FUTURE OF PRIVACY FORUM

2021 年 7 月

数字化接触者追踪技术

隐私与公平原则和框架

简介

长期以来，接触者追踪一直是公共卫生部门用来监测传染病传播情况的人工疾病追踪过程。在新冠肺炎 (COVID–19) 疫情期间，数字化接触者追踪技术 (DCTT) 发展成为暴露通知工具，以帮助经济、工作场所以及其他公共和私人空间及环境重新安全开放。[1]值得注意的是，DCTT 由采用蓝牙和/或地理定位功能的移动应用和设备组成，旨在向用户提供快速、实时的病毒暴露通知。

专家们预计，针对新冠肺炎 (COVID–19) 的 DCTT 工作还将持续一段时间，随着公共卫生官员为 DCTT 项目奠定基础，DCTT 技术和治理也将不断发展，以应对新的、不断出现的疫情威胁。与此同时，随着 DCTT 越来越广泛地被用作公共和私人健康监测工具，有关 DCTT 的有效性和科学性的证据也越来越多。

未来隐私论坛 (FPF) 与以下六家领先的隐私、社会倡导和健康公平组织合作，分析 DCTT 实施过程中可能出现的隐私和公平权衡及风险：多元化对话、全国反对患者健康差异联盟 (NADPH)、BrightHive 和 LGBT Tech。该小组特别关注 DCTT 对弱势群体的影响，讨论了特别的风险，包括但不限于与种族或族裔、阶级、宗教信仰或其他特征有关的被剥夺权利或社会污点的风险。

如果努力实施 DCTT 只是最大限度减少或不承认这些权衡和风险的存在、作用或影响，则会破坏公众对 DCTT 的信任。反之，努力去承认、参与和减少这些风险的治理可以增强公众对数字化接触者追踪技术的信任。政策制定者、数据保护专家以及开发、管理和提供 DCTT 技术的组织都可以发挥重要作用。

行动纲要

作为其隐私和流行病倡议的一部分，FPF 与多元化对话、全国反对患者健康差异联盟 (NADPH)、BrightHive 和 LGBT Tech 合作，制定了一套可操作的原则来支持解决 DCTT 实施过程中的隐私和公平性问题。

这些原则建议实施 DCTT 的组织：

1. 对数据的使用和共享方式保持透明。
2. 应用强大的去身份识别技术和解决方案。
3. 通过分层的启用/停用功能和数据最小化赋予用户权力。
4. 承认并解决隐私、安全和非歧视保护方面的缺口。
5. 创建公平使用 DCTT 的机会。
6. 承认并解决公共和私人环境内部及之间的隐性偏见。
7. 在采用适当的隐私保护措施的同时，将数据民主化以促进公共利益。
8. 采用“将隐私保护融入设计”(Privacy–By–Design) 标准，使 DCTT 得以广泛普及。

FPF 和这六家组织呼吁 DCTT 开发者和实施 DCTT 的组织承诺遵守这些原则。

下面，我们将：

1. 描述每一项原则;
2. 总结案例场景，说明 DCTT 技术如何引起数据保护风险，特别是对弱势个人的风险，包括种族和宗教少数群体、LGBTQ+ 个人和移民社区；以及
3. 强调关键的定义和其他资源，从隐私和公平的角度为 DCTT 的实施提供信息。

数字化接触者追踪技术的可操作隐私和公平原则

1 对数据的收集、使用和共享方式保持透明

DCTT 提供商可以出于公共卫生或相关目的使用和共享接触者追踪数据。历史和现今的证据表明，敏感数据可能会被权力实体（如执法部门）以歧视性的方式使用，从而使某些群体遭受压迫、暴力和其他极端的社会环境。此外，如果 DCTT 的技术精确度或准确性不明确或没有很好的证据，DCTT 可能会在假阳性或不准确的接触者追踪基础之上采取行动，如针对社会弱势群体的执法行动。

应通过醒目的、可理解的和可访问的声明让 DCTT 用户了解他们的数据是如何收集、使用和共享的。例如，数据收集、使用和共享的透明度声明可以在 DCTT 安装前通过应用商店的通知提供，在下载或安装时通过应用内的服务条款披露，或在首次使用 DCTT 时通过“即时”移动应用通知提供。通知和/或隐私设置还应明确说明收集敏感数据的时间和期限。

