NEWSLETTER 数据合规

2020 第三期 /总第十六期

数据合规时事速递

北京市环球律师事务所

2020 年 3 月 5 日

目录

前 言

随着《网络安全法》及相关配套法律法规等文件的出台，中国正日益加强对个人信息安全的保护和对网络安全监管。我国对个人信息保护和网络数据安全越来越重视，监管趋势也越来越严。

环球律师事务所数据合规团队收集了国内外最新出台的重要法律法规、市场监管动向以及相关处罚案例，旨在为本期刊的读者提供最实时的法律动态，帮助读者第一时间了解网络治理、信息安全相关信息。据时代的机遇与挑战。

环球律师事务所
GLOBAL LAW OFFICE

团队介绍：

环球律师事务所数据合规团队专注于网络安全与数据合规、个人信息隐私保护等领域。我们在企业数据合规体系建设等方面具备丰富的经验，为多家大型互联网公司、全球企业提供法律服务。

我们为客户提供在网络安全与数据合规、个人信息隐私保护、跨境数据传输、电子商务与广告法领域的法律咨询及相关方案设计，帮助客户迎接数据时代的机遇与挑战。

孟洁
合伙人律师
直线：86-10-6584-6768
总机：86-10-6584-6688
邮箱：
mengjie@glo.com.cn

一、新规速递

1. 《个人金融信息保护技术规范》发布

近日，全国金融标准化技术委员会发布了《个人金融信息保护技术规范》。据悉，《规范》已经通过全国金融标准化技术委员会审查，向各金融业机构发布。

《规范》将个人金融信息按照敏感程度分为三大类，由高到低，依次为 C3、C2、C1，其中 C3 主要为各类账户密码，C2 主要为账户、身份证信息、短信口令、KYC 信息、住址等，C1 主要为开户时间、支付标记信息等。

据透露，《规范》规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。同时，要求金融业机构不应以默认授权、功能捆绑等方式强制获取个人金融信息，也不应委托或授权无金融业相关资质的机构收集身份证号、手机号等个人信息。

问题一：我的企业处理什么类型的信息需要参考《规范》的要求？

为了对个人金融信息的全生命周期环节建立安全防护规范，《规范》界定了两大核心概念：“金融业机构”与“个人金融信息”。根据《规范》的规定：

“金融业机构”包括两类机构，一类是由国家金融管理部门监督管理的持牌金融机构，另一类是涉及个人金融信息处理的相关机构；

“个人金融信息”系指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

就主体范围而言，结合金融行业的实践，我们理解，“金融业机构”在现实中除了传统的持牌金融机构，还可能包括为持牌金融机构业务提供基础支持服务而需要处理个人金融信息的企业，例如提供身份验证服务的电信服务商、信息技术提供商、风控服务解决方案提供商、市场营销服务提供商等。相较于对主体的概念界定，《规范》适用于“提供金融产品和服务的金融业机构”，这一适用范围似乎并未明确涵盖前述第类机构 。

就企业合规而言，考虑到《规范》对“金融业机构”、“个人金融信息传输的接收方”、“第三方机构”等主体也设置了相应的合规义务，且从《规范》全面保护“个人金融信息”的编制目的出发，我们建议落入“金融业机构”的企业均应参考《规范》开展合规工作，对企业运营过程中涉及个人金融信息处理的环节进行对照自查，并在商业可行的范围内参照落实。

就客体范围而言，《规范》中“个人金融信息”的概念与《实施办法》中“个人金融信息”的概念较为相似，范围较为宽泛。虽然《规范》第 4.1 条并未明确广泛地列举“个人常用设备信息”、“个人上网记录”和“个人位置信息”等《个人信息安全规范》附录所明确列举的个人信息，但是《规范》仍然可以通过该条 g 项的“在提供金融产品与服务过程中获取、保存的其他个人信息”进行兜底规范，甚至可以基于前述个人信息的识别性将其视为 C2 类别的个人金融信息。

考虑到通过移动设备提供金融产品与服务已成大势所趋，设备信息与行为信息在客户身份识别、市场营销、反欺诈与风险控制等领域的使用亦日渐普及，因而在根据《规范》落实合规工作的过程中，金融业机构应当及时梳理提供产品与服务中涉及处理的所有个人信息，而不应仅仅限于《规范》明确列举的信息类型，并参照《规范》第 4.2 条对该等信息进行分级分类，继而相应落实合规要求。

问题二：我的企业如何遵照《规范》开展整体合规，大致有那些步骤？

就整体架构而言，《规范》在参考《个人信息安全规范》的基础上，先行对“个人金融信息”的范围和类别进行了梳理，继而从“安全技术要求”和“安全管理要求”两个维度详细地阐述了金融业机构在处理个人金融信息时需要遵循的规则。相应地，这一架构也在一定程度上为金融业机构开展内部合规提供了基本的思路和策略。

企业在根据《规范》开展合规工作时，应率先进行个人金融信息的统计与整理。具体而言：

企业既需要从静态的数据类型与内容出发，识别自身日常经营过程中所涉及的个人金融信息，按照《规范》中“C1、C2、C3”的级别进行数据等级划分，并尽可能使之与企业内部既存的数据资产分级得以衔接和协调；

企业也需要从动态的数据生命周期出发，进一步识别个人金融信息的“收集、传输、存储、使用、删除、销毁”等环节，为后续合规奠定事实基础。值得企业注意的是，在进行动态统计与整理时，企业不仅应该关注个人金融信息在内部的流转，

更要关注该等信息在企业内部与外部第三方之间的流转，以避免遭遇来自外部的传递式风险。

另一方面，企业需要从技术安全和管理安全两个角度，同步开展安全合规，并需要关注《规范》“增强版”的合规要求，例如：

《规范》结合个人信息保护与金融行业的特点，创新性地对“个人金融信息销毁”、“汇聚融合”与“开发测试”等新环节提出了要求；

《规范》在现有规则的基础上，针对个人金融信息的保护拟制了更为严格的要求，例如严格限制 C2 与 C3 类别信息的收集渠道，禁止 C2 类别信息中的用户鉴别服务信息与 C3 类别信息的共享与转让，要求建立个人金融信息保护制度体系，并明确列举应当制定的管理规定和开展的管理活动等。

因此，在这一过程中，企业将需要着重关注《规范》所拟定的合规要求与既存合规义务的衔接，尤其是网络安全体系下的《网络安全法》、《个人信息安全规范》与《网络安全等级保护基本要求》等关于个人信息保护和网络运行安全的规定，以及金融监管体系下的央行 17 号文、《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》与《中国人民银行金融消费者权益保护实施办法》等关于个人金融信息保护的相关要求。

问题三：个人金融信息的分级分类和相关要求有哪些？

《规范》首次在普遍意义上明确了个人金融信息的分类分级体系。据报道，《规范》早前版本为《支付信息保护技术规范》，其中将支付信息按敏感程度从低到高分为四级；而正式出台的《规范》则在一定程度上简化了分级体系，将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三类。其中：

C3 类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害；

C2 类别信息主要为可识别特定用户身份与金融状况的个人金融信息，及用于金融产品和服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害；

C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个

人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响。

事实上，《规范》也承认上述“静态”的定级规则需要结合实际情况进行具体判断：一方面，“同一信息”在不同的服务场景中可能处于不同的类别；另一方面，低敏感程度类别的信息经过组合、关联和分析后可能产生高敏感程度的信息。因此，如前文所述，企业应当从静态的数据类型与内容出发和动态的数据生命周期两个维度开展个人金融信息的梳理，以免有所遗漏。

鉴于在《规范》的分级体系下，C3 类和 C2 类由于敏感程度较高，金融业机构在处理 C3 和 C2 类别信息时，需要承担相较于处理 C1 类别信息更为严格的合规要求。换言之，位于产业链不同环节的金融业机构将可能需要根据《规范》的要求调整、优化自身的商业模式。

问题四：我的企业主要从事 To B 型业务，什么情形下的处理个人金融信息无需征得用户授权同意？

在《个人信息安全规范》征得授权同意收集、使用个人信息的例外情况的基础上，值得注意的是《规范》结合金融行业的业务实践定制了“用于维护所提供的金融产品或服务的安全稳定运行所必须的，例如识别、处置金融产品或服务中的欺诈或被盗用等”进行的个人金融信息收集使用无需征得个人金融信息主体授权同意的情形 。

实践中，不排除存在个人金融信息主体主观意志上不愿意授权金融业机构在反欺诈、身份验证等场景下采集并使用其个人金融信息，从而导致企业无法按照正常业务的合规逻辑规避可能的业务风险。因此，此次新增的例外情形能够在一定程度上增强企业基于客户身份识别、反欺诈等业务办理所必需却难以获得用户授权同意收集使用信息时的合规依据支持。

值得注意的是，尽管《规范》在一定程度上体现出金融行业监管者在个人金融信息保护上的监管态度与思路，但是考虑到《规范》属于金融行业推荐性标准，其中的例外规定并不必然能够突破《网络安全法》等强制性法律法规规定中的原则性要求。

为此，金融业机构可提前考虑结合《规范》中的相关规定：

梳理与新增例外情况相关的业务，对于确实难以征得客户授权同意的，需规划和完善面对公众和监管者的应对话术和宣传策略；

由于个人金融信息的对外共享并未增加如采集使用类似的例外情形，同时也为了避免个人信息非法买卖的风险，在未获得用户授权同意的前提下，金融业企业仍然需谨慎与第三方共享与客户反欺诈或反黑产相关的黑名单信息等；

仍需注意个人金融信息采集使用的必要性和正当性，对于个人金融信息的采集类型和频率应当与办理金融业务的风险大小相匹配，且应为实现目的最小范围。

问题五：我的企业在个人金融信息委托处理上需要注意什么？

《规范》在委托处理个人金融信息的实践上，提出了较为严格的合规要求，除个人信息保护中常见的合同约定各方权责义务、要求被委托者不得超范围使用、准确记录等要求以外，还进一步提出了更多的技术要求，主要包括：

1.对数据委托收集的主体限制

《规范》要求金融业机构不应委托或授权无金融业相关资质的机构收集 C3、C2 类别信息 。

考虑到《规范》对于 C3、C2 类别信息的定义十分宽泛且目前有关“金融业相关资质”的定义未有明确规定，该新增规定可能导致许多非持牌机构在金融信息的收集环节上需要有所调整，例如可能不再能在业务前端代表金融业企业采集客户 KYC、借贷等相关信息。

建议非持牌机构视具体情况调整业务模式，采取替代方案以避免基于金融机构客户的委托对个人金融信息进行直接采集或使用。例如，非持牌机构是否可以考虑发展面向终端消费者的相关业务。

2. 对委托处理数据的限制

对于个人金融信息的委托处理而言，《规范》相对《个人信息安全规范》新增的要求主要包括：

1)C3 类和 C2 类中的用户鉴别辅助信息，不应委托给第三方处理；

2)应对委托处理的信息采用去标识化进行脱敏处理；

3)应对外部嵌入或介入的自动化工具开展技术检测，并对第三方的收集个人金融信息行为开展审计，发现超出约定行为及时切断接入。

首先，对于某些金融业企业的外部合作机构而言，其产品和服务的提供可能必须基于明文的 C3 类和/或 C2 类中的用户鉴别辅助信息，如目前接受银行等金融机构委托进行身份核验等的助贷企业，可能必须以客户身份三要素的获取为业务开展的基础，依据目前的要求，非持牌机构可能难以再获得明文的上述个人金融信息，因此业务模式可能面临重新调整的需要。

其次，严格按照《规范》规定来看，金融企业客户在选择业务和服务的外包方时，将可能不再仅要求对于产品和服务的合规性和业务逻辑进行说明、承诺，还可能需要进一步地针对自动化工具开展技术检测，并对基于委托收集个人金融信息的行为进行审计。

对于个人金融信息的被委托方而言，为避免不同合作方的反复检测和自证，同时合理考虑委托处理环节的脱敏处理要求，建议：

1)考虑采用本地化部署和交付等方式为金融企业客户提供相关产品或服务，通过由客户自行掌握相关服务系统的方式，避免 SaaS 服务模式下处理禁止委托处理的信息、或者针对被委托处理信息的频繁、多方技术检测成本；

2)有必要时，自行开发面向金融企业客户的技术工具，用于客户全方位了解和掌握相关服务系统运行情况和安全保障状况；

3)如有可能，尽早考虑新的系统架构模式，确保去标识化处理后映射信息仅在客户本地保留，被委托方系统仅对去标识化后不可回溯个人金融信息主体的数据进行处理、分析，进而为客户提供数据分析能力和算法模型构建能力。

对于个人金融信息的委托方而言，为了避免向第三方委托处理禁止性信息、保证数据委托处理的合规性，建议：

1)提高自身的技术研发能力，尤其对于禁止委托处理的信息，尽量使用自身技术予以处理以满足业务经营的需要；

2)建立对于自动化工具应用的全流程管控制度，包括接入前的合规和技术评估、定期审计和应急处理机制等。[1]

2. 《网络信息内容生态治理规定》3 月 1 日开始施行

近日，国家互联网信息办公室发布了《网络信息内容生态治理规定》(以下简称《网规》)，自 2020 年 3 月 1 日起施行。当我们借助互联网的便利自由浏览阅读免费、快捷、海量网络信息的同时，网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等行为也在污染着网络生态。

国家网信办相关负责人表示，《网规》的出台旨在营造良好网络生态，保障公民、法人和其他组织的合法权益，维护国家安全和公共利益。加强网络生态治理，是建立健全网络综合治理体系，培育积极健康、向上向善的网络文化的需要，也是维护广大网民切身利益的需要。

网络暴力危害社会

根据中国社科院发布的《社会蓝皮书：2019》调查显示，青少年在上网过程中遇到暴力辱骂信息的比例为 28.89%。其中，暴力辱骂又以"网络嘲笑与讽刺"及"辱骂或用带有侮辱性的词汇"居多，分别为 74.71%和 77.01%。其次则是"恶意图片或者动态图"和"语言或者文字上的恐吓"，分别为 53.87%和 45.49%。

由于网络中用户的匿名性与隐蔽性的特征，网络暴力已经成为威胁互联网环境的一大危害。许多网民对未经证实或者已经证实的网络事件，随意在网上发表具有伤害性、侮辱性与煽动性的失实言论，对当事人或者社会公众的名誉权和隐私权造成严重侵害。

净化网络空间

国家网信办有关负责人表示，出台《网规》主要基于两个方面的考虑：一是建

[1] 快资讯。

立健全网络综合治理体系的需要；二是维护广大网民切身利益的需要。而《网规》中的生态治理，指的是政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主体治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展弘扬正能量、处置违法不良信息等相关活动。

做好网络信息内容的生态治理，网络信息内容生产者、网络信息内容服务平台需要率先承担责任，规范自身行为。网络内容生产者务必要保证所发布网络信息的真实性，并且具有积极的导向性；网络信息内容服务平台应当履行信息内容的管理主体责任，建立良好网络信息内容生态治理机制。

当然，网民的自律也是必不可少的。根据中国互联网络信息中心发布的数据调查显示，截止至 2019 年，中国网民规模达 8.54 亿，数量庞大的网民群体中多以青少年网民居多。

《网规》的出台，对于新时代中国互联网生态治理是一个良好开端，有法可依、依法治理是实现互联网良性生态治理的根本举措。南京大学法学院教授单勇在接受采访时表示《个人信息保护法》以及《数据安全法》两部关于完善互联网领域治理的法律也正在制定当中了。

网络生态治理是一场攻坚战，这其中包括网络信息内容生产者、网络信息内容服务平台以及网络服务使用者等多个主体都应该参与其中，规范自己的行为、承担相应的责任，共同努力赢得这场战役的胜利。[2]

《网络信息内容生态治理规定》全文参见：

http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm

[2] 青海普法。

二、监管动态

1．中央网信办：为疫情防控收集的个人信息不得用作他途

为做好新冠肺炎疫情联防联控中的个人信息保护，积极利用包括个人信息在内的大数据支撑联防联控工作，中央网信办发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》（简称“《通知》”）。

《通知》要求，收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视。

《通知》提到，为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。

《通知》强调，收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露；鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持；任何组织和个人发现违规违法收集、使用、公开个人信息的行为，可以及时向网信、公安部门举报。[3]

近日，中央网络安全和信息化委员会办公室发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，全文如下：

各省、自治区、直辖市网络安全和信息化委员会，中央和国家机关有关部委：

为做好新型冠状病毒感染肺炎疫情联防联控中的个人信息保护，积极利用包括个人信息在内的大数据支撑联防联控工作，经中央网络安全和信息化委员会同意，现将有关事项通知如下：

1.各地方各部门要高度重视个人信息保护工作，除国务院卫生健康部门依据

[3] 新浪财经。

《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。法律、行政法规另有规定的，按其规定执行。

2.收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视。

3.为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。

4.收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

5.鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持。

6.任何组织和个人发现违规违法收集、使用、公开个人信息的行为，可以及时向网信、公安部门举报。网信部门要依据《中华人民共和国网络安全法》和相关规定，及时处置违规违法收集、使用、公开个人信息的行为，以及造成个人信息大量泄露的事件；涉及犯罪的公安机关要依法严厉打击。[4]

2．北京通州法院：物业不得擅自披露被隔离人员姓名等个人信息

2 月 20 日，北京通州法院召开线上新闻发布会，发布《新冠肺炎疫情期间物业服务企业法律风险防控白皮书》（简称白皮书）。白皮书就物业服务企业在经营运行、小区管理、合同履行、劳动用工和参加诉讼等五个方面，进行法律风险梳理，并提出 40 条防范建议，将向通州辖区内的物业服务企业推送。

物业服务企业是社区疫情防控阻击战的主要力量，其工作主要包括防控预案、员工管理、疫情宣传、出入管控、重点消杀、物资支持等方面。通州法院民三庭负

[4] 澎湃新闻。

责人晋怡介绍，疫情期间，物业服务企业应加强内部管理，做好企业内部防控组织工作，对隐瞒、缓报疫情的，需承担相应法律责任。

白皮书指出，疫情防控期间，各企业要加强内部员工岗位调剂，确保物业服务工作的基本运行；对未在岗的企业内部员工，严格按照北京市规定执行，目前正在湖北地区返乡探亲的员工，要通知员工本人，不得违反规定离开湖北地区返京工作；其他地区返京工作人员，要按有关规定，及时上报社区，采取防控措施，同时建立返京工作人员台账，并将台账报告社区。

与此同时，业主应配合物业工作，不能以疫情发生导致未享受物业服务为由拒缴或要求减免物业费。对于因疫情未及时返京复工的物业服务企业员工，企业可以优先考虑安排职工年休假。员工因履行疫情防控职责感染新冠肺炎的，应认定为工伤。物业服务企业不得违法扣减员工工资或解除与员工的劳动合同。

白皮书指出，如租户等物业使用人体温正常，物业服务企业不得阻止租户等人员进入小区内部。如相关人员体温超过规定温度，则物业服务企业须劝导该人员就近就医，暂时不让其进入小区，并及时向卫生部门或疾控中心报告。如该人员不予配合，物业服务企业可以报警并向疾控中心报告处理。

前述白皮书还强调，物业公司对获取的被隔离人员的信息亦负有保密义务，不得对外披露该部分人员的姓名、房号、身份证号码等个人信息。

根据《传染病防治法》第三十九条第二款规定：“拒绝隔离治疗或者隔离期未满擅自脱离隔离治疗的，可以由公安机关协助医疗机构采取强制隔离治疗措施”。

为此，白皮书指出，物业服务企业可配合政府部门和医疗机构对确诊病人的密切接触者采取隔离措施，并加强相关部位的消毒措施，但物业服务企业不得采取强制隔离措施对房屋出入口进行封闭。[5]

3．央行牵头 国内金融行业首个区块链标准发布

近日，《金融分布式账本技术安全规范》（JR/T 0184—2020）金融行业标准

[5] 澎湃新闻。

（以下简称标准）发布，这是国内金融行业首个区块链标准。

《标准》由全国金融标准化技术委员会归口管理，由中国人民银行数字货币研究所提出并负责起草，中国人民银行科技司、中国工商银行(5.400, -0.01, -0.18%)、中国农业银行(3.460, 0.01, 0.29%)、中国银行(3.600, 0.00, 0.00%)、中国建设银行(6.640, -0.01, -0.15%)、国家开发银行等单位共同参与起草。标准经过广泛征求意见和论证，并通过了全国金融标准化技术委员会审查。

《标准》的编制，旨在规范分布式账本技术在金融领域的应用，提升分布式账本的信息安全保障能力。《标准》提到，分布式账本技术是密码算法、共识机制、点对点通讯协议、分布式存储等多种核心技术高度融合形成的一种分布式基础架构与计算范式。在分布式账本技术形态尚具可塑性阶段，有必要制定关键技术的安全规范，以便金融机构按照合适的安全要求进行系统部署和维护，避免出现短板，为分布式账本技术大规模应用提供业务保障能力和信息安全风险约束能力，对产业应用形成良性的促进作用。

《标准》规定了金融分布式账本技术的安全体系，包括基础硬件、基础软件、密码算法、节点通信、账本数据、共识协议、智能合约、身份管理、隐私保护、监管支撑、运维要求和治理机制等方面。标准适用于在金融领域从事分布式账本系统建设或服务运营的机构。

《标准》发布后，引起了部分业内人士的质疑，认为虽然区块链和分布式账本很多地方看起来差不多，但二者是不同的东西。而通读《标准》全文，也并未见到“区块链”出现。那么，该标准为何会被称为金融行业首个区块链标准？

