



刷脸支付安全吗

□ 唐林鑫 孙小雨

刷脸支付，是结合人工智能、机器学习、三维结构光、在线支付等技术实现的新型支付方式，用户无需携带任何设备，通过人脸识别（即“刷脸”）即能完成支付。与传统支付手段相比，刷脸支付在便捷性和推广成本方面具有明显优势，但其潜在的风险也颇受关注。随着刷脸支付的大规模商业化推广，通过何种途径防范刷脸支付的隐私风险，消除伴随个人生物识别信息的潜在隐患，使刷脸支付能在保障用户隐私安全的情况下尽可能地提升社会效益，无疑是当下值得思考的问题。

（一）

相较于传统支付手段，刷脸支付具备五大优势。

其一，革新支付体验。刷脸支付是对既有支付方式的全新变革，用户无需携带现金或银行卡，也无需扫描二维码或牢记各类账号、密码，仅需摄像头刷脸即可完成支付。在线上场景中，用户不再需要反复输入密码或口令；在线下场景中，用户甚至只需在收银机前“露面”，即可瞬间实现“闪付”。相比之下，输入6位密码平均至少3秒左右，指纹支付大约耗时1秒，刷脸支付却仅需0.3秒。

其二，突破支付障碍。老年人等群体较少使用电子设备，往往赶不上数字化转型的速度。对这部分人而言，刷脸支付明显比刷卡、扫码等支付方式更加友好，因其突破了支付介质，真正实现了“零载体无感支付”。

其三，消除获客成本。在刷脸支付语境中，手机前置摄像头就能完成用户的核验和特征录入；过去必须在营业时间亲自到银行柜台办理的开户手续，现在可以在任何地点、任何时段迅速完成。基于远程刷脸的在线贷款和理财业务，在优化客户体验的同时，大大提升了金融服务效率，获得了更多客户增量。

其四，提升推广效率。传统的指纹、声纹、虹膜等生物识别手段对用

户配合度和设备性能要求较高，商家的推广应用成本不菲。人脸识别并不需要特别的硬件或设备，高于一定分辨率的手机摄像头即可满足要求。配合国家身份证数据库，信息和身份的比对无需用户额外提供身份验证照片，所有用户在使用时均为零成本参与。技术手段无比“接地气”，令刷脸支付比其他生物识别技术更容易大规模推广。

其五，拓展场景边界。现金、刷卡、扫码等支付手段几乎不具备扩展性，刷脸支付则不然。结合购买现状和已掌握的用户信息，商家可通过可视屏幕同支付者交互，或精准推送广告，或推荐会员制服务等，极大地拓展了支付服务的边界，带来更多商业想象空间。

（二）

虽有上述优势，刷脸支付同样存在三方面的安全风险。

其一，人脸识别系统可被破解，隐私侵害可能因此向财产侵害蔓延。人脸识别的不同技术手段，均有被破解的可能：基于活体识别的人脸识别技术，可能被制作精良、细节逼真的面具破解；基于实时重建的人脸识别技术，则可能被3D建模制作出的仿真人像破解。例如，曾有一名小学生用打印照片替代真人刷脸，骗过小区智能快递柜，取出他人货件；某团伙曾非法搜集公民身份信息，使用软件合成3D头像突破支付软件人脸识别认证，从中牟利数万元。人脸识别系统之所以屡遭破解，主要是因为窃取人脸信息比窃取数字密码、套取指纹信息更为容易：人脸信息完全暴露在外，通过多角度拍照即可取得，既不像储存在人脑中的数字密码一样无从下手，也不像指纹信息那般难以采集。

其二，人脸特征具备不稳定性，刷脸支付的稳定性因此也受到影响。同数字或图片密码、指纹或虹膜等生物特征相比，人的脸部特征并非一成不变。随着时间的推移，人的面部外

观会逐渐发生改变，青少年的面部变化尤其明显，事故、整容、过敏以及大幅增重或减肥，都会造成当事人的容貌变化，致使系统无法识别。此外，收容的变化在一定程度上会导致系统难以比对关键点，戴墨镜、口罩、装饰品时，亦是如此。面对人脸识别系统的摄像头时，俯仰幅度较大、左右侧面较多、发型变化较大，甚至表露出丰富的表情，都会降低系统识别的准确度。受制于人脸识别系统的不稳定性，刷脸支付系统的稳定性也无法保证。

