NEWSLETTER

数据合规

2019 第八期 /总第八期

数据合规时事速递

北京市环球律师事务所

2019 年 9 月 17 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. 国家网信办发布《网络生态治理规定（征求意见稿）》

规定概况

国家互联网信息办公室 10 日就《网络生态治理规定（征求意见稿）》向社会公开征求意见。意见反馈截止时间为 2019 年 10 月 10 日。[1]

征求意见稿明确，网络信息内容生产者不得制作含有带有性暗示、性挑逗、性诱惑的；展现血腥、惊悚等致人身心不适的；宣扬炫富拜金、奢靡腐化等生活方式的；过度炒作明星绯闻、娱乐八卦的；使用夸张标题，内容与标题严重不符等内容的不良信息。

对于网络信息内容服务平台，征求意见稿提出应当切实履行网络生态治理主体责任，加强本平台生态治理工作。网络信息内容服务平台采用个性化算法推荐技术推送信息的，应建立健全人工干预机制，建立用户自主选择机制。同时，还应当在首页、账号页面、信息内容页面等显著位置设置便捷投诉举报入口。

关于网络信息内容服务使用者，征求意见稿要求，在以发帖、回复、留言、弹幕等形式参与网络活动时，积极弘扬正能量，不得复制、发布、传播违法信息，自觉抵制不良信息。不得利用网络和相关信息技术，实施侮辱、诽谤、威胁以及恶意泄露他人隐私、散布谣言、人肉搜索等网络侵权、网络暴力行为，侵害其他组织或者个人合法权益。此外，还规定不得通过人力或者技术手段实施流量造假、流量劫持以及虚假注册账号、批量买卖账号、操纵用户账号等行为，破坏网络生态秩序。

[1] 中华人民共和国国家网络信息办公室。

“网信部门根据相关法律法规规定，会同有关部门建立健全网络信息服务严重违规失信联合惩戒机制。”征求意见稿还指出，对严重违反规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

规定原文

网络生态治理规定

(征求意见稿)

第一章 总则

第一条 为了加强网络生态治理，维护良好网络秩序，保障公民、法人和其他组织的合法权益，构建天朗气清的网络空间，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，制定本规定。

第二条 中华人民共和国境内的网络生态治理，适用本规定。法律、行政法规另有规定的，遵照其规定。

本规定所称网络生态治理，是指政府、企业、社会、网民等主体，以网络信息内容为主要治理对象，以营造文明健康的良好生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

第三条 国家网信部门负责统筹协调网络生态治理和相关监督管理工作。国家新闻出版部门和国务院教育、电信、公安、文化、市场监督管理、广播电视等有关主管部门依据各自职责做好网络生态治理工作。

地方各级网信部门依据职责负责统筹协调本行政区域内网络生态治理和相关监督管理工作。地方各级新闻出版部门和教育、电信、公安、文化、市场监督管理、广播电视等有关主管部门依据各自职责做好本行政区域内网络生态治理工作。