对此，巴比特迅速联系到起草人之一，微众银行金融科技首席研究员李斌。李斌表示，“按照 ISO 术语标准 22739 中的表述，区块链是使用密码技术，将共识确认的区块，按照顺序追加形成的分布式账本。也就是说，区块链是分布式账本的子集。不过目前两者基本是指同一样东西，这个标准基本可以理解成金融联盟链的标准。”

实际上，早在 2017 年，中国电子技术标准化研究院发布的《区块链 参考架构》标准，就对区块链做出了定义，指出区块链是一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

对于区块链和分布式账本技术的关系，《区块链 参考架构》指出：

严格意义上讲，区块链和分布式账本技术这两个概念的原始内涵具有明显差异。区块链的基本技术特征是：将一段时间内发生的事务处理编组成区块，区块之间以密码学特征（例如 Hash 值）方式按先后顺序链接起来，形成以区块为基本单元的“链”，并且将该“链”在区块链网络参与节点间复制和共享，同时链上内容依据不同的共识机制由参与节点组成的网络集体维护。而分布式账本技术是一类用来实现分布式账本的技术，强调的是事务处理通过复制和共享的账本来实现，并且该账本由所在网络的参与者进行校验及维护，并不指定具体的技术特征。

在很多应用场景中，区块链和分布式账本技术具有密不可分的联系。区块链是实现分布式账本的一种常用的技术手段，某种程度上可以将区块链看作是分布式账本技术的一种。尤其是在不同的利益、关注点和需求的驱使下，两者的应用实践逐渐体现了一种相互融合的趋势。

近日，由中国人民银行数字货币研究所区块链课题组在《中国金融》发布的《区块链技术的发展与管理》一文中也指出，区块链是一种新型的分布式数据库，也称为分布式账本。区块链技术利用块链式结构验证与存储数据，采用共识算法生成和更新数据，借助密码学保证数据和权属安全，并通过可编程脚本代码实现数据的协同计算。

目前，国内形成了以中国电子技术标准化研究院发起的“中国区块链技术和产业发展论坛”以及中国信息通信研究院发起的“可信区块链推进计划”两大区块链技术标准组织，其中前者发布的区块链标准已有 10 项，后者在研的也有 20 多项，有力地推动了我国区块链技术和产业发展。

然而，目前区块链标准虽然众多，但是何时能够落地到具体的区块链产品上，还是未知数。李斌表示“我国的区块链标准认证还没有起步，目前都是比较宽泛的技术标准，还没到产品标准的层面。毕竟技术类标准不像食品医药安全那些行业一样是要强制认证，如果后续各金融机构的区块链系统符合央行制定的区块链标准，我个人觉得应该会有资质认证之类的，当然更重要的还是如何能像二维码技术一样推动形成事实标准。”[6]

《金融分布式账本技术安全规范》全文参见：

http://www.cfstc.org/bzgk/gk/view/yulan.jsp?i_id=1855

[6] 新浪财经。

4．工信部发布关于涉新冠肺炎疫情的网络安全风险提示

近期，工业和信息化部网络安全威胁信息共享平台收到网络安全企业及机构报告，发现多起利用新冠肺炎疫情实施网络攻击的行为。经研判分析，攻击者利用疫情对公众的心理影响，将计算机病毒、木马、移动恶意程序等伪装成包含“肺炎病例”“防护通知”等热门字样的信息，通过钓鱼邮件、恶意链接等方式传播，一旦点击下载，可能导致计算机、手机等终端设备被窃取信息或远程控制。

为降低网络安全风险，工业和信息化部网络安全管理局组织相关单位加大对伪装成疫情信息传播计算机病毒、木马、移动恶意程序等监测力度，采取了屏蔽病毒木马控制端、下载恶意程序等措施，对发现的网络威胁进行处置。同时，提醒公众提高网络安全风险意识，采取以下措施进行防范：

一、不轻易打开来历不明的电子邮件及其附件。

二、不轻易点击短信或微信中不明来源的链接。

三、从正规应用商店或官方网站下载安装应用程序。

四、安装杀毒软件并及时更新。[7]

5．《2020 数字医疗：疫情防控新技术安全应用分析报告》发布

数字医疗是 ICT 产业融合领域的重要发展方向，新技术的安全应用在提升资源利用率、提高产能、降低成本等方面发挥了重要作用。2020 年初，新冠肺炎疫情在武汉暴发，并迅速蔓延至全国，一场没有硝烟的战争席卷而来。在此期间，众多企事业单位积极参与到疫情防控的工作中，综合应用人工智能、大数据等新技术，更加实时、准确、全面地为疫情防控提供强有力的决策支撑，在预测、防控、诊疗、恢复等环节发挥了重要作用。

中国信息通信研究院安全研究所在有关部门的指导下，联合中国卫生信息与健康医疗大数据学会卫生信息安全与新技术应用专业委员会和数据保护官（DPO）

[7] 中国新闻网。

社群，共同编制发布了《2020 数字医疗：疫情防控新技术安全应用分析报告》（以下简称“报告”）。

报告分析了中国电信、中国移动、中国联通等基础电信运营企业以及平安、腾讯、旷视等科技公司支撑疫情防控工作的典型案例，研究了人工智能、大数据、云计算、区块链等新技术在提升疫情防控效率、构建态势感知能力、支撑防控资源调度和促进工作信息公开等方面的安全应用。基础电信运营企业在有关部门的指导下，基于脱敏后的大数据技术能力，在保证用户隐私安全的基础上，配合相关部门重点开展针对定点医院、发热门诊、人员聚集区等重点区域的人流变化分析，提供疫情防控相关的支撑服务工作。科技企业发挥了大数据资源和技术优势，为疫情防控提供了有效的技术支撑。除报告中列举的案例之外，还有很多的企事业单位用科技赋能抗疫。

在数字医疗领域，ICT 新技术应用的诸多网络与信息安全问题不容忽视。报告以疫情防控为背景，从个人隐私保护、网络和信息安全等方面进行分析，研究了国内外相关疫情防控的大数据应用与信息保护的法律法规与参考标准，阐述了新技术应用安全的重要性。报告最后，在疫情防控的新技术安全应用方面提出了一些工作思路和安全建议，供相关行业主管部门、疾控部门、医疗机构和企事业单位等参考。

数字医疗在不断向前发展，ICT 的产业融合与安全保障是发展必不可少的长效机制。面对严峻的疫情形势，信息通信业上下齐心，充分发挥技术手段与平台优势，强化新技术的安全应用，助力打赢防控疫情攻坚战。[8]

《2020 数字医疗：疫情防控新技术安全应用分析报告》全文参见：

https://mp.weixin.qq.com/s/xOnF45QaVM89STjMmfQj4A

6．欧盟发布人工智能白皮书 公共场所人脸识别五年禁令被取消

欧盟委员会将发布人工智能白皮书并征求意见。值得注意的是，据《金融时报》报道，在最新草案中，“禁用人脸识别技术五年”的相关条款已被删去。

[8] 搜狐网。

作为负责人，欧委会副主席兼竞争专员的玛格丽特•维斯塔格（Margrethe Vestager）对媒体表示，根据欧盟《通用数据保护条例》（GDPR），人脸识别场景通常因无法征得数据主体的明示同意涉嫌违法，欧盟将考虑采取暂停措施。她同时强调，这种“暂停”不会影响各国政府对人脸识别技术的使用。

人脸识别无法征得同意，涉嫌违反 GDPR

2 月 19 日，欧盟将发布人工智能白皮书。维斯塔格指出，欧盟的人工智能发展策略将使欧洲更多地开发和部署人工智能，焦点在于透明度和监管，与美国和中国有所区别——“中国有数据，美国有钱，而我们有目标。”

一直以来，人工智能相关技术在欧洲引发了诸多争议。欧委会认为，在欧洲，尽管人工智能受制于隐私权法、产品安全和责任赔偿法等一系列法律，但是这些法律并没有完全覆盖新技术的潜在风险。

根据自 GDPR 第 6 条，取的数据主体的明示同意是合法处理个人数据的条件之一。但在维斯塔格看来，人脸识别技术就难以满足上述规定，她在 2 月 13 日的新闻发布会表达了这个观点，“就目前的情况下，GDPR 会要求不能使用（人脸识别）”。

根据人工智能白皮书最新草案，如果不能保证人脸识别或其他有风险的人工智能技术符合欧洲价值观，公司必须用欧洲数据集对系统进行重新培训。据悉，人工智能白皮书将涵盖自动驾驶汽车、生物识别 ID 等使用场景。

目前，在 GDPR 框架下，已经针对人脸识别技术的涵盖了公共安全事项的一些例外，但欧盟官员还希望与成员国、企业和其他组织探讨是否应增加新的例外。

公共场所禁用人脸识别五年条款被取消

去年 4 月，欧盟发布《可信赖的人工智能伦理准则》。草稿称，在欧盟现有规定的基础上，未来的监管框架可以“更进一步”，例如，设立三到五年不等的有时限的禁令，禁止公共或私营机构在公共场所使用人脸识别技术。

事实上，据 EURACTIV.com 报道，在之前的人工智能白皮书草稿中，的确有公共场合禁用人脸识别高达五年的相关条款。不过，据《金融时报》报道，在周三即将发布的版本中，这一禁令将被取消。对此，维斯塔格透露，现阶段欧委会将不

采取任何措施，而是思考如何在欧盟层面规范人脸识别技术。“因此，我们将在白皮书里用一种非常合理的方式提出可以暂停并找出是否存在什么特殊情况；如果是，在什么情况下应该远程授权人脸识别”，她补充说，这种“暂停”不会阻止各国政府在现有规则下使用人脸识别技术。

不过，欧盟对人脸识别等人工智能技术的缓和态度并没有令硅谷巨头们感到宽慰。这是因为，欧盟将提议每年花费近 220 亿美元构建新数据生态系统，用于人工智能开发。这项计划的前提是欧洲拥有大量的政府和工业数据，希望通过监管和财务激励措施对这些数据加以汇总，提供给同意遵守欧盟法规的人工智能开发人员。

人工智能白皮书公布后，公众将有 12 周的时间提出建议。欧委会预计于今年下半年提出立法提案。[9]

三、相关案例

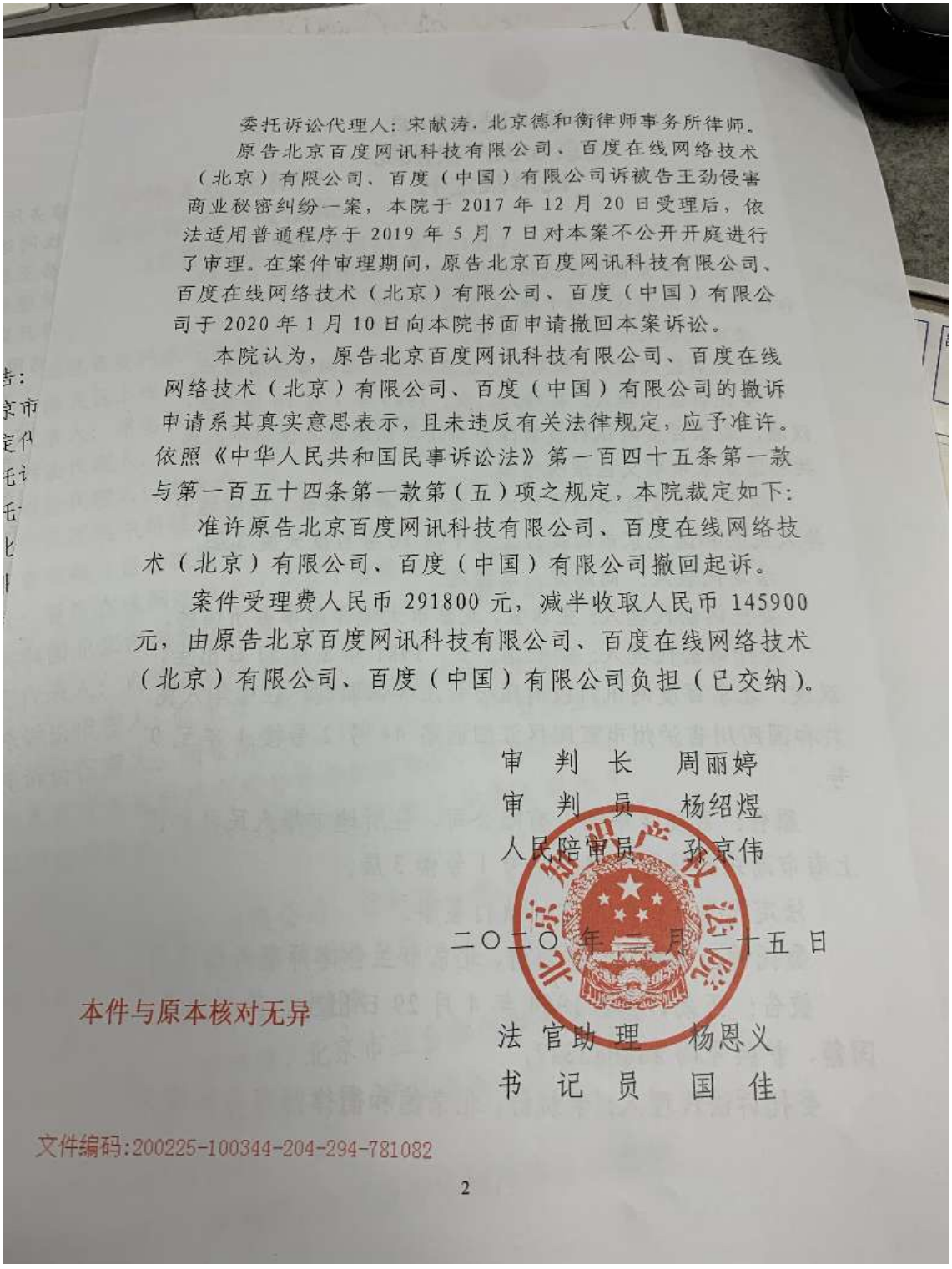
1. “中国无人驾驶第一案”尘埃落定，法庭宣判在即、百度撤诉王劲

2 月 28 日，中智行科技有限公司发布声明称，根据北京知识产权法院下发的（2017）京 73 民初 2000 号民事裁定书，被称为“中国无人驾驶第一案”的百度诉其前高级副总裁、自动驾驶事业部创立者，现任中智行 CEO 王劲侵害商业秘密侵权案，刚刚“尘埃落定”：在经历两次庭审和法庭即将宣判之际，百度最终撤诉。

王劲本人也于 2 月 28 日在其微博发文称——清者自清浊者浊，不忘初心，以回应此事。

中智行在声明中称，此案中，百度始终无法证明商业秘密的存在，更无法证明王劲有侵害商业秘密的行为。中国知识产权界顶级专家曾就此案召开专家论证会，指出应防止企业利用诉讼和程序阻碍技术人员的劳动自由和创新自由。法庭的最终判决即将于近期公布，而百度选择了在此时撤诉。

[9] 南方都市报。



委托诉讼代理人：宋献涛，北京德和衡律师事务所律师。

原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、百度（中国）有限公司诉被告王劲侵害商业秘密纠纷一案，本院于2017年12月20日受理后，依法适用普通程序于2019年5月7日对本案不公开开庭进行了审理。在案件审理期间，原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、百度（中国）有限公司于2020年1月10日向本院书面申请撤回本案诉讼。

本院认为，原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、百度（中国）有限公司的撤诉申请系其真实意思表示，且未违反有关法律规定，应予准许。依照《中华人民共和国民事诉讼法》第一百四十五条第一款与第一百五十四条第一款第（五）项之规定，本院裁定如下：

准许原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、百度（中国）有限公司撤回起诉。

案件受理费人民币291800元，减半收取人民币145900元，由原告北京百度网讯科技有限公司、百度在线网络技术（北京）有限公司、百度（中国）有限公司负担（已交纳）。

审 判 长 周丽婷

审 判 员 杨绍煜

人民陪审员 孙京伟

二〇二〇年 二 月 十五 日

本件与原本核对无异

法官助理 杨恩义

书 记 员 国 佳

文件编码:200225-100344-204-294-781082

2

中智行声明

关于百度撤诉的法院通知显示，百度诉被告王劲侵害商业秘密纠纷一案于2017年12月20日由法院受理，2019年5月7日法院对此案进行了不公开开庭审理，在案件审理期间，百度于2020年1月10日向法院申请撤回本案诉讼。北京知识产权法院准许了百度的撤诉申请，并减半收取百度14.59万元案件受理费用。

中智行
ALLRIDE·AI

中智行官方声明

清者自清浊者浊

“中国无人驾驶第一案”尘埃落定，法庭宣判在即、百度撤诉

今天，我们刚刚获悉，根据北京知识产权法院下发的（2017）京73民初2000号民事裁定书，百度已于日前撤销对中智行现任CEO、百度前高级副总裁和自动驾驶事业部创立者王劲侵害商业秘密侵权案的诉讼。这一诉讼被称为“中国无人驾驶第一案”，自2017年12月至今历时两年有余，在经历两次庭审和法院即将宣判之际，百度最终撤诉。

在百度诉讼上，王劲和他的法律团队始终坚信中国司法体系的公正。**此案中，百度始终无法证明商业秘密的存在，更无法证明王劲有侵害商业秘密的行为。**中国知识产权界顶级专家曾就此案召开专家论证会，指出**应防止企业利用诉讼和程序阻碍技术人员的劳动自由和创新自由。**法庭的最终判决即将于近期公布，而百度“恰”在此时撤诉。

“创业艰难百战多”，中国无人驾驶的发展之路，注定不会是一条平坦的道路。我们感谢中国的司法体系，让中智行得以在王劲的带领下，心无旁骛，携手政府和各领域合作伙伴，不忘初心、脚踏实地，专注开拓属于我们自己的中国式无人驾驶之路。

中智行科技有限公司
2020年2月28日

法院关于百度撤诉的通知

2019年11月12日二次庭审前，中国知识产权界顶级专家曾就此案召开专家论证会，并向法庭提交了《关于百度诉王劲侵害商业秘密纠纷案的法律意见》，该意见书显示，百度无法证明商业秘密的存在，遑论侵害商业秘密行为的存在；百度提交证据应该符合正当的形式要件，不应以保密为由阻止对方获得该证据，影响对方的诉讼权利；商业秘密案件审理过程中应当区分商业秘密和劳动者基本技能，平衡技术公司和劳动者之间的利益关系，亦应防止公司利用诉讼和程序影响技术人员的劳动自由和创新自由。

上述专家组成员包括了中国知识产权法学研究会会长刘春田教授、中国社科院知识产权中心主任李明德教授、中国人民大学知识产权学院副院长郭禾教授、中国政法大学知识产权法研究所所长冯晓青教授、中国人民大学知识产权学院张广良教授等。

公开资料显示，王劲曾任谷歌中国工程院副院长，于 2010 年 4 月跳槽到百度，并于 2014 年升任百度高级副总裁，同时担任百度技术最高负责人。王劲任职百度期间，在百度创建了中国第一个人工智能研究院，又于 2015 年 12 月在百度创立自动驾驶事业部并担任事业部总经理，并招揽了倪凯、余凯、吴恩达等自动驾驶领域知名人物。王劲曾于 2017 年 6 月被福布斯杂志评价为 20 位驱动中国人工智能革命领导者之一，20 人中有 7 位为王劲原下属。

2017 年 3 月，王劲从百度离职，同年 4 月联合他人在美国创立了自动驾驶公司景驰科技。2017 年 12 月，百度以侵犯商业秘密为由，将王劲以及景驰公司，诉至北京知识产权法院，索赔 5000 万元，法院已受理。

百度公司指出，王劲违反高管忠实义务和竞业限制义务，还在百度任职期间就注册成立了景驰科技公司，并且通过创业公司招聘百度的员工。最重要的是，百度认为王劲离职时声称丢失了一台笔记本电脑和一台多功能一体机，这极有可能造成了百度商业秘密与技术秘密的泄露。[10]

2. 泄露学生个人信息应当重视

近日，一所大学发生一起 50 余名学生个人信息泄露事件。这些泄漏的信息均被一家企业所利用，伪装成在这家企业兼职的大学生，利用大学生的身份来达成偷逃税款的目的。

根据税收征收管理法，纳税人伪造、变造、隐匿、擅自销毁账簿、记账凭证,或者在账簿上多列支出或者不列、少列收入，是偷税。利用学生来避税，该企业已经涉嫌违犯法律。

近年来，学生信息泄露的事件屡见不鲜。原因其一是学生缺乏个人信息的保护意识，一些掌握学生信息的个人和组织也对信息保护不够重视，尤其是学生在参加社团活动和社会实习实践时，不经意间留下的个人信息可能被他人利用。2018 年

[10] 澎湃新闻。

常州大学怀德学院就有超过千名学生遭遇个人信息泄露，他们的个人信息被不法企业用于虚报员工身份及工资记录，同样被怀疑是为了偷逃税款。

其二，也有一些学校在公布某些资助、获奖名单时，“坦然”地把学生身份信息放在网站上，根本不做任何“保护”。针对这种问题，教育部全国学生资助管理中心 2017 年 11 月曾发布第 9 号预警《保护学生个人信息和隐私，资助工作者要“拧紧这根弦”》，提醒学校相关部门加强对学生身份信息的保护。

