与自由委员会(Commission Nationale de l'Informatique et des Libertés)主席和欧洲联盟第 29 条工作小组(Article 29 Working Party)主席；

(c) 4 月 5 日，华盛顿，参与国际隐私专业人员协会(International Association of Privacy Professionals)全球隐私峰会专题小组讨论；

(d) 4 月 8 日，威斯康星州，在威斯康星国际法学报(Wisconsin International Law Journal)年度研讨会发表主旨演讲；

[2] 具体而言，审议和讨论了德国对于“信息自决”和隐私保护(“datenschutz”)的理解，认为可以将这一理解作为蓝图，进一步将隐私权理解为有助人格发展的一项赋能权利。特别报告员感谢来自汉诺威莱布尼兹大学法律信息学研究所的 Christian Hawellek 作出贡献。

(e) 4 月 18 日，意大利米兰，在数据保护专员协会(ASSO DPO)年度会议(一般数据保护条例和欧洲联盟数据保护专员作用讲习班)发表会前主旨演讲；

(f) 4 月 25 日，纽约，哥伦比亚大学，全球数字未来论坛；

(g) 5 月 9 日至 13 日，惠灵顿和奥克兰，在新西兰隐私周活动期间发表多场主旨演讲并会晤利益攸关者；

(h) 5 月 14 日至 18 日，悉尼和堪培拉，在澳大利亚隐私宣传周活动期间发表多场主旨演讲并会晤利益攸关者；

(i) 6 月 1 日和 2 日，海牙，2016 年安全研究和创新活动；

(j) 6 月 6 日，华盛顿，电子隐私信息中心(EPIC)，2016 年数据保护大会，“隐私对于下一届政府而言”专题小组；

(k) 6 月 7 日，华盛顿，第六届健康隐私的未来国际峰会，主旨演讲；

(l) 6 月 8 日，华盛顿，由乔治敦大学法学院隐私中心的 Alvaro Bedoya 组织的隐私、财产和互联网治理替代管理方案与特别报告员利益攸关者活动；

(m) 6 月 9 日和 10 日，华盛顿，会晤谷歌、脸书和美国国务院有关人员；

(n) 6 月 13 日，哥本哈根，DataEthics.EU 和丹麦人权研究所，开放讲座和主旨演讲；

(o) 6 月 14 日，日内瓦，进步通信协会，圆桌会议；

(p) 6 月 14 日，日内瓦，红十字国际委员会组织的讲习班，干预；

(q) 6 月 14 日，日内瓦，与因特网学会成员进行在线讨论；

(r) 6 月 17 日，法国斯特拉斯堡，欧洲委员会，“第 108 号公约：从欧洲现实到全球条约”；

(s) 6 月 20 日和 21 日，维也纳，欧洲联盟基本权利机构，基本权利论坛；

(t) 6 月 22 日，维也纳，与《维也纳日报》合作，阿尔卑巴赫会谈：“分享的时刻：每个人都有一席之地“；

(u) 6 月 23 日，维也纳，第 25 工作组，“更加安全的欧洲背景下企业在尊重隐私方面的角色和责任”；

(v) 6 月 27 日至 29 日，里加，第二届欧洲媒体和信息识读论坛；

(w) 7 月 19 日和 20 日，纽约，隐私权问题特别报告员大会，“隐私、人格和信息流动”。

三. 重要进展和实质性问题，2016 年 3 月至 7 月

A. 沉默权(不证己罪)：是否可以迫使智能手机作证，抑或这可能严重侵犯隐私？

19. 2016 年，人们重新开始辩论是否值得对由移动设备存储或产生的个人数据加密。可以说最突出的一个例子是，美国圣贝纳迪诺严重袭击事件的实施人使用了苹果公司制造的智能手机，而美国当局随后试图获取存储于该设备上的个人数据，这些事件都引起了公众的关注。2015 年 12 月 2 日，一对夫妇在南加利福尼亚州的一个地方政府办公室开枪射击，导致 14 人死亡，20 多人受重伤。[3] 美国联邦调查局(FBI)对于存储在设备上并且与苹果公司云计算服务(iCloud)同步的信息产生兴趣。虽然可以恢复 2015 年 10 月 19 日之前存储在外部的数据(该日停止备份)，但是联邦调查局或苹果公司都很难获取本地存储在智能手机上的数据。联邦调查局试图利用法律框架，给苹果公司设立一种义务来更改智能手机软件，降低破解的难度。