领域观察 前沿洞察
专业先导 行业引导

5G

应用场景与隐私保护研究报告

中兴通讯数据保护合规部

2020/5/25

引言

当前，数字经济已成为引领全球经济发展的中坚引擎，带动经济社会进入一个全新时代，驱动传统行业向数字化、网络化和智能化方向发展。5G（5th generation mobile networks，第五代移动通信技术）技术所提供的大带宽、超高密度连接、高可靠低时延等优势，催生了通讯网络的性能跃升，为万物互联和人机交互提供了关键的基础设施平台，为数字经济的创新发展提供了无限想象空间。

5G 技术为众多典型应用场景注入了全新活力。5G 带来的传输速率、连接密度、实时性、可靠性等方面跃升质变，在大视频、工业互联网、车联网、远程医疗、智能安防、智慧校园、智慧电网、智慧机场、智能交通、智慧金融等激活、焕发出的应用场景将开辟了新价值增长点。

万物互联时代，数据成为生产要素，围绕“人”的产品服务成为最核心的价值中枢，关联着用户隐私数据（个人信息）的采集、存储迎来爆发式增长，个人、企业、行业甚至国家均通过数据交互紧密地连接在一起。5G 应用场景覆盖了未来社会生产和经济生活中绝大部分热点领域，而随着全球隐私保护法律法规的进阶深化，隐私保护合规成为这些领域应用的重要前提。如何在促进数字经济发展、规范数据流通共享，助力应用场景创新，加速 5G“新基建”中遵从隐私保护要求，确保合法合规，成为当下需要重点关注和研究的话题。

本报告立足 5G 技术特征和应用场景通识资料，从隐私保护和数据合规工作视角进行切入性研究，致力于通过“领域观察，前沿洞察”，实现“专业先导、 行业引导“，助力 5G 产业链各相关方了解应用场景与隐私保护关切，为良好合规履行和隐私保护设计提供参考。

编者

2020 年 5 月 25 日

目 录

1. 数字经济与 5G 应用场景

当前，数字经济已成为引领全球经济发展的中坚引擎，带动经济社会进入一个全新时代，驱动传统行业向数字化、网络化和智能化方向发展。世界各主要国家和地区纷纷出台数字化国家战略，聚焦工业数字化、金融和文化创意数字化和人工智能等重点领域，以期通过发展数字经济提高国家创新能力。数字经济使用数字化的知识和信息作为关键生产要素，以现代信息网络作为重要载体，以信息通信技术的使用作为效率提升和经济结构优化的重要推力。

通讯技术从 1G（1st generation mobile networks，第一代移动通信技术）到 4G（4th generation mobile networks，第四代移动通信技术），主要设计目标是满足个人用户间的通信需求。产业数字化转型中，大数据、人工智能、云计算、物联网等新技术不断融合和创新，对通讯网络提出了更高要求。5G 通信技术引入网络功能虚拟化和软件定义网络等技术，提供大带宽、超高密度连接、高可靠低时延等特性，实现了通讯网络的性能跃升，为万物互联和人机深度交互等提供了开放性的关键基础设施平台，为数字经济的创新发展提供了无限的空间。

根据国际移动通信标准化组织 3GPP（3rd Generation Partnership Project，第三代合作伙伴计划），5G 网络定义了三大技术特性应用场景：（1）增强移动宽带：提供 100Mbps-1Gbps 的用户体验速率及 100Gbps 的峰值速率；（2）海量机器通信：支持每平方公里 100 万连接以及更长的电池寿命；（3）超高可靠低时延通信：提供 1ms 空口时延及 99.999%的传输可靠性。5G 网络提供了满足多种垂直行业应用场景：（1）增强移动宽带：主要面向带宽敏感型业务，如 4K/8K 超高清视频、VR/AR（Virtual Reality，虚拟现实/Augmented Reality，增强现实）全景直播、VR/AR 娱乐等应用场景；（2）海量机器通信：主要针对物联网业务，如智慧城市、智慧家居、智慧交通、智慧校园、智慧机场、智慧农业等应用场景；（3）超高可靠低时延通信：主要针对高可靠低时延业务，如工业互联网、车联网自动驾驶、远程医疗等应用场景。

目前，5G 网络的标准协议逐步发展成熟，为新的 5G 商业应用及垂直应用做好铺垫，能够满足多种应用场景的网络需求，助力各垂直行业的数字化转型和智能化发展。

2. 数字经济与隐私保护

随着数字经济时代的到来，个人与数字经济间的交融质变深化，隐私保护问题日益凸显。隐私保护相关法律法规在全球如雨后春笋般迅速扩展，较具代表性的立法如欧盟《通用数据保护条例》(General Data Protection Regulation, GDPR)、美国加利福尼亚州消费者隐私法案（California Consumer Privacy Act，CCPA）、巴西《通用数据保护法》（Lei Geral de Proteção de Dados Pessoais，LGPD）、中国《网络安全法》等。

隐私保护立法提案层出不穷，如美国参议院提出《数据隐私法案》（Digital Accountability and Transparency to Advance Privacy Act or the DATA Privacy Act），中国《个人信息保护法》已形成草

案，列入全国人大优先立法清单。隐私保护标准密集发布，如 2019 年 8 月国际标准化组织和国际电委员会联合发布了隐私信息管理体系(Personal Information Management System ,PIMS)国际标准 ISO/IEC 27701:2019，2020 年中国修订了 GB/T 35273《信息安全技术 个人信息安全规范》，为隐私保护工作提供了标准指导。

数字经济时代，数据成为生产要素，围绕“人”的产品服务成为最核心的价值中枢，关联着用户**隐私数据**[1]的采集、存储迎来爆发式增长，个人、企业、行业甚至国家均通过数据交互紧密地连接在一起。隐私数据在社会生产生活中的高频使用和快速流动，对个人行使隐私保护权力带来了深刻影响，企业履行隐私保护义务带来直观挑战。具体地，各类形式丰富、分布广泛的传感器贡献海量数据，云计算以其资源灵活分配的特征为海量数据存储与处理提供支持，大数据技术对数据进行处理、分析和预测，人工智能将数据分析应用高效落地，这些新技术的协同运作，在服务于经济社会发展的同时，使隐私保护面临更加复杂的局面。

当前，如何在加速数字经济发展，促进数据共享助推企业和产业升级的同时，充分保护用户的个人隐私，确保隐私数据处理活动合法合规，成为各相关方需要重点关注的课题。

3. 5G 应用场景与隐私保护

5G 应用场景覆盖了当下和未来社会生产和经济生活中绝大部分热点领域，随着全球隐私保护法律法规的进阶深化，隐私保护合规成为这些领域应用的重要前提。例如，5G 通信技术支撑的泛感知智能设备将在生产生活中无处不在，时刻采集着海量数据并关联到个人。人们的生活和工作越来越离不开这些智能设备，数据采集、存储、传输、使用将进一步加强。与此同时，数据安全和隐私保护尚未跟上数据流动和数据开发的步伐。近年来，屡见不鲜、愈发严重的大规模数据泄露和个人数据滥用事件，为 5G 在各垂直领域的应用开发和场景嵌入时带来启示，隐私保护合规的重要性、紧迫性不言而喻。

3.1. 5G 应用场景隐私保护挑战

5G 时代为技术和场景应用带来新的变化，隐私保护主要挑战表现在：（1）毫米波和小基站带来覆盖范围缩小，用户定位更加精准，实时位置信息收集更加便捷。（2）无处不在的感知设备帮助人与人、人与物、物与物之间建立了更为广泛的联系，个人数据类型和数量爆炸性增长，传统认知中的设备数据与个人关联被打上个人数据标签。（3）联网设备急剧增加，组网环境更加复杂，脆弱设备失效可能性增加。（4）数据流动路径多变，业务合作模式多样，数据处理参与角色众多，多管理更加复杂。（5）各类新技术，如大数据、人工智能、云计算、物联网等融合发展和创新应用，对隐私保护管理和技术措施要求更高。

[1] 隐私是指自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。
个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。
考虑到业界惯例和两者保护方式的相似性，本报告中未对隐私信息和个人数据、个人信息做区分。

