联 合 国 A/HRC/31/64

大 会

Distr.: General
24 November 2016
Chinese
Original: English

人权理事会
第三十一届会议
议程项目 3
促进和保护所有人权——公民权利、政治权利、
经济、社会及文化权利，包括发展权

隐私权问题特别报告员的报告*、**

秘书处的报告

隐私权问题特别报告员在根据人权理事会第 28/16 号决议提交理事会的报告中，介绍了对其任务的设想，以及他的工作方法和三年期工作计划。报告还概述了 2016 年年初的隐私状况。

* 本报告逾期提交，是为了反映最新动态。

** 本报告附件不译，原文照发。

GE.16-20847 (C) 141216 161216

1620847

隐私权问题特别报告员的报告

目录

一. 导言

1. 人权理事会关于数字时代隐私权的第 28/16 号决议确立了隐私权问题特别报告员的任务。在这项决议中，理事会强调，各国必须确保充分遵守其按照国际人权法承担的义务。在隐私方面，这一点特别难以实现，因为信息技术的飞速发展不仅为社会互动提供了新机会，还产生了关于如何进一步发展这项权利以应对新挑战的关切。

2. 根据上述决议，特别报告员将每年向理事会和大会提交报告。在本报告中，特别报告员介绍了他的工作方法(第二部分)、2016 年的隐私状况(第三部分)、他迄今开展的活动(第四部分)和旨在发现和进一步发展二十一世纪隐私权的十点计划(第五部分)。此外，他还将在第六部分提出结论。

3. 应将本报告视为一份不太成熟的初步报告，因为特别报告员在 2015 年 8 月 1 日被任命后，准备了还不到六个月。因此，尽管特别报告员做了大量努力，仍然没有足够的时间与所有利益攸关方磋商。鉴于这个原因，本报告的主要目的是指出一些重要问题，而不一定分出轻重缓急。预计特别报告员在有机会听取世界各地更多利益攸关方的关切后，可在接下来的 12 个月内(也就是到 2017 年 1 月)更好地确定应采取行动的优先次序。特别报告员对其任务的设想和可能面临的挑战，见附件一。

二. 特别报告员的工作方法

A. 国家监测

4. 正在开发现行政策、法律、程序和做法数据库，将收入各种报告和相关立法。它将使特别报告员能够确定所关注的问题和最佳做法，并可与他人分享。

B. 专题研究：分析和评估

5. 特别报告员开展的磋商表明，在一个从不分国界的互联网受益无穷的世界中，人们普遍支持两个一般性原则，即无国界的保障和跨国界的补救。

6. 这种对保护隐私的保障措施和侵犯隐私的补救办法的关切是特别报告员在隐私风险似乎较高的一些部门开展以下专题研究的基础。每项研究都将提出一项特别报告，反映不断开展的磋商、互动和所提出的意见。

1. 不同文化的隐私和个性

7. 这项研究考虑到需要更好地了解在 2016 年，在一个互联网的运作不分国界的数字时代里，隐私对于不同文化而言，指的是什么，或者应当是什么。通过提出“为什么要有隐私”这个问题，并且视隐私为一种促进性的权利，而不是目的，特别报告员将隐私作为一项促进实现个性不受阻碍地自由发展的权利来加以分析。这一分析是与几个非政府组织密切合作进行的，预计将会成为 2016 年举行的一次重大国际会议讨论的重点。分析还是在广泛背景下进行的，对隐私权与其他基本权利的关系予以探讨。因此，预计将通过与联合国其他特别报告员等方面的联合行动，考察隐私与表达自由和获取公共信息的自由之间的关系。已经在与促进和保护意见和表达自由权问题特别报告员开展讨论，以探讨 2016 年和 2017 年就这一专题采取联合行动的机会。

2. 公司在线商业模式和个人数据的使用

8. 万维网在其存在的前 25 年中，促进了私营公司基本上不受监管的增长，有的迅速成长为跨越国界经营的跨国实体，吸引了世界各地的客户。这种增长的标志之一是收集和使用个人数据；每一次搜索、阅读的每一个条目、每一个电子邮件或其他形式的信息传送、所购买的每一项产品或服务都会留下数十万的电子痕迹，加以汇总就能非常准确地了解一个人的好恶、心情、经济能力、性偏好、健康状况和购物模式，及其思想、政治、宗教和哲学兴趣和观点。这就产生了一个总的问题：一些在线服务提供商是否有权跟踪个人行为，以确保获得公正赔偿。这种关于消费者行为的日益详细的数据图导致个人数据成为商品。这类数据的访问或使用现已成为世界上最大的产业之一，创造了以千亿美元计算的收入，最常见的形式是有针对性的广告。很多时候，虽然消费者可能知道他们有意识地放在网上的内容，但确不太知道他们在上网、聊天、购物或进行其他的在线互动时所生成的元数据的数量、质量和具体用途。现在可用于对个人进行分析的数据比 25 年前增加了好几个数量级，但与这些数据的使用或不当使用有关的隐私风险度还没有被完全了解。有些证据表明，个人数据的商品化，尤其是在传统上被认为敏感的行业如处理医疗数据的行业，已经到了这类数据在个人毫不知情或者并未表示同意的情况下被买卖或多重倒卖的程度。尚无足够证据可用来对据称是匿名数据的内在风险进行评估，这些数据通过逆向工程，能与可识别的个人联系起来。这种侵犯隐私的行为可给个人以及相关社区带来多种风险，特别是在访问未经授权以及访问者系意在获得或保持权力的国家当局、有组织犯罪集团或行动非法的商业公司的情况下。在数字计算机的早期，一个主要关切的问题是各国不仅利用个人数据，并能将各种来源中保存的数据加以整理，从而详细了解个人的活动和资产情况。但 2016 年，公司掌握的个人数据似乎比国家多得多。个人数据的货币化所带来的巨大收入意味着，仅仅由于对隐私的关切而改变商业模式，动机并不是很大。事实上，只有在隐私风险最近威胁到商业模式的收入潜力时，一些公司才采取了更严格、更加尊重隐私的方法。现在似是开展全球讨论的良好时机——收集适当证据可为讨论提供参考——以确定就公司收集的数据而言，哪种信

息政策最适于最大限度地保护个人隐私，并使隐私风险最小化。这一讨论可参考第 8 段所述公民关于隐私的概念和期望。预计 2015 年启动的磋商将在 2016 年将涉及网上公司，并计划在 2017 年举行一次有关这一主题的重大公共协商活动。

3. 安全、监控、相称性和网络和平

9. 国际上对安全的关注仍是 2015 年和 2016 年发展考虑的首要问题。上文概述的国家监测进程表明，有些国家议会在匆忙通过立法，以实现其安全和情报部门及执法机构采取的某些侵犯隐私措施的合法化。在许多这样的国家——遗憾的是并非所有国家——所采取的立法措施引进了关于以下问题的公共辩论：

(a) 监督机制的充分性；

(b) 有针对性的监测和大规模监控(一些国家委婉地称为“批量”监控)之间的区别；

(c) 这些措施在民主社会的相称性；

(d) 这些措施的成本效益和总体效力。

10. 打击恐怖主义和有组织犯罪以及其他具有社会敏感性的犯罪，如恋童癖，是这种立法所宣称的主要目标。公共辩论提供了相反的证据，通常表明侵犯隐私的措施，特别是大规模监控，不会带来更大的安全，需要通过其他手段解决情报失灵问题。特别报告员继续实施一项方案，与世界各地执法机构及安全和情报部门持续接触，以更好地了解他们的合理关切，确定可加以分享的最佳做法，以及其有效性尚存疑问，或者可能会在国家和全球范围内给隐私带来不可接受的风险的政策、做法和立法。在有些情况下，这种持续的分析几乎与网络安全和网络间谍问题变得密不可分。少数国家(这一数量在增加)将网络空间视为许多安全和情报机构的另一个行动场所；它们似乎仍不愿意在这些问题上相互接触——有时是与特别报告员接触——而这些问题自然也会对公民的隐私产生直接影响，不论其国籍如何。普通公民虽然不一定是网络安全和反网络间谍措施的主要目标，但常常受到影响，其个人数据和在线活动可能以国家安全的名义受到不必要、不相称和过度的监测。除了为履行任务开展的特别调查工作外，特别报告员还幸运地访问到安全领域以前和正在进行的独立合作研究所提供的丰富的证据基础，特别是欧洲联盟资助的研究。[a] 特别报告员正在四个主要方面开展这项研究：(a) 范围合理并受立法、程序和技术保障适当限制的国家监控能力，包括强有力的监督机制；(b) 侧重于有针对性的而不是大规模的监控；(c) 执法机构及安全和情报部门对私人公司和其他非公共实体持有的个人数据的使用；(d) 重新强调网络和平。特别报告员强烈认为，网络空间有可能被网络战争和网络监控所毁掉，各国政府和其他利益攸关方应努力实现网络和平。至少在这个意义上，保护隐私也是