苹果公司拒绝了该要求，联邦调查局随即将苹果公司诉至法庭，对其施压。最终，联邦调查局在 2016 年 3 月 28 日撤销了针对苹果公司的诉讼，因为联邦调查局可以通过其他方式获取存储在智能手机上的信息。[4] 在诉讼撤销之后，苹果公司发表声明称：“从一开始，我们就反对联邦调查局要求苹果公司在苹果手机上安装后门的做法，因为我们认为这是错误的做法，会树立一个危险的先例。由于政府撤销了诉讼，上面两种情况都未发生。”[5] 特别报告员在 2016 年 3 月 9 日报告第 30 段中概述了他的立场，即允许或授权在加密中设置后门是一个坏主意，其中的诸多原因在荷兰政府于 2016 年 1 月 4 日发布的一份立场文件中得到了最佳总结。苹果公司一案没有改变他对于此问题这一方面的看法。不过，智能手机和其他移动设备的确引发了事关基本权利的其他一些问题，可能对隐私权产生影响，而且，可能需要就这些问题作出决定，下一阶段有关加密问题的“对话”才能进行或是取得有效进展。其中的一项权利就是沉默权。

---

[3] Camila Domonoske，“San Bernardino shootings: what we know, one day after”，全国公共广播电台，2015 年 12 月 3 日。可查阅：www.npr.org/sections/thetwo-way/2015/12/03/458277103/san-bernardino-shootings-what-we-know-one-day-after。

[4] 见以下刊载于《卫报》的文章：Danny Yadron，Spencer Ackerman 和 Sam Thielman，“Inside the FBI's encryption battle with Apple”，2016 年 2 月 18 日。可查阅：https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple；Danny Yadron，“San Bernardino iPhone: United States ends Apple case after accessing data without assistance”，2016 年 3 月 29 日。可查阅 https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone；Danny Yadron，“FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone”，2016 年 4 月 28 日。可查阅：https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino。

[5] Hilary Brueck，“This is Apple's response to the FBI hacking into that iPhone”，2016 年 3 月 29 日。可查阅：http://fortune.com/2016/03/29/apple-response-fbi。

20. 现在，苹果公司与联邦调查局的诉讼案件已不再审理，但愿各方能够冷静下来，可以更清晰地思考。谨以为，既然苹果智能手机的全球销量已达数亿部，这一问题就不仅在美国引起关注，而成了一个全球性问题。同样道理，此案中用来试图强迫苹果公司帮助执法机构获取数据的法律，也可能被用于比苹果公司全球销量高出数亿部的其他智能手机制造商，尤其鉴于越来越多的制造商正在将密码保障措施纳入产品中。看来，随着规模经济的发展，全球三分之一人口将拥有和使用智能手机，而这一比例最终将达到二分之一。因此，如下文所述，我们面临着一个简单的事实：智能手机是一种无处不在的技术，对隐私有着巨大的影响。

21. 在此，特别报告员将概述一些初步意见，希望能使关于智能手机的辩论超越隐私范围，目的是在对事关“大局”的社会价值的确认或放弃基础上最终将辩论引回到核心隐私问题。特别报告员的立场是，需要在社会内部对其他适当行为标准进行审查，才能对使用智能手机涉及的隐私方面问题持有更加明确的观点。