2 应用强大的去身份识别技术和解决方案

DCTT 提供商应采用强大的隐私保护技术和解决方案，以防止恶意和/或未经授权的各方，采用与公共卫生精神不一致、相冲突，或带来损害风险的方式，利用通过 DCTT 收集的敏感数据。组织可以对数据实施技术、政策、合同或法律控制措施来帮助实现这一目标。控制措施可以包括强大的去身份识别技术、数据安全保障、数据去中心化，以及暴露通知数据的隐私防火墙。例如，强大的去身份识别技术可能涉及去除直接标识符和已知的间接标识符，以模糊或掩蔽现实世界的身份。数据安全保障和隐私防火墙包括限制个人访问权限的技术许可，以及禁止第三方识别或重新识别 DCTT 用户的组织和法律控制措施。最后，数据去中心化意味着暴露通知数据保留在设备上，因此，设备所有者的身份在暴露通知后仍然不会被披露。

对于包含个人用户级信息（例如与地理位置数据配对的年龄和性别数据）的可互操作数据架构和数据类型，应使用可在多个数据架构中有效运行的适当而强大的安全保护措施来保护。如果没有此类保护措施，就存在数据误用或滥用、缺乏数据最小化的风险或潜在风险，从而限制了用户的采用和/或传染病检测的合规性。

3 通过分层的启用/停用功能和数据最小化赋予用户权力

DCTT 的参与应该是自愿的（而不是强制性的），并且 DCTT 用户通常可以选择启用特定的 DCTT 功能（即支持“主动”[启用] 与“被动”[嵌套的或基础性的；默认情况下停用] 的参与模式。

默认情况下，DCTT 应仅收集为用户提供服务所需的最低限度的数据。收集更多用户数据的额外功能应提示 DCTT 用户启用或停用进一步的数据收集和共享。应提供有意义且有影响力的启用/停用选项，并且 DCTT 用户应能够轻松访问这些选项。

4 承认并解决隐私、安全和非歧视保护方面的缺口

在监督和规范组织或服务提供商的隐私、非歧视和监视行为方面，可执行的行政保护措施可能有限。因此，DCTT 开发者和 DCTT 的机构采用者应该公开认可倡导 DCTT 多样性和公平性的伦理规范、标准、行动手册和/或框架，并对此类标准负责。例如，这可能包括 FPF 和 BrightHive的“负责任的数字化接触者追踪数据使用手册”，Lo 和 Sim 的“评估新冠肺炎 (COVID-19) 人工和数字接触者追踪的伦理框架”，或全国县市卫生官员协会的“基于社区的员工接触者追踪原则指南”。鼓励或应该鼓励和授权 DCTT 用户积极参与此类伦理规范、标准和/或框架的制定和实施。

5 创建公平使用 DCTT 的机会

鉴于某些设备可能比其他设备更兼容某些 DCTT，开发者必须避免将特定类型的设备与最有益的 DCTT 功能捆绑在一起。在创造公平（相对于平等）使用 DCTT 的机会时，务必要考虑并解决个人或群体在寻求获得使用 DCTT 的好处时可能遇到的特有结构性和程序性障碍。在促进公平获取个人设备和基础设施方面发挥作用，这对于 DCTT 的采用和使用至关重要。例如，创建无需无线互联网服务的 DCTT，或创建与较旧和较新的移动设备版本兼容的 DCTT，可以确保 DCTT 广泛惠及个人，无论其经济状况如何。

6 承认并解决公共和私人环境内部及之间的隐性偏见

务必要承认当前存在于众多重要环境（如医疗保健或公共卫生环境）中的偏见的现实和影响，并解决 DCTT 可能暴露、延续甚至加剧这些环境中的社会偏见的情况。由于在这些环境中受到隐性偏见的个人或群体可能会遇到病例管理不善和/或歧视，他们更有可能因此而避开这些环境，尽管这些环境很重要，而且 DCTT 对于在疫情期间管理公共卫生很重要。例如，如果被社会边缘化的个人或群体在有偏见的公共卫生系统中寻求医疗保健服务时经常遇到尴尬、恐惧或羞耻，那么该个人或群体可能会感到无法信任或不参与由该系统实施或在该系统内实施的 DCTT 项目。因此，承认和解决在实施 DCTT 的环境内及环境之间存在的隐性偏见，可能会增加个人参与 DCTT 的安全感。