[a] 包括诸如 CONSENT、SMART、RESPECT、SiiP、INGRESS、E-CRIME、EVIDENCE、MAPPING、CITYCoP 和 CARISMAND 等项目。

实现网络和平的一部分。这样，网络空间才能真正成为个人可以期望隐私和安全的数字空间，一个不会除了恐怖分子和有组织犯罪的威胁外，还不断受到某些国家的活动危害的和平空间。

4. 开放数据和大数据分析：对隐私的影响

11. 21 世纪的第二个十年，信息政策和治理方面最重要的问题之一是确定以下两方面的适当平衡：一方面是为了社会利益，根据开放数据原则使用数据；另一方面是迄今为止，为了保护基本权利如隐私、自主权和个性自由发展而制定的既有原则。关于特别报告员在这方面的关切，详见附件二。

5. 遗传和隐私

12. 特别报告员注意到约四分之一的会员国建立了国家罪犯 DNA 数据库。法医 DNA 数据库可在解决犯罪问题方面发挥重要作用，但也会引起对人权的关切，包括可能滥用政府监控(例如确认亲属和非亲生关系)，并存在误判风险。此外，为行政目的，例如身份证或移民而使用 DNA 数据库的情况，似乎呈指数增长趋势。在未来几年内，可能还会建立所有公民的 DNA 数据库。与 1990 年代一样，人们对保险业中遗传数据的使用再次感到关切，认为个性化药物将导致许多人自愿向保健行业提交其完整的人类基因组。鉴于这些和其他关切，以及 DNA 数据库在全世界变得更加普遍，需要持续开展更大规模的公共和政策辩论。特别报告员打算通过确立最佳做法，邀请专家、决策者和公众参与公开辩论等方法，继续参与旨在为 DNA 数据库制定国际人权标准的项目。预计这种参与将有助于根据民间社会行动者的投入和反馈，拟订有关最佳做法的准则。

6. 隐私、尊严和声誉

13. 对安全和监控的关切可能转移了许多公民对其隐私、尊严和声誉在互联网上所面临的风险的关切。数字时代意味着媒体在过去二十年有了很大的发展和变化，特别是，互联网使没有经过正式新闻培训的普通公民可以随时并随意发布文本、音频和视频内容。这种发展在很多方面增强了公民的权能，尤其是在避开审查或其他障碍，或者在技术促进言论自由、加强社会民主的情况下。另一方面，在一个快速发展的媒体世界中出现的公民记者和博客撰写人这种新现象，再加上社交媒体的广泛使用，产生了一种普遍的关切，即言论自由权遭到滥用，对其他基本人权如隐私和尊严造成了不良影响。过去五年的研究突出表明，公民越来越担心他们的名誉和声誉可能会在互联网上遭到攻击和破坏，许多网民在遭到诽谤和/或隐私受到侵犯的情况下寻求保障和补救时，感到非常无助。特别报告员愿与促进和保护意见和表达自由权问题特别报告员、民间社会和联合国其他机构如联合国教育、科学及文化组织合作，探讨在互联网上对个人隐私、尊严和声誉的具体保护，以及遭到侵犯情况下的补救办法。与上述其他一些专题研究一样，隐私和互联网治理之间的关系仍然是一个反复出现的根本问题，对隐私、尊严和声誉也具有相关性。

7. 生物识别和隐私

14. 一项关于当前研究的调查表明，为了从执法到个人访问移动设备的各种目的，对使用生物识别技术的兴趣大增。因此，语音识别、视网膜扫描、步态和面部识别以及指纹和皮下指纹技术只不过是 21 世纪的第二个十年为各种目的开发和部署的许多数字技术中的一些例子。特别报告员打算继续与生物识别研究界以及执法机构、安全和情报部门及民间社会合作，进一步确定关于使用生物识别装置的适当保障措施和补救办法。

C. 个人申诉

15. 特别报告员收到了、并且可能会继续收到关于指称个人和民间社会行为者侵犯隐私权的申诉，特别是在他的任务变得更加广为人知的情况下。通过与申诉人和有关政府当局的沟通，对这些申诉采取后续行动。这类后续沟通是按照特别程序任务负责人使用的方法进行的，目的是澄清所提出的指控，确认事实，并在必要时提出纠正行动建议。沟通还可酌情包括举行在线或面对面会议。如果所收到的证据表明需要予以特别或紧急注意，而且正常沟通形式不能奏效时，特别报告员可考虑公开表示关切。

D. 联合行动

16. 特别报告员经常收到与其他特别报告员采取联合行动的请求，有时也会采取这类行动。关于这些联合行动的详细情况，将在特别程序的来文报告中另外公布。

17. 截至 2016 年 3 月 5 日，尚无时间收集上述任何类别的足够证据，因此除参加两项联合行动外，没有开展更多工作。但预计将合并每一类别收集的资料，为特别报告员通过来文、国别访问和其他合作手段与有关国家开展对话和合作提供必要的证据基础。

E. 建立桥梁和制订参与政策

18. 特别报告员利用其任务授权，继续进行并扩大以前开展的与利益攸关方和在利益攸关方之间建立桥梁的工作。通过这项工作，形成了与各种利益攸关方互动的现行政策，其中包括：与政府官员和部长在其各自的首都或者在国际论坛召开的双边会议上接触；与一些数据保护和隐私问题专员、特别是欧洲联盟第 29 条工作组主席和欧洲委员会《个人数据自动处理中保护个人公约》协商委员会理事会主席举行会议；与国际电信联盟(国际电联)及电机和电子工程师学会等技术标准机构开展讨论；与民间社会行为者个人或集体进行深入会谈；以及与来自日内瓦常驻代表团的人权专家或其他官员举行会议。这里所列举的例子仅具说明性，并不是全部。几乎每天都会收到关于发表主旨演讲、参加专题小组讨论和会

议以及与民间社会成员进行会晤的邀请。虽然接受了许多此类邀请，特别是与上述七个专题研究直接相关的邀请，但也不得不拒绝其他一些邀请，尤其是在因时间和/或预算限制无法参与的情况下。除许多其他成果外，通过这种参与政策，数据保护和隐私专员国际会议还通过了一项与数据保护和隐私机构正式合作的决议。[b]

三. 2016 年初的隐私状况

A. 定义和理解

19. 虽然隐私的概念存在于所有社会和文化中——并且在整个人类历史上都是如此——但这一概念缺乏有约束力和被普遍接受的定义。[c] 为了更好地理解隐私，需要从两个不同的角度来考虑。首先，应考虑这一权利的积极核心。第二，问题是如何以否定性定义的形式，界定这一权利的范围。但这两个任务尚未完成。

20. 如人权理事会第 28/16 号决议所重申的，《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条构成了国际人权法中隐私权的基础。与其他一些国际和国家法律文书，包括宪法和相关立法一起，这意味着全世界有一个相当可观的法律框架，可用于保护和促进隐私。然而，由于缺乏得到普遍认可和接受的隐私定义，这一法律框架的有用性被严重削弱。即使 193 个国家签署了保护隐私的原则，除非它们对同意保护的内容有清楚的理解，否则也没有太大意义。