只有对冒用学生信息的企业严惩不贷，才能杜绝此类现象发生。民法总则规定，任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息；刑法则明确了“侵犯公民个人信息罪”的相关处罚；2019 年，国家网信办已就《数据安全管理办法》面向全社会公开征求意见；个人信息保护法也已列入本届全国人大常委会的立法规划。

一些时候企业或个人盗取信息的程度达不到量刑的地步，局限于“民事”范畴，执法机构面临大量的小规模信息侵害也力有未逮，只能“抓大放小”。若是自主维权，根据司法“填平”原则，诉讼往往需要受害人举证损失来进行赔偿，而信息泄露表面上对每个个体都伤害不大，很多时候大家仅仅是接到垃圾短信、推销电话。这样的事件有时就不了了之，涉事企业甚至连一个公开道歉都欠奉。所以，在司法机制难以触及的盲区，需要有更多的社会治理方法来填补空缺。

近年来，随着网络信息空间的拓展，刷脸、换脸等 AI 技术的出现，个人信息保护成了社会讨论的热门话题。在对窃取数据行为的声讨中，已经有不少互联网企业开始研究“数据脱敏”技术，在保护用户的数据道路上迈出第一步。而针对冒用学生信息的行为，也应该在社会层面掀起更多的讨论，给予企业更多压力，培养全民保护信息的意识，对侵犯信息权、隐私权的行为“零容忍”。如此，才能切实保护公民权益，打赢这场“信息保卫战”。[11]

3. 疫情下多地实行扫码出入 扫码小程序是否泄露个人信息？

疫情期间，出于公共安全的需要，居民出行时进行身份信息登记成为了常态，但也有越来越多的人对登记详细信息的必要性产生了质疑。

[11] 人民网。

随着个人信息登记也出现一些泄露个人信息的事件。如根据深圳电视台的报道，光明区马田街道的李先生报料称，社区的一名网格员不知何故，将居民登记表直接发到小区微信群。在群内的登记表上，记录了 600 多人的姓名、身份证号、住址、电话号码等信息，涉及多个小区，而涉事网格中心负责人则对此回应称，个别网格员对社区新出的系统使用不是很规范，产生操作不当的现象。新京报记者统计发现，对于武汉人员的信息泄露更为严重。春节期间，一些地方利用大数据手段摸排从武汉返乡人员信息时，曾发生多起隐私信息泄露事件。

对此，对个人信息保护的利用规范，最大的风险是广大的基层可能没有太多个人信息保护意识，当一些非专业机构的人士收集个人信息时，若出现不太规范的地方，一旦信息泄露出去，可能会在未来带来骚扰电话、诈骗等麻烦事。此时必须特别注意，收集信息最核心的目的是勾勒行踪轨迹，而与此相关的其他信息，要尽量不收集。

在目前这种情况下，合理放宽利用个人信息的范围是没有问题的，但对于不恰当的利用行为要重拳出击，对泄露到微信群的行为要重罚，对大规模的泄露事件甚至拘留的手段也可以考虑，这是因为在当前这一特殊时期，信息泄露除了对当事人的权益会造成影响之外，还有可能让人因担心信息泄露而不愿意去申报，最后导致隐瞒情况的发生。

目前已经出现了因泄露个人信息遭处罚的案例。如广州市公安局曾于 2 月 6 日通报一起“小区的业主微信群内发布多名公民个人信息”案，在该案中，违法嫌疑人郑某将多名曾乘坐某邮轮的游客名单（含个人信息）发送给朋友叶某，叶某又将上述游客个人信息转发至其所在小区的业主微信群内。最终警方依据《中华人民共和国治安管理处罚法》相关规定，对郑某叶某两人予以罚款 500 元的处罚。

多地实行扫码出入 扫码小程序未明示信息保存方式？

在疫情期间，对公民个人信息的登记主要分为两个渠道：前期在街道社区、便利店等进行的手动登记以及后期逐渐流行的大数据扫码。

2 月以来，杭州、天津、广西、云南等多个省市自治区均推出了公共场合实名登记出入的政策，沈阳、南京、贵阳等地推出了乘车实名登记的政策，还有多地出台了买药实名制措施。

2 月 19 日，天津各个街道已经开始实行扫码出入制度。“这个政策是 2 月 18 日开始实行的，出入都需要扫码。”天津光复道街某小区一名社工告诉记者。记者

扫描社区提供的二维码发现，手机会进入“津门战疫”小程序，只需要进行短信验证即可成功注册。云南发布的“云南抗疫情”小程序的扫码注册流程则与天津类似，该小程序只需要短信验证即可成功注册。

此外，天津、广西、云南三地的扫码小程序也有“公共场所注册”选项。据了解，该功能为公共场所负责人所申请。以广西为例，公共场所的负责人需要输入公共场所名称、申请人的姓名、手机号、行政区域以及详细地址，即可生成二维码，之后在该公共场所出入的人员信息就可以通过扫码上传至网络。

公共场所管理员可以看到出入人员的姓名以及隐藏掉四个数字的手机号码，不过为保护个人信息安全，出入人员的登记信息被设置为不可导出。“这一设计是合理的，因为仅仅是个人姓名和隐去部分数字的手机号，并未超过‘最少可用’的采集标准，可以为疫情防控提供人员流动信息，却不足以让采集者识别公民个人。”方超强表示。

但需要注意的是，上述小程序只需要注册即可使用，但对使用信息的目的、方式和范围、保存方式并未有说明。根据《网络安全法》第四章有关规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。因此有观点认为，收集用户信息的小程序应该更加明确标出其收集信息的目的、使用范围、存储期限等情况。

目前有地方政府机构对收集信息的用途做出了明确说明。如安徽蚌埠市在市区范围内开展重点人群及接触者全面排查工作时，要求市民要扫二维码填报健康信息。2 月 18 日，市数据资源局信息资源中心主任张锐在接受当地媒体采访时表示，“所有收集到的数据均汇集在市政府数据机房，不会存储在商业机构中，机房和数据库系统按国家三级等保标准建设，可满足数据安全要求。收集的数据由政府授权并签订安全保密协议的工作人员统一集中管理，并规定本次所有收集的居民信息只限用于我市疫情管理。”

有专家向记者透露，蚌埠市的说明很完善，“这就属于‘明确了收集信息的使用用途、范围’，相比之下建议其他要求提供实名制的地方以明示提醒的方式告知用户收集信息的用途。”

从技术上看，通过短信进行实名验证，验证环节是在掌握比对信息的信息库服务器上完成的，例如中国移动，验证成功之后，只会反馈验证成功、验证不成功等简单信息，不会过多涉及个人信息。从保护公民个人信息的角度出发，如果通过二

维码登记的方式采集了公民个人信息，在疫情防控解除，采集信息完成作用后，及时进行去标识化处理或者删除应该是比较合理的。

疫情过后信息如何处理？确保后续数据安全更重要，要对收集信息的 APP 严格监管

2 月 4 日，网信办发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》。通知要求，除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。法律、行政法规另有规定的，按其规定执行。收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则。

对此，APP 专项治理工作组专家洪延青、何延哲、葛鑫在其公号发文称，疾病防控大数据分析涉及大量个人信息，甚至是对特定人群的追踪分析，不是任何单位或个人都有授权、有能力开展的。在《传染病防治法》《突发公共卫生事件应急条例》中，获得明确授权的有疾病预防控制机构、医疗机构，以及直接参与到国务院和省、自治区、直辖市人民政府制定、实施的“突发事件应急预案”中的单位和个人。非上述单位和个人，不应在未征得个人同意的情况下将个人信息用于疫情管控、重点人群追踪等目的。

在洪延青等专家看来，目前各地疾病防控机构、基层街道社区等普遍开展走访调查工作，统计相关人员个人信息。这个过程涉及个人信息的采集、汇总、共享、披露等多个环节，每个环节都应当注意做好个人信息保护工作，以防出现数据泄露、丢失、滥用等情形。“比如，采集过程中，如果各地疾病防控机构、基层街道社区等以纸质填表方式开展的走访调查，需要严格要求纸质材料不被拍照、复印，进行统一回收，保管妥当。如果以电子方式记录或汇总相关信息，需要责任到人，并保存在特定的终端，并将数据和备份数据加密存储。在个人信息使用过程中，需要做到专采专用，严格限制于疾病防控目的，不得挪作他用，并且在疫情防控结束后按照规定予以妥善处置。”

在电子化的环境下，最重要的是对收集到的信息进行去标识化，这样可以最大限度的降低风险。“在这种情况下，确保后续的数据安全，比知情同意原则更重要，我呼吁政府对疫情期间收集到的个人信息增加追踪过程，等疫情过后，要对收集这些信息的 APP 进行严格监管。

除基本的疫情申报途径外，疫情防控机构最好还能设置单独申报个人信息的

途径，一些人隐瞒病情并非是不想去医院，而是是出于自身原因，想要隐瞒涉及个人隐私的行程，此时需要设立严格保密机制下的个人信息申报途径，这种途径可以最大限度避免疫情隐瞒，对控制疫情发展有利。[12]

4. 面部识别应用服务公司 Clearview AI 泄露 30 亿张人脸数据

2 月 27 日，此前因侵犯用户隐私而被推上风口浪尖的人工智能初创公司 Clearview AI 被黑，平台上超过 2000 家客户数据暴露在黑客的野心下，其中不乏美国移民局、司法部、FBI 等重要执法机构。

Clearview AI 数据库中涵盖了约 30 亿张人脸数据，仅靠一张脸部照片，就可以检索出全网所有的相关图片，包括照片的地址链接。但是，关于更具体的个人信息数据集，诸如姓名、联系方式和家庭住址，Clearview AI 还没有向 C 端公众开放。

2 月 28 日，Clearview AI 律师 Tor Ekeland 表示，公司的系统跟网络并没有受到破坏，目前已修复了相关漏洞，并保证类似事件不会再次发生。根据 Clearview AI 声明，黑客入侵者获得了未经授权的客户访问列表，其客户包括美国执法机构。

目前，苹果已禁用 Clearview AI 的开发者帐户与其 iOS 应用程序，称其违反了该科技巨头与企业开发者协议的条款。

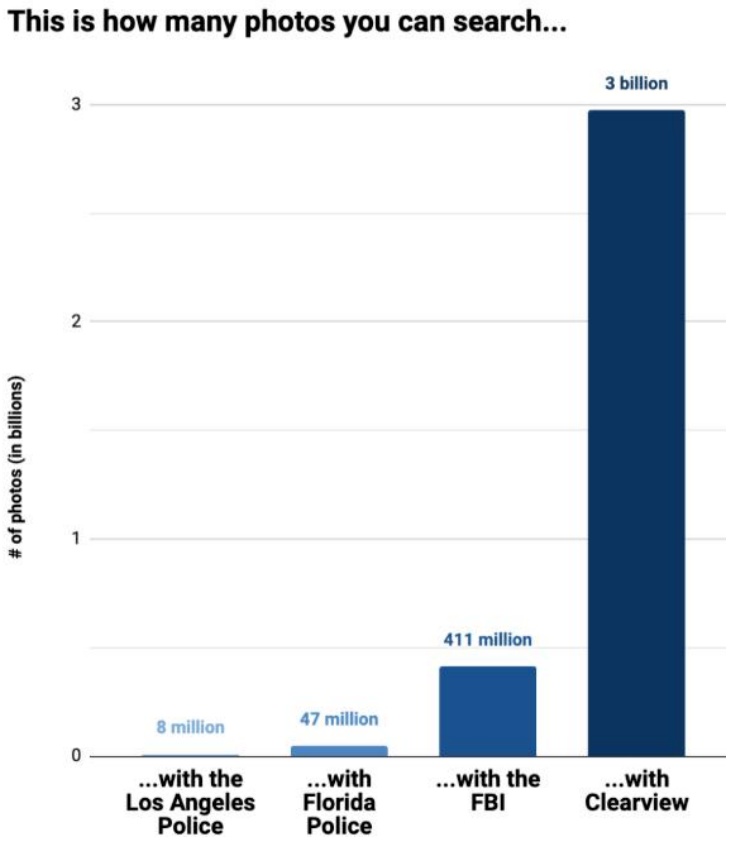
根据 BuzzFeed 披露，Clearview AI 的面部识别应用客户包括了美国移民局、司法部、银行，FBI，ICE，梅西百货，沃尔玛、NBA、阿拉伯联合酋长国的主权财富基金等 2228 多家机构和公司；此外还有更多的私人公司正在通过 30 天免费试用来测试该技术。

这其中至少有 600 家美国执法机构使用了 Clearview AI 最新的面部识别系统，数据涵盖了 Facebook、Instagram、Twitter 和 YouTube 等社交媒体平台上抓取的超过 30 亿张照片，来完善自家的数据库资源。

Clearview AI 所拥有的数据量级已远远超过了美国联邦政府或者任何一家硅谷巨头的数据体量，即使像 FBI 这样的机构，其数据库也仅仅是收集了 4.11 亿张

[12] 新京报社。

照片。



图片来源：纽约时报

单从应用的角度来看，Clearview AI 所具有的能力与服务潜力非常巨大。如抗议游行、暴动中个别激进分子的身份识别，寻找街上偶遇到的心仪对象等，不仅可以搜出他们的名字，甚至还能知道住所、工作单位和社交关系网络，可谓细思极快！

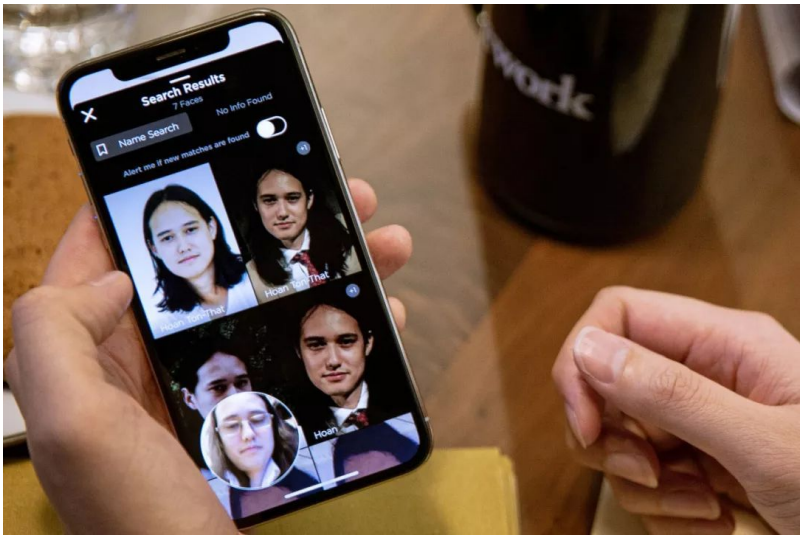
比如，只需一张照片就能从 30 亿张图像中锁定你的姓名、联系方式和家庭住址，Clearview AI 基于自身的面部识别系统和数据库协助 FBI 在内的数百家美国执法机构用面部识别技术抓捕罪犯。

早有前科

2020 年刚刚过去两个月，这家创办了四年的公司就上了两次热搜。一次是 1

月份因侵犯隐私权引发争议，另一次就是此次数据被黑引发了极大的关注。

今年 1 月，Clearview AI 因随意抓取网上照片引发争议。据《纽约时报》当时的调查显示，Clearview AI 允许执法机构使用其识别技术将未知面孔的照片与人们的在线图像进行匹配，从而搜寻潜在罪犯。随即，Twitter 向 Clearview AI 发出了一封勒令停止通知函。



仅靠一张脸部照片，Clearview AI 就可以检索出全网所有的相关图片，包括照片的地址链接。但是，关于更具体的个人信息数据集，诸如姓名、联系方式和家庭住址，Clearview AI 还没有向 C 端公众开放。

2 月 5 日，YouTube 向 Clearview AI 发出了一封勒令停止通知函，要求这家公司停止从其视频中收集人脸，并删除已经收集的数据。2 月 7，Facebook 向人脸识别公司 Clearview AI 发出了一封勒令停止通知函，要求其停止从 Facebook 和 Instagram 上获取数据。

Clearview AI 的做法违反了数据科技公司的服务条款，在这些公司不知情的情况下获取了用户数据，因此得罪了一干科技巨头。

两个月的时间里，Clearview AI 已收到来自微软、Google、YouTube、Venmo、LinkedIn 和 Twitter 的停止与禁止公函。还将面临 500 万美元的集体诉讼索赔。

600 多家执法机构在用

月初，Clearview AI 创始人兼首席执行官 Hoan Ton-That 在接受采访时并没有表现出太多对其技术的担忧。

他想以「最好的意图建立一家伟大的美国公司」，并表示不会将产品出售给伊朗、俄罗斯或中国。Hoan Ton-That 认为这项技术正在挽救孩子，解决犯罪问题。

Clearview AI 首席执行官 Hoan Ton 接受 CBS 采访，图源 | CBS 视频截图

这位越南裔澳大利亚人三次创业、自学 AI，想建立一家「伟大的美国公司」。

2016 年，Hoan Ton-That 和 60 多岁、时任纽约市市长 Rudolph W.Giuliani 助手的 Richard Schwartz 合作，着手研究面部识别工具，这就是 Clearview AI 雏形。

2019 年，Clearview AI 开始向美国的执法机构推广其服务，借助 30 天免费试用鼓励警察购买。

2019 年 2 月，印第安纳州警察局对 Clearview AI 的应用工具进行测试，仅用 20 分钟就通过围观群众拍摄的视频找到了犯罪嫌疑人的社交网站，解决了这起打架斗殴事件。

2019 年底，Clearview AI 爆火，被私家侦探广泛使用。新泽西州克利夫顿的一名侦探甚至在邮件中敦促老板购买这款软件，因为它「能够在几秒钟内识别出嫌

疑人」。

Clearview 数据库的规模让执法部门使用的其他数据库相形见绌，据《纽约时报》，Clearview AI 的应用已被包括联邦调查局和美国国土安全局在内的 600 多家执法机构使用，包括加拿大皇家骑警在内的一些执法部门也在使用，该公司声称其技术在识别个人身份方面的准确率达到 99.6%。

目前，Clearview AI 已经渗透到联邦政府的多个部门。美国司法部的多个部门在使用 Clearview AI 的产品，政府组织名单中包括美国特勤局的多个办公室（搜索次数约为 5600 个），禁毒署（约 2000 次搜寻）；酒、烟、火器和炸药局（搜索超过 2100）和 FBI（至少 20 个不同的总部外办事处进行了 5700 次搜索）。目前，这些机构的发言人对此事要么拒绝置评，要么未回应置评请求。

执法部门认可、私家侦探力荐，成为「爆款」之后的 Clearview AI 也招致了数据黑色产业链的关注，这一过程花了不到半年的时间，轰然变天的速度出乎意料。

越「火」越危险

据了解，Clearview AI 所具有的能力与服务潜力非常巨大。如抗议游行、暴动中个别激进分子的身份识别，人肉路上遇到的心仪对象等。一张照片不仅可以搜出他们的名字，甚至还能知道住所、工作单位和社交关系网络。

Clearview AI 拥有 30 亿人脸数据，一旦数据隐私泄露将带来无法估量的损失。事实上，层出不穷的数据泄露事件对个人、企业、社会的都是一种巨大的威胁。

在我国，仅 2017 年在黑市上被泄露的个人信息就高达 65 亿条次，由数据泄露而衍生出来的黑灰色产业链年获利已超百亿元。买卖公民个人隐私数据为小贷公司的「套路贷」犯罪、暴力催收大开方便之门。

2018 年 3 月曝光的 Facebook 数据泄露事件中，有 5000 万用户的个人资料，一直被用作向其精准投放政治广告的重要参考，而这些人占据着美国选民人数的四分之一。同年，万豪发布公告称旗下酒店喜达屋 5 亿房客信息被泄露；社交平台陌陌的 3000 万用户数据在暗网被销售；问答网站鼻祖 Quora 的 1 亿用户数据被窃……

2019 年 2 月，国内专注于安防领域的人工智能企业深网视界超过 250 万人

的数据被非法获取，680 万条数据疑似泄露，包括身份证信息、人脸识别图像及图像拍摄地点等。

2019 年 5 月，一名自称 GnosticPlayers 的黑客声称窃取了澳大利亚网站 Canva 的 1.39 亿用户数据，包括用户姓名、用户名、电子邮件地址、城市国家信息。

2019 年 9 月，17 万条「人脸数据」在国内的网上被公开兜售，涵盖 2000 人的肖像，每个人约有 50 到 100 张照片，每张照片还搭配有一份数据文件，除了人脸位置的信息外，还有人脸的 106 处关键点，如眼睛、耳朵、鼻子、嘴、眉毛等的轮廓信息等。数据中还能提供人物性别、表情情绪、颜值、是否戴眼镜等信息。

2019 年 12 月 4 日，一个包括 27 亿个电子邮件地址的 Elasticsearch 数据库泄露，其中 10 亿个密码都是以简单的明文存储。据悉，大多数被盗邮件域名来自中国邮件提供商，涵盖腾讯、新浪、搜狐和网易等。

动辄亿级，数据内容极其详细，此类触目惊心的数据隐私泄露事件一直在发生。

据统计，在所有的数据泄露事件中，科技行业因其信息化、数字化程度最高，颗粒度更细、价值更大，发生的数据泄露事件最多，占比为 37%。其次分别是政府机构、金融和医疗机构。

对于任何规模的公司来说，网络安全都不是小事，受众多执法部门青睐的 AI 公司更是如此。

合法合规获取数据将成为行业大势

Clearview AI 此次数据的泄露，将数据风险和数据隐私的讨论再次推上风口浪尖。长期以来，数据面临着三种风险：黑客攻击、明文存储使得数据可以轻易被复制、越权访问带来数据泄露问题。