7 在采用适当的隐私保护措施的同时，将数据民主化以促进公共利益

在可能的情况下，数据应该民主化，以便有益于公共卫生项目和基础设施。DCTT 数据通常能够以有限的、去身份识别的方式共享，以促进这些目标的实现。数据可以与值得信赖的研究合作伙伴共享，作为社区健康信息网络的一部分进行管理，或者在极少数情况下将其公开。政府和其他相关实体应采取强有力的措施来确保隐私，尤其是在 DCTT 数据被公开或广泛使用的情况下。

公共政策应纳入或认可强有力的数据治理过程、实践和程序，以支持和保护将 DCTT 数据在公共卫生研究中的使用。例如，此类过程、实践或程序可能包括确定应提供的最少必要数据类别；应用技术、合同和/或程序保障措施，以防止个人信息被不合理披露；以及通过使用强加密或其他数据安全标准确保 DCTT 用户数据得到保护。

8 采用“将隐私保护融入设计”(Privacy-By-Design) 标准，使 DCTT 得以广泛普及

开发者应采用“将隐私保护融入设计”(Privacy-By-Design) 标准，以确保广泛的用户能够使用 DCTT。这些标准应确保 DCTT 的益处能够最大限度地为公众服务，但在设计过程中不会损害 DCTT 用户的隐私和公平。

要签署数字联系人追踪技术原则，请通过 info@fpf.org 与我们联系。

定义

1. **DCTT**: 用于检测潜在疾病或感染暴露情况的技术。这项技术包括跟踪用户行踪和健康状态的应用程序, 以及关联多个用户的数据以识别潜在的暴露情况。
2. **DCTT 用户:** 出于公共或私人目的在个人设备上或通过个人设备使用 DCTT 的个人。
3. **数据最小化:** 充分、相关且仅限于处理目的所需的数据。(《一般数据保护条例》, 第 2 章, 第 5 条)
4. **去身份识别:** 从组织收集、存储和使用的数据中删除个人身份信息的过程。(未来的隐私论坛, 实用数据去身份识别视觉指南 [2016 年 4 月])
5. **匿名化:** 直接标识符被消除或转换, 但间接标识符保持不变的过程。(未来的隐私论坛, 实用数据去身份识别视觉指南 [2016 年 4 月])
6. **敏感数据:** 受特定处理条件约束的数据, 这些处理条件使数据在以下语境中可被识别: 1) 揭示种族或族裔、政治观点、宗教或哲学信仰的数据; 2) 遗传数据, 仅用于识别个体的生物数据; 3) 健康相关的数据; 4) 有关个人性生活和性取向的数据; 以及 5) 精确的地理定位。(改编自《一般数据保护条例》第 4(13)、(14) 和 (15) 条以及第 9 条和序言 (51) 至 (56); 也改编自《加利福尼亚隐私权和执法法案》第 14 节)
7. **去中心化**: 将现有信息分成多个片段并存储在网络的各个部分 (移动代理、边缘计算中心等) , 而不是将所有内容存储在中央服务器上的过程; 此外, 没有任何一个实体拥有完全的控制权或完整的信息。(Shubina 等, 2020 年)

真实世界的案例场景

案例场景 1

韩国首尔的一个 LGBT 社区

在新冠肺炎 (COVID–19) 疫情的最初几个月，韩国政府于 2020 年 5 月初开始放宽限制，允许酒吧和其他场所开放，韩国的女同性恋、男同性恋、双性恋和跨性别 (LGBT) 人士被指控传播新冠病毒肺炎 (COVID–19) 。此后出现了几起新的新冠肺炎 (COVID–19) 病例，并被追溯到梨泰院 (Itaewon) 的夜总会，梨泰院是首尔市一个以国际餐饮和夜生活闻名的地区，媒体将其描述为“同性恋俱乐部”的社交中心或安全空间。首尔市长表示，“那些没有站出来接受检测的暴露者将在警察的陪同下在家接受检查”，一些人担心，由于此类追踪工作，LGBT 群体可能会面临歧视和对个人性取向的猜测的风险。Thoreson, 2020 年, 人权观察