第二章 网络信息内容生产者

第四条 网络信息内容生产者应当遵守法律法规，遵循公序良俗，加强网络文明建设。

第五条 鼓励制作含有下列内容的信息：

(一)宣传习近平新时代中国特色社会主义思想，全面准确生动解读中国特色社会主义道路、理论、制度、文化的；

(二)宣传党的理论路线方针政策和中央重大决策部署的；

(三)展示经济社会发展亮点，反映人民群众伟大奋斗和火热生活的；

(四)弘扬社会主义核心价值观，宣传优秀道德文化和时代精神，充分展现中华民族昂扬向上精神风貌的；

(五)有效回应社会关切，解疑释惑，析事明理，有助于引导群众形成共识的；

(六)有助于提高中华文化国际影响力，向世界展现真实立体全面的中国的；

(七)其他含有讴歌真善美、促进团结稳定等积极内容的。

第六条 禁止制作含有下列内容的违法信息：

(一)违反宪法所确定的基本原则的；

(二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

(三)损害国家荣誉和利益的；

(四)歪曲、丑化、亵渎、否定英雄烈士及其事迹和精神的；

(五)宣扬恐怖主义、极端主义，煽动民族仇恨、民族歧视，破坏民族团结的；

(六)破坏国家宗教政策，宣扬邪教和封建迷信的；

(七)散布虚假信息，扰乱经济秩序和社会秩序的；

(八)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

(九)侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

(十)含有法律、行政法规禁止的其他内容的。

第七条 不得制作含有下列内容的不良信息：

(一)带有性暗示、性挑逗、性诱惑的；

(二)展现血腥、惊悚等致人身心不适的；

(三)宣扬炫富拜金、奢靡腐化等生活方式的；

(四)过度炒作明星绯闻、娱乐八卦的；

(五)使用粗俗语言、展示恶俗行为、宣扬低俗内容的；

(六)调侃恶搞自然灾害、重大事故等灾难的；

(七)煽动人群歧视、地域歧视等的；

(八)使用夸张标题，内容与标题严重不符的；

(九)对未成年人身心健康造成不良影响的；

(十)其他含有危害社会公德等破坏网络生态内容的。

第三章 网络信息内容服务平台

第八条 网络信息内容服务平台应当切实履行网络生态治理主体责任，加强本平台生态治理工作，积极培育向上向善的网络文化。

第九条 网络信息内容服务平台应当建立网络生态治理机制，健全信息发布审核、跟帖评论审核、版(页)面生态管理、实时巡查、应急处置、网络谣言处置、网络黑产线索处置等制度。网络信息内容服务平台应当设立网络生态治理负责人，配备与服务规模相适应的工作人员，并加强教育培训。

第十条 网络信息内容服务平台应当加强对其用户发布信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

网络信息内容服务平台对网信部门和有关部门依法实施的监督检查，应当予以配合。

第十一条 网络信息内容服务平台禁止复制、发布、传播本规定第六条规定的信息。

第十二条 网络信息内容服务平台不得复制、发布、传播本规定第七条规定的

信息。

第十三条 网络信息内容服务平台应当加强以人工编辑、机器算法等方式推荐、呈现信息环节的管理，营造积极健康的版(页)面生态。包括但不限于以下重点环节(服务类型、位置板块)：

(一)互联网新闻信息服务首页(屏)、弹窗和重要新闻信息内容页面等；

(二)互联网用户公众账号信息服务文章列表标题、封面图及精选、热搜等；

(三)微博客信息服务热门推荐、榜单类及基于地理位置的信息服务板块等；

(四)互联网信息搜索服务热搜词、热搜图及默认搜索等；

(五)互联网论坛社区服务首页(屏)、榜单类等；

(六)互联网音视频服务首页(屏)、发现、精选、榜单类、封面、弹窗等；

(七)网络文学(动漫)服务首页(屏)、精选、榜单类、封面等；

(八)网络游戏服务场景、角色、道具及公共聊天室等；

(九)生活服务平台首页(屏)、热门推荐等；

(十)电子商务平台首页(屏)、推荐区、商品列表封面等；

(十一)移动智能终端预置应用软件首屏、推荐区、弹窗等；

(十二)以未成年人为服务对象的网络信息内容服务。

第十四条 鼓励网络信息内容服务平台开发适合未成年人使用的模式。

网络信息内容服务平台提供网络游戏、网络文学、网络动漫、网络直播、网络音视频及其他各类服务时，应当采取措施防止未成年人接触违法和不良信息。

第十五条 网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当建立体现主流价值导向的推荐模型，建立健全人工干预机制，建立用户自主选择机制。

第十六条 网络信息内容服务平台应当对本平台推送或者展示的广告内容和位置加强审核监看，对发布违法广告的，应当予以制止。

第十七条 网络信息内容服务平台应当完善用户服务协议，明确用户相关权利义务，并依法依约履行相应管理职责。

网络信息内容服务平台应当建立用户账号信用档案，根据用户账号的信用等级提供相应的服务。

第十八条 网络信息内容服务平台应当在首页、账号页面、信息内容页面等显著位置设置便捷投诉举报入口，公布投诉举报方式，细化网络生态违法和不良信息举报分类，及时受理处置公众投诉举报并反馈处理结果。