21. 缺乏得到普遍认可和接受的隐私定义并不是特别报告员面临的唯一重大挑战。即便所有相关法律文书的起草者都纳入一个普遍认可的隐私定义，仍然需要考虑时间、地点、经济和技术方面。由于时间的流逝和技术的影响，再加上不同地区经济发展和技术利用程度的不同，意味着 50 年前(《公民权利和政治权利国际公约》通过时)、甚至 35 年前(例如，《个人数据自动化处理中保护个人公约》)——更不用说 70 年前(《世界人权宣言》)——制定的法律原则可能需要重新审查、进一步制定和可能的话加以补充，使之更符合当今的现实。

[b] 数据保护和隐私专员国际会议通过，2015 年 10 月 27 日，阿姆斯特丹。见 https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf。

[c] 要更详细地了解特别报告员对千年来隐私的存在和时间、地点和空间等方面的评估，见 Joseph A. Cannataci, ed., *The Individual and Privacy. Volume I* (Oxford, Ashgate, 2015)。

22. 由于缺乏普遍认可的隐私定义，并出于对时间、地点、经济和技术的考虑，显然需要确定全球不同地方不同的人在不同情况下对隐私的理解。因此，这种努力初步看来不仅是一项非常重要的任务，也是特别报告员的一个优先事项。

23. 在一些文化中，对隐私权的辩论包括关于堕胎的辩论。在不讨论这种做法利弊的情况下，并为了避免任何疑问，应当指出的是，特别报告员在其任务的这个初步阶段，将把重点放在信息隐私上。这种办法侧重于隐私在决定社会中信息流动方面的功能和作用，以及由此对个性发展产生的影响。另外还将包括相关问题，例如社会中权力和财富的分配。不过，这样做的话，可以清楚地看到，影响社会中信息流动的不仅有隐私权，还有其他权利，例如言论自由和获取公共信息的自由。所有这些权利都很重要，对一项权利的承诺不应减损另一项权利的重要性和保护。在可能的情况下综合考虑各种权利比将其对立起来更为有效。因此，正确地说，谈论“隐私对安全”而不是“隐私和安全”是无所助益的，因为二者都需要。这两项权利均可被视为促进性的权利，而其本身并不是目的。安全对于总的生命权而言是一项促进性的权利，隐私也可被视为社会整个复杂的信息流动网中的一项促进性权利，它们对于自主权以及个人在贯穿一生的人格发展中以知情的方式对各种方案进行识别和选择的能力具有根本的重要性。

24. 在进行关于隐私是什么和应该是什么的辩论时，特别报告员希望重点关注根本问题，避免可视为的或者实际的地方或文化差异将辩论引入歧途，这些差异处于隐私的边缘，而非最终可能获得全球共识的隐私价值观的强大核心。为帮助系统的新辩论把重点放在根本问题上，特别报告员打算不顾有些人的质疑，将隐私视为一种促进性的权利，而不是目的。世界上有些国家已经确定了尊严和个性不受阻碍地自由发展这一首要的基本权利。在地理上相隔如巴西和德国那么远的国家均将这一权利写入了宪法，特别报告员认为：(a) 这种尊严和个性不受阻碍地自由发展的权利应被视为具有普遍适用性；(b) 已被承认的权利，例如隐私权、言论自由权和获得信息的自由权，是三种促进性的权利，最好结合它们在促进人类自由发展个性方面的作用加以考虑。将隐私、尤其是“为什么要有隐私？”的问题置于就尊严和个性不受阻碍地自由发展的基本权利所进行的广泛辩论的背景之下，反映了数字时代的生活现实。这种方法应帮助辩论的所有参与者，不论来自哪个国家或哪种文化，侧重于个性发展的基本方面，以及人们希望隐私权有助于保护什么样的生活，而不是花太多时间讨论他们需在特定文化中重点关注或维护/促进的隐私相关传统。

25. 将会看到的是，在许多情况下，无法将隐私辩论与关于自主或自决权价值的辩论有意义地分开。后一用语已得到详细讨论，就隐私和个人权利而言，它自 1983 年以来在德国形成了一项“信息自决”的宪法权利。这一概念的吸引力和有效性需在 2016 年关于如何更好地理解隐私权的全球讨论、以及可能的话在就保护和促进尊严和个性不受阻碍地自由发展的基本权利所开展的讨论范围内作进一步的评估。

26. 上述三项促进性的权利——隐私、言论自由和获取信息的自由——与尊严和个性不受阻碍地自由发展的权利一样，在数字技术出现之前就存在了。但数字技术对这些权利产生了巨大影响，包括离线(例如，通过信用卡、射频识别和其他电子系统)和在线技术，今天，网民产生的有关其自身的数据集比二十年前他们开始上网之前要多出几万个。移动设备和融合技术——例如融电话、互联网和摄影于一体的移动智能手机——创造了一种新的生活方式，在方便性和隐私方面带来了新的舒适和期望。

27. 新技术的影响还意味着可能需要在尊严和个性不受阻碍地自由发展范围内，重新审视个人和集体隐私之间的区别，以及对公共和私人空间隐私的期望。

B. 2015 年和 2016 年的初步意见

28. 自特别报告员就任以来，选出最重要的隐私事件是一项艰巨的任务，特别是因为没有必要的资源对这些事件进行严格的调查。此外，特别报告员不希望侵害民间社会行为者如隐私国际及其附属机构所发挥的重要作用，它们在 20 年的大部分时间里举办“老大哥奖”活动，[d] 使人们了解到隐私方面的良好和不良作为。另一方面，特别报告员要赞扬可以促进和加强隐私保护的良好做法、法律、法院裁决或想法。因此，特别报告员谨请人权理事会注意以下重要动态，但他并不想说这是一份详尽无遗的清单，也没有按照任何特别的顺序。

1. 明智的克制——荷兰和美利坚合众国对后门通信说不

29. 应当赞扬荷兰和美利坚合众国政府在不允许利用法律来设计后门通信方面所表现出的克制。2016 年 1 月 4 日，荷兰政府宣布正式反对在加密产品中植入后门。在安全和司法部发布并由安全和商务部长签署的一份政府立场文件中，[e] 政府称目前不宜对荷兰加密机制的开发、提供和使用采取限制性法律措施。这个结论是在长达五页的文件结尾提出的，其中既有赞成实现更大加密的论点，也有允许当局访问信息的反论点。通过在加密产品中引入一种技术，使当局得以访问，加密文件也会更容易地被犯罪分子、恐怖分子和外国情报机构访问。这可能会对所传播和存储信息的安全性以及对于社会运作日益重要的信息和通信技术系统的完整性产生不良后果。

[d] www.bigbrotherawards.org。

[e] 见 www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id= 2016Z00009&did=2016D00015 (2016 年 8 月 23 日检索)。

30. 荷兰政府的立场似乎比美国政府的立场更为明确，尽管后者早三个月提出。2015 年 10 月初，联邦调查局局长詹姆斯·科米在国会证词中说，行政当局现在不会要求立法，迫使公司解密客户数据。最近诉苹果公司案中一个变得明显的令人更为担忧的问题是，美国政府将继续努力说服已加密客户数据的公司创造一种方式，使政府仍可在为调查犯罪或恐怖主义所需时，访问个人数据。特别报告员对这一案件的立场很大程度上已在联合国人权事务高级专员 2016 年 3 月 4 日发表的声明中得到独立阐述。[f] 美国国防部长阿什顿·卡特最近的评论令人鼓舞，他称强加密对国家安全至关重要。2016 年 3 月 2 日，他在向由技术行业专家组成的听众发言时表示，他不信任让外人阅读编码文件的后门或加密程序。这与他 2015 年 10 月的发言[g] 相一致，是一个应当鼓励和加强的立场。

2. 在司法上结束大规模监控的开始——实质性问题

31. 2015 年 10 月 6 日，欧洲联盟法院就 Maximillian Schrems 诉数据保护专员案作出判决。法院宣布欧盟委员会建立所谓“安全港”框架并以第 95/46/EC 号指令为基础的决定无效。特别报告员想要强调以下内容，这一内容从确认(和创建)先例的角度来看，可能是该项判决最重要的部分之一：