对于侵犯用户隐私权，Clearview AI 声称拥有对公共信息的美国宪法第一修正案权利，并将其做法与 Google.com 搜索引擎进行参照比较，但这一说法并没有得到广泛「买账」。

据路透社报道，加拿大当局正在对 Clearview AI 进行调查判断其是否违反用户隐私法。在美国伊利诺伊州，Clearview AI 被诉讼指控侵犯了州居民的隐私权。新泽西州这样的部分美国地区甚至还颁布了州禁令，禁止执法机构使用 Clearview AI 的应用工具服务。

技术用于执法、维护社会正常秩序自然是好的，但一旦被黑产盯上后果便不堪设想。涉及用户隐私的问题需要企业自身强化数据管理、保护数据隐私，同时，法律法规的颁布施行也有利于遏制数据泄露的频频发生。

目前，我国「两高」司法已经对公民隐私数据问题有了解释：泄露用户通信内容五百条即可入罪。等级保护法以及有公民隐私数据的企业必须过等保安检的规定也对公民数据隐私问题有了法律层面的保护。

数据有价值，管理、技术有漏洞，数据就会有泄露的可能。目前侵犯用户隐私的行为受到越来越多的诟病，合法合规的获取数据也将成为行业大势，同时，日后更加完善的法律法规也有利于遏制数据泄露的频频发生。[13]

5. 米高梅酒店集团：逾 1060 万用户个人信息被泄露到网上

2 月 20 日，逾 1060 万米高梅酒店集团用户的详细个人信息被泄露到一个黑客论坛。

除普通游客信息外，被泄露的文件中还包含名人、科技公司 CEO、记者、政府官员、部分大型科技公司员工的详细个人信息和联系信息。

米高梅国际集团发言人证实了这一消息，并表示，这些信息是在去年的一次安全事故中泄露出来的，“我们相信，泄露的信息中不包含用户的财务、银行卡或密码信息”。

米高梅酒店集团还表示，公司已根据相关法律，向受影响的用户通报了这一事件。[14]

[13] 澎湃新闻。
[14] 凤凰科技。

6. 某国际化妆品巨头泄露 4.4 亿用户敏感信息，包括邮件地址和网络数据

最近，据安全研究人员透露，某化妆品巨头的官方服务器遭到黑客入侵，导致其未经加密保护的云数据库发生数据泄露，而服务器中则包含了数亿条客户记录以及内部日志。

研究人员表示，该品牌的云服务器中间件被曝光，并未攻击者和恶意软件提供了入侵该品牌应用程序和用户数据的二级路径。

安全研究人员表示，在此次数据泄露事件中，总共有 440,336,852 条用户的敏感数据发生了泄露，其中很多都属于包含了用户明文电子邮件地址的重要隐私信息。更重要的是，该品牌域名@estee.com 下的内部邮件地址也包含在内。除此之外，泄露的数据也包括该品牌内容管理系统（CMS）以及服务器中间件活动的日志条目。不过幸运的是，根据安全研究人员目前的取证数据，此次数据泄露事件中并没有用户支付数据或员工敏感信息被曝光。

安全研究人员在其发布的安全报告中写道：“该品牌这家公司已经家喻户晓了七十多年了，而这家公司在 2019 年的收入约为 147.63 亿美元。因此，该公司肯定会有一个跟其业务相关联的大型数据集或数据库，这也是合乎业务逻辑的。此次数据泄露事件涉及到了大量的消费者电子邮件地址，我们在发现此次事件之后也立即向该公司上报了事件详情。据统计，在此次数据泄露事件中，总共有 440,336,852 条用户的敏感数据发生了泄露。”

在接受采访时表示：“根据目前的分析结果，我只能推测或假设这些电子邮件地址来自于该品牌的线上销售渠道。”安全研究人员指出，至于其他的泄露数据，其中大部分都可以为攻击者今后的大规模网络攻击做准备，因为他们目前已经完成了前期网络侦察阶段的工作。比如说，泄露的日志记录就包含该品牌网络服务器的 IP 地址、端口、路径和存储信息，而攻击者就可以利用这些数据来绘制雅诗兰黛公司内部局域网（LAN）或外网（WAN）结构，以及公司用来连接不同数据生成设备的中间件详情。

中间件通常需要负责处理类似提供一致性前端结构方面的任务，而这些数据管理前端需要跨不同内部系统、应用程序服务、消息、身份认证和 API 管理来实现其功能。

暴露在外或未受保护的中间件可以为恶意软件提供一个辅助的入侵路径，攻击者将能够通过这种二级路径来入侵目标应用程序或窃取目标数据。在这种情况下，任何联网的用户都可以查看到目标系统当前所使用的系统或软件版本，路径地址以及其他可以作为网络后门所使用的数据。

在发现了此次数据泄露事件之后，安全研究人员在几个小时内打了多通电话并发送了几封电子邮件之后，终于得以向该品牌的安全团队传递了一条信息，数据库也于当天下线关闭。目前具体还不清楚该品牌的数据库被入侵了多长时间，也不清楚在这段时间内还有哪些人访问过这些记录，因此广大的客户在这段时间以及今后的日子里应该对网络钓鱼邮件保持警惕。

来自 KnowBe4 的安全意识倡导者通过电子邮件表示：“该品牌所发生的此次数据泄露事件足以证明，一个非常简单的错误就极有可能带来非常严重的后果，就好比这一次，该品牌的工作人员在共享驱动器或数据库中设置了错误的权限一样。”不过，他也对该品牌安全团队的迅速响应表示了称赞。这对于其他公司来说，也是一次教训，很多大型组织应该根据现有的网络态势来改进自己的网络安全事件响应机制，以便快速解决数据泄露等安全问题。尤其是在这个网络技术如此发达的时代，数以百万计的记录都可以存储在一个地方，而任何人几乎可以从世界的任何一个角落随时读取到它们。克朗也表示，他之所以对雅诗兰黛的迅速响应表示认可，是因为很多其他类似的大型组织在这方面采取行动的速度实在是太慢了。

由于错误配置而导致数据库发生泄漏，在当前的互联网中是一个非常常见的事情，很多存储了大量数据的大型公司也同样无法“避免与难”。就比如说，在今年的一月份就有消息称，微软的云数据库中由于错误配置就导致了 2.5 亿条数据记录发生泄漏，而且泄露时间长达 25 天。其中，有的泄露数据以及用户账号最早可以追溯到 2005 年，而最新的用户数据则是 2019 年的 12 月份。毫无疑问，这些泄漏的数据将会让用户暴露在网络钓鱼攻击以及网络欺诈活动的威胁之下。[15]

7. 戴尔 21 亿美元出售旗下网络安全业务

2 月 18 日，戴尔将以 20.8 亿美元的价格，把旗下网络安全业务 RSA 出售给由私募公司 Symphony Technology Group、安大略省教师退休基金会和荷兰养老基金公司 Alpinvest Partners 领导的财团。戴尔表示，此项交易预计会在未来 6 至 9 个

[15] 数安时代 GDCA。

月内完成。

据了解，戴尔在 2016 年通过收购科技公司 EMC 获得 RSA 业务。RSA 为累计 3 万家客户提供安全和数字风险管理软件，以及一项以 RSA 命名的加密技术。

另外，戴尔表示，RSA 可以帮助其检测、调查以及应对安全风险，并且减少知识产权盗窃，欺诈和网络犯罪。

事实上，三个月前，彭博社就曾报道称，戴尔有意出售 RSA 业务的消息。近年来，RSA 一直面对来自 Okta Inc.和 Ping Identity Holding Corp.激烈的竞争。[16]

8. 海能达中招摩托罗拉"美国陷阱" 遭美判赔 53 亿股价跌停

2 月 17 日，海能达（002583.SZ）披露的关于重大诉讼的进展公告显示，海能达及全资子公司美国公司、美西公司与摩托罗拉、摩托罗拉马来西亚公司之间的商业秘密及版权侵权诉讼案件已于美国当地时间 2019 年 11 月 6 日（北京时间 2019 年 11 月 7 日）开庭。美国当地时间 2020 年 2 月 14 日（北京时间 2020 年 2 月 15 日），伊利诺伊州法院陪审团对本案件作出了裁决，认为海能达、美国公司及美西公司侵犯摩托罗拉一项或多项商业秘密及美国版权，应向摩托罗拉支付损害赔偿 3.46 亿美元及惩罚性赔偿 4.19 亿美元，合计 7.65 亿美元（约合人民币 52.71 亿元）。

受此影响，今日开盘，海能达股价一字跌停。截至发稿，海能达报 7.34 元，跌幅 9.94%，成交额 4882.35 万元，换手率 0.63%。

公告显示，2017 年 3 月 15 日，海能达的两家全资子公司美国公司和美西公司收到美国伊利诺伊州法院送达的诉状，摩托罗拉及摩托罗拉马来西亚公司起诉公司及美国公司、美西公司商业秘密侵权，认为公司部分产品侵犯了摩托罗拉商业秘密。2018 年 8 月 2 日，摩托罗拉向伊利诺伊州法院提出增加版权侵权的诉讼请求，认为公司部分产品侵犯了摩托罗拉美国版权。其后案件进入证据开示阶段，至 2019 年 9 月，案件证据开示全部结束。

根据伊利诺伊州法院的安排，上述商业秘密及版权侵权诉讼案件已于当地时间 2019 年 11 月 6 日（北京时间 2019 年 11 月 7 日）进入庭审阶段。当地时间 2020

[16] 观察者网 。

年 2 月 12 日，摩托罗拉在庭审中最终明确其主张公司部分 DMR 产品侵犯摩托罗拉 21 项商业秘密及 4 项美国版权，要求公司、美国公司及美西公司就侵犯其商业秘密行为支付相应赔偿。

美国当地时间 2020 年 2 月 14 日，上述案件陪审团作出裁决，认为公司、美国公司及美西公司侵犯摩托罗拉一项或多项商业秘密及美国版权，应向摩托罗拉支付损害赔偿 3.46 亿美元及惩罚性赔偿 4.19 亿美元，合计 7.65 亿美元（约合人民币 52.71 亿元）。

本次陪审团裁决结果并非一审判决，陪审团裁决结果仍需伊利诺伊州法院审查后作出一审判决。

海能达表示，鉴于上述案件未形成生效判决，对公司本期利润或期后利润影响金额尚具有不确定性，基于谨慎性原则，公司将会就一审判决结果在 2019 年度报告资产负债表日后事项中详细披露，并按照《企业会计准则第 13 号—或有事项》及公司会计政策相关规定预提预计负债，具体数据以公司审计机构的审计结果为准。

海能达还称，公司对本次陪审团裁决表示失望，尊重但不同意本次陪审团裁决。本次陪审团裁决结果仍需伊利诺伊州法院审查并作出一审判决。如果伊利诺伊州法院一审判决支持本次陪审团裁决结果，公司将保留对一审判决进行上诉的权利，以进一步维护公司权益。公司相信美国司法系统终将对该纠纷做出公正的裁决。

上述陪审团裁决涉及赔偿金额较大，本诉讼事项已构成重大诉讼，将对海能达 2019 年度净利润构成重大影响。2 月 3 日，海能达披露的 2019 年度业绩预告显示，预计 2019 年归属于上市公司股东的净利润 4.80 亿元-5.80 亿元，比上年同期增长 0.67%－21.64%。[17]

9. 美检察长指控谷歌侵犯隐私：收集学龄儿童数据

2 月 21 日，美国新墨西哥州总检察长赫克托·巴尔德拉斯（Hector Balderas）周四对谷歌提起诉讼，指控谷歌从该州的学龄儿童那里收集个人信息，侵犯了他们

[17] 中国经济网。

的隐私权。

巴尔德拉斯指控该公司未经儿童父母同意，使用其 Gmail、日历和云盘等产品套件来收集 13 岁以下学生的信息。他说，这种收集个人数据的行为违反了《联邦儿童在线隐私保护法》和《新墨西哥州不公平行为法》。

谷歌发言人何塞·卡斯塔内达（Jose Castaneda）否认了这一说法，并表示学区可以决定如何在课堂上最好地使用这些工具。他补充说：“教育版 G Suite 允许学校控制帐户访问权限，并在必要时要求学校征得家长的同意。”

2018 年，巴尔德拉斯对谷歌和其他几家科技公司提起了类似的诉讼，指控他们从为儿童制作的移动应用程序中非法收集数据。两家公司否认有任何不当行为，此案仍在等待联邦法官的裁决。

去年 9 月，谷歌的 YouTube 视频服务被要求向联邦贸易委员会（FTC）支付 1.7 亿美元，以和解关于其收集儿童个人信息的行为违反联邦法律的指控。

社交媒体公司一直在全球范围内因为其政策和数据监控实践（尤其是针对儿童的政策）面临监管审查。Facebook 本月初表示，该公司计划在其消息应用中为 13 岁以下的用户添加新的工具和功能，从而实现家长控制。[18]

10. 为结束隐私泄露调查 Facebook 或被处罚数十亿美元

2 月 15 日，据《华盛顿邮报》援引两位知情人士消息称，美国联邦贸易委员会（FTC）和 Facebook 正在就一笔数十亿美元的罚款进行谈判，如果谈判成功，该机构对 Facebook 的隐私侵权行为调查告一段落。

这将是 FTC 对高科技公司实施的最高处罚，但双方尚未就具体金额达成一致。其中一位知情人士说，Facebook 的谈判代表对该机构提出的条款表示了担忧。如果 FTC 和 Facebook 无法达成协议，FTC 可能起诉 Facebook，并将其告上法庭，结果可能是会被处以比双方目前正在谈判的罚款金额还要高得多的罚款。

每违反一项同意判决，Facebook 就可能面临最高 41484 美元的罚款。考虑到

[18] 新浪科技。

仅在剑桥分析公司泄露事件中受影响的客户记录数量，理论上将 Facebook 可能要承担高达数十亿美元的罚款。

Facebook 证实正在与该机构商讨有关事宜，但拒绝进一步置评。联邦贸易委员会也拒绝置评。

由于 Facebook 公司出现一系列隐私权问题，立法者指责该公司没有正确处理数据，同时，未能弥补其它数字缺陷，包括未能阻止网上仇恨言论的兴起，以及俄罗斯等势力造成的虚假信息传播。

民主党参议员理查德·布卢门撒尔（Richard Blumenthal）说："Facebook 面临着一个清算时刻，唯一的办法就是通过一项 FTC 命令实行严厉惩罚和其它制裁措施，阻止这种隐私不当行为愈演愈烈。"

对于联邦贸易委员会来说，对 Facebook 施加重大惩罚可能代表着硅谷公司在经历了数年的隐私失策后，迎来了新的审查时代。迄今为止，联邦贸易委员会对科技巨头违反与政府签订的保护消费者数据协议的最大罚款事件，是谷歌在 2012 年支付 2250 万美元罚款来解决调查问题。

电子隐私信息中心（Electronic Privacy Information Center）的执行董事马克·罗滕伯格（Marc Rotenberg）说："目前，一个悬而未决的问题是 FTC 是不是一个有效的隐私机构，同时，FTC 是否愿意利用目前的权力来保护美国消费者隐私，这也是一个悬而未决的问题。"罗滕伯格表示，巨额罚款和其它处罚措施"表明，FTC 现正准备执行同意令。"

FTC 对 Facebook 的调查始于去年三月，是为了回应社交巨头与 Cambridge Analytica 的数据泄露丑闻。后者是一家政治咨询公司，曾采取不正当手段访问了社交网站 8700 万用户的数据。该机构的调查重点是 Facebook 的行为——以及最近几个月公布的一系列隐私问题——是否违反了 Facebook 与 FTC 在 2011 年为改善隐私做法而达成的协议。Facebook 坚持认为自己没有违反这项协议。

《联邦贸易委员会协议》规定，Facebook 在与第三方共享个人数据之前，必须更加透明，并以更清晰的方式通知用户。该命令还禁止 Facebook 在处理隐私问题时欺骗用户，并规定将对后者使用数据的方式进行定期检查。根据 FTC 的规定，该机构可依据企业违反此类命令的次数来决定高额罚款金额。

Facebook 可以与美国政府达成协议，同意支付罚款，并对其业务实践进行一些修改。这项解决方案必须得到法官的批准。另外两名知情人士表示，联邦贸易委员会的处罚可能包括一项新的命令，迫使这家科技巨头接受更严格的检查，以确保其遵守和解协议。

另外，Facebook 也可以选择与联邦机构就其调查结果和提议的惩罚方式进行抗辩。分析人士说，如果这场争斗在联邦法院展开，最终结果可能是两败俱伤，因为 Facebook 的高层管理人员不得不出庭作证，同时，FTC 对科技巨头的制裁将接受备受瞩目的司法审查。

但如果 Facebook 决定与 FTC 抗争，该公司可能面临巨大的信誉风险。《消费者报告》杂志的消费者隐私和技术政策主管贾斯丁·布鲁克曼（Justin Brookman）说："他们在损失用户，他们在丧失信任，我认为这只会使问题雪上加霜。"

去年，英国监管机构曾就社交网络巨头与 Cambridge Analytica 之间的纠纷征收过一笔小额罚款，Facebook 表示抗辩。该公司也在回击哥伦比亚特区司法部长提起的诉讼，该诉讼称 Facebook 在数据收集中误导了用户。纽约、宾夕法尼亚和加利福尼亚等州的一批其他首席检察官此前表示，他们正在对 Facebook 展开调查。

此外，华盛顿州的一批消费者权益倡导者上个月敦促 FTC 对 Facebook 进行"巨额罚款"，总额可能超过 20 亿美元，同时还要求 FTC 发布命令，对 Facebook 收集用户数据的方式和时间作出限制。

"该公司的商业行为给美国、儿童和有色人种社区的隐私和安全以及美国和世界各地民主机构的健康带来了巨大损失，"以美国电子隐私信息中心为首的消费者团体写道，该组织的投诉是 2011 年 Facebook 公司与 FCT 达成和解的最初诱因。

在 Facebook 首次宣布启动调查一年后，立法者也在敦促 FTC 加快工作速度，并对 Facebook 进行处罚。布卢门撒尔和马萨诸塞州民主党参议员爱德华·马基（Edward J. Markey）今年一月在一封信中写道，"当美国人的隐私受到侵犯时，他们应该迅速而有效地做出回应。"[19]

[19] 新浪科技。

11. iphone 这一功能打开 5400 个 APP 或将泄露你的信息

最近，美国就“华盛顿邮报”进行了一个实验。这篇报道标题是：午夜时分，你知道你的苹果手机在跟谁说话吗？这篇文章做出一系列调查和实验，包括在记者的苹果手机上连接上一个监控软件，而在之后的一周之内，发现了超过 5400 个隐藏的用户信息获取跟踪软件。

这意味着，苹果手机上的程序，向第三方跟踪公司不断发送个人数据，尤其是在深夜。而传送的数据包括了用户的邮件、电话号码、IP 地址，甚至用户的具体位置。而文章强调说，除了苹果手机，在谷歌安卓的手机系统上，手机软件向第三方跟踪公司发送数据的情况也有发生。

这个情况发生在什么样的背景下呢？在这里我们不得不解释一个功能，这就是：目前智能手机，包括苹果的“后台应用刷新”功能，允许手机在未被频繁使用的情况下传输数据。这个功能的本意，是给用户提供最新最快的体验。但现在看来，一些第三方的程序为了提高自身的定制广告准确度，以及为了改善应用程序的表现，而会用这样的追踪软件来收集用户信息。

比如，微软的 OneDrive、耐克、收听音乐的 Spotify，乃至于“天气频道”的应用程序中都发现了追踪软件。这使得一个问题浮出水面：“后台应用刷新”功能被滥用了吗？

苹果公司表示，对于第三方应用程序创建的数据和服务，苹果 iTunes 的指引是要求程序开发者清晰地列出其私隐政策，事先得到用户许可。而苹果一旦发现有应用程序没有跟随私隐指引，那么会要求对方修正，或将其下架。但不少用户对这样“事后诸葛亮”的做法，以及智能手机对“第三方应用如何使用用户数据”的监管缺失，仍然感到不满。

也有分析建议说，苹果可以在 iOS 系统中添加“监控软件”，让用户对信息的追踪情况有更好的了解。而另外一个选项是，苹果可以硬性要求，所有第三方程序必须清楚地标记出，其所用的跟踪软件。

对此，苹果公司在接受《华盛顿邮报》采访时则表示，用户可以选择关闭“后台应用刷新”功能，苹果公司也已经提供了一些限制广告跟踪的工具来保护用户的数据隐私。 但不少用户还是对苹果公司的管控不力表示不满： “你的手机就是源源不断的廉价信息的来源”“任何缺乏应有的保护机制的科技都是别有用心和失败

的”

总而言之，对信息泄密建立所谓的“问责制”，也许是所有人能更重视数据问题的解决之道。而现在对于苹果公司来说，此前公司承诺，“iPhone 上发生的事情将保留在您的 iPhone 上”，而现在看来，苹果需要付出更多的数据保护措施，才能坚守这个承诺。[20]

12. 美国被曝控制瑞士公司偷取 120 多个国家情报

美国《华盛顿邮报》日前披露，美国和原联邦德国（西德）的情报部门从 20 世纪 70 年代开始秘密操控瑞士加密设备供应商克里普托 AG（Crypto AG）公司的生产和经营，以获取超过 120 个国家的加密通讯信息。

