Research Note

2020.6.7(Y-Research RN162)

作者：第一财经研究院

Committed to Improving Economic Policy.

www.cbnri.org

研究简报 热点

“数字抗疫”与隐私保护 | 一财智库全球观察

摘 要

YRI 研判及点评：

1. 新冠疫情爆发以来，不少国家通过数字技术排查病患、追踪密切接触者，在阻断疫情传播过程中取得了积极成果。在近期全球“经济重启”中，数字技术用于接触者追踪，也被认为是走出“封锁”的必要条件之一。**数字技术抗疫可以被归纳为四类，分别是数字化文档、数学模型、接触者追踪和远程医疗。**

表 1 主要国家数字技术抗疫及其分类

应用	目的	数据类型	采用国家
数字化文档	了解特定人群所在的位置	手环与手机中的 GPS 数据	韩国、中国、印度、比利时、捷克等
		人像数据	俄罗斯
	健康信息文档	体温信息、隔离状态等	中国、阿联酋

数学模型	了解人群的移动趋势	移动电话基站数据、社交网络数据	美国、英国、意大利、德国、韩国等
接触者追踪	追踪人的活动轨迹	政府从平台获取数据（中心化）	韩国、新加坡、澳大利亚、印度、以色列等
		手机互相提供数据（去中心化）	美国、欧盟
远程医疗	提供远程非紧急医疗服务	健康、病例数据	澳大利亚、中国、韩国、美国、德国、法国等

来源：第一财经研究院整理

2. 随着个人数据在抗疫中的大规模使用，隐私保护的讨论越来越多，主要集中在“接触者追踪”领域。**数字技术使用位置数据追踪密切接触者，可以用来识别特定自然人身份或者反映特定自然人的活动情况。这一类数据具有高度的敏感性，数据一旦被泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇，直接关涉到数据主体的切身隐私利益与个人安全。**数字化文档与数学模型的隐私问题相对较少，因为前者主要针对特定的感染患者，后者使用的多是匿名的聚合数据，这类数据通常不属于个人隐私数据保护的范畴。而在远程医疗领域，由于主要是对专业医生分享个人数据，所以多数国家公民分享数据的意愿都比较高。

3. 如今主要国家疫情趋于缓和，全球范围内的“重启”和复工可能导致疫情反复，此时“接触者追踪”变得更加重要。**5 月 11 日世界卫生组织突发卫生事件规划执行主任迈克尔·瑞安警告，假如不配合强有力的“接触者追踪”机制，“重启经济”犹如“闭眼开车”。**但在传统追踪方法下，对每个疑似病例进行跟踪所需要的资源巨大，并且由于资源有

限，当病例数量规模较大时，广泛的接触追踪可能会变得不可持续。此时需要更加精准追溯的方式，数字技术的“接触者追踪”就成为最佳选择。

4. 数字技术“接触者追踪”的效果取决于用户覆盖率，要充分发挥应用程序的作用，需要民众最大程度地参与、信任并接受创新型数字解决方案。**研究表明，追踪程序至少需要 60%的公民参与才能足够有效。为了增强人们对新技术的认可，监管部门首先需要明确公共健康危机时期与正常时期数据使用的区别，并对个人数据保护做出妥善安排，才能获得公众信任，为抗击疫情打下坚实基础。**需要指出的是，这种对技术的信任还将确保国家在未来技术发展中处于优势地位。

5. 新冠抗疫过程中的数据保护可以参考其他行业的治理原则，例如金融数据。金融数据也是敏感数据，其个人数据保护主要有两个方向的思路：**第一是限制数据的使用，**即通过立法和法规来规范包含个人身份信息的数据收集和使用；**第二是让客户控制其个人数据，**并决定向哪些公司授予数据访问权限，这可以促进竞争并增加社会福利。