22. 如同许多其他基本人权一样，隐私是一种动态而非静态的权利 。数千年来，人们都对隐私抱有期望和偏爱，但这并不意味着对该权利的保护程度或是对于该权利范围的理解一成不变，发展的方向是强化保护。隐私随着时间的推移而发展，而在设立特别报告员任务并任命现任报告员之前，已经找到很多证据表明，对于隐私的理解以及该权利的行使在不同的“时间、地点和空间”维度有所不同。[6] 与很多人所想的相反，认识到这种现实，并无损于该权利的存在或是其普遍性。相反，这种认识让我们反思构成该权利基础的一套复杂价值观，反思我们对于该权利的理解应该如何随着情况的改变而变化，只有这样才能继续保护这些基础价值观，并且尽可能加强保护。像智能手机这样的新技术的出现和应用是一个典型的例子，说明我们应如何更新对隐私的理解。正如在具有里程碑意义的 2014 年美国 Riley 诉加利福尼亚一案中，美国最高法院法官 Samuel Alito 所说的那样：

> 我们不应机械地将数字时代之前的规则应用于手机搜索中。如今所用的许多手机能够存储和获取大量信息，包括一些高度个人化的信息。若将这些信息转换成打印文本的形式，谁也不能带在身上。[7]

Alito 这段话认同了多数意见，也即如大法官 John Roberts 所说：

> 现代的手机不仅是科技带来的一项便利。手机包含并可能揭露大量信息，掌握着很多美国人的“生活隐私”。现在，科技使得人们可以随手携带此类信息，但这并不意味着，信息已不再值得我们像当年的创始者们一样奋力保护。[7]

---

[6] 如欲更详细了解特别报告员对几千年来隐私的存在以及时间、地点和空间维度的评估，见 Joseph A. Cannataci 所编的 The Individual and Privacy (英国，法纳姆，Ashgate Publishing，2015 年)。

[7] 美利坚合众国最高法院，Riley 诉加利福尼亚，2014 年 6 月 25 日裁判，第 13-132 号。可查阅：https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf。

不用说，有意或无意间把“生活隐私”交让给手机的，不只是美国人。事实上，地球上的每一个人，不论其信仰、肤色、族裔、性别、国籍或地理位置为何，只要携带智能手机，就已经把自己的生活隐私委托给了最常用的便携设备。这就是为什么在 Riley 诉加利福尼亚一案中表达的许多意见同样具有全球意义。在这里，特别报告员将从美国这一案件中大量引用，因为此案概括出了一些论点，而在苹果与联邦调查局间纠纷这一总体背景之下，全球各地都有此类问题提出，下一步应考虑这些论点。

23. 正如 Riley 诉加利福尼亚一案中概括的那样：“现代的手机……已经牢牢渗透到日常生活之中。传说中的火星访客可能会以为，手机是人类结构的重要特征。”[7] 最高法院的法官们正确地指出：

> 与被捕者可能随身携带的其他物品相比，手机在量和质的意义上都有所不同。“手机”一词本身就是一个具有误导性的简称；很多此类设备实际上是微型计算机，只是恰巧可以当作电话使用。它们完全可以被称为相机、视频播放器、名片盒、日历、录音机、书库、日记本、相簿、电视、地图或是报纸。现代手机最显著的特点之一就是其巨大的存储能力。手机出现之前，对某人的搜查受到实物条件的限制，通常只构成对隐私的有限入侵。[7]

美国最高法院的法官们不止一次指出：

> 渗透性这一要素是区别手机和实物记录的主要特征。数字时代之前，人们通常不会整天都把大量敏感个人信息带在身上。现在，不随身携带手机以及手机里内容的人反而成了特例。一项民意调查显示，将近四分之三的智能手机用户称，他们大部分时间都距离手机不超过 5 英尺，12%的用户称他们即使在洗澡时也使用手机。[7]

法官们同样认识到，智能手机能够提供关于使用者的非常详尽和准确的资料：

> 虽然仅凭数量就可以区别存储在手机上的数据和实物记录，但是某些类型的数据还具有性质上的不同。例如，对于可以上网的手机，可以查阅其互联网搜索和浏览历史，从而揭示某人的私人兴趣或关注点，例如，某人可能搜索过某种疾病的症状，还经常访问医疗健康服务网站 WebMD。手机上的数据还能够揭示某人去过的地点。[7]