> 94. 特别是，允许公共当局通常能够访问电子通信内容的立法，应被视为损害了《宪章》第 7 条保障的私生活得到尊重的基本权利的本质……

32. 今后无疑会就“通常能够访问”的确切含义展开一些辩论，在这里，法院显然是指通信的内容而不是元数据，但引人关注的是，如果法院倾向于继续严格适用这一标准，则将大规模监控合法化的哪部欧洲法律会符合该标准。不过，如将 Schrems 案的判决与以下所述 Zakharov 案的判决一并阅读，至少可以部分消除这种模糊性，后一判决构成了欧洲联盟的法律，也构成了欧洲委员会其他成员国的法律。

3. 制定补救办法的重要性——执行和程序问题

33. 特别报告员再次参照 Schrems 案，欣见欧盟法院已成为诸如申请人等人民的论坛，申请人提起这一案件，是因为他作为一个个人，担心现代信息技术的发展对他作为一个民主社会中的人的尊严所产生的影响。个人有机会向一个超国家的公共机构就其案件进行辩护，维护其权利，并质疑现有权力关系，这对创造知识以增强我们社会的福利非常重要，并与国际人权法的发展相一致。这种机制的存在对于保护人权和恢复对各国或其他行为者使用技术的信任至关重要。

---

[f] 见 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E。

[g] 见 http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu。

34. 这也是社会新发展的前兆，表明权利在任何地方都需要得到尊重和执行，而不仅仅是在服务器所在地。

35. 法院的判决还表明了区域政策办法的附加值，这些办法今后可能有助于促进自下而上的、具有更广泛全球影响力的参与性法律文书。

4. 秘密监控措施的存在本身就是对私生活得到尊重的权利的侵犯

36. 欧洲人权法院大法庭在 2015 年 12 月 4 日对 Roman Zakharov 诉俄罗斯案的判决[h] 中一致认为，俄罗斯秘密拦截移动电话通信的系统违反了《保护人权与基本自由公约》(《欧洲人权公约》)第 8 条。此外，非常值得关注的是，法院认为，如果满足某些条件，申诉人可以仅因秘密监控措施的存在而声称是违反第 8 条行为的受害者。也许最重要的是，法院以甚至比 Schrems 案中更加明确的方式宣布，大规模监控系统是非法的：

> 270. 法院认为，秘密监控系统在俄罗斯的运作方式赋予了安全部门和警察规避授权程序和在事先未经司法授权的情况下截取任何通信的技术手段。虽然任何系统都不可能完全排除一个不诚实、粗心大意或过于热情的官员的不当行为(见上文所述的 Klass 等人案，第 59 段)，但法院认为，一个使保密部门和警察能够直接截取每个公民的通信而不要求他们向通信服务提供商或任何其他人出示截取授权令的系统，就像俄罗斯的这个系统一样，特别容易被滥用。因此，似乎特别需要制定防止任意和滥用的保障措施。

37. 这项裁决建立了一个非常重要的基准，强调需要有合理的怀疑并事先获得司法授权，以及“一个使保密部门和警察能够直接截取每个公民的通信而不要求他们出示截取授权令的系统”的不可接受性。这将成为对任何欧洲国家所有现行和新提议的监控立法加以衡量的标准。特别报告员还严重关切地注意到关于俄罗斯杜马(议会)的一项决定的若干报告，该决定会使欧洲人权法院的裁决被推翻。[i] 如果这些报告是真的，那么实际上可能会取消已批准《欧洲人权公约》的国家的公民可以利用一种非常重要的补救办法，包括私生活获得尊重的权利受到侵犯情况下的补救措施。特别报告员请俄罗斯联邦政府协助他进一步核实这些报告，更深入地审查有关法律的细微之处，如果报告基本属实，则说服杜马废除 2015 年 12 月 4 日的法律，恢复俄罗斯公民根据《欧洲人权公约》可以获得的补救的效力，包括其隐私权受到侵犯的情况下国家应采取的补救措施。

[h] *Roman Zakharov* 诉俄罗斯[GC]，2015 年 12 月 4 日，第 47143/06 号，《判决和裁决汇编》。

[i] 见 www.bbc.com/news/world-europe-35007059。

5. 大不列颠及北爱尔兰联合王国的调查权力法案

38. 应当感谢联合王国的三个议会委员会——科学和技术委员会(2016 年 2 月 1 日)、议会情报和安全委员会(2016 年 2 月 9 日)、以及最重要的是调查权力法案草案联合委员会(2016 年 2 月 11 日)——对目前正由议会审议的调查权力法案草案一贯和有力(尽管有时过于礼貌)的批评。调查权力法案草案联合委员会在其报告中提出了 86 项关于修改该法案的建议，重点是各种权力的明确性、司法监督和合理性等问题。还应感谢联合王国政府，它听取了各方的意见，正在利用该法案加强急需加强的监督机制。虽然在这方面可能还有改进的余地，但所采取的步骤是正确的。不过，在提交本报告时，特别报告员对于最近对该法案 2016 年 3 月 1 日公布的最新版本所作的一些修订有何价值感到严重关切。在编写本报告时，政府的一些建议不仅似乎与反恐中注意促进与保护人权和基本自由问题特别报告员 2014 年报告的逻辑和结论相悖(该报告除其他外涉及大规模监控)，[j] 而且明显不符合欧洲联盟法院在 Schrems 案和欧洲人权法院在 Zakharov 案中所确定的基准。特别报告员强烈鼓励上述三个委员会以新的活力和决心，继续发挥其影响，以便将该法案中设想的大规模监控和大规模黑客攻击等不相称和侵犯隐私的措施宣布为非法，而不是将其合法化。将大规模截取和大规模黑客攻击合法化的严重和可能意外的后果似乎没有得到政府的充分肯定。鉴于联合王国的立法在依然是英联邦一部分的超过四分之一联合国会员国中仍有巨大影响，并且联合王国作为主要区域人权机构如欧洲委员会创建者之一的民主国家，有着令人骄傲的传统，特别报告员鼓励该国政府利用这个黄金机会树立良好榜样，避免采取其负面影响可能远远超出联合王国海岸的不相称措施。具体来说，特别报告员请该国政府更加致力于保护本国公民和其他公民的基本隐私权，并且不再为其他国家树立坏榜样，继续提出显然不符合联合王国一些议会委员会的标准，并且违背欧盟法院和欧洲人权法院最近的判决、损害隐私权精神的措施，特别是大规模拦截和大规模黑客攻击。最后，特别报告员请联合王国政府与他密切合作，尤其是在他所进行的监控专题研究方面，以努力确定相称措施，在不过度侵犯隐私的情况下加强安全。

6. 迈向网络和平的第一小步？

39. 应当感谢中国和美国在开始缓解网络空间紧张局势方面发挥的领导作用。

40. 网络和平可能有三个主要方面，它们均受到网络间谍的威胁：

(a) 破坏和战争；

(b) 知识产权和经济间谍；

(c) 民权和监控。

[j] A/69/397。

41. 隐私主要涉及第三个方面，但也经常出现在关于其他两个方面的讨论中。2015 年 9 月，美国和中国宣布“同意两国政府均不得支持或从事网络盗窃知识产权活动”，“两国致力于找到国际社会网络空间适当的国家行为规范。双方同意设立一个高级专家组来进一步讨论网络事务”。[k] 美国和中国不仅在这一重要步骤之后于 2015 年 12 月举行了网络会谈，似乎也为其他国家树立了榜样：“继美国宣布之后，联合王国与中国签署了类似协议，并有一份报告称，柏林将在 2016 年与北京签署‘无网络盗窃’协议。2015 年 11 月，中国、巴西、俄罗斯、美国和 20 国集团其他成员国接受了禁止实施或支持网络盗取知识产权的规范。”[l] 虽然这与达成关于网络战争或网上监控以及间谍活动对公民隐私影响的完整协议还有点距离，但它至少是一个开始，特别报告员也可以试图说服有关各方扩大讨论，将尊重在线隐私的具体措施也包括在内。