6. 在抗击疫情的数据使用中，欧盟委员会针对疫情中数据保护的指引更加直接，值得充分重视。2020 年 4 月 16 日，欧盟委员会发布了“支持抗击新冠疫情应用程序的数据保护指引”，该指引旨在提供必要的框架，以确保公民在使用数字程序时个人数据得到足够的保护，并对侵犯行为进行限制。根据该指引，开发抗击冠状病毒相关应用程序的必要条件有 7 个，具体包括：

- 鉴于数据的高度敏感性和明确的最终使用目的，**国家卫生部门应**

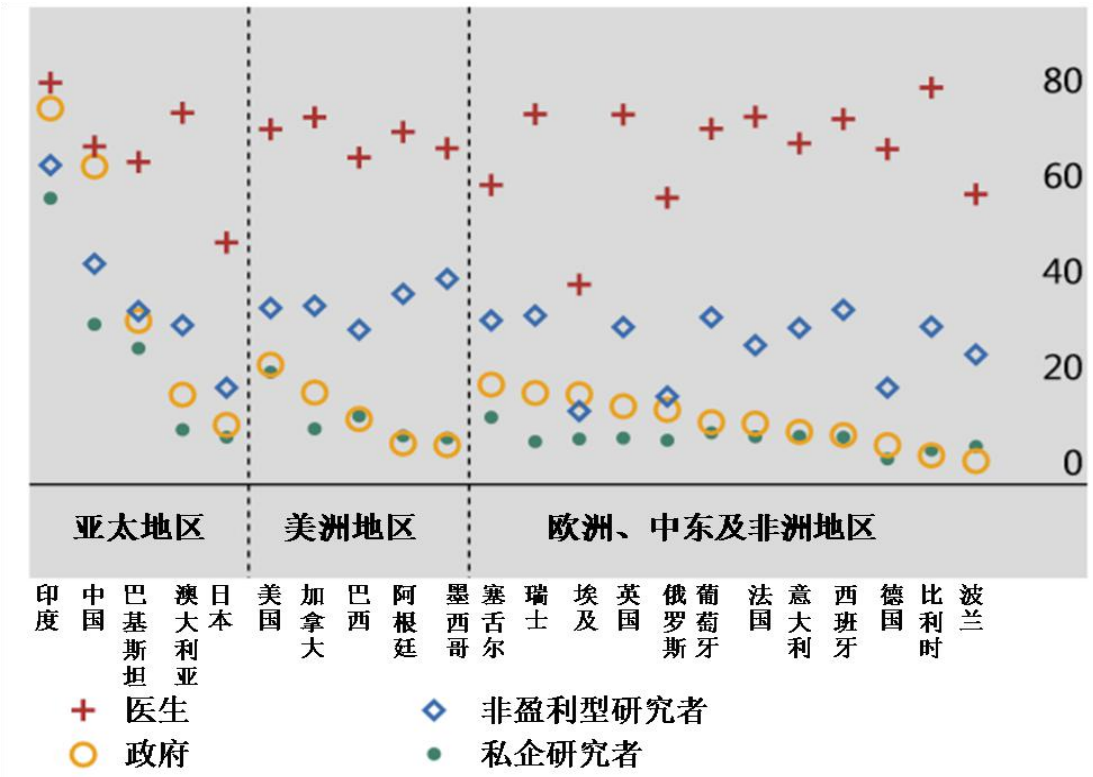
负责确保搜集、使用数据时符合数据保护原则。

- 用户设备上安装应用程序应该是自愿的，且用户应该能够对应用程序的每个功能分别给予同意。**如果使用了近距数据（proximity data，如蓝牙等），应将其存储在个人设备上，并且只有在用户同意的情况下才可以共享。**
- **应用程序应坚持数据最小化原则，**即只能处理与目的相关且仅限于相关目的的个人数据。
- **个人数据的保存时间不应超过所必须的时间，**时限应根据医疗相关性以及采取必要的行政措施的实际时间来确定。
- 数据应存储在个人的设备上，并进行加密处理。
- 确保所处理数据的准确性，第三方处理的任何个人数据必须准确无误。为了确保最大程度的准确性，这也是确保接触追踪应用程序的效率所必需的，应该使用蓝牙等近距技术对接触进行更精确的评估。
- 在开发应用程序时，应充分征询数据保护当局的意见，并由数据保护机构负责审查应用程序的部署情况