24. 也许，最重要的是，美国最高法院的法官们意识到，手机上的内容数量巨大，私密性非常高，它们涉及的隐私程度远远高于受美国宪法第四修正案保护的传统住所搜查可能侵犯的隐私。

> 与最彻底的住所搜查相比，对手机的搜查通常会使政府获得更多：手机不仅以数字形式含有许多在过去的住所搜查中找到的敏感记录；还含有不可

> 能以任何形式在住所中找到的各种私人信息，当然，如果手机是在住所内找到的话，就另当别论了。[7]

美国最高法院的法官们以此展示了智能手机体现的新技术是如何改变游戏规则，而此“时”(2014 年)、发现个人信息的此“地”(美国——以及在美国发现的手机)已经发生巨变，个人信息的便携性、数量和性质能够完全改变并强化个人“空间”中的隐私维度。

25. 在 Riley 诉加利福尼亚一案中，美国最高法院的法官们主要关心的是，出于美国宪法第四修正案所固有的隐私考虑，禁止对智能手机的无证搜查。然而，需要指出的是，手机安全和加密的情况可能会复杂得多，不仅仅是有关隐私和安全的争论而已。世界上许多国家都承认沉默权或避免自证己罪的权利，将其作为民主社会认同的道德标准之一，而这些国家面临与美国最高法院法官们一样的两难处境，可能只是个时间问题。这是因为，正如 Riley 诉加利福尼亚一案中概括的那样，移动电话因其自身特点而成为一种特殊的个人数据存储库，也成为了最显而易见的完全和彻底破坏沉默权的工具。自 16 世纪以来，沉默权逐渐被各司法系统承认，而美国在第五修正案中承认了此权利。简单地说，在世界上很多、但并非全部司法系统中，被告有权在针对自身的刑事诉讼中保持沉默从而避免自证己罪。在澳大利亚、孟加拉国、德国、印度、新西兰、美国等众多相距甚远的国家，此权利罕有例外，且鲜见附加条件。然而，一纸允许获取手机存储数据的司法授权令就可以有效地破坏此权利。被告——迄今为止不可迫使其作证——可能有权保持沉默，但被告的手机却可以充分揭示其最私人的想法、兴趣和行动。在许多司法系统中，被告的配偶或近亲被赋予同样的地位，不可迫使其作证。然而，大多数人都会说，智能手机比他们的配偶更了解自己。那么，即使有了获取手机信息的司法授权令，是否就可以迫使智能手机作证呢？ 因此，逻辑——以及逻辑一致性——应将我们引领至何方？

26. 在目前时刻，隐私权问题特别报告员将关于智能手机和类似设备(包括可穿戴设备和植入式设备)的问题列入未来的讨论范围，可能由其他特别报告员进行讨论或与其他特别报告员协作进行讨论。在此初步阶段，特别报告员不发表特别意见或建议。现阶段的任务只是确定需进一步调查的问题，这一问题严重侵害隐私，但不仅仅涉及隐私权，还涉及诸如刑事诉讼中的正当程序之类的基本权利。一些人可能认为，如果将 Riley 诉加利福尼亚一案应用于沉默权而不是隐私权，得出的逻辑结论将意味着，在大多数情况下，不能迫使刑事诉讼被告的智能手机作证。这一立场同样将对隐私权产生重大影响，至少是由于它承认了智能手机所含数据的私密性和私人性程度。

27. 沉默权在大不列颠及北爱尔兰联合王国的起源可追溯到四百多年前，但具有讽刺意味的是，该国实际采取的立场却是，事关电子设备而言，国家安全或打击犯罪的重要性高于隐私或沉默权。按照 2000 年《调查权监管法》第 49 部分和第