案例场景 2

美国艾滋病时代尚未解决的紧张局势。

在加利福尼亚州旧金山，接触追踪者和同性恋社区之间悬而未决的紧张关系持续了近 40 年。自 20 世纪 80 年代以来，接触追踪者和同性恋权利律师表示，公共卫生机构强制执行的广泛艾滋病病毒接触者追踪工作，已导致同性恋社区反对接触追踪。在同性恋群体中，识别出暴露于艾滋病病毒的个人可能并已经导致其失业、失去住房以及其他基本需求和服务的丧失。

根据公共卫生机构中同性恋群体之间未解决的不信任问题的几个故事和经验教训，旧金山公共广播电台 (KQED) 的一名记者得出结论说，如今，地方、州和县公共卫生部门正在“通过与社区团体合作，与受影响人群建立联系”，这些团体与同性恋群体有着信任关系。Dembosky, 2020 年, KQED

真实世界的案例场景

案例场景 1 和 2：经验教训

案例场景 1 和 2 强调了应用以下原则非常重要的原因：

- **原则 4：承认并解决隐私、安全和非歧视保护方面的缺口**
  为加强信任，DCTT 开发者和 DCTT 的机构采用者可以公开认可伦理规范、标准、行动手册和/或框架并承担责任；这些伦理规范、标准、行动手册和/或框架的制定，直接听取了在某些机构中曾遭遇滥用或不信任的群体的意见。

- **原则 6：承认并解决公共和私人环境内部及之间的隐性偏见**
  针对 DCTT 可能会暴露、延续或加剧一系列或大量私人和公共环境中的有害偏见的当前或可能出现的情况，DCTT 开发者和 DCTT 的机构采用者必须进行预测并予以解决，以帮助确保个人感到安全并受到保护，避免因系统或环境中的隐性偏见而导致的下游伤害或不幸事件。

- **原则 8：采用“将隐私保护融入设计”(Privacy–By–Design) 标准，使 DCTT 得以广泛普及**
  “将隐私保护融入设计”(Privacy–By–Design) 的功能或标准，如匿名暴露通知，促使个人在暴露于传染病后，可选择以私密方式监测和控制他们的个人行为、环境、与他人的交流以及踪迹。

要点总结

为监测传染病在社会弱势群体中的传播情况而进行的接触者追踪工作，可能会使这些群体在家里或社区内面临歧视或排斥的风险。从社会和经济角度来看，这些人群可能受害最深，他们可能不太愿意参与任何可能泄露其私人社会关系和行踪的技术，包括 DCTT。

真实世界的案例场景

案例场景 3

中国南部城市广州的一个非洲人社区

中国政府在社交媒体上发布了针对输入性冠状病毒的表面中立的警告后，广州一个非洲人社区的成员遭到了歧视。广州当局表示，五名尼日利亚人的新冠肺炎 (Covid–19) 检测结果呈阳性，将冠状病毒风险追溯到广州的越秀区和白云区，据悉非洲人社区主要在这两个区。CNN 的一篇新闻文章称，这个非洲人社区的成员被赶出他们的出租屋，并被拒绝提供酒店服务，尽管该社区成员声称最近没有旅行史，也没有与新冠肺炎 (COVID–19) 阳性者的已知接触。这个非洲人社区的许多成员依靠短期商务签证，每年数次往返于非洲和中国。

对非洲居民的敌意在该市出现新冠肺炎 (COVID–19) 之前就已经存在了，但在疫情期间更加恶化了。与“非洲接触者”接触个人被要求进行自我隔离。美国驻广州领事馆警告非裔美国人，在敌意日益加剧的情况下，避免前往广州。美国领事馆警告说：“……警察命令酒吧和餐馆不要为看起来是来自非洲的客户提供服务。Marsh、Deng 和 Gan，2020 年，CNN；美国驻中华人民共和国广州总领事馆 [2020 年 4 月13 日]：广州对非裔美国人的歧视