四. 特别报告员的重点活动

A. 特别报告员任务的资源情况

42. 由于此任务是一项新任务，任务的正式预算到 2016 年 1 月才核准，而且 2015 年 8 月 1 日──即欧洲大部分都在放假时──才开始这项任务，特别报告员在获得联合国人权事务高级专员办事处的任何形式支持方面花了几个星期的时间。目前，在征聘工作人员之前提供的这种行政支持是暂时性的，而征聘工作预计将在 2016 年 6 月前完成。在评估资源情况时，特别报告员立即采取了步骤，从联合国以外获取资金。聘用了一名博士后研究员(拥有隐私和被遗忘的权利博士学位)，自 2015 年 10 月开始兼职工作，并自 2016 年 1 月起全时任用，以提供关于实质性问题的帮助。外部资金将持续到人力资源情况得到解决时为止。特别报告员正在工作的机构，即马耳他大学媒体和知识科学学院信息政策和治理系，以及荷兰格罗宁根大学法学院安全、技术和电子隐私研究小组的专家和其他工作人员也非常友好地提供了自愿援助。特别报告员非常感谢这一援助与联合国日内瓦工作人员的援助，这些援助使特别报告员得以履行职责，直到能力得到适当增强，并建立符合目的的更具可持续性的支助结构。

[k] 见 www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html。

[l] 见 http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement。

B. 特别报告员任务的路线图——制订十点计划

43. 除了第二节概述的日常活动外，还投入了大量时间制订下文第五节所述的10点计划，以及与许多利益攸关方进行协商。

C. 参与多项活动

44. 特别报告员接受了参加会议、大会和专家组及个人协商的邀请，特别是那些有助于维持关于上述七项专题研究的现行互动政策的活动。以下是这类活动并非详尽无遗的清单：

(a) 关于“密不可分的联系：互联网治理中的言论自由和隐私”的小组讨论会，MAPPING项目，第一次大会，德国汉诺威，2015年9月22日；

(b) 与人权观察全球事务主任会晤，2015年9月30日；

(c) 参加2015年10月13日至14日在日内瓦举行的数据保护和统计隐私研讨会，并作了发言；

(d) 2015年10月14日与国际电联副秘书长在日内瓦举行会晤；

(e) 在2015年10月16日于布加勒斯特举行的2015年知识社会中的情报问题会议上，组织并领导了隐私与监控专题小组；

(f) 在2015年10月27日于阿姆斯特丹举行的数据保护和隐私专员国际会议非公开会议上，发表了关于数字时代隐私的主旨演讲；

(g) 参加2015年10月29日在阿姆斯特丹举行的数据保护和隐私专员国际会议上的“环游世界”圆桌讨论；

(h) 参加2015年11月9日至13日在巴西若昂佩索阿举行的互联网治理论坛期间的多个公开和双边会议；[m]

(i) 在2015年11月16日至17日于巴西里约热内卢举行的全球南方大数据国际讲习班非公开会议上发表主旨演讲；[n]

(j) 2015年11月18日在巴西利亚与巴西司法部官员举行会议，对巴西新的隐私法草案进行深入分析；

(k) 2015年11月18日在巴西利亚与巴西电信、司法和内政部官员就巴西新的隐私法草案举行联席会议；

(l) 2015年11月18日在巴西利亚检察长办公室举行会议；

[m] 见 www.intgovforum.org/cms/igf-2015-schedule。

[n] 见 http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global。

(m) 2015 年 11 月 19 日在巴西利亚与巴西外交部人权事务主任举行会议；

(n) 2015 年 11 月 19 日在巴西利亚举行的消费者国际世界大会上发表演讲(通过视频连接)；[o]

(o) 2015 年 11 月 25 日在马耳他与患者隐私权组织的创始人兼负责人举行了深入会谈和协商；

(p) 2015 年 12 月 8 日在欧洲议会公民自由、司法和内务委员会与科学技术方案评估小组联合举行的“通过加强信息技术安全和欧盟信息技术自主权保护在线隐私高级别会议”概况发言会议上发表演讲；[p]

(q) 在 2015 年 12 月 9 日于罗马举行的一次关于“安全港 2.0”背景下的安全与隐私会议上发表主旨演讲；[q]

(r) 在 2015 年 12 月 11 日于荷兰乌得勒支举行的隐私与身份实验室年度大会上发表关于隐私、身份、安全和自由的主旨演讲；[r]

(s) 参加 2015 年 12 月 14 日至 16 日在日内瓦举行的特别报告员入职介绍会；

(t) 2015 年 12 月 17 日在日内瓦与联合王国代表团会晤；

(u) 2015 年 12 月 17 日在日内瓦与中国代表团会晤；

(v) 2015 年 12 月 17 日与俄罗斯联邦代表团会晤；

(w) 通过视频连接参加 2015 年 12 月 17 日在纽约举行的反恐怖主义委员会关于防止恐怖分子利用互联网和社交媒体招募恐怖分子和煽动恐怖主义行为，同时尊重人权和基本自由的特别会议；

(x) 在 2015 年 12 月 18 日于日内瓦举行的有隐私国际、大赦国际、无国界记者组织、互联网学会、人权观察和美国公民自由联盟等代表参加的非政府组织圆桌会议上发言并主持讨论；

(y) 2015 年 12 月 18 日在日内瓦与国际电联电信标准化局副局长会晤(并有国际电联法律股参加)；

(z) 通过视频连接参加 2016 年 1 月 18 日在新加坡举行的国际电联智能城市会议，并作关于“隐私、生活质量和智能城市：加大监督”的发言；

[o] 见 http://congressprogramme.consumersinternational.org/speakers.html。

[p] 见 www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy。

[q] 见 www.dimt.it/tag/cannataci。

[r] 见 www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published。

(aa) 2016 年 2 月 3 日在马耳他与联合王国基因观察组织的 Helen Wallace 和 Andrew Jackson 会晤；

(bb) 在 2016 年 2 月 5 日于日内瓦举行的国际组织数据保护问题第五次讲习班上发表主旨演讲(通过视频连接)；[s]

(cc) 参加 2016 年 3 月 3 日在荷兰海牙举行的荷兰外交部利益攸关方大会并发表主旨演讲。

五. 十点行动计划

45. 为进一步详细阐述隐私权的各个方面及其与其他人权的关系，特别报告员制定了一个 10 点行动计划大纲。应该铭记的是，计划中提到的要点并没有按照特别的顺序，也不是一个具体确定了轻重缓急的工作方案。特别报告员认为他所起的是类似于探路者的作用。换言之，目的是寻求前进的方向，同时确定需要解决的紧急问题，或者响应必须就责任问题开展紧急工作的个人或国家需要。下面的 10 点行动计划是一个待做事项列表，而不是一个单纯的愿望清单。特别报告员已经开始就这 10 点中的每一个要点开展工作，但进展将取决于是否有时间和资源。

1. “隐私权”的含义

46. 超越现有法律框架而更深入地了解承诺保护的内容，需要努力提出一个更好、更详细和得到更普遍理解的“隐私权”含义。隐私权在二十一世纪指的是什么，应当指什么？如何在数字时代更好地保护隐私权？将组织活动并支持研究，以探讨对这些关键问题的可能答案，这将有助于为特别报告员行动计划的其他部分提供重要基础。

2. 提高认识

47. 另一个重要问题是提高公民的认识，以帮助他们了解什么是隐私。应当就他们的隐私权是什么，以及他们的隐私可能受到的侵犯，特别是由于新技术及其在网络空间中的行为而受到的侵犯开展一般性讨论。他们需要了解其个人数据是如何货币化的，在保护他们的隐私权方面有哪些现行保护措施和补救办法。他们可以如何减少隐私权受侵犯的风险，以及如何与立法者和企业部门互动以改善对隐私的保护？提高认识是一项重大任务，特别报告员打算在整个任职期间，通过与所有利益攸关方特别是民间社会的持续接触，为这项任务作出贡献。