3.2. 5G 应用场景隐私保护简析

3.2.1. 车联网

【应用场景概述】

随着车辆智能化的提升，车联网成为国内外车企的布局重点，5G 大带宽低时延主要应用在自动驾驶和车路协同，主要场景包括：**车辆信息化服务**：车辆行驶过程中高精度地图、交通信号灯提示及周边服务信息推送等；**交通安全类应用**：智能化交通管理，车路行驶过程中的安全类信息要快速获取等；**交通效率类应用**：车、路、人协同，道路车速引导、车辆路径优化、道路流量优化等；**高度协同类应用**：运输、物流等行业，车队协同、车路协同以及远程调度等。

【数据处理简析】

车联网领域的数据处理过程涉及主体繁多、数据种类复杂，事关交通安全，具有强烈公共利益属性，成为公众关注重点。汽车制造商，车载系统开发商，修理厂，信息娱乐系统提供商，内容提供商，道路基础设施管理者，保险公司，车辆经销商，公共管理机构，车载服务提供商，电信运营商等，众多主体可能不同程度的参与到同一个数据处理活动。车联网产生了海量数据，其中大多数可被视为个人数据。

车联网应用主要包括的个人数据种类示例如下：

数据类别	数据类型	潜在的控制者/处理者
驾驶人信息	姓名、身份证号、驾照、手机号码、邮箱、支付信息、生物识别信息、驾驶习惯、健康状态、位置信息等	租赁或共享服务商、系统服务商、救援机构、保险公司、车载服务提供商等
车辆相关信息	车辆识别码 VID、出行线路记录、车辆配置信息、车辆状态信息（如行驶里程、器件磨损情况、充电记录）、车辆实时运行信息（车速、发动机转速、胎压、油表、冷却液状态）、维修记录、保险信息等	主机制造商、配件制造商、租赁或共享服务商、系统服务商、救援机构、保险公司、系统服务提供商、车载服务提供商、维修商、二手交易商、交通主管部门等
车载终端/应用相关信息	车载终端及应用手机的各类信息，如姓名、账号密码、位置信息、支付信息、播放记录、个人喜好、线路规划、通讯录、通话记录等	系统服务商、车载服务提供商、内容提供商等
其他信息	环境感知信息、车主信息、乘客信息、气象信息、位置信息等	车辆销售商、救援机构、保险公司、车载服务提供商等

【主要关切点】

车联网隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
数据处理关系的全面梳理	车路协同、交通安全管理、车载应用服务等	高风险
用户位置信息	车路协同、交通安全管理、车载应用服务等	高风险

人脸识别、声纹识别、指纹识别等生物识别信息	车载应用服务等	高风险
生物健康信息	交通安全管理、车载应用服务等	高风险
儿童信息	交通安全管理、车载应用服务等	高风险
用户精准画像	车路协同、交通安全管理、车载应用服务等	高风险
数据安全管理	车联网相关信息	高风险

【相关案例】

2011 年 9 月，美国联邦贸易委员会（Federal Trade Commission，FTC）曾对通用安吉星进行调查，指控其能够跟踪司机行为，在修改用户信息共享策略后，可能将车辆位置、速度和安全带使用情况等信息共享甚至出售给第三方 ,包括执法机构、无线网络供应商和数据管理公司等。美国白帽黑客 Miller 和 Valasek 于 2011 年成功入侵丰田 Prius 和福特 Escape，2015 年又远程控制一辆克莱斯勒切诺基。不仅控制了车内的设施，还可以操控汽车的行驶速度和路线。荷兰某网络安全公司于 2018 年公布，某些车载信息娱乐（In-Vehicle Infotainment, IVI）系统存在严重问题。攻击者可以直接通过车载的套件收听司机正在进行的谈话，打开或关闭话筒，以及访问完整的地址簿和对话历史记录，甚至是通过车载导航系统来精确地发现车辆所在的位置，并随时自动更新。

3.2.2. 智慧校园

【应用场景概述】

5G 在智慧校园中主要应用场景包括：云 VR 教育、校园高清直播、远程互动教育、校园视频监控。5G 正在推动重构教育服务方式，形成以泛在感知网络为支撑的无缝的、沉浸式的教育体验。教育领域的管理业务、教学业务、培训业务与服务业务将共享信息，实现数据互通，智能学习服务系统将对个体进行精准分析，按照个体特定需求及其特征为其提供适合的优质资源和服务，加速智慧校园建设。

【数据处理简析】

智慧校园的各个层面均广泛涉及个人数据的处理：**基础设施方面**，可通过电脑、手机、传感器、摄像头、可穿戴设备等对校园“人-物-景”全方位感知，涉及对定位信息、生物识别信息等敏感信息的处理。如考勤管理上，可对学生、教师、实验室管理员等进行考勤/打卡管理，对巡逻值班人员进行路线考勤管理，涉及个人位置信息的处理。**数据支撑方面**，可通过对教育教学过程中规律的分析、模式的总结建立校园基础库、个体教育库、课程教育库、班级教育管理库以及学校教育管理库等，涉及对个人教育基本信息和用户画像的处理。**平台能力方面**，可实现面向智慧校园物联网应用的平台能力支撑服务的构建，包括统一的用户认证和开放接口接入能力、安全认证能力、云计算与存储的服务能力、大数据分析与决策支持能力、情境感知能力，可能涉及人脸识别等生物特征数据处理。**用户方面**，可针对不同情境、终端设备下不同角

色进行智能支持，如针对学习者的个性化学习服务、针对教师的精准教学教研服务、针对管理者的数据驱动的管理服务以及教育治理服务等，可能涉及个人用户画像的敏感数据处理。

智慧校园涉及的数据类型示例如下：

数据类别	数据类型	潜在的控制者/处理者
基本身份信息	姓名、身份证号、校园 ID、指纹、人脸识别等	政府机构、学校、安防产品供应商等
考勤相关信息	指纹、位置等	政府机构、学校、安防产品供应商等
监控设备相关信息	位置、人脸识别等	学校、监控设备供应商等
VR/AR 设备相关信息	声纹、指纹等	VR/AR 设备供应商、可穿戴设备供应商等
远程互动教育	账号、密码、个人画像等	学校、人才市场、运营商、数据库供应商、网站虚拟平台、云存储供应商、大视频供应商等
大数据平台相关信息	个人基本信息和教育履历、课堂表现、学习效果分析等结合而成的个人画像信息	政府机构、学校、人才市场、运营商、数据库供应商、网站虚拟平台、云存储供应商等

【主要关切点】

智慧校园隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
个人位置信息	对巡逻值班人员进行路线考勤管理等	低风险
人脸识别、声纹识别、指纹识别等生物识别信息	对学生、教师、实验室管理员等进行考勤/打卡管理等	高风险
个人用户画像	闭环教学评价和教务管理、分析教学效果等；基于个人喜好推荐学术/生活/娱乐信息；AI 机器人助教、个性化教学等；	高风险
监控	安防监控等	高风险
用户同意、权限设置	云端数据处理等	中风险

【相关案例】

2019 年 11 月，瑞典 Anderstorps 高中在一个实验项目中使用人脸识别技术来记录学生的上课考勤，目的是简化操作并自动进行课程注册。该实验项目持续了三周，涉及到 22 名学生。学生们的面部生物识别数据及全名被以照片形式捕获，被存储在没有连网的本地计算机中。学校在收集学生的生物识别数据之前征得了监护人的明确同意，但学校没有就此进行隐私影响评估，也没有事先与瑞典数据保护机构进行协商，瑞典数据保护局因其违反 GDPR 而对该高中进行了违规处罚。

3.2.3. 工业互联网

【应用场景概述】

工业互联网是工业技术和信息通信技术结合的产物，是 IT（Information Technology，信息技术）、CT（Communication Technology，通信技术）和 OT（Operational Technology，运营技术）等技术的全面融合和升级。目前工业领域整体数字化和智能化水平还处于较低水平。工业互联网的主要诉求包括解决设备移动性，设备运行状态数据的采集，机器远程控制，远程智能巡检，远程设备维护，工业柔性生产，解放劳动力，危险场景保障人身安全，以提升生产力和运营效率，降低总体成本，加速工业互联网化和云化进程。满足这些需求和应用场景，通信网络需要：实现**连续覆盖**，满足安全性及高可靠性。上下行均支持**高速率的数据传输**。提供**毫秒级的实时控制**。支持局部区域内**海量高并发**、中高数据速率的物联网连接