7. 不同国家的公民对于个人数据分享时的隐私考虑差别甚大。根据调研数据，**主要国家70%的受访者对于将个人医疗数据（DNA、健康信息等）交给医生都表示信任，但对于将金融等个人数据交给政府或私人公司，主要国家大多数受访者表示不信任。**印度的情况却完全不同，人们对医生和政府表示相似程度的信任。**中国对私人公司的信任程度虽然高于全球水平，但明显低于对于医生和政府的信任。**各国在数字抗疫中制定隐

私保护的具体思路时，应在符合公众偏好的基础上建立具体相关规则。

图 1 不同国家数据分享时的隐私考虑



注：受访人群会被问及是否愿意对上述 4 个实体（医生、非盈利型研究者、政府和私营企业公司研究人员）分享自己的医疗数据（DNA、健康信息等），纵轴对应同意的百分比。

数据来源：BIS、Middleton and Milne(2019)；EY(2019)；Chen et al(2020)

8. 中国在全球范围内较早运用了数字技术——“健康码”的方式来抗击疫情，**中国的数据运用模式是“中心化”的，这里需要特别关注个人数据的隐私保护，政府须对参与数据收集和运营的公司（主要是阿里和腾讯）的个人数据保护情况进行监督和干预；同时，应采取技术手段防止数据泄露；并在一定期限之后（确保今年年底和明年没有第二波疫情的情况下），中止这些数据的继续使用，或者删除在商业公司的相关数据。**

此外，随着跨地区人员流动将在未来大规模恢复，全国各地“健康码”系统的无缝对接也至关重要。

正 文

新冠疫情的爆发可以说是近百年来威胁人类社会最严重的公共卫生事件，人类应对疫情的思路与历次传染病爆发基本一致，控制人员流动、防止交叉感染仍是抑制疫情蔓延的有效手段，区别在于新技术使用。一些国家或地区在排查疫情、阻止疫情传播等领域的数字技术实践已经获得了积极的成果。

随着主要国家疫情趋于缓和，复工需要更加精准的防疫措施。越来越多的政府开始积极探索数字技术在抗疫领域的应用，希望借助信息科技做好复工与抗疫之间的平衡。但是对于个人位置等隐私数据的应用也引发了公众对于数据泄露和滥用的担忧，这将影响人们对相关应用程序使用的积极性，从而使数字抗疫技术的效果大打折扣，因此这个过程中的个人数据保护就变得至关重要。

本文梳理了数字技术抗击疫情的主要应用类型与相关隐私保护讨论，并整理了目前国际上抗击疫情数字应用中的个人数据保护思路，希望给中国使用数字技术抗击疫情提供参考。

一、 数字技术抗击疫情

自新冠疫情爆发以来，主要国家纷纷宣布实施“社交隔离”等防疫措施减缓病毒传播速度。然而隔离措施隐含巨大的经济成本，经济活动

不可能永远停滞，4月下旬开始，疫情趋缓的欧美主要国家已经开始分阶段重启经济。

隔离措施的放松意味着已经得到控制的疫情有可能出现反复，在前期防控被视为较成功的德国与韩国，已经再次出现公共场所聚集性感染事件。如何平衡经济重启与控制疫情之间的关系成为各国都面临的新挑战。在这一背景下，越来越多的政府将目光转向数字技术，希望借此平衡好复工与防疫之间的关系，此前部分国家已经使用数字技术防疫并收获了积极的成果。