其三，形式审查、把关不严，直接影响用户资金使用安全。在签订刷脸支付用户协议阶段，用户并不需要提交自己的照片。有资质的刷脸支付机构在进行身份核实时，通常是向全国公民身份证号码查询服务中心提出申请，将摄像头中的人脸信息同库中的照片进行比对，此外，也会参考人民银行和公安部联网核查系统中的照片留档。但是，无论作为参考基准的身份照片从何而来，照片更新速度慢、像素有限等情况，都会成为制约人脸识别系统准确性的因素，而多个源头的比对和验证，又必然增加通信成本。由于用户的资金同人脸验证相绑定，验证环节的把关不严将给掌握他人人脸信息的不法分子以可乘之机，最终给用户资金带来安全风险。

（三）

刷脸支付具有远高于传统支付方式的技术门槛，实践中，银行和金融机构通常无力完全自主研发一整套的刷脸支付方案，一般是通过“第三方硬件+自有算法”的方式，构建自身的刷脸支付体系。近年来，通过“提升算法响应精度”“内嵌支付环境检测”等技术手段提升刷脸支付安全性，但是，技术方案更多地聚焦于算法和设备的识别准确度和支付稳定性，无法防范人脸识别技术的非合理使用，也不能确保人脸信息的传输和储存安全，更难以杜绝基于刷脸支付的后手

自动化决策行为。因此，作为对技术手段的补充，应在法律维度构建贯穿支付流程的外部专家审查体系。

面对具体的支付场景，由业界专家主导的外部审查体系应内嵌四组审查机制。其一是正当目的审查，即考察刷脸支付中人脸信息的搜集是否满足《人脸识别标准》第6条“持续告知数据主体验证目的”的规范性要求，以及身份识别目的之外的“合理商业目的”是否满足个人信息保护法第6条“与处理目的直接相关，采取对个人权益影响最小”的够用原则。其二是信息安全审查，即考察在提供刷脸支付服务时，信息处理主体是否充分考虑了个人生物识别信息的敏感性，并采取与之匹配的安全保护措施，将业界“加强数据资源整合和安全保护”的共同呼吁落实到位。其三是权利保障审查，即考察在推广刷脸支付时，信息处理主体是否采取相应措施保障信息主体的知情权、拒绝权以及获解释权等，将刷脸支付的潜在风险一一告知，是否为信息主体提供了刷脸支付之外的其他支付手段，且未对其他支付手段设置毫无必要的使用障碍。其四是歧视鉴别审查，即综合信息主体的身份及信息处理主体的数据耦合机制，判断刷脸支付之后的自动化决策，是否有可能对信息主体的平等权以及思想与行为自由带来风险，是否有可能在远期对信息主体造成不良影响。外部审查的标准和强度，应视具体应用场景而定。可以根据实际应用的场景划分，对人脸验证、人脸辨识、人脸分析等场景分别进行低强度、中强度和高强度的外部审查。在不涉及后手自动化决策的人脸验证和人脸辨识场景，可以完全豁免歧视鉴别测试，并相应降低正当目的测试的强度。



如何防范政府数据开放的安全风险

□ 吴茵

当前，人类社会正在进入数字经济时代，数据已经成为重要的生产要素。政府数据中蕴含着巨大的价值，如何在更好维护数据安全情况下，挖掘和释放政府数据的价值，是当前经济社会发展面临的重要议题。政府部门聚集了海量数据，利用好政府数据，不仅能够为经济增长注入发展新动能，也能加快整个社会的数字化、智能化转型步伐。但是，我们也必须看到，如何处理数据隐私保护和数据开放共享之间的矛盾已成为数据使用过程中亟须解决的问题，需要权衡利弊，统筹推进。政府数据开放面临着隐私安全、行政安全、经济安全、国家安全等方面风险和挑战。如何在准确认识政府数据开放中的安全风险、有效规避风险情况下，发挥好政府数据开放的作用，成为关注的热点问题。

政府数据开放存在多方面的风险。一是隐私安全风险。政府数据具有样本量大、敏感度高、聚集性强等突出特点，极易成为隐私数据泄露的高发地。二是行政安全风险。政府数据开放会让政府决策、监督和服务等面对新的挑战。政府数据采集如果范围不够全面，没有好的标准、制度和工具，就会对数据质量产生严重影响，而依托低质量数据进行决策，会误导政策制定。三是经济安全风险。在政府采集数据的过程中，可能会涉及部分企业数据，如果数据泄露，将给企业带来损失。政府数据开放过程中，如果不能采取有效的规避措施，可能会导致平台垄断，如果利用具有公共性的政府数据，谋取超额垄断收益，会给政府带来监管困难。四是国家安全风险。政府数据开放的过程中，不同数据集如果被大量泄露，就会引发国家安全风险。其中，国防、军事信息安全风险尤为突出。