第十九条 网络信息内容服务平台应当编制网络生态治理工作年度报告，包括网络生态治理工作情况、网络生态治理负责人履职情况、社会评价情况等内容。

第四章 网络信息内容服务使用者

第二十条 鼓励网络信息内容服务使用者积极参与网络生态治理，以投诉、举报等方式加强对网上违法和不良信息的监督，共同建设良好网络环境。

网络信息内容服务使用者应当文明健康使用网络，按照法律法规的要求和用户协议约定，切实履行相应义务，在以发帖、回复、留言、弹幕等形式参与网络活动时，积极弘扬正能量，不得复制、发布、传播违法信息，自觉抵制不良信息。

第二十一条 网络群组、论坛社区版块建立者和管理者，应当履行群组、版块管理责任，依据法律法规、用户协议和平台公约等，规范群组、版块内信息发布等行为。

第二十二条 网络信息内容服务使用者不得利用网络和相关信息技术，实施侮辱、诽谤、威胁以及恶意泄露他人隐私、散布谣言、人肉搜索等网络侵权、网络暴力行为，侵害其他组织或者个人名誉权、财产权等合法权益。

第二十三条 网络信息内容服务使用者不得通过发布、删除信息等干预信息呈现的手段谋取不正当利益。

第二十四条 网络信息内容服务使用者不得利用深度学习、虚拟现实等新技术新应用从事法律、行政法规禁止的活动。

第二十五条 网络信息内容服务使用者不得通过人力或者技术手段实施流量造假、流量劫持以及虚假注册账号、批量买卖账号、操纵用户账号等行为，破坏网络生态秩序。

第二十六条 网络信息内容服务使用者不得利用党徽、国旗、国徽等代表党和国家形象的标识，或者借党和国家领导人名义及国家重大活动、重大纪念日等，违法违规开展网络商业营销活动。

第五章 网络行业组织

第二十七条 鼓励行业组织推进行业自律，建立健全网络生态治理行业准则，指导、督促会员单位及从业人员依法提供网络信息内容服务。

第二十八条 鼓励行业组织开展网络生态治理教育培训和宣传引导工作，提升会员单位、从业人员治理能力，增强全社会共同治理意识。

第二十九条 鼓励行业组织建立相应评价奖惩机制，支持会员单位开展网络生态治理，加大对会员单位激励和惩戒力度。

第六章 监督管理

第三十条 地方各级网信部门应当会同有关部门，切实履行属地管理责任，做好本行政区域内网络生态治理工作。

第三十一条 地方各级网信部门建立社会各界共同参与的监督评价机制，定期对本行政区域内网络信息内容服务平台生态治理情况进行评估。

第三十二条 各级网信部门会同有关部门，建立健全信息共享、会商通报、联合执法、案件督办等工作机制，协同开展网络生态治理工作。

第三十三条 各级网信部门对网络信息内容服务平台履行生态治理主体责任情况开展监督检查，对问题突出的平台开展专项督查，及时向社会公开检查情况及查处结果。

第三十四条 各级网信部门建立网络信息内容服务平台违法违规行为台账管理机制，根据台账依法依规进行相应处理。

第七章 法律责任

第三十五条 网络信息内容生产者违反本规定第六条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新、关闭账号等处置措施，及时消除违法信息内容，保存记录并向有关主管部门报告。由有关主管部门依法采取相应措施。

网络信息内容服务平台违反本规定第十条第一款、第十一条规定的，由网信等有关主管部门依照《中华人民共和国网络安全法》的规定，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本规定第六条规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第三十六条 网络信息内容生产者违反本规定第七条规定的，网络信息内容服务平台应当依法依约采取警示整改、限制功能、暂停更新等处置措施，保存有关记录，并向有关主管部门报告。由有关主管部门依法采取相应措施。

网络信息内容服务平台违反本规定第十二条规定的，由网信等有关主管部门依据职责采取约谈、责令限期改正等管理措施。拒不改正或者情节严重的，依法给予警告、罚款、责令停业整顿直至吊销许可证；构成犯罪的，依法追究刑事责任。

第三十七条 网络信息内容服务平台违反本规定第十六条规定的，由有关主管部门依照相关法律、行政法规的规定处理。

第三十八条 网络信息内容服务平台违反本规定第九条、第十条第二款、第十三条、第十五条、第十七条至第十九条规定的，由网信等有关主管部门依据职责采取约谈、责令限期改正等管理措施。拒不改正或者情节严重的，依法给予警告、罚