表1 主要国家数字技术防疫及其分类

应用	目的	数据类型	国家
数字化文档	了解特定人群所在的位置	手环与手机中的GPS数据	韩国、中国、印度、比利时、捷克等
		人像数据	俄罗斯
	健康信息文档	体温信息、隔离状态等	中国、阿联酋
数学模型	了解人群的移动趋势	移动电话基站数据、社交网络数据	美国、英国、意大利、德国、韩国等
接触者追踪	追踪人的活动轨迹	政府从平台获取数据（中心化）	韩国、新加坡、澳大利亚、印度、以色列等
		手机互相提供数据（去中心化）	美国、欧盟
远程医疗	提供远程非紧急医疗服务	健康、病例数据	澳大利亚、中国、韩国、美国、德国、法国等

数据来源：第一财经研究院整理

数字技术防疫可以归纳为四类，分别是数字化文档、数学模型、接触者追踪和远程医疗。第一类是数字化文档，该技术通常用于隔离环节，

将传统的电话访问与上门检查替换成数字化远程检查。这不仅节省人力，还可以将人们目前在哪里、曾经去过哪里与身体状况等信息一并生成文档以备工作人员查询。第二类是借助数学模型，通过搜集人口流动信息尝试刻画疾病的传播特征，以此作为防疫依据。第三类是接触者追踪（contact tracing），通过数字技术识别那些“与感染病毒的人有密切接触者”，帮助密切接触者及时获得护理和治疗，从而防止病毒的进一步扩散。最后一种是远程医疗，为用户提供远程诊断、治疗和其他非紧急医疗服务。

数字化文档是最先被用来辅助防疫的。二月初，中国大陆就推出了“健康码系统”，是最早推行此类追踪监控系统的国家之一。该系统依托于几乎覆盖全部中国大陆居民手机的应用程序（APP），用红、黄、绿三色二维码区分使用者的健康程度，并以此判断居民是否可以自由出行。

其他国家和地区的数字化文档主要用于了解隔离人群的位置识别。在韩国、中国香港和印度，当地政府通过手机 APP 提醒隔离人群不要离开指定区域。中国台湾、比利时与捷克等地区则会追踪隔离人群的手机信号完成上述工作。在中国台湾，如果运营商检测到某人越界，会发送短信通知此人手机并将相关信息报告当局。如果人们不带手机离开隔离地点将可能受到罚款等处罚，在韩国这不仅意味着折合约 17000 人民币的重罚，还可能面临监禁指控。俄罗斯则会使用人像识别技术判断隔离人群是否违反隔离规定。

研究人员利则用大数据的数学建模来分析传染病的传播特征，以此

作为防疫依据，此时移动电话公司和社交网络平台拥有的海量客户及其访问位置数据将提供有利支持。研究人员据此可以尝试预测疾病的传播，从而实现更精准抗疫措施，另外政府部门也可以借助这些数据评估政策的实际效果。

美国疾病控制和预防中心（CDC）建立了一个名为“新冠疾病移动数据网络”（Covid-19 Mobility Data Network）的抗疫计划。通过收集和分析移动广告商提供的匿名手机用户位置数据，预测并降低新冠疫情在全国的传播。目前，联邦和各州政府已经建立了覆盖 500 多个城市的用户手机数据库。英国也有类似计划。伦敦国王学院、盖伊医院和圣托马斯医院正在与健康数据科学公司 ZOE 合作开发新冠患者跟踪应用程序，利用新冠病毒感染者提交的相关数据来分析疫情发展和传播的路径。

科技巨头谷歌(Google)可能是全球拥有最多个人用户数据的公司，其也在考虑如何帮助政府和研究人员使用匿名的聚合数据（aggregated data）应对疫情。例如使用谷歌地图的出行数据可以帮助政府了解街道或博物馆的拥挤程度，这对评估社交隔离的影响十分重要。欧盟部分国家已经开始了类似计划，德国、意大利已经在欧盟隐私法许可范围内使用匿名的电信数据分析人群是否遵守社交隔离规定。