5G 网络的大带宽、低时延、广链接，结合 XR（VR/AR）、MEC（Mobile Edge Computing，移动边缘计算）、AI（Artificial Intelligence，人工智能）和大数据等技术，具备感知泛在、连接泛在、智能泛在等特点，可以很好的满足工业智能化发展的网络需求。通过在工业领域部署 5G 网络，结合云服务和 MEC 等技术，可加速工业智能化改造，快速打造新型数字化应用。

【数据处理简析】

当前工业互联网主要应用场景下，涉及个人数据处理的场景主要包括：XR 辅助装配、XR 辅助远程维修/巡检、XR 远程控制操作、XR 辅助培训和工业 APP 等。工业互联网涉及的个人数据种类示例如下：

数据类别	数据类型	潜在的控制者/处理者
人员身份信息	人员姓名、工号、操作账号、密码等	工业企业、设备/软件/云服务提供商等
作业相关信息	各类操作可能涉及的生物识别信息（如指纹、面部识别、声纹、瞳孔等）和各类生理检测信息（如眼球追踪、心率、血压等）、操作记录、活动记录、环境信息、以及对操作信息的进一步分析信息等	工业企业、设备/软件/云服务提供商等
培训相关信息	人员参加培训的记录、操作记录、反应信息以及进一步的分析信息等	工业企业、设备/软件/云服务提供商等

【主要关切点】

工业互联网隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
作业人员生物监测信息、操作记录分析信息	各类 XR 辅佐作业、操作记录辅助分析	高风险
生物识别信息	身份识别与验证	高风险
作业人员身份信息	身份识别与验证	中风险
云端数据安全	工业互联网云服务	高风险

3.2.4. 大视频与云 XR

【应用场景概述】

大视频与云 XR（VR/AR）业务应用，主要使用 5G 网络大带宽的特性，典型应用如 8K/4K 视频直播、云 XR 游戏、视频会议、高清远程示教等，都需要 5G 网络的带宽保障。在本次新冠疫情防控中，高清视频在医疗领域的积极作用有目共睹。

【数据处理简析】

大视频与云 XR 对网络带宽要求高，视频渲染往往放置在边缘云计算，减少对汇聚层传输的压力，同时降低时延。大视频类业务在诸多领域都有应用，主要参与方有泛娱乐平台、大视频解决方案提供商以及提供基础资源的云平台。XR 作为移动云的终端设备，通过大带宽传输将源信号以直观体验呈现，同时又可通过可穿戴设备识别生物体征的信息作为设备间交互的信号，驱动应用功能的实现。可穿戴设备将人、事、物与互联网连接得越来越紧密，它记录着用户的健康指数、生活偏好、行为习惯、行动轨迹等信息，个人隐私保护面临越来越大的挑战。

大视频与云 XR 应用涉及的个人数据种类示例如下：

数据类别	数据类型	潜在的控制者/处理者
生物信息	人脸识别信息、健康信息、指纹、声纹、虹膜、步态信息等	大视频播放平台、APP、直播平台、网站、大视频解决方案提供商
设备信息	终端设备编码等	视频终端设备商、大视频解决方案提供商、应用平台
位置信息	轨迹、路线等	大视频播放平台、APP、直播平台、网站、大视频解决方案提供商
上网记录	操作日志、收藏列表、个人喜好等	直播平台、网站、大视频解决方案提供商
金融信息	银行卡账号、支付记录等	直播平台、银行、相关服务提供商
特殊信息	儿童信息等	大视频播放平台、APP、直播平台、网站、大视频解决方案提供商

【主要关切点】

大视频与云 XR 应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
人脸识别、声纹识别、指纹识别等生物识别信息	直播中的声图画面、安防产品中个人身份识别功能	高风险
用户健康信息	穿戴设备中反应自然人生物体征的信息，可能还会与其他应用形成功能交互，如支付、解码等	高风险
儿童信息	互联网教育应用、在线课堂等会出现儿童的图像信息	高风险

【相关案例】

2017 年 11 月，可穿戴设备 Strava 被曝隐私泄露。Strava 是一款风靡欧美的户外运动健身追踪应用，主要功能是把自行车爱好者们的成绩和名将们的成绩加入同一个排名中，让他们能和世界名将们一较高下。Strava 发布了一个世界用户活动热图，其中包含 10 亿次活动轨迹和 10TB 的输入数据。网友们从 Strava 数据中挖掘出了澳大利亚军队的演习路线，进一步挖掘揭露了世界各地隐藏的军事基地，中国也未能幸免。

Strava 具有一定隐私设置功能，允许用户创建长达 1km 半径的隐私区域，在这个区域内，用户轨迹会消失，以隐藏他们居住或工作的地方。遗憾的是这个功能是默认关闭的，也很少有用户会去主动打开这个功能。从隐私保护设计 PbD 的角度，隐私保护功能应默认打开，以降低不必要的隐私风险。

3.2.5. 远程医疗

【应用场景概述】

5G 网络大带宽、低时延为智慧医疗提供必要的移动网络支撑，推动医疗智能化发展。主要的应用场景：远程会诊：通过打通医疗机构资源，实现远程高清视频对话，共享病情信息、远程检测患者，为快速确诊争取宝贵治疗时机。高清视频的传输，需要 5G 网络提供网络基础。这类服务需要实现 5G 网络院内全覆盖，以及 40Mbps 以上带宽。远程超声：基层医院普遍缺少优秀的超声检查医生，而 5G 网络可以实现高清无延迟的远程超声检查，并且还能惠及专线建设难度大的偏远地区。远程超声需要实现 5G 网络院内全覆盖，以及低于 20ms 的时延。远程培训：我国地域之间医疗水平高低不等，同时医生培养周期时间长，医疗专家可以通过 4K/ 1080P 高清示教，多种接口对接手术现场设备，进行远程示教，同时这种教学方式互动方式多，个人可以通过多种方式听课：电脑、智能手机、智能 AR 或 MR（Mixed Reality，混合现实）眼镜等。远程培训需要实现院内会诊室全覆盖，以及 100Mbps 以上带宽。远程手术：医生可以在远端，通过高清回传的视频画面内容，远程控制手术仪器，完成手术。远程手术需要实现手术室内全覆盖，以及低于 10ms 的时延。

【数据处理简析】

远程医疗场景涉及大量患者的敏感个人数据，而数据收集和处理的参与方众多，这些参与方之间各类法律关系和权利义务存在交叠和模糊之处，为厘清各方主体的数据保护义务责任更增加了困难。此外，由于一般医疗相关数据都需要长期保存，数据处理链条长，节点多，数据资产管理难度大，用户行权也存在诸多限制和不确定性。医疗服务本身的公共服务属性，各方都很关注医疗数据的安全和合法使用问题。

远程医疗场景，涉及的个人数据类型和相关处理方示例如下：

数据类别	数据类型	潜在的控制者/处理者
基本身份信息 个人基本资料	姓名、身份证号、性别、民族、家庭关系、住址、电话号码、社保卡、居住证等	首诊医院、会诊医院、社会保险机构、商业保险公司等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等	首诊医院、会诊医院、保险机构、智能医疗平台等
监护设备、可穿戴设备收集信息	心跳、心率、睡眠、运动、血压、血氧、血糖、体温等	设备供应商、设备 App 开发者、医院、保险机构等
医疗消费记录	银行账号、口令、支付记录等	银行、支付服务提供方、医院、社保机构等

【主要关切点】

远程医疗应用隐私保护主要关切点及对应场景为：

主要隐私保护风险	应用场景	风险等级
患者大量健康生理数据、在医院的交易记录属于个人敏感数据需要予以特殊保护。	远程会诊、远程手术、远程监护等	高风险
远程医疗场景中个人数据在医院、社保机构、保险机构、智能设备软硬件供应商等机构之间流转，涉及主体众多	可穿戴设备、远程培训、远程会诊等	高风险
远程医疗场景中收集的个人数据除了用于医疗目的外 ,还可能被用于商业保险销售和定级、医学统计分析、远程培训、医疗服务广告画像等	可穿戴设备、远程培训、远程诊疗等	高风险