53 部分的规定，被要求却不披露加密数据的密码，则构成犯罪(可判处两年监禁，对于儿童性虐待案件，则可判处五年监禁)。因此，在联合王国，不仅可以迫使智能手机作证，而且如果某人不提供设备密码的话，还可能被判处更长的刑期。苹果诉联邦调查局的案子略有不同，因为被告实际上已经死亡，并且其罪责毫无疑问，但是，需要获取手机中的信息才能了解各项事实以及恐怖主义行为筹备过程等全局情况以及可能是全国性或国际性恐怖主义网络的同伙和相互关系信息。不过，该案件引起广泛兴趣，完全理所应当，因为它将我们引向了隐私、安全和沉默权相关讨论的核心。也许，接下来应该组织一场关于隐私权和沉默权的交叉研究。特别报告员将与国际律师协会、欧洲各律师协会以及其他各利益攸关方进行协商，然后就进行深入调查的时机是否成熟以及是否需要为此领域的循证决策提出建议形成观点。

B. 数据保留、大规模监控和更多的加密

28. 虽然无数的国家宪法法院和地区人权法院已做出裁决，但是特别报告员注意到，各国政府越来越倾向于推进更具侵入性的监控法律，允许几乎是不加掩饰地对公民实施长期大规模监控。

29. 联合王国下议院三读通过《调查权法案》，朝此方向又进了一步。按照计划，该法案将在 2016 年 9 月进入上议院委员会审议阶段。特别报告员必须假定，读者们熟悉他在 2016 年 3 月 9 日的报告中对该法案所作的批评。该法案中涉及大规模监控和大宗黑客攻击的部分继续受到国际社会审查。欧洲联盟法院计划将就此事做出裁决，在之前的 2016 年 7 月 19 日，法院检察长发表意见称，成批处理仅在严重犯罪案件中合法，这比该法案允许的范围狭窄许多。该法案仍然是隐私领域的雷场，如果要进行透彻分析，需要的文字数量将 10 倍于本报告必须遵守的 10 300 字限制。不过，令人高兴的是，议会的各位大臣、自由组织(Liberty)、法律学会、开放权利组织(the Open Rights Group)和隐私国际正勇敢地挑战该法案。只能希望联合王国政府能按下暂停按钮，认真聆听欧洲人权法院和欧洲联盟法院关于监控的意见，让理智占上风。还应该聆听来自本国上议院议员的一些意见。曾任高级警官的上议院议员 Paddick 勋爵多次抨击该法案关于互联网连接记录的规定，称：“互联网连接记录——法案中唯一的处女地——将侵入无辜民众的隐私。”后来他指出，鉴于法案允许警察在没有搜查令的情况下获取联合王国所有互联网用户的个人数据，互联网连接记录囊括一切的性质异乎寻常。[8]

30. 《调查权法案》原本就不应该以现在的形式提出，或是在下议院获得通过。上议院迄今的讨论并不令人乐观。2016 年 7 月 13 日，担任国防大臣和上议院副领袖的厄尔 • 豪表示：

[8] 大不列颠及北爱尔兰联合王国上议院，《调查权法案》辩论，2016 年 6 月 27 日，第 773 卷。可查阅：https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill。

> 政府与(通信服务提供商)合作，确定采取措施开发和维护移除通信或数据加密的技术能力是否合理可行，这可能是完全明智的做法。
>
> 执法部门和情报机构必须保留在有限的情况下要求电信运营商移除加密的能力。[9]