案例场景 4

柬埔寨的一个穆斯林社区

柬埔寨卫生部在其官方社交媒体网页上点名了据报道感染新冠肺炎的特定人群，此前对接触者追踪发现“他们 [当地] 社区的人与人之间没有传播的迹象”。其中一个特定团体名为“高棉伊斯兰”。据报道，这篇社交媒体帖子导致在网上和日常在市场、商店和其他公共场所“爆发”了针对柬埔寨少数民族穆斯林群体的歧视性和仇恨言论和手势。发生这些事件后，柬埔寨政府发言人要求媒体不要提供有关感染新冠肺炎 (COVID–19) 患者的身份信息。Chhin，2020 年，人权观察；Penh，2020 年，美国之音

案例场景 3 和 4：经验教训

案例场景 3 和 4 强调了应用以下原则非常重要的原因：

- **原则 4：承认并解决隐私、安全和非歧视保护方面的缺口**
  为加强信任，DCTT 开发者和 DCTT 的机构采用者可以公开认可伦理规范、标准、行动手册和/或框架并承担责任；这些伦理规范、标准、行动手册和/或框架的制定，直接听取了在某些机构中曾遭遇滥用或不信任的群体的意见。

- **原则 6：承认并解决公共和私人环境内部及之间的隐性偏见**
  当卫生机构或政府当局等权力实体公开将一种传染病归因于高度隔离的地区或经常前往某一地区旅行的人群时，可能会激发或加剧个人对这些高度隔离或旅行人群的有害偏见。DCTT 开发者和用户应制定和实施 DCTT 和数据报告策略，以防止隐性和有害偏见的下游影响，如剥夺权利和仇恨言论，并保护已知的高度隔离社区或前往某些地区旅行的社区群体的福祉和声誉

- **原则 7：在采用适当的隐私保护措施的同时，将数据民主化以促进公共利益。**
  公开收集和分享最低限度的必要数据，就能够帮助防止个人因其个人归属、生物属性或其他个人固有的偏见和假设而成为社会的靶子或以有害的方式被误定为靶子。

要点总结

DCTT 不应将具有某些特征或社会关系的群体作为执法、媒体诽谤或公众羞辱的目标。DCTT 开发者、政策制定者和其他有影响力的利益相关方，包括媒体和社交媒体公司及用户，应该预见到接触者追踪数据可能被滥用的情况。此举旨在保障弱势群体或个人不因宗教信仰、不可改变的特征或其他个人属性而受到社会排斥或歧视。

真实世界的案例场景

案例场景5

美国北达科他州的新冠肺炎 (COVID-19) 接触者追踪应用程序

Care19 应用程序是北达科他州的 ProudCrowd 公司开发的一款自愿应用程序，是为应对新冠肺炎 (COVID-19) 疫情而实施的首批接触者追踪应用程序之一。该应用程序得到了北达科他州和南达科他州政府官员的正式认可。后来，科技隐私公司 Jumbo Privacy 发现，Care19 应用程序包含将应用程序用户的位置和身份数据发送给当地和国际第三方公司（包括从事商业广告的公司）的代码。虽然该应用程序包含了这些代码，但该应用程序的隐私声明告诉用户，他们的位置数据“不会与任何人共享，包括政府实体或第三方，除非您同意或 ProudCrowd 根据联邦法规的要求被迫共享。Groves，2020 年，今日美国

真实世界的案例场景

案例场景 5：经验教训

案例场景 6 强调了应用以下原则非常重要的原因：

- **原则 1：对数据的收集、使用和共享方式保持透明。**
  如果 DCTT 用户充分了解个人数据是否以及如何被收集、使用以及与第三方共享，那么他们就能够就他们希望与谁共享个人数据做出知情选择。这不仅可以保护 DCTT 用户的利益，而且也可以保护旨在提供高标准用户/客户服务的 DCTT 开发者的利益。