【相关案例】

2017 年 10 月，亚马逊数据库有 47GB 医疗被曝数据泄露，预计至少 15 万患者受影响，泄露信息包括患者的血液测试结果、个人信息，如患者的姓名、家庭住址、医生信息以及病例管理记录。2019 年 3 月，美国医疗机构 Medical Collection Agency 泄露近 2000 万条付款记录，实验室客户的逾期付款记录被泄露，包括社会安全号码和银行账户信息等敏感信息。2019 年 9 月，中国医疗 PACS 服务器疑似泄露涉及中国近 28 万条患者记录，数据记录包括个人和医疗细节：姓名、出生日期、检查日期、调查范围、成像程序的类型、主治医师、研究所/诊所和生成的图像数量。

3.2.6. 智慧安防

【应用场景概述】

随着智慧安防的发展，安防系统逐步向数字化、网络化、智能化升级。伴着平安城市、雪亮工程等项目在全国范围内的开展，安防产业已逐步从公安、政府等专用领域普及到了各个民用领域，深入群众的生活。智慧安防主要应用场景包括：通过人脸识别技术分析公共区域监高清摄像头画面，快速高效地辨别犯罪嫌疑人。执法人员安防巡检时，使用前端摄像机或手机进行抓拍，进行人员信息比对分析，快速确认人员身份。重点区域重大节日活动，无人机安防巡检， 360 度无死角监控场所，保障现场安全。

【数据处理简析】

基于 5G 网络的安防解决方案，在公共场所架设超高清摄像头，实时拍摄监控画面，实时上传高清画面至智能分析服务器。服务器对画面进行分析处理，报警信息上报到统一平台。巡逻治安人员携带智能 AR 电子眼镜，实时拍摄看到的画面，通过 5G 网络传输到智能分析服务器，对嫌疑人员进行身份核对，当发现可疑人物，通知安防人员。在大型演唱会、体育馆、公园等人员密集场所，使用无人机实时采集现场画面进行补盲监控，实时把拍摄到的画面传输到智能分析服务器，发现异常通知治安人员进行处置。

智慧安防涉及的个人数据类型示例如下：

数据类别	数据类型	潜在的控制者/处理者
基本身份信息	姓名、身份证号、家庭地址等	当地公安机关，政府机构、开发和部署智能安防方案或利用智能安防技术系统的方案解决组织、企业
生物识别信息	人脸识别数据，指纹等	当地公安机关，政府机构、开发和部署智能安防方案或利用智能安防技术系统的方案解决组织、企业
位置大数据	位置信息	当地公安机关，政府机构、开发和部署智能安防方案或利用智能安防技术系统的方案解决组织、企业
其他敏感信息	儿童信息、犯罪记录、车牌号等	当地公安机关，政府机构、开发和部署智能安防方案或利用智能安防技术系统的方案解决组织、企业

【主要关切点】

智慧安防应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
数据处理满足合法性要求	在公共场所中涉及隐私的空间内不得安装监控设备,视频监控系统的摄像部分的安装位置应当作出明显标识，使得公众知晓监控设备的存在	高风险
人脸识别、指纹识别等生物识别信息的处理	对进入监控活动范围自然人进行安防巡检，重点防控，对嫌疑人员进行身份核对	高风险
儿童个人数据处理	进行安防监控时，会将儿童信息与其他成人个人信息收集处理	高风险
数据存储安全	通过安防系统收集的数据量大而复杂，其中包含大量的敏感数据，存储在数据保护程度不同的当地派出所或政府机构	高风险
数据共享	公安机关，政府部门等跨部门进行大数据共享	中风险

【相关案例】

2019 年 5 月，世界首例警方使用人脸识别技术“AFR Locate”合法性案件：南威尔士警方对从闭路电视中获取的公众人脸进行实时处理，抽取面部识别信息，并将该信息与监视名单上的人的面部识别信息进行对比。若匹配未成功，数据不会被存储。与成功匹配相关的数据则最多会被保留 24 个小时。闭路电视记录根据相关标准保存 31 天。2019 年 2 月，深网视界科技有限公司的 MongoDB 数据库未做访问限制，导致超过 250 万人的数据泄露，数据类型包括人脸识别图像及图像拍摄地点身份证号、国家、住址、生日、照片和过去 24 小时内的位置等。

3.2.7. 智慧电网

【应用场景概述】

智慧电网和 5G、MEC 以及大数据等技术结合，主要应用于以下场景：实现在电网中配网同步相量测量、差动保护、配电自动化、高级计量等电力业务应用，达到对故障识别、定位、隔离、自愈毫秒级响应。开展无人机、智能机器人、视频监控等业务应用，实现电力运检视频的实时回传，结合 AI 实现故障智能识别、分析、预测。配电终端泛在连接智能化管理，满足点多面广的设备“最后一公里”的泛在连接。5G 通过端到端的网络切片服务，有针对性的解决智能电网的业务通信需求，提供差异化的网络服务，并实现资

源的安全隔离。

【数据处理简析】

智慧电网应用中，涉及个人数据的业务场景主要体现为智能电表相关的计量抄表等活动和 AR 辅助维修/检修等。智能电网一般会高频采集电表数据，主要包括智能电表 IP 地址、用电实时数据等，并可能在此基础上做用户需求和使用习惯的进一步挖掘分析。隐私属性较强的是用电实时数据。

数据类别	数据类型	潜在的控制者/处理者
用户身份信息	用户身份、账号信息、支付信息等	电力公司、云服务提供商等
智能终端相关信息	终端 ID、IP 地址、用电数据、用电实时数据等	电力公司、设备制造商、运营商、云服务提供商等
数据画像类	用户需求、用户使用习惯等	电力公司、设备制造商、运营商、云服务提供商等
AR 作业信息	操作人员身份、位置信息、生物健康信息等	电力公司、设备制造商、运营商、云服务提供商等

【主要关切点】

智慧电网应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
用户画像	对用户需求和使用习惯的画像等	高风险
人脸识别、指纹识别等生物识别信息的处理	AR 辅助作业等	高风险
数据安全管理	隐私信息的存储和使用管理等	高风险

3.2.8. 智慧轨交

【应用场景概述】

智慧轨道交通运用更加智能的定位设备、大数据融合分析以及更加生动的可视化手段，进一步提升了城市管理效率。主要的应用场景包括：**智能出行，**满足用户购买、查询车票需求，检测客流量，进行人员分流处理。**列车运行**，采集列车位置、状态信息和图像监控信息，进行智能化的列车控制和调度，提高列车运行效率。**设施维护**，分析海量检测和告警数据，合理安排设施的维护计划。发生紧急故障时，及时安排维护人员，特殊情况下可以通过远程专家指导模式完成故障检修。**应急防灾**，轨道交通场景人流密集，当发生安全事件时，第一时间调度指挥救援力量，完成快速响应。

【数据处理简析】

智慧轨道交通站点和轨道、停车场部署 5G 网络：轨道交通站点通过 5G 网络**实时采集监控**画面，对人流量和乘客信息进行分析，完成智能出行分流处理。获取列车运行的图片监控信息、列车状态、列车控制等内容，完成设施维护场景的流程。列车运行数据通过 5G 网络实时传输至数据分析服务器，完成对海量检测数据的分析和预测，协同完成设备监控。检修人员通过 5G 网络，和远程专家建议连接指导模式完成故障检修。通过 5G 网络实时传输的监控画面，使用 AI 进行人脸识别。当发现嫌疑人员时，及时通知安保人员

快速处置。

智慧轨道交通涉及的数据类型示例如下：

数据类别	数据类型	潜在的控制者/处理者
基本信息	姓名、身份证号、电话号码、家庭地址等	当地公安机关，政府机构、交通运营者等
生物识别信息	人脸识别数据，指纹等	当地公安机关，政府机构、交通运营者等
位置大数据	位置信息等	当地公安机关，政府机构、交通运营者等
其他敏感信息	儿童信息、犯罪记录、车牌号等	当地公安机关，政府机构、交通运营者等
其他信息	手机信令、出行路径、个人喜好等	当地公安机关，政府机构、交通运营者等