两德统一不久后德国方面退出这个行动，而美国直至 2018 年才停止这个被称为“世纪情报政变”的情报窃取行动。

赚钱的同时还窃取别国秘密

《华盛顿邮报》2 月 11 日刊登了一篇题为《中情局买了一个向世界各国售卖加密设备的公司，然后他们的间谍就坐下来慢慢听》的长文。报道称，瑞士克里普托 AG 公司早在二战期间因向美军提供密码加密设备而发家。经过几十年的发展，克里普托 AG 公司已经成为世界主要加密设备生产商之一。

进入 21 世纪以来，克里普托 AG 公司的产品销往世界 120 多个国家，其中包括伊朗、印度、巴基斯坦和拉美国家等。然而这些国家不知道的是，他们信赖的这家瑞士公司从 20 世纪 70 年代以来就一直被美国中情局和主管破译密码的国家安全局所控制。克里普托 AG 公司几乎所有行为都受到这两家美国情报机构和原联邦德国情报部门的左右，包括人员雇佣、技术研发、破译算法、销售对象的选择等等。只要是克里普托 AG 公司生产的设备传送的加密信息，理论上中情局都可以轻易破译。中情局给克里普托 AG 公司行动计划起的代号早期叫做“分类词典”，后来改名“卢比孔河”。

《华盛顿邮报》称，其与德国电视二台一起获得了一整套有关冷战期间中情局

[20] 中国科学院。

克里普托 AG 公司相关专项行动的材料。材料中甚至包括了中情局负责该专项行动的人员姓名，以及克里普托 AG 公司内部与中情局对接的高层管理人员姓名等。材料描述了美国及其盟国多年来如何利用其他国家的轻信，在赚取经济利益的同时还窃取别国秘密。中情局在材料中高度评价了克里普托 AG 公司相关行动，称其为“世纪情报政变”。

报道称，通过克里普托 AG 公司的设备，美国与西德情报人员曾在 1979 年美国驻伊朗大使馆人质危机期间监视伊朗最高领袖的言行，在 1982 年马岛战争中向英国提供阿根廷军方的情报，在 1986 年柏林舞厅爆炸案后掌握利比亚领导人的相关情报等。1990 年两德统一后，德国情报机构认为上述情报窃取行动暴露风险太大，不久便退出。美国中情局随即花 1700 万美元买下了德方持有的股权并继续执行该行动直到 2018 年。

报道还称，除美国和德国外，至少还有 4 个国家知晓克里普托 AG 公司行动的存在，它们分别是以色列、英国、瑞典和瑞士。

美军正为网络战加强准备

《华盛顿邮报》的报道并不是国际媒体首次聚焦克里普托 AG 公司可能的窃密行为。克里普托 AG 公司一名职员 1992 年因疑似从事间谍活动，在伊朗监被监禁 9 个月。美国和德国媒体早在 1995 年和 1996 年就怀疑德美两国机构在克里普托 AG 公司的设备上“动了手脚”，但当时克里普托 AG 公司回应称报道毫无依据。

美媒披露的克里普托 AG 公司行动只是美国网络恶行的一个例子，这样的例子还有很多。2017 年 4 月，媒体爆料与美国国家安全局相关的黑客组织攻击转账结算系统 SWIFT 在中东地区最大的金融服务提供商 EastNets，窃取了大量主机信息、登录凭证等。去年 6 月，美国情报部门被曝对伊朗计算机系统发起攻击，使伊朗的火箭发射系统瘫痪；向俄罗斯电力系统植入恶意代码，以便刺探情报或对俄电力系统发动网络攻击。

而在体制和战略方面，美国政府 2017 年将美军网络司令部正式升级为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平；2018 年发布网络战略报告，强调要在网络空间里“先发制人”。有分析认为，种种动向表明，美国正紧锣密鼓地为网络战加强准备。

分析人士指出，美国素来以“网络安全卫士”自居，频频指责他国发起网络攻

击、破坏网络安全，却无视自身的斑斑劣迹。此次曝出的通过瑞士公司设备窃取他国情报事件，再次凸显出美国贼喊捉贼的网络霸凌思维。

瑞士“中立地位”将受影响

克里普托 AG 公司在 2018 年已经重组为两家公司，两家公司目前都拒绝置评公司 2018 年以前的经营行为。有报道称，瑞士联邦经济事务部已经暂停了两家公司的出口许可。

该行动曝光后，有来自瑞士的评论认为，这起事件恐将影响瑞士这个永久中立国“政治身份认同的基础”和今后在国际事件中的中立性。《新苏黎世报》说，瑞士向来以在国际事务中保持中立而著名，瑞士科技公司也依赖国家的中立地位发展业务。“斯诺登事件”以来，美国供应商被贴上了不安全的标签，瑞士公司则在国际市场上取得领先。如果直到两年前克里普托 AG 公司实际上还是美国中情局监听网络的一部分，这会影响瑞士整个行业的声誉，从而损害竞争优势。[21]

13. Facebook Dating 因监管问题无法如期在欧洲上线

据外媒报道，在爱尔兰监管机构提出数据保护担忧后，Facebook 被迫推迟其在欧洲推出约会服务的时间。根据欧盟规定，企业在推出可能影响客户数据的产品或服务之前必须进行数据处理影响评估(DPIA)才行。

爱尔兰数据保护委员会披露，Facebook 本来打算在情人节的前一天推出 Facebook Dating，但他们对此表示非常担心，因为他们一直到昨天（当地时间 2 月 12 日）才得知这一消息。

Facebook Dating 于去年在美国推出，目前已经在全球 20 个国家上线。用户可以利用自己现有的 Facebook 账号数据来快速创建一个 Dating 个人档案，同时还可以整合来自 Instagram 上的照片。然后，用户就可以选择跟好友的好友中的潜在约会对象进行配对或选择完全不在自己好友圈的人。

在提供给《华尔街日报》的一份声明中，Facebook 表示，他们需要更多点的时间来确保产品准备好进入欧洲市场，另外它还补充称，它已经在努力工作进而建立

[21] 新浪新闻。

起强有力的隐私保护措施，并会在欧洲推出之前跟 IDPC 共享这些信息。Facebook 指出，他们已经完成了所需的数据隐私评估并在监管机构要求时将其分享给它。但不管怎样，这款应用应该是无法在情人节这天来到欧洲用户的身边了。[22]

14. 迪卡侬数据库泄露 1.23 亿条记录

体育连锁巨头迪卡侬（Decathlon）发生大范围数据泄露，起因是 1.23 亿条记录被保存在一个并不安全的数据库中。这是由 vpnMentor 安全研究人员发现的，并在本周一公布。该数据库属于迪卡侬西班牙和迪卡侬英国公司。

泄露的数据涉及员工系统用户名、未加密的密码、API 日志、API 用户名、个人身份信息等。对于迪卡侬员工来说，涉及的信息包括姓名、地址、电话号码、生日、学历和合同明细，而对于客户来说，涉及的信息包括未加密的电子邮件、登录信息和 IP 地址。

该数据库漏洞于 2 月 12 日被发现，迪卡侬于 2 月 16 日得到通知，随后数据库于 2 月 17 日下线。研究人员指出：“迪卡侬位于西班牙的这个数据库包含了员工数据信息和更多内容。从理论上讲，这包括了恶意黑客想要接管帐户、盗取私人信息甚至是专有信息的所有内容。”迪卡侬尚未对此发表评论。

安全意识培训公司 KnowBe4 的安全意识倡导者 James McQuiggan 表示：“负责保护和使用数据的员工需要有一个强大的安全程序，了解存储数据的系统，监控所有访问行为。”“该数据库在互联网上是可以查看的，没有安全和加密；这种危险的做法肯定会导致大量敏感数据的泄露。把数据放在面向互联网的服务器上，其中包含大量未加密的、不安全的敏感数据，这就好比敞开你家里的后门一样。”

McQuiggan 指出，由于此次泄露涉及所有个人数据，员工很可能遭到身份盗用、鱼叉式网络钓鱼、以及人身伤害的风险。“如果数据被罪犯窃取，他们就会铤而走险发布网络钓鱼电子邮件。他们应该密切关注他们的信用帐户，确保知悉所有操作，例如更改地址或者开设新帐户。”[23]

[22] 搜狐网。
[23] 快资讯。

四、环球评论

1. 花季守护——ICO 依“龄”设计规范（上）

英国信息专员办公室（ICO）于 2020 年 1 月份发布了最终版本的《适龄设计规范》（Age Appropriate Design Code，以下简称“《规范》”），《规范》将被提交至议会，预计将于 2021 年秋季生效。

英国议会要求 ICO 制定《规范》的目的在于确保英国《数据保护法案》（DPA）的真正落地。《规范》具体解释了如何将 GDPR 的相关规定适用于使用网络服务的儿童。并在制定过程中充分咨询了父母、儿童、学校、儿童保护团体、开发者、技术和游戏公司以及在线服务提供商的意见，并与之进行充分对话。

ICO 认为，制定《规范》的必要性在于，英国五分之一的互联网用户是儿童，但他们使用的网络却不是为他们设计的。在 ICO 此前进行的调查中，英国儿童将现有的实践情况描述为“管闲事”、“粗鲁”和“有点怪异”的。而 ICO 针对人们最关心的数据保护问题进行过全国调查，结果显示，儿童的隐私保护问题位居第二，仅次于网络安全。这一情形与英国通信管理局和伦敦经济学院进行的调查所反映的情况类似。《联合国儿童权利公约》（UNCRC）指出，儿童在其生活的各个方面都需要特殊保障。欧盟数据保护法也反映了这一点，并为儿童提供了附加保护措施。《规范》基于 UNCRC，并反映出了全球治理的方向，美国、欧洲和经济合作与发展组织（OECD）也正在考虑进行类似的改革。

一、《规范》目的

英国议会要求 ICO 制定《规范》的目的在于确保英国《数据保护法案》（DPA）的真正落地，《规范》要求公司在设计、开发或提供可能被儿童访问的在线服务时将儿童的利益放在首位。具体而言，《规范》旨在确保网上服务提供商使用儿童数据的方式合规，保护儿童享有隐私权、言论自由、思想和宗教自由等基本的权利和自由。

《规范》由 15 条灵活的标准组成，其重点是提供高度隐私的默认设置，该默认设置应当确保在信息收集和使用的最小化，同时使得儿童能够最大程度地访问在线服务。并且应当确保选择更改默认设置的儿童在更改之前获得正确的信息、通知和建议，并为其个人数据的使用提供适当的保护。

《规范》为每一项标准提供了详细的解释和合规指引，以帮助企业证明其履行了 GDPR 和《隐私与电子通信条例（2003）》（PECR）等数据保护义务。对企业而言，是否符合《规范》所制定的标准将成为企业是否遵守数据保护相关法律的关键指标。换句话说，若企业不遵循《规范》，将很难证明其符合 GDPR 和 PECR 的规定。

二、《规范》的适用范围

《规范》适用于信息社会服务（Information Society Service）的提供者。不仅适用于专门针对儿童的在线服务，也包括**可能被英国儿童访问**的在线产品或服务，例如 App、程序、新闻、教育等网站、网络游戏或社区环境，以及带或不带屏幕的联网玩具或设备、搜索引擎、社交平台、直播服务等。[24]需要注意的是，如果企业无论如何都不希望儿童使用其服务，那么就需要关注如何阻止儿童访问，其服务不应当对儿童友好（child-friendly）。如果企业的服务并非面向儿童，但是儿童也可使用，那么企业应当关注其服务是否对儿童有吸引力，如果企业认为其提供的服务性质、内容对孩子具有吸引力，那么就应当遵守《规范》中的标准。如果企业用户群体已经包含了实质性且可识别的（substantive and identifiable）儿童群体，则需要适用《规范》。如企业认为其不需要适用《规范》，则需要对相应的理由进行记录和支撑，例如进行市场调研、关于用户行为、类似或现有服务的用户基础的证据等。

关于《规范》是否适用于英国以外的 ISS 提供者，ICO 指出，《规范》的发行根据是英国《数据保护法》【DPA（2018）】。DPA（2018）适用于英国的在线服务，也适用于英国以外的、在英国设有分支机构或办事处或其他“机构”（establishment）并由该英国外实体处理个人数据的在线服务提供者。此外， ICO 指出，若机构不在欧洲经济区（EEA）范围内，但向英国用户提供服务或者实施监控用户的行为，则仍然适用 DPA（2018）。若儿童可能访问上述服务，则将适用《规范》。

如果企业在英国没有机构，但是在 EEA 的其他地方设有机构，则不适用《规范》（即使向英国用户提供服务或监视用户在英国的行为）。若企业的在线服务适用《规范》，但是根据 GDPR 的“一站式”（one-stop-shop）安排，企业拥有除 ICO 以外的主要监管机构，那么 ICO 将要求该监管机构在判断企业是否遵守 GDPR 和 PECR 时将《规范》纳入考量范围。如果为“本地”案例（仅影响英国用户），则 ICO 可以自己采取行动并将《规范》纳入考量范围。

关于“脱欧”对《规范》效力和适用范围的影响，ICO 指出，《规范》的主要依

[24] 《规范》对 ISS 的含义、ISS 之外的在线服务类别、“可能被儿童访问”等概念进行了详细的说明。

据是 DPA(2018)和 GDPR。如实现无协议脱欧，英国版本的 GDPR 将会被写入英国法律，即 UK GDPR，届时《规范》的基本原则和义务将会保留在 UK GDPR 项下。如英国和欧盟就此达成协议，则在退出之前的实施期内，《规范》和 GDPR 将依然适用。在实施期结束后，默认状态和无协议脱欧的情况相同，ICO 预期《规范》依然有效。因此，尽管可能面临脱欧的问题，但是《规范》始终将会被适用。

三、《规范》的实施

ICO 指出，《规范》的发布依据是 DPA（2018）。根据 DPA(2018)第 123 节，ICO 必须起草行业规范。如果企业无法证明其遵守《规范》，则无法证明其满足法律法规的要求，从而引起监管问题。《规范》也可能被作为诉讼中的证据。需要，《规范》并非数据保护合规的穷尽式指南，企业也可根据自身情况采取合规措施。

为此，《规范》首先要求企业实施责任机制，根据自身规模、资源和业务情况，有效地执行《规范》中的标准和要求。其次，企业应当有相应的政策来支持和证明其符合数据保护的要求。再次，企业应当注重对员工的培训。最后，企业需要注重对处理活动、DPIA 等进行适当记录，并及时做好证明自己符合《规范》的准备，以备核查，或者在可以申请认证时通过认证的方式证明自身合规性。

ICO 将通过一系列的主动审核来监管企业对《规范》的遵守情况，并考虑投诉情况，将监管重点放在涉嫌重复或故意或严重违反法律的组织和个人身上。其惩罚措施包括：发出评估通知（assessment notices）、警告(warnings)、谴责(reprimands)、要求立即停止和罚款。ICO 在行使权力时，将会考虑企业处理活动对儿童引发的风险、企业规模和资源、技术可行性以及企业是否努力满足《规范》等因素。

四、实务指南

ICO 主要针对 15 项标准均给出了具体的解释和合规建议，对此梳理如下：

（一）儿童最大利益

在设计和开发可能被儿童访问的在线服务时，儿童的最大利益应该是首要考虑的因素。儿童最大利益原则来自 UNCRC 第 3 条，英国议会要求 ICO 在起草《规范》时必须考虑到英国根据 UNCRC 所承担的义务。该原则提供了一个框架来帮助企业了解儿童的需求以及设计在线服务时必须考虑的儿童权利。企业在使用儿童的个人数据时，应当考虑如何：

· 使他们免受剥削风险，包括商业或性剥削和性虐待的风险；

· 保护和支持他们的健康和福祉；

· 保护和支持他们的身体，心理和情感发展；

· 保护和支持他们发展自己的观点和身份的需求；

· 保护和支持他们的结社和娱乐自由权；

· 根据在英格兰、苏格兰、威尔士和北爱尔兰的相关平等法规下的义务，支持残疾儿童的需求；

· 认识到父母在保护和促进儿童的最大利益中的作用，并支持他们完成此任务；和

· 认识到儿童形成自己观点的能力，并给予这些观点应有的重视。

考虑到儿童的最大利益并不意味着不能追求商业利益或其他利益。而只是意味着，在企业的商业利益和儿童的最大利益无法兼顾时，企业需要将儿童的最大利益作为首要考虑因素。

（二）数据保护影响评估（DPIA）

采取 DPIA 以评估并减轻相关风险，保护可能访问在线服务的儿童的权利和自由。进行 DPIA 时应将不同的年龄、能力和发展需求纳入考虑范围。DPIA 必须特别关注使用在线服务的儿童的相关权利和因数据处理而导致其承受的风险，还应当评估和记录企业对《规范》的遵守情况。企业应该将如下元素构建到 DPIA 的每个阶段中——

步骤 1：进行 DPIA 的时间

一旦设计了新的线上服务并且可能会被儿童使用，则必须进行评估。企业必须在服务发布之前完成 DPIA，并确保评估结果能够影响服务的设计。如果现有在线服务可能有儿童访问，在处理操作发生任何重大更改时，也必须进行 DPIA。

在线服务的外部因素发生变动时，企业也可能需要审核 DPIA。例如，发现了新的安全漏洞，或者服务的特定功能或对儿童的特定风险引起了社会关注。

步骤 2：对数据处理的说明

需要描述处理活动的性质、范围、背景和目的。特别应包括：服务是否为儿童设计；如果不是，儿童是否可能使用该服务；这些儿童的年龄范围；家长控制计划（如有）；确定个人用户年龄的计划（如有）；带给儿童的预期利益；已经考虑的（企业或第三方的）商业利益；涉及的任何画像或自动决策；地理位置定位；轻推技术的使用；对特殊类别数据的处理；对推测得到的数据的处理；当前公众关注的任何有关儿童线上风险的问题；相关的行业标准或行为规范；根据英格兰、苏格兰、威尔士和北爱尔兰的适用法律所承担的责任；相关年龄范围内儿童的发展需求，福祉或能力的相关指南或研究。

步骤 3：咨询儿童和父母

ICO 希望大型组织在大多数情况下都能进行某种形式的咨询。例如，从存量用户获取反馈、进行一般的公众咨询、进行市场调查、进行用户测试或者征求相关儿童权利组织的意见。如果无法进行任何形式的咨询，或者咨询不适当，则应将该决定记录在 DPIA 当中，并向 ICO 证明此决定的正当性。但通常而言，某种形式的市场调查或者用户反馈是可行的。

在此阶段，关于儿童权利和发展需求，企业还应该考虑寻求专家的独立建议。尤其对于以下服务：（1）专为儿童设计的；或者（2）为一般用途而设计，但已被儿童广泛使用（例如游戏或社交媒体网站）；或者（3）以新奇或者超出预期的方式使用儿童的数据。

步骤 4：评估必要性、比例性和合规性

企业需要解释数据处理符合必要性和比例性。企业还必须提供有关如何遵守 GDPR 的信息，包括：（1）数据处理的合法依据；(2)处理任何特殊类别数据的情形；(3)确保准确性、避免偏见并就使用 AI 进行解释；以及技术安全措施的详细信

息（例如，哈希或者加密标准）。在此阶段，企业还应说明如何遵守《规范》的每个标准。

步骤 5：识别和评估风险

企业必须考虑对儿童的潜在影响以及数据处理可能造成的任何伤害或损害，无论是身体上、情感上、发育上还是物质上。还应该专门检查数据处理是否会导致以下风险：

· 人身伤害；

· 在线诱骗或其他性剥削；

· 社交焦虑、自尊心问题、欺凌或同辈压力；

· 访问有害或不适当的内容；

· 错误信息或对信息的不当限制；

· 鼓励过度冒险或不健康行为；

· 降低父母的权威或责任；

· 丧失自主或权利（包括对数据的控制）；

· 强制使用或注意力缺陷障碍；

· 面对屏幕时间过多；

· 睡眠模式中断或不足；

· 经济剥削或不公平的商业压力；

· 任何其他经济、社会或发展方面的重大不利条件。

步骤 6：确定降低风险的措施

必须考虑是否可以对服务进行任何改变以降低或避免已确定的各种风险。企业至少需要实施《规范》中所提及的措施，在适当情况下可以采取额外的保障措施。

步骤 7：记录结论

如果企业拥有 DPO，则在做出任何最终决定之前，必须记录 DPO 对 DPIA 结果的独立建议。企业应该记录拟采取的任何额外措施，并将它们整合到服务的设计当中。若企业发现未被减轻的高风险，则必须在采取进一步行动之前咨询 ICO。ICO 认为，公布 DPIA 是值得推荐的做法。

（三）适合年龄的应用

适合年龄的应用是指以特定方法识别单个用户的年龄并确保将《规范》中的标准有效地应用于儿童用户。设计服务的核心在于考虑到受众的年龄范围，以及不同年龄和发展阶段中儿童的不同需求，这是“适合年龄的设计”这一概念的基础。这通常意味着企业需要确认用户的年龄范围，据此为其个人信息提供定制化的保护和保障。如果企业无法或不希望这么做，那么可以选择将这些标准适用在所有年龄段的用户。这样一来，即使不确定是否为孩子，也可以为其提供一些保护措施，以防止由使用其个人信息而引发的风险。