款、责令停业整顿直至吊销许可证；构成犯罪的，依法追究刑事责任。

第三十九条 违反本规定第二十一条至第二十六条规定的，依照相关法律、行政法规的规定处理。

第四十条 网信部门根据相关法律法规规定，会同有关部门建立健全网络信息服务严重违规失信联合惩戒机制，对严重违反本规定的网络信息内容服务平台、网络信息内容生产者和网络信息内容使用者依法依规实施限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

第八章 附则

第四十一条 本规定所称网络信息内容生产者，是指制作网络信息内容的组织或者个人。

本规定所称网络信息内容服务平台，是指提供信息内容复制、发布、传播等服务的网络信息服务提供者。

本规定所称网络信息内容服务使用者，是指使用网络信息内容服务的组织或者个人。

第四十二条 网络信息内容服务平台应当依据本规定，制定本平台网络生态治理具体标准和工作细则。

地方网信部门可结合本地实际，制定实施细则。

第四十三条 本规定自 2019 年 月 日起施行。

2. 国家移民管理局发布《出入境证件身份认证管理办法（试行）》

办法解读

2019 年 9 月 12 日，国家移民管理局公布了《出入境证件身份认证管理办法(试行)》。国家移民管理局高度重视公民隐私保护，从四个方面做出周密安排，确保不出现泄露个人隐私情况。

为推进移民和出入境领域“放管服”改革，优化营商环境，国家移民管理局运用现代科技建设了出入境证件身份认证平台，向社会提供出入境证件身份认证。为确保认证服务有章可循、有规可依、安全有序，国家移民管理局制定了《出入境证件身份认证管理办法(试行)》，规定了出入境证件身份认证提供方、服务对象、服务内容、资质条件、申请材料、办理流程、违规处理措施、安全管理责任等事项。

国家移民管理局授权并指导、监督出入境管理信息技术研究所开展出入境证件身份认证，运行出入境证件身份认证平台。研究所利用平台技术，对外提供出入境证件信息一致性的核验和证件识读服务。服务有三种方式：实名认证，即对出入境证件持有人的姓名、证件号码等信息进行一致性核验；实人认证，即对出入境证件持有人的人像信息进行一致性核验；证件电子信息识读，即对出入境证件所载芯片内电子信息进行识读。

《管理办法》规定了使用单位的资格条件，应当提交的申请材料以及申办流程。使用单位可以通过网上用户管理系统在线申请，通过审核后，与研究所签订使用和保密协议，并在研究所指导下开展技术对接，开通认证。使用单位可以采用移动数字证书或者签名验签服务器方式接入平台。

《管理办法》还对协议中双方的权利和义务作了要求。

国家移民管理局高度重视公民隐私保护，从四个方面做出周密安排，确保不出现泄露个人隐私情况。

一是出入境证件身份认证平台经国家权威机构检测，通过了信息系统安全保护第三级要求。

二是使用单位与认证平台之间采用硬件密码设备加密数据，保证数据传输过程安全保密。

三是对使用单位的信息系统提出了明确安全性要求。

四是在服务提供过程中，实时监控服务使用情况，并对违规行为作出提示纠正、暂停服务或者终止服务的处理措施。

《管理办法》以国家移民管理局公告形式对外发布，同时，在互联网上同步推出网上用户管理系统。研究所将在国家移民管理局的指导监督下，本着公开透明、公平公正的原则，努力提高服务质量与能力，为使用单位做好服务保障工作，欢迎社会各届进行监督。[2]

办法原文

出入境证件身份认证管理办法（试行）

第一条 为保证出入境证件身份认证工作正常开展，规范认证管理服务，根据《中华人民共和国出境入境管理法》《中华人民共和国护照法》《中华人民共和国网络安全法》《国务院关于在线政务服务的若干规定》等法律法规，制定本办法。