【主要关切点】

智慧轨道交通应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
位置信息	对人流量和乘客位置定位、用户智能出行等	高风险
人脸识别、指纹识别等生物识别信息的处理	对进入轨交活动范围对自然人进行安防巡检，重点防控，对嫌疑人员进行身份核对等	高风险
儿童个人数据处理	进行轨交监控时，会将儿童信息与其他成人个人信息统一收集处理等	高风险
数据存储安全	智慧轨交系统收集的数据量大而复杂，其中包含大量的敏感数据，存储在数据保护安全能力程度不同的交通部门或当地政府机构等	高风险
位置数据共享	交通部门、公安机关，政府部门跨部门进行位置大数据共享等	高风险

3.2.9. 智慧机场

【应用场景概述】

智慧机场中包括航站楼、贵宾厅、停机坪、后勤保障中心等场所，多样化的场所对业务需要多样化，主要的业务应用场景有：**贵宾厅、航站楼提供视频娱乐服务**，本地 VR/视频热点内容，可以提供更好的高清、低时延的用户体验。VR 游戏服务器部署在边缘云，提供低时延高游戏画质的游戏服务。**机场的安防应用场景**，执法人员携带 AR 智能眼镜，实时拍摄所见画面，可以快速识别嫌疑人员。**安保机器人自动巡检**，按照预定路线行驶，实视传送视频到分析服务器，分析结果返回给执法人员，实现快速响应。**智能清洁**，人工进行机场清洁费时费力，操作人员通过 5G 网络控制机器人自动进行清洁，可节约人力资源，提高保洁效率。**自动驾驶**，机场车辆行驶线路相对固定，适合采用 5G-V2X（Vehicle to Everything）分级决策自动驾驶方案，接入迷你巴士、摆渡车、通勤车等适用场景的车辆，充分共用 5G 网络覆盖和智慧基础设施，降低运营成本，提升机场运营效率。

【数据处理简析】

智慧机场的数据处理参与者主要包括机场运营者、海关边检、安防公司、航空公司、银行、贵宾厅运营者、商铺、客运公司、快递公司、大数据平台供应商等。涉及的数据主体主要包括乘客、机场工作人员、接送机人员等。

智慧机场涉及的数据类型示例如下：

数据类别	数据类型	潜在的控制者/处理者
乘客基本信息	姓名、身份证号、航班号、座位号、人脸识别数据等	机场运营者、海关边检、航空公司、大数据平台供应商等
贵宾服务相关信息	姓名、身份证号、银行卡号、资产所在银行、资产达标情况、飞行里程、贵宾厅使用习惯、出行时间规律、餐饮爱好等	航空公司、银行、贵宾厅运营者、大数据平台供应商等
安检相关信息	姓名、身份证号、人脸识别数据、犯罪记录等	机场运营商者、海关边检、安防公司、航空公司大数据平台供应商等
其他信息	购物习惯、会员卡信息、出行信息、发件人姓名、地址、电话号码等	机场运营商者、航空公司、商铺、客运公司、快递公司、大数据平台供应商等

【主要关切点】

智慧机场应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
个人位置信息、个人轨迹信息	安防监控：全息影像及高清视频监控引发了必要性、利益平衡测试、权限管控、数据安全保障等隐私保护问题	高风险
人脸识别、声纹识别、指纹识别等生物识别信息	对工作人员进行考勤/打卡管理，进出港、边检等安防要求，对作业人员工作状态实时监控并智能分析；	高风险
用户个人画像	通过贵宾服务和购物习惯等信息形成用户画像 ,可向特定人群推送商业广告和定制化服务	高风险

【相关案例】

2018 年 10 月，英国隐私监管机构 (Information Commissioner's Office， ICO)对希思罗机场处以 12 万英镑罚款，起因是 2017 年 10 月某平民在伦敦大街上捡到一个含有机场敏感安全信息的 U 盘。ICO 处罚依据是 U 盘数据中 1%的个人信息 ,一段视频片段暴露了某欢迎队伍中 10 个人的详细信息 ,还有 12-50 位安全人员的信息。视频暴露的信息包括姓名、生日、登记号码、国籍、护照号及有效期、职位，还有手机号。事件发生后，希思罗机场雇佣了第三方专家监视暗网和互联网，找寻被泄露数据在网上售卖的迹象。虽然并未发现被泄露数据的售卖迹象，但 ICO 还是因机场隐私保护管理问题开出了罚单。

3.2.10.智慧金融

【应用场景概述】

5G 网络推动金融智能化发展，对金融领域的推动主要体现在前台服务优化，提升客户体验。后台集中化，提高效率，防风险。其主要应用场景包括：**智慧网点，**为了提升客户的体验，一方面使用自主迎宾机器人，让客户自助完成业务。另一方面使用智能监控，进行 AI 表情分析，识别客户标准，精准服务客户诉求，同时能够识别潜在危险，保障客户和银行安全。**远程虚拟银行**，客户使用 VR 设备，通过 5G 网络体验新型的虚拟银行办理业务，无需再进入银行，节约了客户的时间。**移动支付，**基于 5G+MEC 网络，可以满足云 VR 技术低时延高带宽的需求 ,为支付提供更丰富的决策数据以及更真实的场景 ,改变现有的支付体验。**惠普金融**，汇聚和挖掘海量个人数据和企业数据，避免信息不对称导致的风险，推动金融服务的均衡性。**财富管理**，基于 5G 网络，借助大数据分析，给每个客户精准画像，为客户提供千人千面的服务。

【数据处理简析】

5G 赋能金融领域，带来的最直接的变化是数据的海量收集和分析，在人们享受到更加快捷便利的金融服务的同时，也使得金融机构及支付机构等对个人可以进行更精准的画像，通过个人的习惯、财产状况等，精准地推荐相关金融服务和理财产品，人们的财产状况几乎透明。

数据类别	数据类型	潜在的控制者/处理者
个人财富数据	各类金融账号数据、交易数据、信用数据、财产数据以及关联的账户信息等	金融机构、金融服务软件提供商、信用机构等
生物识别数据	用于身份验证的指纹、声纹、面部识别数据等	金融机构、识别服务提供方等
消费数据	消费记录、交易流水、用户画像数据等	消费平台、支付机构、金融机构等

【主要关切点】

智慧金融应用隐私保护主要关切点及对应场景为：

隐私保护主要关切点	应用场景	风险等级
个人财产信息以及金融账号数据、生物识别数据属于敏感个人数据需要特殊保护	智能投顾、智慧银行等	高风险
财产数据、信用数据、消费数据相关联，可以对个人进行精准金融服务和产品推荐	智能投顾、智慧银行等	高风险

3.3. 5G 应用场景隐私保护启示

5G 与大数据、云计算、AI、物联网等技术充分融合，形成丰富的应用场景，在基于这些场景进行价值开发，促进经济社会发展、高效服务民生的同时，也需要高度关注隐私保护并付诸实施。主体角度，以体系化方式建设，明确方针，投入资源，成立团队，建立管理制度和实施指引，进行意识培训和技能教育，并辅以必要的工具、系统和技术，确保落地实施。实践角度，明确隐私保护的基本原则，做好隐私处理过程合规，管控高风险场景，聚焦新技术应用的隐私关切点。

3.3.1. 隐私保护基本原则

面向 5G 应用场景的各相关方协同中，应重点关注适用的法律法规，如中国《网络安全法》、《个人信息安全规范》、《数据安全管理办法》、《个人信息出境安全评估办法》、《儿童个人信息保护规定》，欧洲 GDPR，美国 CCPA 等。隐私保护基本原则主要包括：

- **合法、公正和透明：**以合法的、公正的和透明的方式来处理个人数据。
- **目的限制：**个人数据的收集具有具体的、清晰的和正当的目的，对个人数据的处理不应当违反或超出初始目的。
- **数据最小化：**为实现数据处理目的而处理的个人数据，是适当、相关且必要的。
- **准确性：**个人数据应当是准确的，采取合理措施及时清除或更正不准确的个人数据。
- **限期储存：**个人数据储存时间不得超过实现处理目的所必需的时间，到期及时清除。
- **数据完整性与保密性：**个人数据处理过程中采取合理的措施确保安全，避免数据被未授权处理，避免数据发生泄露。
- **可问责性：**有责任遵守以上要求，并提供遵守证明。