- **原则 3：通过分层的启用/停用功能和数据最小化赋予用户权力。**
  分层的启用/停用功能和数据最小化给予 DCTT 用户选择权，以最适合他们的隐私偏好、个人福祉和利益的方式进行参与。DCTT 公司或开发者应仔细审核他们打算采用或使用的代码，以确保他们不会在其隐私声明和政策中误导自己、其用户/采用者和监管机构。

要点总结

隐私政策、使用协议条款和类似的通知应透明、准确地反映 DCTT 开发者的隐私做法，并以广泛民众可理解的水平来编写。隐私政策不应包含令人生畏的行话、规定或大多数用户难以理解或解释的关于应用程序隐私做法的术语。这类通知不应包含胁迫性条款，迫使用户选择使用隐私程度较低的功能，特别是在用户需要、严重依赖或被要求出于个人、法律或其他必要目的使用该应用程序的情况下。应用程序开发者（包括 DCTT 开发者）应仔细审核其采用或采购的代码，以确保其代码符合其内部隐私标准、政策和条款以及应用商店规则和用户/采用者的隐私期望。

美国关于数字化接触者追踪技术的主要立法提案

州法案

- **纽约州：**关于接触者追踪信息保密的公共卫生法修正案 (A10500C/S8450C)
- **纽约州：**有关收集和使用紧急健康数据和个人信息的要求，以及在新冠肺炎 (COVID–19) 期间使用技术帮助的要求 (A10583/S8448)
- **加利福尼亚州:** 个人信息: 接触者追踪 (AB660; AB 814)

联邦法案

- 2020 年新冠肺炎 (COVID–19) 消费者数据保护法
- 公共卫生紧急隐私法
- 暴露通知隐私法
- 制定美国框架以确保数据访问、透明度和责任法案（安全数据法）
- 公共卫生紧急隐私法
- 接触者追踪数据和隐私保护法案

DCTT 立法工作总结

- FPF 对截至 2020 年 8 月的美国其他立法趋势的总结

关于 DCTT 实施中的隐私和公平的主要资源

- 数字化接触者追踪: 负责任数据使用行动手册
- 数字化接触者追踪和数据保护法
- 私人生活和公共政策、政府统计数据的保密性和可获得性
- 健康数据生态系统定义的分类
- 新冠肺炎 (COVID–19) 时代的权利, 从艾滋病毒中吸取有效的、社区主导的应对措施
- 冲突中的技术: 新冠肺炎 (COVID–19) 接触者追踪应用如何加剧暴力冲突
- 接触者追踪应用程序: 妇女和边缘化群体面临的额外风险
- 在新冠肺炎 (COVID–19) 疫情控制中使用手机应用程序即时追踪接触者的伦理
- 与“人权观察”研究人员举行的新冠肺炎 (COVID–19) 与人权虚拟圆桌会议
- 接触者追踪应用程序是解决办法吗? 美国可以从其他国家/地区吸取的教训
- 代码之前的上下文: 紧急状态下的人权保护
- 数字化接触者追踪的负责任数据使用行动手册
- 评估新冠肺炎 (COVID–19) 人工和数字化接触者追踪的伦理框架
- 实用去身份识别视觉指南
- 消费者可穿戴设备和健康应用及设备的最佳实践
- Norton Rose Fulbright 对主要国际司法管辖区的主要监管和政策问题进行实时、全面的调查或总结

1 公开可用的 DCTT 的例子包括: 弗吉尼亚州卫生部开发的应用程序 COVIDWISE (美国)；科罗拉多州公共卫生与环境部和科罗拉多州应急行动中心开发的 CO 暴露通知 (美国)；以及由多州流行病学家和华盛顿大都会政府委员会开发的公共卫生实验室协会平台, 用于哥伦比亚特区、马里兰州、弗吉尼亚州和西弗吉尼亚州等邻近州的暴露通知 (美国)。在美国以外使用 DCTT 的例子包括奥地利联邦卫生部开发的 Stopp Corona 和巴西联邦政府开发的 Coronavirus – SUS。

该计划的支持由罗伯特伍德约翰逊基金会提供。此处表达的观点不一定反映基金会的观点。

1400 EYE STREET NW | SUITE 450 | WASHINGTON, DC 20005 INFO@FPF.ORG | 202-768-8950