完善数据隐私保护和脱敏处理机制。数据脱敏指的是在信息质量得以保障的情况下，对数据中涉及个人隐私和敏感信息进行数据变形处理。第一，政府数据开放中，规范去隐私化、去敏感化数据处理流程，健全数据销毁和遗忘机制。制定信息安全规则尽可能保护无法更改的个人生物特征数据。对个人信息区分敏感部分和非敏感部分，对指纹、虹膜、人脸等个人敏感信息强制收集并进行严格限制。第二，明确数据开放相关者的责任，对隐私信息安全保护制定统一的规范。政府部门在数据安全和隐私保护方面实现相互协同、相互监督。提高数据泄露的惩治成本，规范数据流通合规审查和伦理审视。第三，不能无限扩大数据脱敏范围，脱敏强度不宜过高。数据脱敏中，要尽量做到准确细致甄别，技术路径不能做到极致，否则就会对数据质量和使用效率产生较大影响，脱敏成本过高。数据脱敏遵循基本原理，其对数据安全性的作用不能过度夸大，也要重视其他数据安全防护措施。

推进政务数据安全保障制度建设。第一，提高政务数据标准化、结构化和体系化建设。以数据的全样本形态、全生命周期、全流通环节覆盖为目标，整体性推进数据安全配套保护制度，形成数据安全闭环管理，在使用中迭代升级、不断提升数据安全保障能力。避免数据低质量和碎片化，以高质量政务数据辅助政府决策。第二，政府提升自身运行效率，以更加敏捷的组织形态和运行方式来应对数字经济时代的挑战。加强政府层级间、条块间、地域间防范数据安全风险的协同性。在开放多样化的政府数据中，摸清数据底数，了解部门间数据共享情况，完善数据安全调用制度，有效规避数据流转中的安全风险。第三，维护公平的市场秩序，注意对企业商业秘密的保护，保持市场监管的公平性，防止垄断巨头侵害消费者权益。第四，以公众需求为导向，提升数字化治理能力。随着数字政府建设步伐加速，社会公众更加了解政府运行状况，必然会对政务服务的整体性和敏捷性产生更高要求。从需求侧实际需要出发，推进政府数据开放的程度和水平，借助社会力量进行数据安全监管。各地政府要着力推进政府数据统一开放平台建设，让政府数据公开使用更加便捷、整体和高效。

提高政府数据公开的透明保障水平。推进高水平科技自立自强，掌握数据、网络核心技术和关键技术。第一，加快数据安全和隐私保护的新技术研发进展，如推进计算和存储分离的数据沙盒、多数据中



心节点协同的联邦学习等具有应用前景的新技术研发，提升数据安全和隐私保护的技术水平。第二，突出企业在数字安全保护技术研发中的主体地位，让骨干企业真正发挥支撑作用，利用市场机制做好知识产权保护和数据风险防范。第三，让政府数据成为数字经济时代新的基础设施，发挥政府数据的公共性，提升基础数据的质量，推进基于政府数据开放的相关学术研究和市场开发，让政府数据创造更大经济社会效益。第四，政府提高数据安全监管技术能力，逐步推进以数字化、智能化为特点的新监管工具和新监管手段，有效履行监督职能。政府、企业与社会协力推进数据安全维护，在合作中带动整个社会的数据化转型步伐。

筑牢数据开放的安全屏障。在政府数据开放过程中，把维护国防安全数据安全，作为维护政府数据安全的底线。第一，健全全过程数据安全监测体系，对高度敏感数据跨境流动进行有效监测。第二，增强人人关心的全民数据安全意识，培养人人预防的数据安全素养，引导群众树立科学的总体国家安全观。第三，数据安全关系到全人类的福祉，是各国关注的共同议题。构建数据安全机制需要各国共同维护。

当前，我国各地政府数据开放和共享平台正在如火如荼的建设当中。数据安全防护和数据开放共享之间需要权衡利弊，统筹推进，在充分认识政府数据开放风险的情况下，强化个人隐私安全保护，推进政府数智化转型，保护市场经济秩序，切实维护国家安全，大力推进政府数据开放，推进经济社会数字化、智能化转型。



数字经济平台如何实现价值创造

□ 李玉梅

当前，我国进入数字经济时代，数字经济通过数字的产业化、产业的数字化直接或间接利用数据来引导资源发挥作用，推动生产力发展。数字经济的发展催生了平台经济。平台经济是以信息技术为基础，以网络协同、开放平台为支撑，以数据驱动为重要组成部分的新经济模式。通过整合、归纳、分析、预测平台受众的数据信息，为消费者、企业、政府提供价值连接，推动各方形成有机互补的整体。平台经济具有的数据要素、数字技术优势，也为我推动产业结构优化升级带来新的机遇。数字经济时代，云计算、大数据等数字技术以及数字化平台的广泛应用推动了平台经济的发展。