3.3.2. 数据处理过程要求

面向 5G 应用场景的各相关方协同中，应重点关注隐私数据处理的全生命周期的管理。如以透明和信任为目标，告知数据处理的目的、方式、范围，采用包括去标识化在内的多重技术手段，保护用户隐私安全。建立配套的用户行权响应机制、数据安全应急响应机制和审查审计制度。处理过程要求主要包括：

- **收集：**满足合法性、最小必要等原则，应由数据主体自主选择，给出授权同意。
- **存储：**关注存储安全，数据存储应优先做去标识化处理，保存时间满足最小化要求，到期清除。
- **使用：**使用权限满足职责必需和最小授权原则，所使用的数据和使用范围应满足最小必要原则，不超出初始授权目的和范围使用。自动化决策等可能导致给数据主体造成显著影响的处理活动，进行隐私影响评估。
- **删除：**建立数据存储管理机制，到期后及时清除数据。
- **对外提供**：隐私数据涉及向外部实体提供时，如委托处理、共享、转让、公开披露等情形，需要事前进行隐私影响评估，确保接收方具备相应的隐私合规能力。通过协议或合同等方式，约定接收方的隐私合规责任与义务，并对其处理进行评估。
- **数据出境**：规定适用时（如大规模、高敏感隐私数据出境）事前报监管机构审批。进行隐私影响评估，通过协议或合同等方式约定接收方的责任与义务，对其数据处理情况进行审计。
- **数据主体权利保障机制：**建立有效机制。及时响应主体的行权请求。
- **隐私保护设计：**产品和服务方案设计之初嵌入隐私保护的需求，综合使用技术、管理、和物理性等多种措施，以最优方式实现隐私保护目标，保证隐私信息全生命周期的安全与合规。
- **隐私安全事件响应**：建立数据安全事件处理流程，制定应急预案、组织人员培训，定期进行演练。
- **过程审查与定期审计：**建立审查与审计制度，确保隐私合规落地实施，提升合规成熟度。

3.3.3. 隐私保护高敏感数据处理

面向 5G 应用场景的各相关方协同中，应重点关注高风险敏感数据的应用和隐私合规问题。常见的高风险敏感数据主要包括：

3.3.3.1. 精确位置信息

【概述】 精确位置信息，移动数据或行踪轨迹信息，是描述设备和人员的位置和如何随时间在空间中移动的信息。精确位置信息既直接包含住址、办公场所等隐私信息，又隐含了用户的生活习惯、个人爱好、健康状况、社会地位等其他敏感信息。位置信息的不当使用，会给用户隐私带来严重威胁。

【立法执法】精确位置信息在法律上属于敏感数据。在大多数司法管辖区，位置数据被视为受更高保护的一类特殊数据，需要明示同意和更高的安全标准。

- **中国**：位置信息“运动轨迹”写入了刑法所保护的公民个人信息之中，明确非法获取、收集或向他人提供运动轨迹信息达到 50 条提上便可定罪量刑：违法获取、出售、提供公民个人位置信息的行为，依照规定最高可以处一百万元的罚款。
- **欧洲：**在欧盟，获取位置数据通常受到电信保密的监管，受到《电子隐私指令》（ePrivacy Directive）的严格规定，该指令要求个人同意(只有极少数例外)。部分成员国对位置数据也出台了相关要求和指南。2019 年 7 月，法国国家信息与自由委员会(Commission Nationale de l'information et des Libertes，CNIL）在 Cookies 和其他追踪设置的使用指南中规定，在获得同意之前，运营商不得在用户终端中读取或写入任何数据。
- **美国：**美国联邦贸易委员会（FTC）长期以来要求对位置数据要求需要获得肯定的同意。 美国各州对位置信息的保护也提上了日程，纽约市正在制定一项法案，以禁止手机和 App 企业在未经消费者同意的情况下共享其收集到的用户定位数据。

【隐私保护合规遵从】在使用位置数据时，除了必须遵守的隐私保护基本原则外，还应尽可能的对数据进行去标识化或匿名化处理，将处理数据控制在最小必要的范围内。此外，存在位置信息对外提供时，应通过隐私政策明确说明信息共享情况，获取明示同意。当因公共利益使用精确位置信息时，如在前期疫情防控中，在获取相关授权的情况下收集公民位置信息，仍应考虑在收集时向公民告知信息使用的目的和范围、存储时间和到期处置方案等信息。如果初始目的是用于疫情跟踪，疫情防控结束后，位置信息就不应被继续保留，用于其他用途。

【相关案例】美联社一起针对 Google 的调查指出 Google 在用户选择关闭定位服务或者关闭位置历史记录的情形下，仍然采集用户位置标记，涉嫌滥用用户的个人数据。例如，Google 地图应用会提醒用户，需要用户允许使用地理位置信息进行导航服务。如果用户同意，Google 地图便会在“时间轴”中为用户显示该历史记录，即用户的日常活动地理位置信息。Google 在 dashboard 中为用户提供了关闭位置记录的选项，声称关闭位置记录后，Google 将不再存储的用户的地理位置信息。而事实上美联社的调查发现，即使

关闭了位置记录，某些 Google 应用会在不经用户允许的情况下自动存储带有时间戳的地理位置数据。此外，即使所有的位置服务都已关闭，Google 还通过收集附近手机信号塔的地址来跟踪 Android 用户的位置。

3.3.3.2. 用户精准画像

【概述】在 5G 各类应用场景中，用户精准画像与个性化推荐已经越来越普遍，越来越多的企业在收集个人的浏览记录、购买记录、交易方式等信息，并依据这些信息来分析用户行为，对用户进行精准画像和营销。用户画像（User Profiling）是指用户信息标签化，通过收集与分析消费者社会属性、生活习惯、消费行为等信息之后，抽象出一个用户的全貌。用户画像的焦点工作就是为用户打标签，而一个标签通常是人为规定的高度精炼的个人特征标识，如年龄、性别、地域、用户偏好等，最后将用户的所有标签综合勾勒出该用户的立体画像。用户画像的个人信息标签化与个性化推荐对用户隐私保护提出了挑战。

【立法执法】对于用户画像的法律规制，全球不同国家和地区采取了不同的规制方式。

- **中国：**目前并没有直接的法律规定，对于网站使用 Cookie 等技术收集用户的行为信息，并利用此类信息进行个性化推荐并没有明确禁止。《电子商务法》第 18 条规定：“电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。”但这一规定并未直接规定网站收集与处理个人消费行为信息是否合法，对于这一规定应当如何进行解读，目前也还存在争议。
- **欧洲：**欧盟 GDPR 对用户画像进行了专门规制，特别是对数据控制者的用户画像处理行为施加了多项义务，并赋予数据主体多项数据权利，来降低、消除隐私保护风险和影响。
- **美国**：在联邦层面，美国没有对网站利用消费者行为进行用户画像与个性化推荐的法律规制。但美国联邦贸易委员会（FTC）在 1998 年发布了一份报告，对商业网站披露用户隐私的做法进行了全面审查，并制定了公平信息实践原则 FIP。 根据 FIP 原则，在收集个人信息时，网站需要向消费者提供关于其信息实践的清晰和明显的通知，包括他们收集什么信息、他们如何收集信息（例如 Cookie）、如何使用它、如何向消费者提供选择、可访问性与安全，是否向其他实体披露收集的信息，以及其他实体是否正在通过网站收集信息。在公平信息实践原则的指引下，联邦贸易委员会采取了基于透明性的监管原则，即当网站违反隐私政策而收集个人信息，或者网站对个人信息收集不透明的情形下，联邦贸易委员会可以要求网站遵守信息收集透明的要求。

【隐私保护合规遵从】在基于用户画像目的进行数据收集和分析、判断或预测过程中，除了遵守的隐私保护基本原则外，还需要特别关注数据收集应

- **告知同意要求：**给予用户自主选择的权利。如网站利用 Flash Cookie、Ever Cookie、Fingerprint 等技术收集用户行为数据时，应对用户进行更为明确的告知，只有在用户明确选择同意加入的情况下方可收集。
- **风险规制原则：**避免使用某些可能给用户带来困扰的敏感数据，即使个人授权收集其所有行为信息，