有些国家还将数据的使用扩展至“接触者追踪”领域，具体操作有两种做法。一种是中心化的，由政府直接从平台获取用户的位置数据，搜集数据可能来自警察局拥有的个人出行数据，也可能是手机 App 的位置数据，借此追踪那些与感染者到过同一地点的人们。

第二种方法则是去中心化的，主要依靠用户手机互相之间传递信息，确定是否接触过感染者，这需要通过专门的手机应用来完成。首先感染者的手机会收到一段专属代码，并自动与周围的手机匹配，当附近有人与感染者相处一定时间后，对方手机会自动通知使用者，并告知可能在何时何地接触过感染者。这个过程中无论是感染者还是接触者都不会被第三方识别。

4 月 10 日，谷歌和苹果罕见的宣布合作，他们将共同促进其移动平台用于公共健康监控应用程序的接触者追踪。两家公司使用的是去中心化的方法。

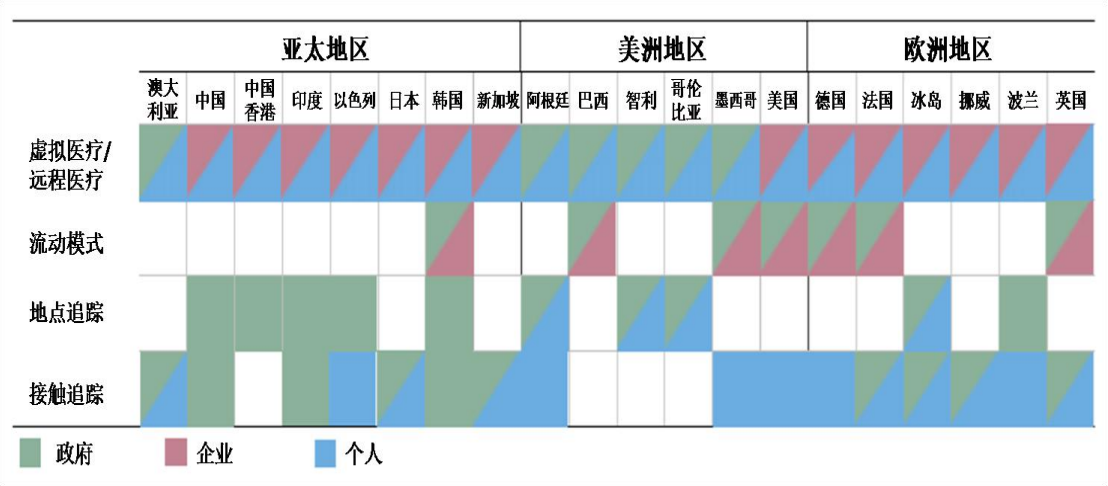
远程医疗是过去就存在的服务，此前主要通过电话等方式进行。新冠疫情以来，社交隔离措施使得人们出行受限，远程医疗需求大大增加，越来越多的机构参与进来。

二、 数据隐私：问题的提出

个人位置的数据使用在疫情防控中的积极作用值得肯定，但随着越来越多的国家和地区开始使用数字技术抗击疫情，个人隐私数据使用也让隐私保护与确保公共卫生安全之间的关系变得紧张起来。

在上文中讨论的四种数字技术防疫应用中，隐私保护的讨论主要集中在“接触者追踪”领域。数字化文档与数学模型的隐私保护问题相对较少，因为前者主要针对特定的感染患者，后者使用的多是匿名的聚合数据，这类数据通常不属于数据保护法的范畴。而在远程医疗领域，由于主要是对专业医生分享个人数据，所以多数国家公民分享数据的意愿都比较高。