31. 此类言论说明下列四种情况之一：(a) 该大臣得到的情况通报非常糟糕；(b) 向大臣通报情况的人不了解加密的真实运作原理；(c) 大臣没有理解情况通报；(d) 大臣有意向上议院曲解情况。特别报告员不愿相信这是蓄意的曲解，因此呼吁议员阁下和所有的上议院议员了解一些简单的事实。如果上议院议员们能够了解荷兰政府在 2016 年 1 月 4 日发表的意见，或许就能够懂得为什么试图制定弱化加密的法律是一个糟糕的想法，在实践中尤其愚笨。他们会懂得，这种建议不仅远非“完全明智”，而且是完全荒谬的。他们还会懂得，“执法部门和情报机构必须保留在有限的情况下要求电信运营商移除加密的能力”之类的言论为什么完全虚幻，脱离现实。绝大多数情况下，执法部门和情报机构没有能力要求电信运营商移除加密——要不然他们可能会气急败坏地要求电信运营商这么做——其中的原因很简单，大多数情况下，电信运营商本来就不具备此能力。如果联合王国议会因被误导而批准这一异常荒谬的法律，那么，个人仅花费一点力气就可以下载在联合王国或美国以外制作并在互联网上免费提供的任意数量的加密算法/加密通信程序，然后使用此类程序与其他蓄意在联合王国境内造成伤害的人进行通信。在这种情况下，电信运营商束手无策，而信号情报机构除了努力破解代码之外也别无良方。

32. 上议院一些议员对此问题有着正确的理解。Strasburger 勋爵简明扼要地指出：

> 端到端加密的一个特点就是，提供者不能破解；加密对于两端的用户来说都是私有的。(厄尔·豪)似乎在暗示，提供者只能使用可以破解的加密，因而不可能是端到端加密，由此，下一版本的苹果手机在理论上将成为非法。我认为此方面有很多工作要做。[9]

特别报告员也这么认为，并建议，工作的重点方向应该是，使联合王国政府摆脱可以有效取缔端到端加密或使联合王国境内人员无法使用端到端加密的幻想。这一想法是不合逻辑的思维，如同与因刀具可用于伤人而完全禁止刀具、因汽车有时被用作逃跑车辆而禁止汽车一样。此外，故意削弱加密带来的安全风险远远超出收益。Strasburger 总结道：

[9] 同上，《调查权法案》辩论，2016 年 7 月 13 日，第 774 卷。可查阅：https://hansard.parliament.uk/lords/2016-07-13/debates/16071337000437/InvestigatoryPowersBill。

> 我要强调——加密技术行业的任何人都会对此详加说明——两者不可兼得。加密要么是安全的，要么是不安全的；不可能在对一小群用户不安全的同时对其他人安全。[9]

Paddick 勋爵提到的办法可能更加符合近期 Zakharov 诉俄罗斯一案体现出的欧洲人权法院判例法：“不要用权力强迫公司从一整项服务或技术中移除加密，而应使用更有针对性的替代权力。”[9] 在目前阶段，特别报告员只想知道，要等到何时，常识——更不用说对如隐私之类基本人权的应有尊重——才能在该国关于此问题的争论中最终胜出。

33. 几十年来，德国为某些领域的创新型隐私保护树立了杰出典范。2016 年 4 月，德国宪法法院延续了这一传统，裁定一项赋予联邦警察监控权的法律(“BKA-Gesetz”)部分内容违反宪法，因为这些内容没有提供充足的保障措施在调查潜在犯罪的过程中确保个人隐私权与国家利益之间的平衡。法院认为，对于某些权力，如通过录音对话或照片进行监控、实施监听或远程搜索电脑等能力，未设置足够的限制，包括进行司法审查的可能性在内，来保证侵犯德国公民隐私的行为拥有正当理由且程度适当。[10]

34. 德国情报部门的民主监督仍然令人关切。对于欧洲委员会人权专员尼尔兹·穆兹涅金表达的关切问题，特别报告员有同感，并且指出，他在 2015 年 10 月公布的调查结果未遭质疑。特别是：

> 对德国情报和安全部门进行有效监督，当前面临的挑战包括缺乏资源和专门知识、电信监督的范围、协调问题以及未能向受电信监控影响者提供有效补救措施。

专员尤其关切的是，监督机构及其秘书处缺乏资源和技术专业知识。在这方面，监督者与受监督者之间的人数比例尤其说明问题：13 名成员组成的两个机构，由一个小型秘书处提供支持，负责拥有 6 000 名工作人员的最大机构(联邦情报局)的监督活动。[11]