ICO 承认，儿童是个体，以年龄范围划分儿童的兴趣、需求和发展能力并非完美的解决方案。但是，为了帮助评估服务设计是否适合该年龄段儿童，可以使用年龄范围作为划分儿童在各个发育阶段可能表现出的能力、技能和行为的指引。《规范》将将儿童的年龄范围划分为以下五个阶段：

· 0-5 岁：识字前和识字的早期

· 6-9 岁：小学的核心阶段

· 10-12 岁：过渡期

· 13-15 岁：青少年时期

· 16-17 岁：即将成年

关于如何以恰当的确定性水平确定用户的年龄，ICO 提供了一些具体的参考方法，包括：

· **自我声明。**仅需用户主动提供他们的年龄但不提供任何证据进行佐证。适用于低风险的数据处理或者与其他技术结合使用。

· **人工智能。**即通过使用人工智能来分析用户与服务进行交互的方式以估算用户的年龄。企业可以使用此方式对用户的自我声明进行核对。此方式可以提高用户年龄预估的确定性。如果选择使用此技术，则需要注意：提前告知用户；仅收集为此目的所需的最少的个人数据；不将收集的任何个人数据用于其他目的。

· **第三方年龄验证服务。**企业可以选择使用第三方服务，来确认用户年龄。使用第三方服务需要进行一些尽职调查，并且应当向用户提供有关所使用第三方服务的明确信息。

· **帐户持有人确认。**企业可以依靠已知的成人帐户持有人对用户年龄进行确认。例如，如果企业提供基于登录或订阅的服务，则可以允许主要（已确认的成年人）帐户持有者设置儿童资料，使用密码或 PIN 限制进一步的访问，或者仅确认其他帐户用户的年龄范围。

· **技术措施。**如阻止虚假年龄声明，识别并关闭未成年人账户的技术措施等，可以对自我声明的确定性进行相应的支撑。

· **“硬标识符”。**采取可以链接到正式身份证明文件或“硬标识符”（如护照）的年龄确认方案。但是企业应当避免将提供“硬标识符”作为唯一选择，除非数据处理所产生的风险确实需要此种方法。原因在于，即使年龄合适，某些儿童无法获得正式的身份证明文件并且其获取来自父母的支持较为有限。“硬标识符”的要求有可能还会对成年人的隐私产生过度的影响。

若企业需要收集个人数据以确定用户的年龄，企业对个人数据的收集和存储应当遵守数据保护义务，包括数据最小化、目的限制和安全保障义务。核心是确保收集的数据是实现合理确定用户年龄目的所需要的最少的个人数据，并且确保不

将收集到的数据用于其他的目的。年龄确认工具依然是一个正在发展的领域，ICO将会就此提供支撑，来建立行业标准和认证机制。

（四）透明度

透明度要求是指企业向用户提供的隐私政策，以及其他已发布的协议、政策和社区标准，必须简洁、突出并使用适合儿童年龄的清晰语言。为确保达到透明度标准的要求，企业应当做到：

· **提供清晰的隐私政策，并确保儿童及其父母可访问到该政策。**

· **在个人数据被使用时即提供细致说明（bite-sized explanations）。这也被称为“及时通知”（just in time notice）。**根据儿童的年龄和数据处理固有的风险，还应促使儿童在激活最新的数据使用之前先与成年人沟通，若儿童对此不确定，则不应继续进行。除此之外，企业还应当考虑用户使用服务的过程中是否存在需要提供相关说明的其他节点。

· **提供明确清晰易读的条款、政策和社区标准。包括用户服务协议等。**

· **以对儿童友好的方式展示信息。**可能包括使用图表、卡通、图形、视频和音频内容以及游戏化或交互式内容，使其能够引起儿童的兴趣并吸引他们。可以使用诸如隐私控制面板、分层信息、图标和符号之类的工具来帮助儿童理解并以对儿童友好的方式呈现信息。

· **根据儿童的年龄调整信息。**ICO 区分不同年龄段对此提供了合规建议，现总结如下：

年龄段	合规、完整的隐私政策	更改隐私设置	备注
0-5	由监护人阅读	仅监护人	监护人主导

年龄段	合规、完整的隐私政策	更改隐私设置	备注
6-9	监护人阅读	仅监护人	监护人主导 + 以卡通、音视频形式提供基本隐私概念介绍，由家长与儿童共同使用
10-12	监护人阅读 + 儿童阅读（支持文字/音视频切换）	仅监护人 + 以卡通、音视频向儿童解释更改后的后果	监护人主导
13-15	儿童阅读（支持文字/音视频切换）	以卡通、音视频向儿童解释更改后的后果； 引导寻求监护人帮助	儿童主导 + 为家长提供相关信息
16-17	儿童阅读（支持文字/音视频切换）	以卡通、音视频向儿童解释更改后的后果； 引导向监护人确认。	儿童主导

总体而言，ICO 将儿童的年龄分为五档，从 0 岁到 18 岁，根据儿童的认知水平程度，决定父母在其隐私中的参与度。年龄越小，对其个人数据的参与度越低，越需要父母的陪同。而年龄阅读，认知水平能力随之增强，在为其父母提供完整信息的前提下，可以为其提供简单的信息，并可以减少父母的参与，同时为儿童自身提供修改隐私设计的权限，此时依然需要对儿童进行提示。

（五）数据滥用

企业使用儿童个人数据的方式，不得对儿童健康带来损害，也不得违反行业规范、其他监管规定或政府建议。企业应当及时跟进相关建议和意见并不以明显有害或与此类意见相悖的方式处理儿童的个人数据。具体而言，企业应当避免为儿童提供个性化的游戏服务以换取长时间玩耍，同时采取措施放置儿童沉迷，例如尽可能引入诸如暂停按钮之类的机制，使儿童可以在不中断游戏进度的情况下随时休息等。相关的行业规范或者建议包括但不限于营销和行为广告、广播、新闻、在线游戏等方面的规定。

（六）政策和社区标准

企业需要遵守其发布的条款、条件和政策（(包括但不限于隐私政策、年龄限制、行为规则和内容政策等)，在为用户设置社区规则和使用条件时，企业需要积极的维护和执行这些规则和条款。企业应当遵循“说自己所做，做自己所说”的原则。例如，如果企业已声明其禁止霸凌，那么需要建立相应的机制来迅速有效地处理霸凌事件。

（七）默认设置

除非能提供令人信服的原因，并基于保护儿童的最大利益，否则默认设置必须是高水平的。此项标准要求：

其一，企业提供“高度隐私”的默认设置。“高度隐私”的默认设置意味着：默认设置下儿童的个人数据对其他用户是不可见和不可得的；企业对儿童个人数据的使用仅限于提供服务所必须的范围（超出此范围之外的数据使用如用于个性化服务，必须由用户选择和激活）；任何允许第三方使用个人数据的设置只能由儿童用户激活。

其二，企业不仅需要确保默认设置本身可降低儿童遭受的风险，同时也需要考虑在儿童用户试图更改默认设置时是否需要采取进一步的措施以降低儿童可能遭受的风险。

其三，企业需要证明其已经支持保持或恢复到高隐私设置的功能，允许用户选择永久保持高隐私设置或仅针对当前用途更改隐私设置。

其四，更新软件时保留用户的选择或者高程度的默认设置。

其五，在多用户设备上允许不同的用户进行选择。例如，儿童和成人使用同一台设备时，不需要共享同样的隐私设置。25

[25] 作者：孟洁律师团队。

2. 花季守护——ICO 依“龄”设计规范（下）

英国信息专员办公室（ICO）于 2020 年 1 月份发布了最终版本的《适龄设计规范》（Age Appropriate Design Code，以下简称“《规范》”），《规范》将被提交至议会，预计将于 2021 年秋季生效。

英国议会要求 ICO 制定《规范》的目的在于确保英国《数据保护法案》（DPA）的真正落地。《规范》具体解释了如何将 GDPR 的相关规定适用于使用网络服务的儿童。并在制定过程中充分咨询了父母、儿童、学校、儿童保护团体、开发者、技术和游戏公司以及在线服务提供商的意见，并与之进行充分对话。

ICO 认为，制定《规范》的必要性在于，英国五分之一的互联网用户是儿童，但他们使用的网络却不是为他们设计的。在 ICO 此前进行的调查中，英国儿童将现有的实践情况描述为“管闲事”、“粗鲁”和“有点怪异”的。而 ICO 针对人们最关心的数据保护问题进行过全国调查，结果显示，儿童的隐私保护问题位居第二，仅次于网络安全。这一情形与英国通信管理局和伦敦经济学院进行的调查所反映的情况类似。《联合国儿童权利公约》（UNCRC）指出，儿童在其生活的各个方面都需要特殊保障。欧盟数据保护法也反映了这一点，并为儿童提供了附加保护措施。《规范》基于 UNCRC，并反映出了全球治理的方向，美国、欧洲和经济合作与发展组织（OECD）也正在考虑进行类似的改革。

数据最小化

数据最小化要求意味着企业应当收集及存储最少必要的个人数据。企业应当确定特项服务所需要的个人数据，并由儿童来选择其希望使用的特定服务。同时，企业仅可在儿童积极而有意识的使用该部分服务时收集儿童的个人数据。

（九）数据共享

企业需要做到考虑儿童的最大利益，除非能给出一个令人信服的理由，否则不应共享儿童的个人数据。“高度隐私”的默认设置意味着共享数据的数量被限制，儿童需要主动更改默认设置以允许企业共享其个人数据。若企业可合理预见数据共享将导致第三方以损害儿童利益的方式使用数据，则不应当进行数据共享，企业应当获取第三方的保证，并对第三方的数据保护措施和任何数据再共享问题进行尽职调查。关于数据共享的默认设置应当明确数据共享的目的和对象。

总的来说，企业应当确保接收数据的第三方遵守 GDPR 的相关要求。但是确保数据共享的公平性这一责任由企业承担。除非具有出于儿童最大利益考量的令人信服的理由，否则企业不应进行数据共享。构成上述“令人信服的理由”的如：出于安全保护的目的，防止对儿童进行性剥削和线上虐待，或者为了防止或者侦查针对儿童的犯罪（如在线诱骗）等。为商业再利用的目的出售儿童的个人数据则不构成上述“令人信服的理由”。

（十）地理位置

首先，企业应当确保地理位置选项默认关闭。其次，企业应当在注册、每次使用服务时提示儿童向其告知其位置正在被追踪；如果儿童无法理解，则需要引导其与成年人沟通。最后，企业应当确保儿童位置对其他人可见这一隐私设置在每次使用以后都被关闭。

需要注意的是，若企业使用的地理位置信息同时构成 PECR 下的“定位信息”，则企业还应当满足 PECR 的相关要求。

家长控制

家长控制是允许父母或监护人对儿童的在线活动进行限制的工具，从而减轻儿童可能遭受的风险。其中包括设置时间限制或就寝时间，限制访问特定网站以及限制 App 内购买。可以被用于监视儿童的在线活动或跟踪他们的实际位置。

满足此项标准的重点是向儿童明确说明是否存在家长控制以及儿童是否正在被跟踪或监视，并提供显著的标识。这就要求企业向儿童提供与其年龄相适应的信息或者关于家长控制的解释；同时企业也需要向家长提供儿童权利相关信息。针对不同年龄段，企业需要就此向儿童或父母提供不同的信息，ICO 分年龄段提供了指南，具体总结如下：

告知儿童		告知家长	其他
0-5	-告知形式:音视频； -告知内容：	-告知内容： 儿童的隐私权；	无

	告知儿童	告知家长	其他
	父母会被告知他们在网上做什么，以确保他们的安全； 监视或追踪已开启。	随着年龄的增长，他们对此的期望可能会增加。	
6-9	-告知形式:音视频； -告知内容： 父母会被告知他们在网上做什么，以确保他们的安全； 监视或追踪已开启。	-告知内容： 儿童的隐私权； 随着年龄的增长，他们对此的期望可能会增加。	沟通渠道：提供资源以帮助父母向孩子解释服务并与他们讨论隐私。
10-12	-告知形式:音视频 -告知内容： 父母会被告知他们在网上做什么，以确保他们的安全； 监视或追踪已开启。	-告知内容： 儿童的隐私权； 随着年龄的增长，他们对此的期望可能会增加。	-告知内容： 儿童的隐私权； 随着年龄的增长，他们对此的期望可能会增加。
13-15	-告知形式:音视频或文字 -告知内容：具体服务内容、父母和儿童隐私的平衡; 监视或追踪已开启。	-告知内容： 儿童的隐私权。	无
16-17	-告知形式:音视频或文字 -告知内容：具体服务内容、父母和儿童隐私的平衡; 监视或追踪已开启。	-告知内容： 儿童的隐私权。	无

（十二）画像

除非企业可以证明存在令人信服的原因，并且是在保护儿童最大利益的情况下，否则隐私设置中的画像选项必须默认关闭。

但是，要求默认设置中关闭画像选项并不意味着画像被绝对禁止。在获得用户有效同意的情况下或者有充足保障的情况下，企业可使用用户的个人数据对用户进行画像。特别地，若画像对于在线服务的核心业务而言是必须的，则无需提供关闭画像选项的隐私设置；但只要企业可以做到，企业则应当向儿童提供控制其个人数据是否被使用以及使用方式的功能。如果企业提供的核心业务没有进行画像，那么对于依赖于画像的其他功能，则需要提供隐私设置。比如在大多数情况下，行为广告并不构成核心业务的基础。因此，在大多数情况下，行为广告应当遵循默认关闭画像选项的隐私设置。

其他不适于默认关闭画像选项的情形包括：法律法规明文规定的情形、为防止儿童遭受性剥削或者线上虐待，或者企业为了确定用户的年龄等。

从技术的角度，画像往往依赖于 Cookie 或类似技术的使用以便存储或者记住用户在线活动的过往信息，因此需要同时满足 PECR 的要求。

为满足《规范》要求，企业需要：首先，区分为不同目的而进行的不同类型的画像，并为之提供不同的隐私设置，不可将多种目的进行捆绑；其次，需要除非有其他令人信服的理由，否则必须确保画像功能处于关闭状态；再次，在打开画像选项时，企业需要提供适当的介入和干预，例如提供适龄信息，使其了解儿童的个人数据将要发生的后果和可能引发的任何风险。还应该提示儿童寻求成年人的帮助，如果儿童不确定或不了解该提示，则不要开启画像选项。最后，如画像设置已开启，企业需确保采取了保护儿童的适当措施，例如确保内容适宜儿童观看等。如果企业无法采取适当措施，则需要确保画像的设置不被开启。

（十三）轻推技术

轻推指的是用于引导或者鼓励用户在决策时遵循设计者更偏好的路径的一种技术。例如，在下面的图形中，绿色的“yes”按钮比小号的“no”选项更显眼，用户被引导为点击“yes”而不是“no”。除了颜色区别之外，语言描述的积极程度、选择选项的操作难易程度的差别等，均可被用来“轻推”。“轻推”技术可能鼓励儿童提供更多的个人数据或者选择更低程度隐私保护的选项，这一利用人类心理偏见的技术违背了 GDPR 第 5（1）（a）条的公平原则。

《规范》要求，企业不可使用“轻推”来引导或者鼓励儿童提供不必要的个人数据或者做出不利于隐私保护的决定。具体而言，企业不应当利用儿童无意识的心理过程进行“轻推”，更不应使用可能导致儿童撒谎的“轻推”技术，例如为儿童预先选择年龄段或者不允许儿童选择真实的年龄段。

企业可在适当的场景使用 “轻推”技术来提高隐私保护水平。年幼的儿童需要更多指令性的干预措施，更少的说明和更为明确的规则以及更高水平的家长控制。企业可以通过鼓励提高高隐私保护水平和设置家长控制的方式，使用“轻推”技来满足这些需求。随着年龄的增长，企业应当支持儿童发展自主决策的技巧，并对功能、风险和后果提供清晰的解释。

企业可考虑利用“轻推”技术保护儿童健康。如该技术被用于保护儿童健康，则不被禁止，例如提供诸如暂停或者保存按钮之类的工具，防止儿童长期使用网络等。

（十四）联网玩具和设备

若企业的玩具或设备会收集个人数据并且会通过网络传输，那么企业需要符合《规范》的要求。

第一，明确处理个人数据的企业和其责任。例如，若企业同时提供线下产品和支持该产品的线上功能，则由企业独立承担合规义务。其他企业的责任范围取决于其角色是数据处理者还是控制者。企业不能通过将玩具或设备的联网项目外包给其他企业来免除自己的数据保护义务。

第二，可能被各个年龄的多个用户使用。诸如交互式玩具、家庭用设备等，可能被包括儿童在内的多个家庭成员使用。对此，企业可采取的措施包括：确保默认提供的服务适合所有儿童使用；为经常使用该设备的人提供用户画像选项，以支持成年人使用或根据某一儿童的年龄来定制服务。

第三，在购买和设置服务时提供有关个人数据使用的清晰信息。实物产品的包装以及产品传单或说明手册（纸质或电子版）均可载有清晰的标志（例如图标）以表明该产品已联网并将处理用户的个人数据。企业应允许潜在的购买者在线查看隐私政策、用户协议以及其他相关信息，以便其可以就是否购买设备做出明智的决定。

第四，寻找“及时”交流信息的方法。例如，使用自动播放音频消息，仅允许通

过使用 App 来更改默认设置，或促进与用户的自动互动式“对话”。

第五，避免被动收集个人数据。企业应提供一些功能，以便在收集个人数据时让孩子或父母知晓，例如，当设备收集个人数据时，灯光会亮起。如果设备处于待机或“监听”模式，企业应该清楚告知该设备处于活动状态，且不应当在此模式下收集个人数据。

（十五）在线工具

在线工具是一种可以帮助儿童建议、轻松地在线行使权利的机制，可用于帮助行使访问、提出投诉等相关权利。为了让儿童行使自己的权利，他们首先需要知道这些权利的存在及其内容。因此，企业需要做到：

第一，企业所提供的帮助儿童行使权利和报告问题的工具必须明显且便于儿童查找。企业可在设置过程中突出在线工具，并在屏幕显著位置上提供清晰易于辨认的图标等。如在线服务还包含实体产品，则可以在产品包装上印上图标，突出显示作为产品功能的在线工具。

根据不同年龄，在线工具应当满足适龄和易于使用的要求。对此，ICO 提出了具体的参考指南，具体总结如下

	展示图标、音频提示或类似工具	在按下了这些按钮或做出了其他响应后	提供在线工具
0-5	需做到：即使是最小的儿童也可以理解含义，即“我不高兴”或“我需要帮助”。	需做到：提示儿童寻求父母的帮助。	需满足：适合父母使用
6-9	需做到：儿童可以理解含义，即“我不高兴”或“我需要帮助”。	需做到：提示儿童寻求父母的帮助，并引导儿童至在线工具界面	需满足：儿童可自行使用或在父母帮助下使用
10-12	需做到：儿童可以理解含义，即“我不高兴”或“我需要帮助”。	需做到：引导儿童至在线工具界面，并鼓励获得父母的帮助	需满足：儿童可自行使用或在父母帮助下使用
13-15	需做到：儿童可以理解含义，即“我想提问题”、“我想要访问我的信息”或“我需要帮助”。	需做到：引导儿童至在线工具界面，并鼓励获得父母的帮助	需满足：儿童可自行使用而不需要成年人帮助

	展示图标、音频提示或类似工具	在按下了这些按钮或做出了其他响应后	提供在线工具
16-17	需做到：儿童可以辨认出“我想提问题”、“我想要访问我的信息”或“我需要帮助”。	需做到：引导儿童至在线工具界面，并鼓励获得父母的帮助	需满足：儿童可自行使用而不需要成年人帮助

企业应当确保在线工具具体细化，可用于支持相应权利。企业需要定制工具以支持儿童在 GDPR 下享有的权利，例如数据可携权、删除权、更正权等。

第四，确保在线工具包含跟踪进度和与企业交流的功能。企业应当提供响应要求的相关时间表，并应在 GDPR 第 12（3）条规定的时间内处理所有要求。在线工具应具备相应的功能，使儿童可以表达紧急情况和原因。企业应当积极考虑用户提供的此方面的信息并且进行优先级排序。

五、《规范》对企业的启示

目前《规范》已提交英国议会。在正式生效之前，又给予相关企业一部分时间来进行判断和自我评估。建议企业结合自身情况，首先按照《规范》的规定，判断自身是否会适用《规范》。对此，我们的建议主要分为两种情况，一是受《规范》管辖并适用《规范》的企业；二是不需要适用《规范》的企业，具体建议如下：

（一）针对受《规范》管辖的企业

如企业判断《规范》适用，则需要尽快做好准备，根据《规范》的要求和标准进行逐项整改。需要注意的是，《规范》生效之后，ISS 提供者将有 12 个月的过渡时间以确保其服务符合规范确立的标准。在 12 个月的过渡期内，企业应当首先确认现有服务是否属于《规范》所规制的范围。对于《规范》所涵盖的服务，企业应当尽快对已有的 DPIA 进行审查或进行一次新的 DPIA。企业应当重点评估该服务是否符合《规范》中的标准，并确定符合《规范》所需采取的措施。

企业应该在过渡时期结束之前，尽快更改服务。如果更改的对象不仅包括在线产品，还包括实体产品，则应确保将必要的更改并入过渡期结束后的生产计划中。例如，更改联网玩具或设备的包装、印刷信息等。在《规范》生效之时，企业无需召回或修改现有的库存产品，也无需修改原于过渡时期结束之前开始的生产周期。