图 1 主要国家和地区抗疫应用搜集数据情况分类



注：颜色标识哪个实体可以控制个人数据。如果政府和公司都可以直接或在经过个人同意的情况下使用个人数据则标识为两种颜色。

数据来源：BIS

得益于移动数据和相关技术（如 GPS 监测手环）的发展，个体追踪变得容易。截至 2019 年 6 月，OECD 国家中每 100 人拥有 113 个移动宽带账号，这意味着绝大多数人携带着可用于创建个人位置详细日志的设备。通过比较来自不同个体的位置线索就可以实现“接触者追溯”，并通知可能接触的人。

然而位置数据具有高度的敏感性，可以用来识别特定自然人身份或者反映特定自然人的活动情况。而且一旦被泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇，直接涉及到数据主体的切身隐私利益与个人安全。

实际上，即使使用匿名数据，仍存在对个人进行身份识别的风险，无论是确诊患者、疑似感染者都有可能因此产生“污名”。比如疑似或确诊感染者光顾的企业也可能被泄露并导致收入损失，即使在这些地方

已经关闭并消毒以后仍是如此。另一方面，接触者追踪系统与任何信息系统一样，也存在网络安全风险、数据泄露和被勒索软件攻击的可能性。勒索者可以利用接触者追踪系统，谎称自己确诊并曾光顾过该企业的方法要求企业支付赎金。最后，如果对接触者没有明确和可操作的建议，还可能产生错误信息，造成适得其反的行为、甚至恐慌。

除了位置数据，另一种侵犯隐私的技术是无人机使用。一些国家正在使用或考虑部署无人机，对人群拍照、进行自我隔离宣传或对被监视者进行包括发烧、咳嗽、呼吸和心率在内的监测。这些无人机和闭路电视摄像机一样都可与面部识别算法联合使用，容易引起公众的不安。

三、 数据隐私：各国实践

限制病毒传播对人民健康和确保医疗卫生系统正常运转极为重要，在一定程度上减少隐私保护也许是必要的。但并非一定如此，只要遵从一定的原则，数字技术抗疫中也可以做到保护隐私权。

中国在 2020 年 3 月 6 日发布了新版《信息安全技术个人信息安全规范》。规范明确了“行踪轨迹”属于“个人敏感信息”，在收集此类信息时，需满足“最小必要原则”和“合法性原则”，只有在“与公共安全、公共卫生、重大公共利益直接相关”等 11 种例外情形下才不必征得授权同意。

在抗击疫情的数据使用中，欧盟委员会的针对疫情中数据保护的指引值得参考。2020 年 4 月 16 日，欧盟委员会发布了“支持抗击新冠疫情应用程序的数据保护指引”（Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection）。该

指引旨在提供必要的框架，以确保公民在使用程序时个人数据得到足够的保护，并对侵犯行为进行限制。这将提高公民对创新应用程序的信任度，以此保障公民最大限度的参与，从而充分发挥应用程序的潜力。根据学者的研究（Hinch et al，2020），追踪程序至少需要 60%的公民参与才能足够有效。

该指引主要针对自愿下载的与抗击疫情有关的应用程序。这些应用程序可能包括以下功能：1）提供新冠肺炎的相关信息；2）提供自我评估和调查问卷等症状检查功能；3）提醒曾在感染者附近的人接受检测或自我隔离的接触者追踪功能；4）提供隔离患者与医生之间的沟通功能，包括诊断和治疗建议等远程医疗功能。

根据该指引，开发抗击冠状病毒相关应用程序的必要条件有 7 个，具体包括：

- 国家卫生当局负责。鉴于数据的高度敏感性和明确的最终使用目的，指引首先明确了国家卫生部门应负责确保搜集、使用数据时遵守《通用数据保护条例》（GDPR）。
- 用户可完全控制其个人数据。在用户的设备上安装应用程序应该是自愿的，且用户应该能够对应用程序的每个功能分别给予同意。如果使用了近距数据（proximity data，如蓝牙等），应将其存储在个人设备上，并且只有在用户同意的情况下才可以共享。
- 限制个人数据的使用。应用程序应坚持数据最小化原则，即只处理与目的相关且仅限于相关目的的个人数据。委员会认为位置