> 特别报告员希望在包括 2016 年国际情报监督论坛在内的各种论坛上跟踪此类关切问题，并且在适当时候与德国政府直接沟通。

---

[10] Wenzel Michalski，“Dispatches: rare victory for privacy in Germany's ‘war against terror’”，人权观察，2016 年 4 月 27 日。可查阅：https://www.hrw.org/news/2016/04/27/dispatches-rare-victory-privacy-germanys- war-against-terror。

[11] 欧洲委员会，“欧洲委员会人权专员尼尔兹·穆兹涅金在 2015 年 4 月 24 日和 5 月 4 日至 8 日访问德国之后的报告”，2015 年 10 月 1 日。可查阅：https://www.ecoi.net/file_upload/1226_1447235185_commdh-2015-20-en.pdf。

35. 2016年6月28日，德国政府签署了一项关于联邦情报局(the Bundesnachrichtendienst，简称 BND)的法律草案，此草案修订了包含监控德国境外非德国公民规定的几项现行法律。2016 年 7 月 8 日，议会一读通过该法律草案。预计该法律草案的二读和三读，包括最终投票在内，最早可能在 2016 年第四季度进行。

36. 在这里要提出的第一点意见有关国籍问题。该法律草案继续将德国公民和非德国公民区分开来。这根本没有清楚地反映现实。过去两年以及更长时间以来，发生在欧洲的恐怖袭击大部分都是由欧盟公民实施的，实施者通常都是袭击发生国的本国公民。如果主要风险在于此(即本国公民)，那么区分国民和非国民的法律有什么真正的价值呢？ 特别是，根据《公民权利和政治权利国际公约》第 17 条的规定，每个人都享有隐私权，而不论其国籍或公民身份。由此，我们必须要问，此类规定的实用性和适当性究竟如何，合法性就更不用说了。穆兹涅金先生也注意到这一不正常现象，在报告中表示：“当局称，《基本法》第 10 条提供的保护不适用于德国以外的活动，仅限于德国公民或发生在德国境内的活动。” 与其他国家法律中将基本权利保护限制于本国公民或居民的主张一样，这一解释无法令人接受。事实上，穆兹涅金先生在报告中还指出：

> 然而，这一解释受到争议，因为联邦宪法法院曾在 1999 年裁决，《基本法》提供的保护不限于德国领土，而且基本权利必须得到尊重，至少对于在德国境内处理从国外获得的信息的情况而言是如此。[11]

德国这项新法律草案失去了一次宝贵的机会，未能澄清，隐私权及相关保障均适用于个人，不论国籍、公民身份或地点，也不论进行监控的地点是德国境内还是境外。

37. 此外，德国这项法律草案引发了许多其他关切问题：

(a) 目的明确：收集和处理数据的条件模糊，过于宽泛；

(b) 大规模监控：如果通信拦截在德国境内进行，对非德国公民之间域外通信的大规模有针对性监控将得到有效授权。虽然符合 Zakharov 诉俄罗斯一案所述标准的有针对性监控不太令人关切，大规模监控仍令人严重关切，而且初步证据有悖于欧洲法律确立的标准；

(c) 独立监督：新法律没有包含适当的独立司法监督；

(d) 法律草案为监督拟议的大规模监控所提供的资源远远不足且不对口。新法律设想成立一个三人委员会，仅要求其每年开会四次。该委员会可能没有足够的工作人员或资源来监督大规模监控行动，而顾名思义，大规模监控活动的范围非常广泛。为此，特别报告员持有与穆兹涅金先生同样的关切。此外，该委员会成员的任命和组成由行政部门决定，这丝毫不能加强独立监督的印象。