也应当限制对此类敏感数据进行精准画像。

【相关案例】2018 年初某公司推出年度账单回顾功能。人们就发现，在年度账单的首页左下方利用小字体、接近背景色和默认勾选同意，让相当多的用户在不知情的情况下“被同意”。签署了这份极易被用户忽略的《服务协议》，意味着其可以对用户的全部信息进行分析画像并将分析结果推送给合作机构。XX 公司当日向公众致歉，并调整页面，取消默认勾选。案例中该公司使用小字体、接近背景色和默认勾选同意等方式，诱导用户忽略提示，侵犯了用户的知情同意权和选择权，违反了《消费者权益保护法》和《个人信息安全规范》等法规标准的要求。

3.3.3.3. 生物识别数据

【概述】生物识别数据（Biometric Data），又称生物识别特征，是指对自然人身体、生理或行为进行一定的技术处理所得的能够识别特定自然人的信息。常见的身体、生理信息包括指纹信息、掌纹信息、面部识别信息、声纹信息、虹膜信息、基因信息、血管分布信息等。行为特征则包括手写签名、键盘输入、特定的步行或说话方式等。生物识别数据具有唯一性，一旦发生泄露、非法提供或被滥用，将极大危害数据主体的人身和财产安全。

生物识别数据因其便捷、快速等特点被广泛应用于社交、消费、交通、金融等领域，具体应用场景包括电子支付、门禁、考勤、手机解锁等。5G 应用场景中很多可能涉及到生物识别数据的处理，如智能安防，穿戴设别，远程医疗，智慧轨交等。需要结合数据利用目的和方式综合判断是否构成生物特征数据的处理，从以下要点考虑：（1）数据性质：与自然人的身体、生理或行为特征有关的数据；（2）方法和处理方式：数据源于特定的技术处理；（3）处理的目的：数据必须用于唯一识别自然人的目的。

【立法执法】各国对于生物识别数据的法律规制差异性较大。多数国家和地区的法律法规将生物识别数据视为敏感数据，严格限制生物识别数据的使用。

- **中国：**《GB/T 35273-2020 个人信息安全规范》将生物识别数据定义为个人敏感信息，要求收集、使用此类信息，应当取得明示同意。《信息技术 安全技术 生物特征识别信息的保护要求（征求意见稿）》对生物识别数据的保护和管理作出了详细规定。《信息安全技术 个人信息安全工程指南（征求意见稿）》要求在生物识别数据用于身份鉴定时，应采取不可逆向保护。《信息安全技术 个人信息安全影响评估指南（征求意见稿）》要求对生物识别应用进行影响评估，并针对生物识别数据的收集、使用、存储、销毁全生命周期提出合规要求。
- **欧洲：GDPR** 第 9 条对包括生物识别数据在内的特殊类型个人数据的处理加以严格限制，采取一般性禁止处理的立场，并在第 9 条第 4 款对基因数据、生物识别数据或健康数据的处理规定了成员国可以维持或引入更进一步的限制条件。
- **美国：**虽然美国暂无专门的联邦法律规范生物识别数据的收集和使用，但《联邦联贸易委员会法》第 5 条赋予了联邦贸易委员会（FTC）广泛的执法权，以保护消费者免受不公平和欺骗性贸易行为的影响。FTC 可以对从事涉及生物识别数据的不公平或欺骗性贸易行为的商业组织采取执法行动。

目前州层面，共有 7 个州或城市制定了与生物识别数据相关的法律，分别是伊利诺伊州、德克萨斯州、华盛顿州、马萨诸塞州萨默维尔市、俄勒冈州和新汉普郡以及加利福尼亚州旧金山市。伊利诺伊州于 2008 年已经通过了《生物信息隐私法案》，德克萨斯州在 2009 年通过了《采集和使用生物识别数据法》，其他州也在考虑出台相似立法，美国在人脸识别技术应用方面正逐渐趋于保守，例如旧金山市和萨默维尔市禁止政府使用面部识别技术。

【隐私保护合规遵从】生物识别数据应用场景广阔，在国内生物识别数据保护法律规制相对缺失的情况下，通过企业内部行为规范、行业标准和行业协会的监督，实现收集、处理生物识别数据的企业的自我规范、自我约束和自我完善不失为目前可取的方式。

生物识别数据处理除了必须遵守的隐私保护基本原则外，需重点关注：

- **最小化**：对于人脸识别等生物识别数据的使用应持谨慎态度，只有在其他方式无法达到业务目的时，才可以考虑使用此类数据，否则将存在较高的合规风险。应严格限制在社交或消费等商业用途上过度使用生物识别数据。
- **明示同意**：通过清晰、易懂的且易于访问的隐私说明，获取数据主体的明示同意。
- **隐私影响评估**：事前进行隐私影响评估，对潜在的风险制定处置措施。
- **隐私保护设计**：涉及生物识别数据处理的产品/服务，应从设计源头系统地考虑隐私保护方案，增强透明性，最大程度降低违规风险。

【相关案例】2019 年 8 月 20 日，瑞典一高中使用人脸识别技术来记录学生的上课考勤被认定违反欧洲《通用数据保护条例》。国内南京某高校在校门、教室、图书馆等处安装人脸识别系统用于门禁、考勤以及监控记录，学生发呆、玩手机都能被感知到，涉嫌侵犯学生隐私引发舆论热议。2019 年 9 月，国内某网络商城被发现有商家公开售卖人脸数据，数量高达 17 万条。

3.3.3.4. 儿童数据处理

【概述】根据《2019 年全国未成年人互联网使用情况研究报告》，中国未成年网民规模已达到 1.75 亿。如此庞大的儿童网民的基数，加之儿童的隐私保护意识更加不足等原因，不法分子利用网络侵害儿童合法权益，危害儿童身心健康的案例屡见不鲜。

【立法执法】全球范围许多国家都出台了有关保护儿童的网络权益的法规。在 5G 应用场景中很多场景可能会涉及到儿童数据的处理，如智慧校园，可穿戴设备等，儿童隐私保护是无法忽视的重要问题。

- **中国**：我国《儿童个人信息网络保护规定》已于 2019 年 10 月 1 日起生效，在《网络安全法》等一般规则的基础上，针对儿童这一特殊保护主体，规定了更为严格的信息保护义务，赋予儿童及其监护人更为全面、更为有力的权利。
- **欧洲：**欧洲《通用数据保护条例》（GDPR）对儿童个人信息的保护提出了更高的要求。GDPR 第 8 条规定，在收集或处理不满 16 周岁儿童的个人数据之前，需要取得其父母的同意或授权，成员国可以设定更低的年龄界限，但不能低于 13 周岁。GDPR 序言第 38 条指出儿童应避免营销和数字

画像等数据处理活动。序言第 71 条则特别表明基于数字画像的自动决策不应包括儿童。

- **美国**：美国联邦贸易委员会（FTC）频繁地依据《儿童网络隐私保护法》（Children's Online Privacy Protection Act，COPPA）作出调查和指控，和解数额也越来越大，显示出美国对于儿童个人数据的重视程度和保护力度都在不断增强。

【隐私保护合规遵从】儿童的特殊性决定了对儿童个人信息和隐私保护应当有所区分，并通过上文提到的立法和实践对各组织和企业儿童个人数据处理合规提供指引。对于企业或组织来说，在处理儿童个人数据时，除了必须遵守的隐私保护基本原则外，还应重点关注：

- **告知同意**：针对以儿童为主要对象的产品或服务，应以高标准设计收集、使用的授权同意机制，包括充分告知收集处理规则、获取儿童监护人的明示授权同意，识别监护关系和监护人授权同意的有效性，并通过技术措施满足业务功能的逐一授权。从自身业务模式特点入手，设计有效的识别及身份认证机制，确保信息处理活动具备合法依据。
- **数据安全**：在收集儿童个人信息之前，相应当针对数据处理活动进行数据保护影响评估，并采取有效措施降低风险，充分保障数据安全。
- **遵从教育行业标准**：根据近两年"互联网+教育"的立法及监管安排，对于教育类产品，如远程教育 App，应对标教育 App 的最新监管要求，完善网络安全及个人信息保护制度并优化相应技术措施，满足教育行业的监管要求。
- **儿童用户分类管理**：对于面向全年龄段用户的产品及服务可以设置儿童模式，并将相应儿童个人信息分割独立存储，以降低儿童个人信息保护合规风险。