数据对接触追踪来说并非必须，因此建议在这种情况下不使用位置数据。

- 严格限制数据存储。个人数据的保存时间不应超过所必须的时间。时限应根据医疗相关性以及采取必要的行政措施的实际时间来确定。
- 数据的安全性。数据应存储在个人的设备上，并进行加密处理。
- 确保所处理的数据的准确性。根据欧盟个人数据保护规则的要求，第三方处理的任何个人数据必须准确无误。为了确保最大程度的准确性，这也是确保接触追踪应用程序的效率所必需的，应该使用蓝牙等近距技术对接触进行更精确的评估。
- 国家数据保护机构的参与。在开发应用程序时，应充分征询数据保护当局的意见，并由数据保护机构负责审查应用程序的部署情况。

目前已经有包括法国、德国、意大利在内的 8 个欧盟国家联合开发了确保隐私保护同时具有“接触者追踪”功能的应用程序——欧洲保护隐私的近距离追踪（Pan-European Privacy-Preserving Proximity Tracing）。

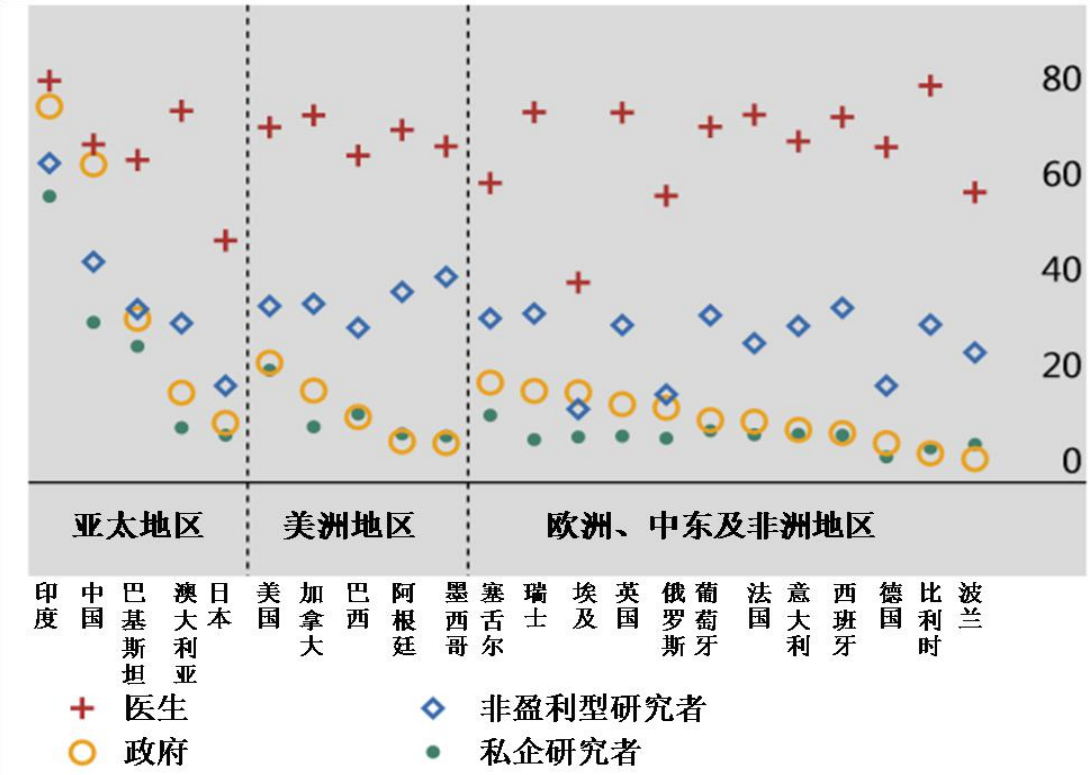
该应用程序的功能通过加密存储每个人手机中与附近其他手机蓝牙连接的信息实现。如果一个人的新冠病毒检测呈阳性，卫生部门会给他一个代码，他可以根据自己的意愿向运行该应用程序的国家信托服务(national trust service)提供这个代码。然后信托服务会向接近感染者的手机发送警报。这个过程中无论是感染者还是接触者都不会被识