38. 鉴于以上所述，有关德国新法律草案的初步证据表明，德国当局没有从穆兹涅金先生 2015 年 10 月的报告中学到任何东西。德国政府未能向特别报告员提供一项可在全球各地成为良好做法范例的示范法，而是提出了一份令人失望透顶的东西。联合王国的《调查权法案》草案虽然有诸多缺陷，至少还试图部分纠正特别报告员和其他人之前批评过的薄弱监督制度。联合王国新提出的监督制度虽然远非完美，但看上去还是比之前的情况有所改进。然而德国的情况却并非如此。如果德国不悬崖勒马、改弦易辙，定将取代联合王国，成为西方世界中监督制度与情报部门规模相比最为薄弱的国家。

39. 特别报告员可以理解近期发生在德国的一连串袭击事件所引发的焦虑情绪，但他仍然希望该国可以在隐私和数据保护领域发挥领导作用，并且，与联合王国的情况一样，邀请德国与特别报告员合作制定一项新法律和适当的监督资源制度，成为全球范围内的最佳做法范例。

C. 进一步认识隐私与人格的关系

40. 2016 年 7 月 13 日，墨西哥国家透明度、信息获取和个人数据保护研究院(INAI)发布了一项非常令人感兴趣的意见(Expediente PPD.0050/16)，称道：“应当指出，虽然根据宪法规定，保护个人数据的权利是一种保护私人生活的自主权力，但是，这两个概念应该有更广泛的解释，后者指的是一个范围，在此范围内任何人都可以自由发展个性。”因此，一般而言，对私人生活的保护包括涉及信息存储的其他权利和具体保障、个人数据的获取以及关于保护私人通信、姓名、人身和道德健全性的规定。

四. 结论

41. 特别报告员在上任后第一整年中，为完成任务负责人业务而旅行 20 次，访问了 14 个国家。访问的各国相距遥远，包括澳大利亚、巴西、新西兰、美国以及 10 个欧洲国家。虽然从技术上讲，这些都属于“非正式”国家访问，但是，在许多情况下，这些访问都包含了特别报告员传统正式访问的全部活动内容，其中包括会晤部长、各部官员、情报部门、监督机构、数据保护专员、执法部门、民间团体和大公司。大多数情况下，特别报告员收到了非常积极的反馈。今后 12 个月，将要进行至少两次、可能三次正式国家访问，日程都已初步排定，三大洲各访问一次(非洲、亚洲和拉丁美洲)。

42. 特别报告员启动了一个世界范围内的结构化协商体系。民间团体、个人、政府、公司和其它利益攸关方已致信特别报告员并/或要求会见，表示对各种隐私相关话题有兴趣，其中大部分会见要求已予满足。通过这些会见，特别报告员建立起各部门利益攸关方名单，并使用这些名单来邀请利益攸关方参加在世界各地举

行的会见。结构化协商往往是(应利益攸关方的要求)关起门来进行，但是，来自不同方面的受邀者以及致信要求参加已公布活动的人士也可包括在内。

43. 此外，特别报告员建立了开展进一步调查和协商的结构，设立了五支工作队，各负责首批优先事项中确定的专题行动流之一：大数据和开放数据；安全和监控；健康数据；由公司处理的个人数据；“更好地理解隐私”。这些将为预计于 2017-2018 年开始提交的专题报告提供基础。通过这一方法，特别报告员可以部分克服资源的限制，利用全球各地愿意无偿志愿提供领域专业知识的专家库。不过，特别报告员将继续寻求外部资金，并欢迎一切形式的援助，以妥善执行其任务。

44. 本报告受到武断的强制字数限制约束，未能对任务负责人开展工作的其他十余个领域发表评论。希望能在未来的专题报告和一般报告中详细介绍这些领域。

45. 特别报告员对迄今的协作情况总体感到满意，但建议更多的政府关心此项任务，仿效过去一年中其他政府的做法，积极就仍处于初期阶段的隐私法律草案以及诸如监控之类的相关领域进行协商。此外，特别报告员大力鼓励并赞赏各界参与和推动任务负责人组织的各项举措，如 2016 年国际情报监督论坛、非正式国家访问和各种讲习班会议。