在数字经济时代背景下，平台为经营主体提供了更具规模、更有秩序的交易场所，促进了主体之间的供需流动。数字经济平台构建起一个联动交互的经济形态，极大地改变了各类要素生产及创造价值的方式，对当前的资源调配和经济组织模式起到了重要作用。

（一）

实际应用中，数字经济平台主要通过规模效应以及提高撮合效率这两种机制来创造价值。其一，数字经济平台通过突破时空限制，拓宽交易范围，把更多的供需信息融入平台交易之中。这一对外扩张引起了规模效应，即因规模增大所带来的经济效益提高。一方面，当平台规模达到一定

水平后，其产业链趋于完整，资源配置与再生效率也逐新提高，这些经营主体与生产要素的有机结合带来的边际效益增加，产生了“1+1>2”的效应，达到盈利增长；另一方面，随着市场规模的扩大，其所带来的规模效应降低了数字经济平台的交易成本，使参与者获益。其二，数字经济平台提高了撮合效率。数字平台的核心特征之一是数据信息的融通共享，平台可将产品信息进行集中展示，及时了解消费者需求。例如，线上电商平台可根据消费者输入的需求，展示符合描述的商品，并允许客户按价格、销量、评价等标准排名比较。平台所提供的广泛、及时、针对性强的信息将供需双方进行高效对接，使交易更易达成。

具体指标上，数字经济平台所创造的价值可从就业、消费、经济增长等方面体现。首先，数字平台在创造新增就业、优化就业结构、提升就业质量等方面发挥了重要作用。在数字产业化和产业数字化过程中，许多新产业、新业态和新商业模式被催生，带动了新就业岗位、新就业形态的快速增长。同时，数字技术进一步扩大供求匹配的范围，挖掘出更多更优配置生产力和人力资本的机会，使就业结构得以优化；数字分析为市场提供了更加科学合理的工作策划，推动工作条件改善，减轻劳动者负担。其次，数字经济平台对消费有极大的促进作用。平台经济通过链接更多商品和服务，为消费者提供 stronger 搜索功能与个性化推荐工具，以降低用户搜索和比较成本，挖掘消费者需求。另

外，平台企业与内部客群之间的强信任机制降低了服务消费过程的复杂程度，提高了消费者的服务消费意愿。整体来看，数字经济的快速崛起带动了信息产业、通信产业、互联网产业以及各种基于数字技术的新产业的发展，促进经济整体增长。然而，随着大量的商业新场景、新业态、新模式持续涌现，世界经济结构也在不断调整，面对产业结构的飞速变化，数字经济平台发展也需要进一步提高。

（二）

近年来，随着算法、人工智能、大数据的飞速发展，数字经济平台的智能化转变将为数字经济创造价值开拓新路径。

数字经济平台新的价值创造路径可加强对数据的分析应用，现阶段绝大部分数字经济平台的投资经营处于“互联网+”模式，未来将更趋向于“人工智能+”模式。在追求利润和增强市场竞争力的作用下，努力提高人工智能匹配大数据的技术水平，突破目前平台经济搜集、储存、整合和分类大数据的技术手段限制，即在继续运用现有的互联网、传感器、云平台、社交媒体、定位系统等的基础上，寻找更有效率的新技术手段来搜集、储存、整合和分类大数据，从而在数据利用的基础上增强价值创造能力。进一步完善云计算、机器学习、物联网、区块链等人工智能技术，探索新的匹配大数据的人工智能技术。由于从“互联网+”模式到“人工智

能+”模式具有较高的技术壁垒，需要依靠更高技术层级的头部平台发挥引领作用，从而全面带动平台健康快速发展。

数字经济平台的价值创造方向将进一步集中在新一代创新模式的构建、新一代产业生态的形成和新一代经济和社会形态的孵化。通过加强数字核心技术创新和科研成果的转化，将使我国经济发展具备数字化的生产模式和动力；通过加强落实产业数字化、数字产业化，经济产业生态将更好地融合数字经济和实体经济，放大相互资源的价值；通过完善数字经济治理及配套的法规和标准，现代社会的治理模式将会更加优化，从而催生新的社会形态和公序，创造出更多的平台经济价值。

数字平台经济下，数字技术可以将部分外部性问题内部化。平台可将外部费用纳入到价格中，从而激励市场买卖双方生产或购买更接近社会最优的量，来消除因外部性而引起的市场失灵。此外，对平台经济实施分级、分类、精准调控，充分考虑不同类型平台的运营差异，确定合理的监督强度和支持力度，引导企业自身规范发展。随着外部发展环境及市场空间的开放，平台企业将更加具有勇气去投资新产业、新领域，加速平台规模增量，有利于数字经济平台优化增值。