[s] 见 www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations。

3. 建立关于隐私的系统、持续的对话

48. 在不同利益攸关方之间建立更加系统、开放、全面、有效、特别是永久的对话至关重要。为了保护隐私，需要建立桥梁。特别报告员打算高度重视这项活动，利用现有的论坛并创建新论坛。在这方面，促进非政府组织、数据保护和隐私专员、执法机构及安全和情报部门之间的系统对话十分重要。必须与所有类别的利益攸关方合作，以改进内部程序，通过将保护措施纳入所采用技术和所遵循程序的设计工作，加强隐私。应实现最大限度的透明和问责，并加强公正和有效的监督，大幅提高其有效性和可信度。

4. 对法律、程序及业务保障和补救采取全面的办法

49. 适当的保障和有效的补救自有数据保护法以来，一直是其存在的部分理由。这种法律的目的是在一个由于不断的技术变革而变得更加复杂的世界中提供适当的指导和保护。为防止侵犯隐私，应为公民提供更明确、更有效的保护。应在实际发生侵权的情况下，为所有有关方面提供真正的补救办法。寻求保障和补救的工作是横向的，是上文第二节所述特别报告员各项专题研究的基础。

5. 重新强调技术保障

50. 向公民提供的保障和补救绝不能单单是法律或业务上的。仅有法律是不够的。特别报告员将继续与技术界接触，努力促进开发有效的技术保障，包括加密、重叠软件和各种其他技术解决方案，使设计的隐私真正付诸实施。

6. 与企业界的重点突出的对话

51. 今天，越来越多的公司已经收集了比大多数政府所能够或将会收集的更多的个人数据。对于个人数据严重货币化的当前商业模式，社会应当期望什么样的替代模式或重要修改？在国家当局要求提供私人公司持有的数据情况下，有哪些适用的保障措施？任务的这一方面需要花费很多时间和精力。特别报告员已开始与企业界代表直接联系，并将与一系列行业参与者保持与这些问题有关的、以隐私为重点的对话，以期了解企业部门的新发展并向它们提供关于特别报告员任务其他部分的信息。

7. 促进隐私保护机制方面的国家和区域发展

52. 应在全球一级更好地认识隐私保护机制方面国家和区域发展的重要性。特别报告员在与全世界数据保护和隐私专员密切合作时，可发挥重要补充作用。通过相互合作和对话，可以显著提高全球隐私保护标准。特别报告员已开始与数据保护当局计划和执行一系列全球活动。其中包括计划 2016 年在澳大利亚、摩洛哥、新西兰、突尼斯和北爱尔兰举办活动，今后几年还将开展许多其他活动。

8. 利用民间社会的能力和影响

53. 特别报告员在上任的前六个月，已经会见了 40 个非政府组织的代表，并打算继续投入相当多的时间听取民间社会代表的建议，并与他们进行合作，这些代表正在作出很大努力，以更好地保护全世界的隐私。

9. 网络空间、网络隐私、网络间谍、网络战和网络和平

54. 全球社会需要对网络空间中实际发生的事情，包括大规模监控、网络间谍和网络战争持好奇、坦率和开放心态。处理这些现实问题时，应以上述其他行动点的结果以及上文第二节所述专题研究的结果为基础。特别报告员预计这些问题将不断成为其报告和许多国别访问的内容，他希望通过就这些问题与利益攸关方开展透明合作，在改善数字时代的隐私保护方面发挥建设性作用。

10. 在国际法方面加大投资

55. 虽然仅有法律是不够的，但法律非常重要。应当探索发展有关隐私的国际法的一切可能性；特别报告员愿意审查任何法律文书的价值，不论其属于软法还是硬法。通过扩大对隐私权含义的理解来更新法律文书，像这样的优先问题似乎是一个重要的起点。一些利益攸关方似乎一致认为，其中一项法律文书可采取《公民权利和政治权利国际公约》第十七条附加议定书的形式，[t] 特别报告员被敦促“在其第一个任期内促进开始有关这一议定书的谈判”。[u] 不过，确切的时间安排可能取决于根据上文第 1 点──即实现对隐私核心价值观更好、更普遍的理解──所开展的深入和广泛讨论的持续时间和结果。除非有明确的国际协议，否则其他一些与隐私有关的事项，特别是网络空间的管辖权和属地问题，将无法得到令人满意的解决；这种协议通常采取多边条约的形式，很可能涉及一个具体专题或一组问题。为免生疑问，应当指出的是，所设想的并不是一个新的、全球性和包罗万象的国际公约，涵盖与隐私或互联网治理有关的所有问题。期望通过国际法的逐渐发展，澄清并最终扩大现有的法律文书，从而加强对隐私的保护，要现实得多。从中长期来看，这可能包括拟订全新的法律文书。特别报告员还将监测关于互联网治理领域的国际法和新法律文书的持续讨论，以确定联合国机构内的行动时机，以及特别报告员最终可能希望向人权理事会和大会建议的法律文书的类型和范围。

[t] 见 https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf。

[u] 同上。

六. 结论

56. 社会大多数阶层和多数类别的利益攸关方所给予的极其热烈和热情的欢迎使特别报告员深受感动。

57. 隐私在以前从未像 2016 年这样引起这么多政治、司法或个人关注。

58. 安全、公司商业模式和隐私之间的紧张关系继续占有核心位置，但过去 12 个月出现了相互矛盾的指标：一些政府继续在实践和/或议会中对隐私采取敌对态度，而世界各地的法院，尤其是美国和欧洲的法院则明显倾向于保护隐私权，特别反对不相称的、侵犯隐私的措施，如大规模监控或破解加密信息。

59. 一些有力的指标显示，隐私已成为一些大公司重要的商业考虑因素，将其作为一个卖点。如果有隐私市场，市场力量将会为其创造条件。加密设备和软件服务供应的快速增加有力地表明，全世界的消费者越来越意识到他们的隐私所面临的风险，并将越来越多地选择有利于保护隐私的产品和服务，而不是对隐私保持中立或不利于保护隐私的产品和服务。

60. 虽然一些政府继续抱有将不相称、不合理的侵犯隐私措施(如大规模收集数据、大规模黑客攻击和无授权拦截)合法化或坚持这些措施的不合理、不明智、判断错误、不合时宜和有时无礼的企图，以荷兰和美国为首的其他政府则更加公开地采取了加密无后门政策。特别报告员鼓励更多政府联合起来支持这一立场。

61. 世界各国不仅清醒地认识到自己的责任和诸如加密等技术保障，还慢慢地但明确地认识到，如果它们通过网络战争和网络间谍活动破坏网络空间，则会收益有限，而风险极大。在这方面尚待取得进展，但 2015 年已经有了一些重要的开端。因此，特别报告员鼓励各国政府──而不只是 20 国集团的政府──就适当的国家行为和相关的网络空间治理措施展开讨论；其中除其他外应涉及公民权利，特别是隐私权、言论自由和监控。

62. 特别报告员的工作方法和 10 点计划应当对在数字时代保护和促进隐私问题采取的整体做法有所启示。整体做法有助于确定所需开展工作的总体情况，但由谁在何时做什么工作的时间安排取决于两个主要因素：一是可用于实施行动计划和完成专题研究的资源；二是各利益攸关方愿意接受和促进一个有利于隐私的议程，而不是坚持“指挥和控制心态”。对那些乍看之下以为行动计划不仅雄心勃勃，而且可能过于雄心勃勃的人而言，特别报告员想要表达的信息清楚而简单：如果你同意计划的目标及其将若干复杂但相互关联的问题综合起来的做法，就行动起来，为计划的实施提供额外资源，这将有助于使计划变得更加可行。特别报告员正在利用他作为项目经理的经验──他曾成功筹集数千万美元用于隐私相关研究──来制定一项增加任务负责人可用资源的战略；实际上，这 10 点计划将取决于该战略的成功与否。即便这项战略完全成功，特别报告员也完全相信，10

点计划的各部分将由下一任务负责人继续实施和(可能的话)予以完成。本阶段的挑战是提供清晰、全面的愿景和坚实的基础，作为在保护隐私领域作出可靠和循证决策的依据。

Annex I

Challenges faced by the Special Rapporteur and his vision for the mandate

1. The Special Rapporteur immediately set about building up his team composed of persons working for the mandate on a part-time or full-time basis. One of these persons is currently a full-time United Nations (UN) Human rights officer, hired on a temporary contract, while the position is under recruitment. The work of this person is supervised by a more senior UN employee who is also responsible for supporting the work of six other mandate holders. A second part time professional and a part time administrative officer will soon be recruited, as well as a part-time consultant. The SRP is grateful that the Human Rights Council endowed his mandate with this still limited (given the scope of his mandate) but unprecedented level of support to a mandate holder. The other persons in the SRP team are not employed by the UN but are resourced by extra-mural funding obtained by the SRP or may be volunteers. The team is often physically spread across at least three geographical locations (currently Malta, the Netherlands and Switzerland) and, as befits the digital age, most of the team meetings are carried out in cyber-space with the working day being opened by an on-line conference call involving all team-members who may be available. During the "morning meeting" team members typically report on work carried out in the previous day, consult about tasks planned for the rest of the working day and plan tasks and events for the following weeks and months. When doing so, their tasks reflect the fact that the work of the SRP may be broadly divided into four categories and any team member may be working concurrently on tasks from each of these categories.