【相关案例】2019 年 2 月， FTC 与 Tik Tok(抖音国际版)就其违反 COPPA 法案达成和解，Tik Tok 支付 570 万美元的罚款。FTC 对其指控包括：未能在其网站上显示在线收集的儿童信息、如何使用信息、如何披露的通知、未能直接通知家长、在收集儿童的个人信息之前未能得到父母的同意等。2019 年 9 月 4 日，FTC 因 YouTube 违反 COPPA 法案，向谷歌公司开出了 1.7 亿美元的罚款，这也是 FTC 根据 COPPA 法案执法所开出的最大罚单。FTC 对 YouTube 的执法依据包括：未能提供清晰的、容易理解的、完整的收集儿童信息的隐私政策、在收集、使用、分享儿童个人信息前，未能获得可核实的父母同意等。

3.3.4. 新技术应用的隐私关切

面向 5G 应用场景的各相关方协同中，新技术应用涉及到一系列隐私保护关切，可参考合规建议。

新技术	主要隐私关切点	隐私合规建议
物联网	高维数据（特别是个人敏感数据）多渠道采集； 实时数据共享和交换； 安全隐患多，易引发数据泄露；	遵守隐私保护合规的基本原则 加强物联网的安全管理，提高设备和数据安全防护能力 采用增强隐私保护能力的设计和技术，如同态加密、安全多方计算、K-匿名等 加强对隐私合规的审查审计
云计算	数据开放和共享合规风险；	遵守隐私保护合规的基本原则

	数据泄露风险；	采用隐私保护技术，如同态加密、安全多方计算、联邦学习、K-匿名、差分隐私、密文检索、外包计算、区块链、ABAC/PBAC 访问控制等 加强对开放和共享的管控 加强对隐私合规的审查审计
大数据	数据发布去标识化； 大数据分析和画像； 自动化识别、推断与决策； 数据泄露后果严重；	遵守隐私保护合规的基本原则 采用隐私保护技术，如同态加密、安全多方计算、联邦学习、K-匿名、差分隐私、密文检索、外包计算、区块链、ABAC/PBAC 访问控制等 加强对开放和共享的管控 加强对隐私合规的审查审计
人工智能	实施数据获取，深度学习； 超强的数据整合、分析和画像能力； 信息获取更加隐蔽； 侵犯隐私后果更严重；	遵守隐私保护合规的基本原则和 AI 伦理 采用隐私保护技术，如联邦学习等 加强对隐私合规的审查审计

结语

数字经济正通过不断升级的网络基础设施与智能设备等信息工具，催化互联网、云计算、人工智能、区块链、物联网等信息技术的融合发展。人类处理大数据的数量、质量和速度的能力不断增强 ,推动社会经济形态由工业经济向数字化和智能化转变 ,极大的降低社会交易成本，提高产品、企业、产业附加值，推动社会生产力快速发展，同时也为发展中国家后来居上实现超越性发展提供可能。

未来，随着 5G 通信技术对社会生产生活各领域的进一步赋能，必将推动加快产业融合应用创新，成为社会经济数字化和智能化的加速引擎。在向数字经济转型升级的过程中，数据成为与劳动、资本、土地、知识、技术、管理等并列的核心生产要素，在经济发展中的重要地位日益凸显。对数据特别是个人数据的合规应用，已经成为社会广泛关注的问题。

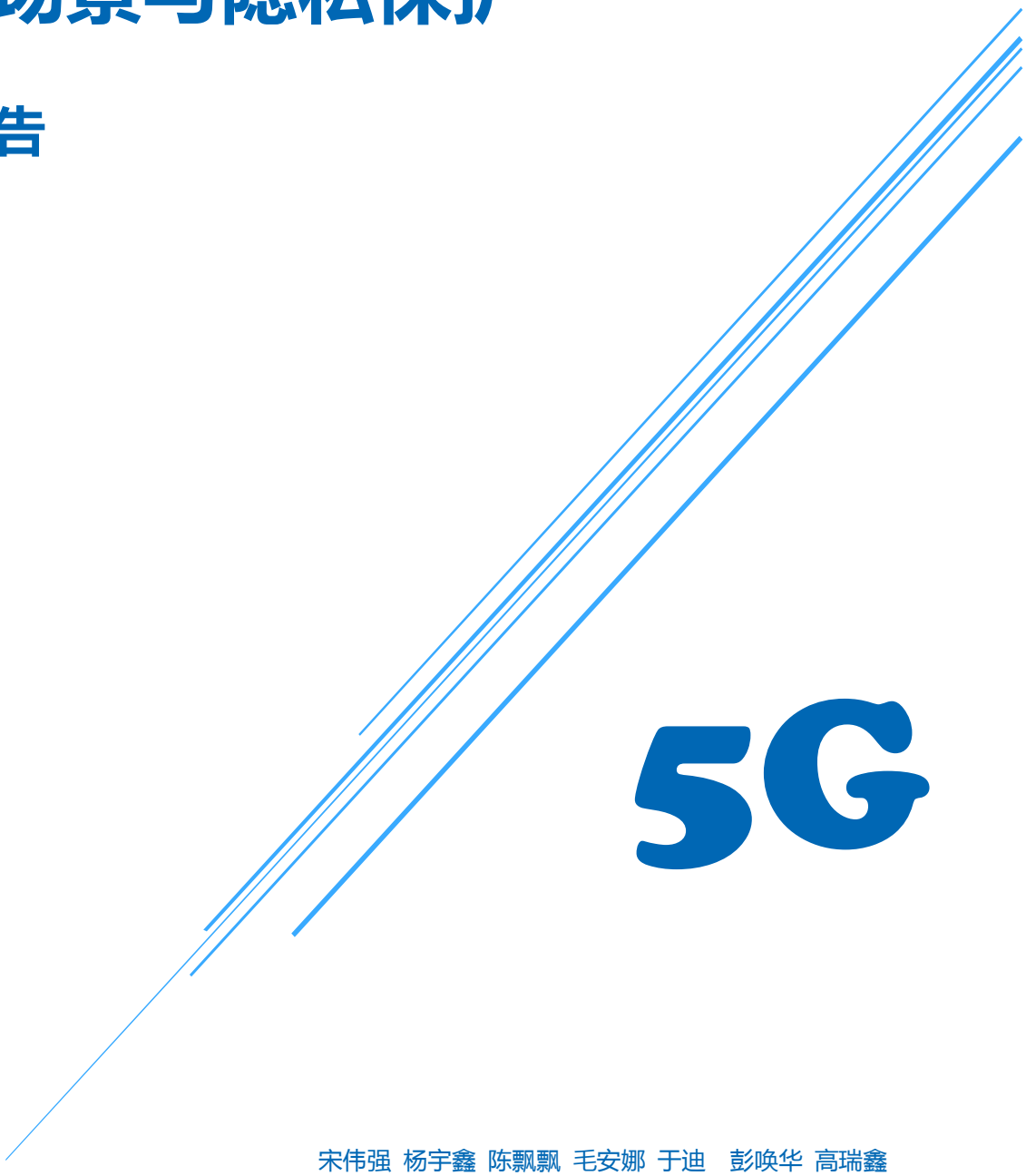
为此，全球各国都在探索如何在海量数据的隐私保护与开放共享之间保持平衡，并最大限度的发挥数据的潜在价值。欧盟 GDPR、美国 CCPA、中国的《网络安全法》都在对个人数据的合规应用给出各自方案。

5G 无疑将为我们开启新的开端。随着隐私保护相关的法律法规、标准规范、技术方案和行业实践的不断完善成熟，公民隐私保护意识的觉醒和跃升，社会对隐私保护的日益关注，各行各业对隐私合规实质投入，相信所面临的挑战和疑难都将得到妥善的解决。

一个推崇科技，尊重隐私的社会生态体代表着未来，而这需要包括 5G 产业链所有相关方在内的全社会的共同努力，积极开展隐私保护实践探索，共建可信任的开放、透明、合规、安全的 5G 应用生态。我们相信，随着 5G、物联网、数据中心等纳入国家信息基础设施范畴，“新基建”启航也必将加速数据合规建设进程，助推万物互联时代的全面到来。

应用场景与隐私保护

研究报告



宋伟强 杨宇鑫 陈飘飘 毛安娜 于迪 彭唤华 高瑞鑫
曲绅维 陈正伟 汪竞飞 王红欣 陈成标 谷布