别。

个人数据保护在金融行业中的实践也具有参考意义。金融数据本身也是敏感数据，并且通常需要值得信赖的保管人（金融机构）保管。金融领域解决隐私问题的政策组合主要有两类思路。一个思路是限制数据的使用，例如欧盟、巴西、日本等国在最新的《数据保护法》中规范了包含个人身份信息的数据收集和使用。这些法律面临的挑战是如何在尽职调查中平衡个人数据使用。另一个思路是让客户控制其个人数据，并决定向哪些公司授予数据访问权限，这可以促进竞争并增加社会福利（Jones & Tonetti， 2020）。欧盟、澳大利亚和墨西哥最近推进的“开放银行”都遵循了这个思路。

实际上，不同国家的公民对于个人数据分享时的隐私考虑差别甚大。根据调研数据，主要国家 70%的受访者对于将个人医疗数据（DNA、健康信息等）交给医生都表示信任，但对于将数据交给政府或私人公司，主要国家大多数受访者表示不信任。印度的情况却完全不同，人们对医生和政府表示相似程度的信任。中国对私人公司的信任程度虽然高于全球水平，但明显低于对于医生和政府的信任。各国在数字抗疫中制定隐私保护的具体思路时，应在符合公众偏好的基础上建立具体相关规则。

图 2 不同国家数据分享时的隐私考虑



注：受访人群会被问及是否愿意对上述 4 个实体（医生、非盈利型研究者、政府和私营企业公司研究人员）分享自己的医疗数据（DNA、健康信息等），纵轴对应同意的百分比。

数据来源：BIS、Middleton and Milne(2019);EY(2019);Chen et al(2020)

四、 “重启经济”时期的“接触者追踪”

如今主要国家疫情趋于缓和，复工可能使疫情反复。在一些前期防控被视为较成功的国家，近日再次出现公共场所聚集性感染事件，包括德国三家屠宰场和韩国一家夜店。此时接触者追踪变得更加重要。5 月 11 日世界卫生组织突发卫生事件规划执行主任迈克尔·瑞安就警告，假如不配合强有力的“接触者追踪”机制，“重启经济”犹如“闭眼开车”。

感染者可能在出现症状前就传播病毒，这就需要对所有可能具有传

染性的人采取严格的隔离措施。在传统追踪方法下，对每个疑似病例进行跟踪所需要的资源巨大，当感染病例数量众多，并且由于资源有限，广泛的接触追踪可能会变得不可持续。此时需要更加精准的追溯的方式，数字化的“接触者追踪”成为最佳选择。

这种大范围的数据使用不仅将影响抗击疫情的结果，还可能会影响未来的数据使用。如果公共部门或其私人部门合作伙伴成功的使用应用程序抗击疫情，并同时对个人数据使用负责，将获得公众的信任并得到强有力支持。但如果出现数据保护的问题，负面的使用体验很容易失去公众的信任，这对未来使用数据也会产生深远的负面影响，因为信任的建立需要长时间的积累。

此时，透明的公共政策可以更好的根据社会偏好构建医疗程序，并逐步积累公众的信任。监管部门应当着手建立透明的规则，并与公众进行清晰的沟通。目前许多亚洲国家已开始调整法律和政策框架，以确保数据使用是适当的。

展望未来，疫情终将过去，对于公共健康危机时期的数据使用应该与正常时期有所区分。在这场公共健康危机中，只有监管部门对个人数据使用做出合理安排，才能获得公众的信任，为抗疫成功打下坚实的基础，而这种对技术的信任并不会消失，还将使成功运用数字抗疫的国家在未来技术发展和竞争中处于优势地位。