2. The fact that the mandate on privacy is a new one presents both advantages and disadvantages. Amongst other things it means that the Special Rapporteur on Privacy (SRP) had no roadmap to follow and indeed one of his first priorities in this case is to work on designing and developing such a roadmap. This means that some of the issues identified in this and later reports are not necessarily capable of being resolved within the time-constraints imposed by one or even two three-year mandates. They are mentioned however in order to provide a more holistic picture of what needs to be done in the short, mid and long-term. In doing so, this incumbent is conscious of possibly identifying issues which may possibly be more appropriately tackled in a more timely manner by later holders of the mandate.

3. One of the recurring themes of this and later reports will undoubtedly be the time dimension. The rapid pace of technology and its effects on privacy means that action on some already-identified issues may increase or decrease in priority as time goes by while new issues may emerge fairly suddenly. It may also mean that sometimes it may be more opportune to launch or intensify action on a particular issue not necessarily because it is much more important than other issues but rather because the timing is right, because the different international audiences and classes of stakeholders may be far more sensitive and receptive to that particular issue for reasons and circumstances over which the Special Rapporteur may have absolutely no control but in which case it would be foolish not to take advantage of favourable opportunities which may result in the creation or improvement of privacy safeguards and remedies.

4. The later prioritisation of action will also depend on the extent of the resources made available to the Special Rapporteur and the extent to which he can succeed in attracting fresh resources to support the mandate on privacy. This resource issue is fundamentally important and will directly affect the extent of the impact the mandate on Privacy may have in practice in real life. It is clear that, however good in quality in some respects, the

quantity of resources provided to the mandate by the UN is woefully inadequate and even if the mandate's human and financial resources are increased tenfold, it would still be hard-pressed to achieve the minimum required to persuade the incumbent that the work of the mandate is really making a difference to the protection of privacy of ordinary citizens around the world. The experience of the first six months in office has persuaded the mandate-holder that not only must the SRP be omni-present 24/7 on the many privacy-related issues which arise literally every day in many countries around the world but that he must also act as rainmaker, somehow attracting funds and human resources in order to make the work of the mandate both possible and sustainable in the short, mid and long-term. The effort required by what is, in essence, a part-time, un-paid position which must, by definition, co-exist with a demanding day-job, should not be under-estimated. This effort can be encouraged by the positive response of all stakeholders not least that of the nation-states, members of the UN to whom this report is addressed. If these stakeholders do not support the mandate adequately, if they do not put their money where their mouth is, then this will only serve to increase the frustrations already inherent to any work being carried out within the UN's systems and bureaucracy.

5. The incumbent's vision of the mandate is therefore analogous to the process required to design, finance, project manage and complete the building of a house or other building suitable for human beings to live and/or work in safely. Firstly we need to understand the function of the building: is it a residence for an individual living alone or for one nuclear family, or for a large and extended family or indeed for several of such individuals and families? Should it include a working space and if so for what type of work: is this to be a farm-house, a baker's *casa bottega* or a black-smith's lodge or an urban block of multi-rise apartments? Form follows function so the function or functions must be clearly identified and understood in-depth. Secondly, form follows function so the design of the house — or the mandate's range of activities — must be completed on the basis of the function. Thirdly, the size of the building and its interior may be basic, cramped, spartan i.e. just barely enough to provide basic shelter and sanitation or else it may be more comfortable and spacious and functional or else it may be downright luxurious. Whether it is one or the other will depend on the resources and especially the finances which can be projected to be available to the builder — and these will influence the final design of the plan for the building — and the mandate. Fourthly, the time available to complete essential parts of the building will also influence the design of the plan. Fifth, it will need to be borne in mind that life gets in the way of the best-laid plans and the design may, from time to time, have to be more of an emergent design process rather than the fulfilment of a rigid, prescriptive pre-ordinate design. This analogy is useful to explaining the scope of this report especially to emphasize that while the building itself may not necessarily be capable of completion within the time-frame of one or even two three-year mandates, it is very important to decide on what the final building needs to be like, otherwise we would be unable to design the type of the foundations we require to build...and unless the foundations are sound and fit-for-purpose the building will ultimately prove to be unsustainable and collapse

Annex II

A more in-depth look at open data and big data

1. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality.

2. At first sight Open Data sounds fine as a concept, a noble and altruistic approach to dealing with data as a common good, if not quite "common heritage of mankind". Who could object to data sets being used and re-used in order to benefit various parts of society and eventually hopefully all of humanity? It is what you can do with Open Data that is of concern, especially when you deploy the power of Big Data analytical methods on the data sets which may have been made publicly available thanks to Open Data policies. Of course, it is important to differentiate between data sets of one type and another. If what is put into the public domain consists of, say, the raw data arising out of tens of thousands of questionnaire responses about perceptions of privacy which responses would have been gleaned from across 27 EU member states and processed in an anonymised manner, the risk to individual privacy from aggregated data sets would appear to be very low if not non-existent. If, on the other hand, one uses Big Data analytical methods to develop links between supposedly anonymized medical data and publicly available electoral registers in a way that links identified or identifiable individuals to sensitive patient information then society has genuine cause for concern. Pioneers like Latanya Sweeney in the USA have demonstrated these abilities and exposed these risks on numerous occasions over the past two decades but the question remains: how should society intervene? More precisely how should policy-makers act in the face of such risks? Which is the correct information policy to develop and adopt? Especially since society has already intervened in a number of ways. Open Data is an information policy born out of specific information politics. For example, the EU legislated in favour of re-utilising public data more than 12 years ago (Directive 2003/98/EC), indeed five years after Prof Sweeney's first eye-opening discoveries.[v] Is this one of many cases where Open Data Policies were embraced before unintended consequences were properly understood and may now need to be remedied?

3. It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide. For the best part of forty years, our entire *forma mentis* has been founded upon something

[v] "In 2000, Sweeney analyzed data from the 1990 census and revealed that, surprisingly, 87 percent of the U.S. population could be identified by just a ZIP code, date of birth, and gender" according to Caroline Perry, SEAS Communications "You're not so anonymous" October 18, 2011 last accessed on 13 Jan 2016 at http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/ . However, in testimony to the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS") on 15 June 2005 Sweeney states that it was in 1997 that she "was able to show how the medical record of William Weld, the governor of Massachusetts of the time could be re-identified using only his date of birth, gender and ZIP. In fact, 87% of the population of the United States is uniquely identified by date of birth (e.g., month, day and year), gender, and their 5-digit ZIP codes. The point is that data that may look anonymous is not necessarily anonymous". http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf last accessed on 13 January 2016.

we call the purpose-specification principle. Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose. Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.