对于存量用户，企业还应该考虑如何对服务方式的更改进行管理。应该考虑他们的使用体验可能会如何变化，以及如何最好地进行交流并为这些变化做好准备，以便适当的管理对他们造成的影响。

（二）针对不受《规范》管辖的企业

针对部分国内企业，可能不存在向英国用户提供服务的情况，因此可能不适用《规范》。但是，2019 年 8 月 23 日，国家互联网信息办公室正式发布《儿童个人信息网络保护规定》（以下简称“《规定》”）。《规定》于 2019 年 10 月 1 日起正式生效。《规定》中值得注意的重点内容包括：在收集、使用、转移、披露儿童个人信息时，需要经过监护人的同意；要求监护人正确履行监护职责，教育并引导儿童增强个人信息保护的能力和意识；根据《规定》的《征求意见稿》，在收集使用儿童个人信息时，应当征得监护人“明示同意”，《正式稿》则删除了“明示”二字，意味着同意隐私政策的方式即代表授权同意。这实际上可能是在一定程度上想避免通过过多收集信息来验证谁是家长谁是儿童这一难题。

就此而言，对于这部分企业，尽管 ICO《规范》并不适用，但是不妨从以下几个维度考虑合规方向：

1、用户年龄段的划分

正如 ICO 指出的，不同年龄阶段的儿童，其理解能力和决策能力存在较大的差别，因此需要合理划分年龄阶段，针对不同的年龄阶段设计不同的隐私政策和数据保护措施。这不仅是为确保企业隐私政策、用户服务协议对儿童而言是可理解的，更是为了在家长控制和儿童隐私权、自主决策权之间寻求平衡。ICO 将 18 岁以下的儿童划分为五个年龄段，并在默认隐私设置等方面针对不同年龄段的儿童制定不同的合规指南，而非仅以监护人同意为儿童信息保护的概括性原则。就此内容而言，部分企业的用户群体可能有明显的年龄段，比如早教类产品、初中阶段学习产品等等，可以首先定位到《规范》中的某一年龄段，并且借鉴 ICO《规范》中针对该年龄段的做法，以不同的方式提供分别适合儿童及其监护人阅读的隐私政策（例如以音视频方式进行介绍等等），并根据该年龄段用户的特征，确定由儿童还是其监护人来更改隐私设置等。

2、年龄确认机制的落地

我国《规定》第九条、第十条和第十四条第一款规定了收集、使用儿童信息必须经过监护人同意制度，并在第五条规定了监护人应当履行监护职责的义务。但是，要实现监护人同意制度的落地，首先需要对年龄进行识别。目前很多企业的合规难点在于无法确认其识别方式是否有效。对此，我国仅出台了《规定》，而无具体的合规指引。在此情况下，企业可借鉴 ICO《规范》的具体做法，根据自身情况，考虑选择自我声明、成年账号确认、技术措施、上传身份证件等方式中的一种或结合多种来进行识别。

3、家长控制机制的优化

目前很多企业都设置了青少年模式，从不同程度上实现了家长对儿童上网时间、浏览内容的控制。根据 ICO《规范》提出的标准，家长控制不仅需要做到向儿童明确说明是否存在家长控制以及儿童是否正在被跟踪或监视，还需要提供显著的标识。随着儿童年龄的增长，其认知能力也随之提高，一刀切地一味满足家长对儿童的控制和监视可能也会引发相关问题。对此，也可以考虑进入家长控制模式以后，以显著标识提示儿童。此外，也可以考虑区分不同年龄段，针对对于认知能力达到一定程度的儿童，也可以提供儿童与家长的沟通渠道，从而实现使用相关服务过程中家长与儿童的有效沟通，为儿童提供更加有利于身心发展的服务。[26]

3. 反垄断监管下的互联网平台数据采集和处理

个人数据权益或数据隐私保护，本属于数据保护法的范畴，但近来反垄断机构却越来越积极地参与其中了。2010 年以来，“数据与反垄断”一直是美国、欧盟等国家和地区反垄断机构关注且热烈讨论的话题，大家都在思考和探索数字经济时代的竞争问题。2019 年 12 月 17 日，日本公平交易委员会发布了《关于数字平台与消费者涉及个人信息交易中滥用优势交易地位的指南》（以下简称《个人信息指南》），直指数字平台中有关个人信息收集和使用的垄断问题，这是全球第一个关于个人信息收集和使用的反垄断指南。当然，更引人瞩目的还是全球第一起针对数据收集和使用行为的反垄断调查案件，即德国联邦卡特尔局（Bundeskartellamt）对 Facebook 的调查。欧亚两大反垄断机构先后对同一问题采取动作，巧合中也有必然，非常值得关注。

[26] 作者：孟洁律师团队。

一、德国 Facebook 滥用数据案的调查过程、主要结论和简要评述

2016 年 3 月，德国联邦卡特尔局开始调查 Facebook，并于 2019 年 2 月 6 日作出决定书，禁止 Facebook 采集（Facebook 旗下的）WhatsApp, Oculus, Masquerade, Instagram 等平台的用户信息及设备（如手机、电脑）关联数据，以及通过 API 接口（“Facebook 商务工具”）采集 Facebook 用户访问第三方网站及手机 App 的相关数据，并且禁止其将这些信息与用户 facebook.com 的帐户信息进行融合。德国联邦卡特尔局的认定结论是，Facebook 在社交网络相关市场上具有支配地位，违反 GDPR 的规定采集、融合用户数据，参照德国联邦最高法院审结的 VBL-Gegenwert 案和 Pechstein 案的判例，27Facebook 构成了德国《反限制竞争法》所规定的滥用市场支配地位行为。

Facebook 随即向杜塞尔多夫高等法院上诉。由于联邦卡特尔局没有严格去论证 Facebook 的数据处理行为具有排除限制竞争的效果，即其行为具有剥削性（消费者）或排挤性（竞争对手）。8 月，杜塞多夫高等法院基于两个理由推翻了联邦卡特尔局的决定：1、Facebook 具有市场支配地位，但联邦卡特尔局没有证明其行为构成《反限制竞争法》第 19 条规定的滥用行为。Facebook 的数据处理行为既没有剥削用户也没有排挤竞争者，并不构成滥用行为；2、用户对社交网络的任何依赖并不会导致其接受社交网络一般性条款和声明的无效。

联邦卡特尔局随即上诉至德国联邦最高法院，尽管德国联邦最高法院尚未作出判决，但客观而言，德国联邦卡特尔局作出的决定是有相关事实基础和法律依据的。

（一）相关市场界定

本案的相关产品市场界定为用户的私人社交网络及其相关的多边市场。地域市场为德国。Facebook 利用 Facebook.com 作为媒介，进行了网络和多边市场的整合。其最终产品是基于定向广告（targeted advertising）盈利的社交网络，并且基于这种商业模式形成了一个多边市场。关键的用户群体一边是无偿使用 facebook.com 的私人用户，一边是广告商，这两个群体之间存在间接网络效应。而 Facebook 在这个核心产品中融入了更多边的市场，例如商户可以在 Facebook.com 上编辑、发布商业内容，与用户建立联结，推广业务；而程序开发者可以借助应用程序接口（APIs）将 Facebook 整合进他们自己的网站或 App，私人用户与后面两者之间也

[27] 两个案件的判决结论是具有市场支配地位的企业实施侵害公民或法人基本宪法性权利的行为构成滥用行为。用户的数据隐私权同样属于基本权利，因此本案也可以上述两个案件的判例规则。

存在间接网络效应。下图是本案相关产品市场的结构：

联邦卡特尔局还分析了 Linkedln 和 Xing 等专门化的社交媒介，以及 WhatsApp，YouTube，Snapchat, Twitter, Pinterast，Instagram 等（因其仅仅提供社交网络的部分服务），认为它们与 Facebook 都不属于同一相关产品市场。

（二）Facebook 具有市场支配地位

首先，用户市场份额数据是最重要的衡量指标。Facebook 的用户市场份额非常高，尤其是日活跃用户的份额超过 95%，月活跃用户份额超过 80%，注册用户超过 50%，而其中日活跃用户份额是关键指标。即便是把 YouTube，Snapchat，Twitter，Pinterast，Instagram 等纳入同一相关市场，Facebook 的市场份额也远超过了德国《反限制竞争法》规定的市场支配地位的门槛。

其次，商业模式具有直接和间接的网络效应。Facebook 的商业模式具有很强的直接网络效应，其用户很难转向其他的社交网络。近年来德国本土市场上的其他社交网络竞争者的市场份额在持续的减少，有一些早已退出市场（如 google）。至于间接网络效应方面，Facebook 提供的广告服务也具有很高的市场壁垒，其他的广告服务平台很难进入社交网络的用户市场和在线广告市场。

最后，庞大数据资源积累使其在数据驱动的社交网络市场上极具有竞争力。尤其在个性化广告方面，直接和间接网络效应叠加下，Facebook 的巨大数据资源优势令市场壁垒非常高。

当然，联邦卡特尔局还考虑了互联网创新力对于市场支配力的影响，但没有迹象显示 Facebook 会因互联网的巨大创新力而显著丧失其市场分额。

（三）用户对 Facebook 的数据隐私政策的接受并不构成 GDPR 下的自主同意

根据 GDPR 序言第 32 条，用户只有在“自由”给予、“充分知情”且“明确表明数据主体同意处理其个人信息”的前提下，同意才能被视为数据主体有意义的表达。GDPR 序言第 43 条阐明，为了确保数据主体的同意是基于自由意志作出的，在数据主体和数据控制者之间存在明显的不平衡时，……不可能所有的同意都是自由作出的情况下，数据主体的同意不能作为处理个人数据的有效法律基础。如果不允许对不同的个人数据处理操作分别作出同意（尽管在个别情况下是合理的），该同意被推定为不是基于自由意志作出的。

Facebook 的数据来源主要有两类，一类是 Facebook 自己平台的用户数据和设备关联数据；另一类是 Facebook 所拥有的旗下网站的用户数据以及无关的第三方运营的网站/App 中的用户数据。关于第二类数据，许多用户并不知道其同意了 Facebook 的隐私政策后便意味着允许 Facebook 从第三方来源几乎无限制地收集任何类型的用户数据，并将这些数据与用户 Facebook 帐户数据融合处理。第三方来源可以是 Facebook 旗下拥有的服务，如 Instagram 或 WhatsApp，还可以是嵌入 Facebook“喜欢”或“分享”插件的第三方网站。在网站和应用程序中嵌入此类可见插件的情况下，用户甚至不需要例如滚动或点击“喜欢”插件，访问嵌入了“喜欢”插件的网站时，将自动启动向 Facebook 的数据传输。德国的网站和应用程序上存在数百万个此类嵌入 Facebook“喜欢”或“分享”插件的网站和应用程序界面。在这样的网站上，用户看不到 Facebook 的 logo，但用户的数据却会从这些网站传输至 Facebook。

在本案中，作为一家具有市场支配地位的公司，Facebook 必须考虑到，鉴于其优势力量，用户实际上无法转向使用其他社交网络，其要求用户勾选同意所有条款与条件后方可使用产品，实际上是迫使用户要么接受全部条款和条件，要么不使用社交网络服务，而根据 Facebook 的数据隐私条款和条件，在很多情况下用户是不知道其私人数被收集处理的，因此，根据 GDPR 的规定，用户对 Facebook 收集、融合、使用其数据的接受并不能称为自主同意。

（四）Facebook 违反 GDPR 的规定从而构成滥用市场支配地位行为

如上所述，联邦卡特尔局认同 Facebook 为维持其商业模式处理社交网络内部的用户数据，但是 Facebook 采集外部的用户数据违反了 GDPR 的规定。

第一，Facebook 具有市场支配地位，在拥有超过 90%市场份额以及极强的直接网络效应的压力下，它的用户无法转向使用其他社交网络服务，因此，用户在注册时接受全部条款与条件和隐私政策便成为了用户得以使用 Facebook 服务的唯一选择，这并非 GDPR 第 6 条 1（a）下的自主同意，即有效的同意。

第二，除了需要考虑 GDPR 第 6 条 1（a）下的自主同意原则以外，还应该考虑 GDPR 第 6 条 1（b）款下的履行合同所必需原则，即个人数据的处理应当是为了实现数据处理目的而适当的、相关的和必要的。Facebook 基于社交网络本身庞大的用户数据库就可以实现社交网络服务和个性化广告的投放，没有必要从第三方获取并处理数据，否则任何公司都可以仅仅因为其商业模式及产品质量、丰富性等原因无限制地处理数据。因此，无法基于效率考量和个性化服务的需求等理由认为 Facebook 处理外部数据是履行其合同义务的必要性体现。

第三，根据 GDPR 第 6 条 1（f）款来综合评估衡量各方权益，当数据控制者进行必要的数据处理与个人数据利益或基本权利和自由相冲突时，数据控制者不得进行这样的数据处理。Facebook 没能阐明在此过程中它的权益究竟是什么，其所谓个性化或私人化的社交网络商业模式并不构成收集第三方数据的充足理由。相反，执法机构考虑了数据的类型、处理方式，用户的合理期待以及 Facebook 与用户之间的地位对比--Facebook 是拥有巨大谈判优势的支配性企业，而用户大多是缺乏经验的年轻人，无法阻止其大范围地处理数据，而且也没有其他的监控方法，因此，用户的法定权益（数据权益）很有可能在此过程中受损。

此外，联邦卡特尔局还指出，Facebook 的行为进一步强化了它的市场支配地位。通过这种方式，Facebook 拥有更多渠道的数据源，获得了面对竞争对手的不合法的竞争优势，提高了市场壁垒，保障了 Facebook 面对终端消费者的市场支配力。

总之，德国联邦卡特尔局认为，数据保护法和竞争法都会考虑不平等的谈判地位，无论是从竞争法还是数据保护法的角度衡量都会得出相同的结论。由于 Facebook 是一家具有支配力的企业，用户无法保护个人的数据不被广泛收集，在数据披露方面他们自己做不了主。如果服务提供方作为一个支配性企业，且没有足够的竞争压力的话，其交易对手的利益就需要被充分考虑到。尽管数据驱动型的商业模式能够被认可，但 Facebook 从其体系之外收集用户和设备关联数据并将这些数据与 Facebook 的帐户数据进行融合，属于德国《反限制竞争法》第 19（1）条规定的滥用（社交网络市场上的）支配地位实施的剥削性行为。同时，根据欧盟 GDPR 的规定，这些行为也给私人用户与竞争对手造成了伤害。

（五）简要评述

对剥削性滥用行为进行监管的合理性在于具有市场支配力的企业压榨弱小交易对手方的行为，剥削了交易对手的利益进而牟取自身的高额垄断利润，违背了市场交易公平性原则。如果长期容忍此类行为，会损害市场活力，降低社会经济效率。当然，难点在于交易的不公平性很难证明。德国联邦卡特尔局循着 GDPR 的逻辑证明 Facebook 侵害了用户的数据权益：用户在不得不选择无替代性的社交网络工具的压力面前，接受 Facebook 服务协议条款条件与隐私政策并不是其真实自由意志的表现；Facebook 拥有强大的数据资源，实际上没有必要从体系外再采集和使用用户个人数据，但其对不同数据源的收集和融合行为，大大促成了 Facebook 能够为每个用户专门构建专属的独特的数据库（即用户画像），并进一步维持和巩固其市场支配地位。但这样做损害了用户的合法权益，也并不能给社会带来更大的利益。由于 Facebook 侵害的是用户不能被侵害的基础性权利（不存在交易不公平性的证明难题），而它能这样做的原因是因为其具有市场支配地位，那么 Facebook

自然就构成了反垄断法中的滥用行为，同时根据 GDPR，该数据主体的同意也不能作为处理个人数据的有效法律基础。虽然 Facebook 就该数据处理行为对其商业模式运转、实现和提升的重要性和必要性进行了积极抗辩，但显然没能说服执法机构。

二、日本《个人信息指南》的主要内容

2018 年末，日本通产省、公平交易委员会等几个部门联合组织研究并形成了一个关于平台经济治理的政策报告，其中提及运用反垄断法对数字平台进行监管的政策选项。为此，日本公平交易委员会着手拟定《个人信息指南》，并于 2019 年 8 月发布了征求意见稿，在一个月内收到 140 多条意见，经修改完善后，于 2019 年 12 月 7 日正式发布。指南共有 5 条，第 1 至 4 条分别解释了“滥用优势交易地位的监管”、“交易相对人（即消费者）”、“面对交易相对人的优势地位”以及“超越普通商业行为的不公正性”的概念，第 5 条则详细列举了滥用优势交易地位的行为，分为不恰当地收集和使用消费者个人信息两类。指南有不少因应德国 Facebook 案之处。例如，关于如何判断数字平台面对消费者具有优势地位：（1）没有其他数字平台可以给消费者提供替代性服务；（2）即便有其他数字平台可以提供替代性服务，消费者实际上也很难停止使用该服务；（3）该数字平台多多少少能单方面决定一些交易条款（如价格、品质、数量）。此外，关于不恰当地采集消费者个人信息的行为中，列明有：（1）未向消费者申明个人信息的使用目的，其中包括未通过一般性身份识别的情况下采集消费者浏览网页或移动设备位置的信息，即鉴别了个体身份但却未告知对方；（2）违背消费者意愿且超越必要性范畴的情况下采集个人信息，其中也包括消费者被迫同意的情形，而判断消费者是否被迫要基于普通消费者受损的程度来判断；.....（4）将消费者提供个人信息作为使用数字平台服务的先决条件。

三、德国与日本的数据隐私竞争政策对中国的启示

日本《个人信息指南》透露的在数据隐私方面的竞争政策取向与德国是非常相近的。德国和日本的反垄断法是少有的明确采纳“滥用相对交易优势地位”概念的反垄断法，两国的反垄断执法机构对于大企业滥用支配力侵害不对等交易对手的行为警惕性更高，因此也不难理解两国在互联网在线平台的隐私政策监管方面也走在第一线。一般而言，企业的隐私政策应当遵守数据保护法，处于数据保护机构的监管之下。反垄断机构之所以要介入，是因为具有市场支配力的互联网在线平台其隐私政策或数据处理行为对个体消费者或用户显失公平，从而对普通私人用户构成了“剥削性滥用行为”。

根据反垄断法，那些可能被数据保护法认可的消费者（用户）对隐私政策的同意以及用户服务协议的达成等行为都将在新的框架和价值标准下重新被审视。如

果这一干预措施成立，意味着互联网平台并不能因为用户接受了用户服务协议和隐私政策，即可高枕无忧地随意采集和使用用户个人数据。隐私政策也不可能变成互联网平台无限制采集、整合数据甚至垄断数据资源的避雷针，反而，隐私政策需要将数据采集、使用的目的清晰、明确地告知用户，并获得用户自由、充分、明确的同意；在数据采集上需确保最小且必要原则，使用数据的目的与方式符合用户的合理期待；并且，隐私政策中需要给予用户享有撤回同意的权利以及保留当不再需要用户个人数据时，将数据进行匿名化或者删除的措施。

在传统反垄断法中，不公平高价行为是典型的"剥削性滥用行为"，互联网平台在数据隐私政策方面的"剥削性滥用"显然是反垄断法在数字经济时代面临的新课题。中国是世界上少数对"剥削性滥用行为"（不公平高价）采取严厉监管措施的国家，中国的反垄断机构对此也拥有丰富的经验。近年来中国的数字经济蓬勃发展，世界级的互联网平台企业在此聚集，中国的反垄断机构对数字经济并不陌生，对该领域的监管水平并不落后于欧美国家。我们相信，日本和德国反垄断机构的做法对包括中国在内的全世界各国反垄断机构都具有很强烈的借鉴意义，也许我们很快就将迎来一场"数据与反垄断"的大风暴。[28]

4. 评析澳大利亚《消费者数据权利规则》及对我国立法与产业的启发

澳大利亚的《消费者数据权利规则》（"Consumer Data Right rules"，以下简称"CDR 规则"）于上周 2020 年 2 月 5 日生效，而此前（即 2019 年 8 月）澳大利亚已经通过了《消费者数据权利法案》（"Treasury Laws Amendment(Consumer Data Right) Bill"，以下简称"CDR 法案"）。因此，本次生效的 CDR 规则可视为 CDR 法案的具体实施细则，由澳大利亚竞争与消费者委员会（"Australian Competition& Consumer Commission"，以下简称"ACCC"）制定并监督实施，目前主要针对银行业的相关举措进行了规定。

我们先来了解一下 CDR 法案及其规则的基本内容。

CDR 法案及规则的主要内容

CDR 允许消费者个人"拥有"其个人数据，方法是法律授予消费者对银行、能源、通信和互联网交易的开放访问权，从而拥有并控制消费自己的个人数据。

[28] 作者：万江，孟洁。

CDR 法案的主要内容包括：数据持有者（如四大银行）必须向消费者或经消费者许可的数据接收者分享消费者数据。同时数据持有者必须公开自己的产品参数，包括利率、费用和收费等信息，以及申请信用卡和抵押等银行产品需要符合的相关资质要求。该法案一并要求数据持有者在分享消费者数据时实施隐私保护的相关措施。

CDR 规则主要是对 CDR 法案进行了细化规定，包括对产品参数请求、消费者数据请求、代表消费者提出请求的认可人员、争端解决、数据标准在内的重要问题提出操作方案。值得一提的是，对受到广泛关注的消费者隐私保护措施也提出了具体规定：（1）数据持有者和数据接收者必须公开化和透明化其对数据管理的政策；（2）数据接收者允许数据持有者以匿名或者假名方式提供消费者数据；（3）禁止非法使用数据；（4）禁止数据接收者通过数据对用户进行精准营销等。另外还提出了将这些规则逐步应用于银行业的时间表，以及今后还可能修改这些规则以解决其他问题。