4. The purpose-specification principle is not something invented by Europeans. One of the first places where it is articulated as such is in a 1973 report by an Advisory Committee to the US Department of Health[w] where it was held that "There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent". This quickly became a fundamental value in many other fora. The OECD Guidelines of 1980 have the Purpose specification Principle as the third out of eight principles "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose". In this context it is also important to note the OECD's corollary fourth principle usually recognised as the Use Limitation Principle whereby "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3 above except a) with the consent of the data subject; or b) by the authority of law" These principles are also found in the Council of Europe's influential Data Protection Convention of 1981 and the EU's Data Protection Directive (46/95).

5. In an important regional development, the European Union is now at an advanced stage of devising and implementing the next generation of its data protection laws. When one examines the texts produced by the EU between 2012 and 2015, it is not as if the European Union appears ready to abandon the principle of purpose limitation. In the latest available version[x] of the draft text of the EU's General Data Protection Regulation (GDPR) the importance of the purpose specification principle does not appear to be in any way to be diminished. Article 5 b retains the principle prominently, stipulating that personal data shall be

> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

an approach reinforced by the next principle to be found in the GDPR's Article 5 which lays down that personal data shall be

> (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

[w] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41.

[x] s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf.

6. The meaning of these key principles had been similarly announced in the recitals of the GDPR

> (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

7. It is clear therefore that the current thinking in Europe on Data Protection still relies on the purpose specification principle taken in tandem with anonymization or deletion despite all the risks inherent in the use of Big Data Analytics and Open Data. Likewise, in the United States where on May 9, 2013, President Obama signed an executive order[y] that made open and machine-readable data the new default for government information",[z] some have attempted to downplay the concerns raised by Latanya Sweeney and have generally held that the risks of de-identification are not as great as previously made out.[aa] Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab[bb] and some of her more recent research[cc] persuade the SRP that we are running the risk of using outmoded safeguards, almost twenty years after our attention was drawn to the fact that stripping personal data of some basic identifiers may not be enough to protect privacy.

8. A careful examination of the pivotal thinking in Europe in 2015-2016 does not provide much reassurance especially if one carefully examines the pertinent part of the latest version[dd] available of the draft EU General Data Protection Regulation which holds that

> (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

[y] https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- last accessed on 13 Jan 2016.

[z] https://www.whitehouse.gov/open last accessed on 13 January 2016.

[aa] See for example Barth-Jones, Daniel C. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now" June 2012 last accessed on 13th January at https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf.

[bb] http://dataprivacylab.org/index.html.

[cc] Sweeney L, Matching Known Patients to Health Records in Washington State Data, 2012 last accessed on 13th January 2016 at http://dataprivacylab.org/projects/wa/1089-1.pdf.

[dd] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 last accessed on 13th January 2016.

9. This latest version from December 2015 after negotiation with the Council is less detailed than the one approved by the Parliament in October 2013 which held that

> (23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

10. Is the change an improvement, a factor which strengthens privacy protection in the era of Open Data or Big Data or is it a compromise which weakens protection? Whereas, it seems to the SRP that the very standard formulation of October 2013,[ee] dependant as it was on the costs and time required to identify an individual, is rapidly becoming archaic in the era of big data analytics, the rather vaguer 2015 version seems to be a bit more elastic, but that could be a double-edged sword. If we are to insist on maintaining information policies built around the principles of Open Data then we need to develop much stronger, complex algorithmic solutions and procedural safeguards. The application of the newest EU proposals pivot almost entirely on what constitutes anonymous data yet Latanya Sweeney[ff] and others have clearly demonstrated that there are huge limits to anonymization and it would seem that practically most personal data may actually be identifiable with such minimal effort that they would not meet eligibility criteria to qualify as anonymous data, thus bringing the GDPR into play.

11. Things get even more complicated when taking into consideration the factors legitimising research[gg]

> (88) For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

12. While the issue of sensitive data such as health information still presents a quandary within the EU's GDPR

> (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

[ee] "inofficial consolidated version" https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf last accessed on 13th January 2016.

[ff] http://latanyasweeney.org/publications.html.

[gg] Though this recital 88 has been expanded in the latest 17 Dec 2015 version.

13. How do Open Data and Big Data analytical capabilities fit into the scenarios and thinking portrayed above? Which would be the suitable safeguards to apply in Open Data policies which would protect privacy in the era of Big Data? Are the latest legal innovations being contemplated in Europe the right response to the evidence presented by Sweeney and do they represent best practice for the world to follow or dubious practice for the world to shun? The only thing that is certain is that if we are to get things right then it is clear that we need much more in-depth analysis of both the risks of Open Data as well as existing and new safeguards. Moreover, in this field too there appears to be a huge need for increasing public awareness. Relatively few people seem to know about the existence of open data policies or the consequences of applying big data analytics to different data sets put into the public domain by Open Data policies. In the course of participating in debates about Open data and Big data during tenure as SRP, one reinforced the impression that Open Data policies and their privacy and autonomy implications remain very much an area of interest to a tiny group of domain specialists and then again may be restricted further by the language in which they are made available to the public. The SRP is very sensitive to and is working with NGOs interested in protecting personal data in a number of sectors, including medical data and will, during 2016-2017 be engaging in events aimed at promoting discussion and on-going, in-depth investigation of related matters. The SRP is also very concerned that entire nations or trading blocs including major nations or regional federations such as China, the European Union and the United States have adopted or are adopting Open Data and Big Data policies the far-reaching consequences of which may not as yet be properly understood and which may unintentionally put in peril long-standing social values as well as the fundamental rights to privacy, dignity and free development of one's personality. Some studies on posthumous privacy suggest that in 2016 the citizens of some countries may be better off dead from a privacy point of view since their rights to privacy are better protected by law if they are dead than if they are alive in a world where Open data and big data analytics are a way of life endorsed by the information policies of the countries concerned. These developments may well be unintentional but the impact on privacy, autonomy, dignity and free development of personality may be far-reaching.

Annex III

Further reflections on the notion of privacy

A. Core values and cultural differences

1. As a result of the processes described in Section III of the report, an improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age.

2. This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to restrict privacy in a proportionate manner. The Special Rapporteur invites all actors in the field to contribute to the development of this urgently needed and improved understanding of the right to privacy and is convinced that significant progress is possible.

B. Enforcement

3. Apart from the absence of a clear universal understanding of privacy, the lack of effective enforcement of the right is an issue which is evident at most turns of the debate. Thus, not only is it not entirely clear what needs to be protected but also how to do it. Regretfully though perhaps hitherto inevitably, the super-fast development of privacy-relevant technologies and especially the Internet has led to a huge organic growth in the way in which personal data is generated and the exponential growth in the quantity of such data. This is especially evident in an on-line environment where, when seen from a global perspective, it would appear that the triangle of actors consisting of legislators, private (mostly corporate) actors and citizens all try to shape cyberspace using their possibilities in an uncoordinated manner. This may lead to a situation where none of the three is able to unleash the full potential of modern information technology.

4. In order to disentangle this triangular relationship an ongoing and open dialogue needs to be set up which eventually would provide for a more clear and harmonious regulation of cyberspace. This can only be achieved as a result of a sincere, open and committed dialogue of all parties which is to be held in a respectful and open manner. Sturdy and reliable bridges need to be built between all actors which are shaping the developments. It is the intention of the Special Rapporteur to listen closely to all parties and to facilitate this dialogue. In this way a basis for a positive and sustainable long-term development in the field of privacy protection should be achieved.

Annex IV

A "State of the Union" approach to privacy

It would appear to be useful to, at least once a year, have the SRP present an independent stocktaking report on where the right to privacy stands and this may be one of the primary functions of both the reports to be made to the Human Rights Council (HRC) and the General Assembly (GA). Since these reports are constrained by a word-limit it is clear that they can be little more than an extended executive summary of the findings and activities of the mandate throughout the reporting period. It should follow that the reports will also reflect the working methods of the mandate as outlined in Section II of the main report, in particular the thematic investigations as well as salient developments identified in the country monitoring activities carried out by the SRP team. It is expected that the report presented to the March 2017 session of the Human Rights Council would be the first such report reflecting a "State of the Union" approach. The report to the March 2016 session of the HRC will not attempt to prioritise risks or landmark improvements in privacy protection but simply refer to a few cases which illustrate particular progress or difficulties.