为了更好的了解 CDR 以及 ACCC 批准其规则的意义，需要进一步回顾澳大利亚关于消费者数据权利法案及规则的立法历程，并且给大家介绍 CDR 规则生效后的推进时间表。

立法历程与推进时间表

2017 年 7 月 20 日，澳大利亚时任财政部长 Scott Morrion（2018 年当选总理）委托 Scott Farrel 主持“澳大利亚开放银行评估”工作，即为澳大利亚开放银行业务推荐最合适的运作模式。随后，澳政府在 2017 年 11 月 26 日宣布引入**消费者数据权**（“Consumer Data Right”，以下简称“CDR”）。政府决定在银行业率先引入 CDR 作为“开放银行”的一项策略，随后将会在能源行业、通信行业效仿并实施，以更好地从竞争角度上促进产业发展。

如上所述，CDR 数据包含了（1）产品参数和（2）消费者数据两类共享数据，此次生效的规则对这两类数据又提出了进一步分类完成共享给其他数据平台的时间表。

对于**产品参数**，包括利率、费用和收费等信息，以及申请信用卡和抵押等银行产品需要符合的相关资质要求。CDR 法案要求四大银行与经认可的数据接收者进行共享，且自 2019 年 7 月起，银行已经开通 API 接口提供此类信息的共享了。

对于**消费者数据**，CDR 规则要求银行（在消费者提出要求的情况下）将消费

者数据共享给其他数据平台，但可以分以下阶段进行：（1）与信用卡和借记卡、存款账户和交易账户有关的消费者数据将从 2020 年 7 月 1 日起开放共享；（2）与抵押和个人贷款数据有关的消费者数据将从2020年11月1日起开放共享。(注：2019 年 12 月， ACCC 曾宣布出于隐私保护与信息安全的考虑，与信用卡和借记卡、存款账户和交易账户有关的消费者数据共享将从 2020 年 2 月 1 日推迟至 2020 年 7 月 1 日；与抵押和个人贷款数据有关的消费者数据共享将从 2020 年 7 月 1 日延迟至 2020 年 11 月 1 日）。尽管比原计划时间表略有延迟，但是澳大利亚在开放银行计划上的步伐是相当进取的，尤其与其他许多国家相比，例如最先带动开放银行节奏的英国。

CDR 对金融业和消费者的影响

澳大利亚政府积极推进 CDR 立法，将对澳大利亚金融业产生极大影响。目前澳大利亚有超过五百家分布在资本市场、支付、保险、私人理财、贷款、电子货币等专业领域的金融科技公司。数据对于金融科技公司来说至关重要。举例来说，金融科技公司可以通过大量客户数据，更加全面地了解客户（个人或小型企业）的财富状况、消费习惯、风险态度和信贷情况，从而准确评估其资信状况，为其提供相对应的信贷服务或其他个性化服务。在控制风险的同时，为公司创造收益。而传统的澳大利亚四大银行目前占据着 80%的市场份额，公开产品参数、共享消费者数据可能让他们流失大量的客户，将产生巨大冲击。但从整体上说 CDR 的根本目标是尽快实现“开放银行”，刺激行业竞争，促进澳大利亚金融创新与发展。

加剧金融业竞争，加快产业转型升级当然也会给消费者带来好处。更加透明的市场信息可以帮助个人和小型企业选择更合适的产品。市场竞争可能促使银行或其他金融机构推出条件更加优惠的信贷产品，使个人和小型企业都从中受益。

但是，无论是 CDR 法案还是其刚刚生效的规则，在草案制定期间曾饱受争议。人们最担忧的是数据开放同时可能产生隐私泄露问题。澳大利亚隐私基金会（APF）在 2019 年 3 月时指出，针对 CDR 的隐私保护措施并不充分，政府“严重”低估了其在整个立法进程中需要进一步思考的必要性。APF 认为澳大利亚信息专员办公室（OAIC）应当参照 GDPR 模式，为一个严厉的隐私监管机构提供充足的资金，而目前 OAIC 被认为“严重缺乏资源”并且在监管方面“不太活跃”。可以看出，数据共享是一把“双刃剑”，给人们带来便利，同时也引起人们在隐私安全方面的担心。

对于这些顾虑，ACCC 已经有所回应。除了适用隐私保护的一般性原则和举措（如数据最小化原则，被认可的第三方只能要求收集和使用与提供产品或服务相关的消费者数据；删除消费者数据（或去标识化））外，ACCC 在本次生效的 CDR 规则中专门提出了特别的隐私安全保障措施。ACCC 认为， CDR 规则第 7 部分规

定的 13 项措施覆盖了 CDR 数据收集、处理、诚信与安全、更正等方面，具体包括要求数据持有者和接收者公开 CDR 数据的管理规则、允许以匿名或假名的方式提供 CDR 数据、CDR 数据收集的通知、受认可的数据接收者资质、及时删除冗余数据、及时回应数据更正请求等多项内容，应当足以保护消费者的隐私。人们相信并期待，CDR 在增强和保护消费者权益，推动参与方竞争和创新，带动国家金融发展等方面将有良好的表现。

CDR 与 GDPR 下数据可携带权的比较

实现 CDR 需要区分对产品参数的请求和对消费者数据的请求。针对产品参数的请求，无论消费者还是代表消费者的第三方机构均可以提出。根据 CDR 规则，有两种消费者数据请求服务：（1）**消费者直接请求服务**：符合资格的消费者可以直接请求数据持有者（如四大银行）披露自己的消费者数据，数据持有者需要以**人类可读**的形式提供 CDR 数据；（2）**受认可的第三方请求服务**：受认可的第三方可以代表符合资格的消费者向数据持有者请求披露该消费者数据，第三方的请求需要符合相关数据标准，数据持有者需要以**机器可读**的形式提供 CDR 数据。

GDPR 第 20 条第 1 款规定数据主体有权以结构化、常用地和机器可读的形式接收数据控制者提供有关数据主体的个人数据，并有权将这些数据传输给另一个数据控制者，不受前者的任何限制。第 20 条第 2 款规定，在技术可行的情况下，数据主体在行使第 1 款规定的数据可携权时，也可以要求数据控制者直接将其个人数据传输至另一个数据控制者。这个规则能够实现消费者数据不被一个数据控制者“锁定”，让消费者真正获得数据的权能。通过相关立法保障数据分享请求的许可，给予消费者控制权，可要求数据控制者以安全可靠的方式分享其个人数据。

上述 GDPR 下“数据可携权”体现了数据主体实现对自身数据的重要权能。消费者有权访问自己的数据，有权决定向谁开放自己的数据，以获取更好的产品或服务。CDR 的实现方式与 GDPR 可携权的相关机制非常接近，都是消费者有权要求获取自身数据副本或者将自己的个人数转移到另一个新的数据平台。

但是这两者的权利范围有所区别。GDPR 规定中，数据主体，即消费者可以得到机器可读版本的个人数据，并且有权将这些数据发给其所认可的第三方数据控制者。即，数据主体有权获取自己的数据副本，并将副本进行迁移。在 CDR 中，消费者可以直接请求获得人类可读的个人数据，也就是获得一个人类可读懂的数据副本，或者通过请求被认可的第三方向数据控制者提出传输机器可读版本的消费者数据请求，因此 CDR 对消费者权利的保护更加人性化。但是对比于 GDPR 均是由个人数据主体控制者提出获取数据副本或者数据迁移的请求，CDR 多出了一类情况，即个人数据主体可以要求另一个数据控制者直接向持有消费者数据的原

控制者提出数据共享的请求，也因此 CDR 对受认可的代表提出了严格的资质审查要求和相关隐私安全保障措施要求，从而来提升消费者数据迁移的安全性与可靠性。

另外我们注意到，GDPR 下数据可适用携带权的行业范围远比 CDR 要大。CDR 目前只被引入银行业（当然随着 CDR 的进一步推广，还可能扩展至其他行业），但是从 GDPR 的适用性上来看并没有对某一个行业做出专门的允许或者限制，换言之，GDPR 项下的数据可携带权是一个适用于全行业的方案。另外，在设计可携权方案时，两者的目标和理论基础也是不同的。CDR 的颁布是为了促进银行间部分数据开放，本质上是鼓励竞争。我们可以看到，虽然人们对 CDR 的讨论停留在消费者保护层面，但 CDR 的本质其实是财产权问题。然而，将 GDPR 数据可携带权上升到基本权利层面 ，就会产生基本权利与其他权利优先性的问题。一般来说，基本权利具有人格属性，不可让渡，具有当然的优先性。但不可否认的是，是在数字经济时代，个人数据还具有财产权的属性。将数据可携带权作为基本人权，可能在根本上损害到一些对用户个人数据进行了加工和处理的公司的利益，甚至对整个产业发展也可能存在不利之处，因此 GDPR 可携权的实施一直是个执行上很不好落地的问题。

CDR 与我国相关立法的比较

2019 年 12 月底刚刚出台的《中国人民银行金融消费者权益保护实施办法（征求意见稿）》（以下简称《实施办法（征求意见稿）》）第三十六条规定，鼓励金融机构在技术可行的前提下，基于金融消费者的请求，将其金融信息转移至金融消费者指定的其他金融机构。这一条规定与 CDR 中“消费者可以请求第三方请求数据持有者披露消费者数据，第三方的请求需要符合相关数据标准，数据需要以机器可读的形式提供”的部分内涵比较接近。我们可以看到中国和澳大利亚在构建“开放银行”问题上也有相似的努力。

当然两者有很大不同。其一，CDR 是一项消费者权利，消费者有权访问、提取或者要求转移自己的消费数据，只要符合相关要求，并由数据持有者和接收者共同保障数据安全。但是《实施办法（征求意见稿）》中仅提出了对消费者金融信息进行跨机构转移的探索，并没有提到消费者对自己的消费数据拥有的相关权利。在《实施办法（征求意见稿）》中甚至没有提到消费者可以要求查询自己的消费数据。其二，CDR 法案及其规则提出了一系列可操作的标准，以实现不同数据平台共享这一目标，例如在数据分享形式上要求以机器可读形式。并且提出了争端解决规则，便于在数据持有者和接收者之间分配责任。实现数据共享，需要政府及其相关部门和企业的共同努力，需要解决包括在联合控制数据情况下的责任分配、技术上可兼容的或者存在至少无传输障碍的系统等在内的大量问题。澳大利亚已经完成了大

量工作，而我国目前尚处于探索尝试的阶段。

CDR 的法案和规则，以及将来的具体实践都对我们有很高的参考借鉴价值。CDR 是一项不同于 GDPR 可携带权的方案，在这一方案中，消费者对自己的数据拥有控制权，数据控制者和接收者共同保障数据安全，人们期待以这样的方式实现经济价值与数据安全的双赢。

对我国而言，构建开放银行，推动数字经济发展是我们的目标。同时我们要注重个人信息保护。怎样在消费者和金融从业者之间准确划分权利范围，怎样在金融从业者之间进行责任分配，怎样把消费者数据与个人隐私进行区分是我们当下面临的主要课题。相信 CDR 的实际执行可以给我们带来更多启发。

对中国法律与企业实践的启示与意义

首先，CDR 的相关规定对我国在开放银行和数据共享方面的立法具有较高的参考意义，至少在以下几个方面值得进一步思考与借鉴：

第一，坚持消费者拥有其个人数据的总体理念，通过法律更强地保障消费者对个人数据的控制权。

第二，廓清消费者数据共享的范围。通过行业细则的方式明确哪些类型的消费者数据可以共享和开放。数据利用需要充分，但是数据开放也需要节制，也要考虑到经过企业加工和衍生后的数据权益。因此，开放可共享的数据类型需要既有确定性，又要兼顾平衡各方得益。CDR 中明确规定了可以共享产品参数和消费者数据两类数据。能否从中概括为，为了节省社会资源，保护企业与消费者的权益，如注册类信息、产品参数类信息和消费者信用信息等可以考虑在消费者同意的前提下由不同机构间进行共享呢？对每类数据如何共享可以在具体实施细则中得到体现。例如，信用信息需要有更高的保护强度，在提出共享迁移申请时应有更高的验证标准等。

共享数据实现方式的创新。CDR 规则的实现方式是可以通过消费者直接请求，也可以通过由消费者受认可的第三方在消费者要求下，向数据控制者提出请求。企业与个人往往实力不对称，如何由消费者对第三方的资质和相关安全措施保障情况进行审核，也是一个需要考虑的问题。比如说是否可由第三方公布其 Code of Conduct 或者经过相关权威机构颁布的 Certificate 来表明已经符合接收标准呢？在我国或许还可以考虑建立一个专业的消费者金融数据平台，根据消费者的请求，统一通过平台向各银行或其他金融机构提出消费者数据交互的要求并进行一致性管

理。此外，对于这样一个平台本身来说需要有更高的安全保障要求，因为它更大程度上实现了各机构间数据的汇集，那么是否可由行业组织或者金融机构的直接主管机构人民银行来牵头，可能人行也已经开始在尝试了，因篇幅所限，本文不再进一步展开叙述了。

第四，对共享数据格式的要求。GDPR 规定可携带权相关的数据迁移仅以机器可读版本提供。CDR 规定了二条路径，即向机构迁移数据的，需提供机器可读版本；向消费者提供其个人数据的，则需提供人类可读版本。这增强了消费者对数据的了解程度，从实际意义上保障消费者的权利并加强其对个人数据的控制能力。我国《实施办法（征求意见稿）》仅规定了在消费者提出要求向其认可的第三方金融机构提供数据时，控制者需要以机器可读的形式提供数据。那么，除了推荐性国家标准《个人信息安全规范》有提到在个人信息主体提出获取四类个人信息副本的请求时，数据控制者需要满足以外，我国是否可以从立法上进一步明晰个人信息主体有权向银行等金融机构请求获取其个人数据，并明确要求金融机构需要以人类可读的版本向个人信息主体提供个人信息副本呢？值得进一步思考与讨论。

第五，在不涉及特定消费者的问题上，CDR 规则要求数据控制者应当以匿名或假名的方式向数据接收者提供消费者数据。数据匿名化或脱敏处理可以在极大程度上提高数据分享的安全性。这也是对数据最小化原则的贯彻。这点也应当建议被将来我国的立法所吸取，这将在极大促进社会的整体效率的同时，能够最大程度地保护单个消费者的个人信息安全和其内心的安全感。

第六，确立禁止性规定。共享与数据开放是为了让数据成为资产的流动性更强，提升客户更个性化的服务。但是为了避免有些企业和人浑水摸鱼，将共享来的数据另作他用，需要建立一套完善的数据共享机制。比如事先授权、事中管理与跟踪、事后审计与追责，建立透明且合理的数据流通措施与流程，不得将共享的数据用于非法用途和对消费者进行营销等，设置开放银行的禁止性要求，划定合规红线。

第七，高度重视并提前防范数据泄露风险。CDR 规则中采取了安全控制措施与隐私保护措施相结合的方式。如果某一共享数据不停地在不同机构之间进行共享，那么链条一长，就需要充分考虑在数据共享机制中设计防数据泄露的防护体系，加强数据接口间的安全，提升系统级别与应用层安全的双重防护，建立开放银行统一平台的可信环境，通过实施数据共享全流程的安全控制措施来充分保障消费者隐私安全与业务的可连续性。

第八，尽快建立行业统一标准。银行之间、银行与金融科技公司之间，银行与各大企业平台之间，甚至金融公司与企业平台之间，如果需要真正实现数据共享，从单一银行业务转化为多层次多业态联通的综合系统，就需要建立统一的行业标

准，包括技术类标准、数据管理类标准、数据质量标准、风险评估标准等，这是都是实现数据共享与多场景融合的基本要求。只有遵循同一标准与要求，才可能构建一体化的开放银行体系。

但是 CDR 的做法未必能够完全符合我国的监管要求与社会环境的土壤。首先我们需要考虑，我国可能需要实现多大范围内的数据共享，是特定一个或几个行业，还是全行业的数据流通。比较于全行业的计划，实现在特定行业内部的数据共享将会相对容易。但是不同行业之间也有区别。举例来说，与社交软件数据共享相比，银行业的数据共享可能还算容易得多。想象如果我们可以从“微信”提取所有的转账记录并要求实时分享到“支付宝”，这会是怎样的场景。如果我们可以跨行业分享数据，金融科技公司（假设经过授权）可以通过提取“微信”的聊天记录来判断一个人的信用状况，这又是怎样的情景。这些情况意味着更激烈的行业竞争，虽然一定程度上企业、消费者都可能从中获益，但是那时我们可能会更加深入地去思考数据安全和隐私保护的问题了。

其次，如何保障实现开放数据共享的这些银行以及企业获得相应的收益与回报。CDR 以重视消费者权利为中心切入，要求银行公开产品参数和消费者的相关数据，这对传统占据垄断地位的银行业是构成巨大挑战的。试想，他们要从其本来垄断的资源中分一块奶酪给对其可能构成竞争的第三方，那肯定需要被反馈其认为更有诱惑力的回报，否则单纯为顺应政府监管或者通过立法强压而形成的模式是不稳定和持久的。因此，我国需要慎重考虑以怎样的方式分配和平衡好消费者、数据持有者和新兴企业之间的利益分配机制？

另外，我们还应该考虑如何在不同企业间分配责任。数据共享的目标是刺激竞争，同时促进银行业务形态多样化并帮助金融科技企业有所发展，便利个人和小型企业获得更合适的信贷项目，解决融资难题。但是大银行与小金融公司之间实力悬殊，如果对金融科技企业课以过高的数据合规义务可能反倒会极大阻碍其发展，但如果安全标准定得过低就有可能发生数据泄露，产生侵犯消费者隐私的风险。因此，我们应当考虑到各参与方间的实力差距，也应当考虑到消费者信贷需求和其提供个人数据意愿的平衡。比如在开放银行生态打开前，大银行、大企业可以适当地多承担数据安全能力适配、安全标准研发、行业规则制定等社会义务与责任，当然在这过程中，这些大企业从趋利的角度出发，可能会在政策标准中向自己倾斜更多的利益；这就要求在生态开放后，请这些大企业和银行多共享数据，并接受首当其冲的消费者隐私保护合规性审查，对其进行利益与责任的适当分配。

再有，我国应该设立怎样的监管机构实现有力监督。如前文所述，澳大利亚有其独特的监管模式，ACCC 与澳大利亚信息专员办公室（OAIC）和数据标准机构（DSB）合作开发和实施 CDR。OAIC 负责接受 CDR 计划下的投诉、调查和执行，

以处理隐私投诉并开展其他有关隐私的监管活动。我国目前尚无统一的隐私监管机构，因此从保护消费者隐私角度来说，由谁来承担监管机构的角色并实施有效监管最合适？是与行业监管机构（如人民银行）合一，还是单独对消费者隐私保护和数据安全另设一套监管机构？另外，在有监管的情况下，应该配套怎样的处罚标准和措施（民事、行政或刑事），这一系列问题都有待回答与进一步思考和探索。

当然，CDR 法案与规则对我国企业赴海外投资也可能产生重大影响和启发。目前来看，CDR 可能促进竞争，动摇澳大利亚银行业原本的“锁定效应”，对金融科技企业的发展提供法律支持，让更多消费者具有更丰富的选择。同时，对传统银行业而言，这必然是巨大的挑战但也蕴藏着另一层巨大的机遇。在大数据时代，通过分析消费者数据，了解更加全面的信息，提供个性化服务是一个企业乃至许多产业发展的方向。

对于中国中小企业赴澳投资，CDR 可能是一个利好消息，我们有机会获取更低价格的信贷产品。对于中国在澳大利亚的金融科技企业，如能尽早获取牌照，通过 CDR 可能会争取更多新用户，创造新一轮的业务增长点。澳大利亚政府在很大程度上希望帮助金融科技企业不断壮大发展。

虽然存在着机遇，我们还是需要提醒中国的金融科技企业需要高度重视在澳大利亚关于个人隐私保护、数据安全方面的合规工作。CDR 在给消费者数据带来更大透明度和流动性的同时，对数据安全提出更高的要求。澳大利亚政府也将为相关监管配备充足资金支持。从银行业起头，后面的数据开放步骤会越来越密，因此在实施数据共享的过程中，金融科技企业需要提前做好一系列合规准备工作。[29]

[29] 作者：孟洁。

中国首家律师事务所

北京市朝阳区建国路81号华贸中心
1号写字楼15层&20层 邮编: 100025
15 & 20/F Tower 1, China Central Place,
No. 81 Jianguo Road Chaoyang District,
Beijing 100025, China
电话/T. (86 10) 6584 6688
传真/F. (86 10) 6584 6666

上海市黄浦区湖滨路150号企业天地
5号楼26层 邮编: 200021
26F, 5 Corporate Avenue,
No. 150 Hubin Road, Huangpu District,
Shanghai 200021, China
电话/T. (86 21) 2310 8288
传真/F. (86 21) 2310 8299

深圳市南山区铜鼓路39号大冲国际中心
5号楼26层B/C单元 邮编: 518055
Units B/C, 26F, Tower 5,
Dachong International Center, No. 39 Tonggu Road,
Nanshan District, Shenzhen 518055, China
电话/T. (86 755) 8388 5988
传真/F. (86 755) 8388 5987