[2] 中新网。

第二条 国家移民管理局负责建设出入境证件身份认证平台，授权并指导、监督出入境管理信息技术研究所开展出入境证件身份认证工作。

第三条 本办法所称出入境证件身份认证，是指向依法依规应当查验个人身份信息的经营者（以下简称使用单位）提供对当事人所持出入境证件信息进行一致性核验。

第四条 出入境证件身份认证采取以下方式：

（一）实名认证，对出入境证件持有人的姓名、证件号码、出生日期等信息进行一致性核验，返回核对结果；

（二）实人认证，对出入境证件持有人的人像信息进行一致性核验，返回核对结果；

（三）证件电子信息识读，对出入境证件所载芯片内电子信息进行识读，返回识读结果。

第五条 使用单位应当符合以下条件：

（一）在中华人民共和国境内注册，具有独立法人资格，遵守中华人民共和国相关法律法规；

（二）依法依规应当查验当事人身份；

（三）对使用出入境证件身份认证的信息系统具有所有权或者运营权；

（四）具备安全使用出入境证件身份认证的技术保障环境；

（五）使用出入境证件身份认证不会危害国家安全、损害公共利益和他人合法权益。

第六条 使用单位申请开通出入境证件身份认证应当提供以下材料：

（一）使用单位基本情况表；

（二）企业营业执照复印件，事业单位、社会团体、基金会、社会服务机构法人登记证书复印件；

（三）使用出入境证件身份认证的合法性说明材料，包括需要使用出入境证件身份认证的法律法规依据，业务领域、应用场景、认证内容等；

（四）对使用出入境证件身份认证的信息系统具有所有权或者运营权的权属证明；

（五）使用出入境证件身份认证的信息系统的安全性说明材料，包括软硬件运行环境、网络架构、系统模块组成、安全防护措施等。

使用单位应当对上述材料的真实性负责。如果上述材料登记事项发生变更或者失效的，应当自变更或者失效之日起十五日内重新提交。

第七条 出入境证件身份认证提供方为使用单位开通出入境证件身份认证，应当按以下程序办理：

（一）使用单位在线申请并提交本办法第六条规定的材料；

（二）出入境证件身份认证提供方对申请材料进行核查，发出通过核查、不通过核查和补充申请材料通知；

（三）核查通过后，双方开展平台对接调试；

（四）调试结束后，双方签订使用和安全保密协议；

（五）开通出入境证件身份认证业务。

第八条 出入境证件身份认证提供方评估使用单位认证量需求，确定采用移动数字证书或者签名验签服务器方式接入出入境证件身份认证平台。

第九条 使用和安全保密协议中应当包括以下内容：

（一）使用单位应当在约定的业务范围内合法合规正当使用出入境证件身份认证，不得将出入境证件身份认证功能转让给任何的第三方使用；

（二）使用单位应当制定安全管理制度和应急预案，保障使用出入境证件身份认证的信息系统、移动数字证书和签名验签服务器的安全；

（三）出入境证件身份认证提供方保证平台能足够满足正常的认证需求；

（四）出入境证件身份认证提供方应当及时提供身份认证结果；

（五）暂停或者终止出入境证件身份认证业务的各类情形。

第十条 出入境证件身份认证服务提供方应当依据相关规定，指导和监督使用单位依规正确规范使用出入境证件身份认证平台。

第十一条 使用单位不得利用出入境证件身份认证业务以任何理由向任何单位或者个人收取费用。

第十二条 使用单位具有以下情形之一的，出入境证件身份认证服务提供方应

当及时提示并纠正：

（一）未遵守、执行安全管理制度和管理措施；

（二）访问流量异常的；

（三）使用运营中存在安全风险的。

使用单位应当在接到提示通知之日起十日内改正并反馈结果。

第十三条 使用单位具有以下情形之一的，出入境证件身份认证提供方应当暂停认证服务：

（一）接到提示通知后，未能在十日内改正的；

（二）未按照本办法第六条第二款规定重新提交材料的；

（三）超范围使用出入境证件身份认证的；

（四）因使用单位的信息系统存在管理问题，影响出入境证件身份认证平台正常运行的；

（五）违反使用和安全保密协议的行为；

（六）违反法律法规、本办法的其他行为。

使用单位应当在接到暂停出入境证件身份认证通知之日起三十日内改正，对于在上述时限内改正并经核查确认后，可以重新开通认证业务。

第十四条 使用单位具有以下情形之一的，出入境证件身份认证提供方应当终

止认证业务：

（一）接到暂停认证通知后，未能在三十日内改正的；

（二）提交不真实或者虚假资料的；

（三）不再符合本办法第五条规定条件的；

（四）转让出入境证件身份认证功能或者泄露身份认证结果的；

（五）利用出入境证件身份认证业务向任何单位或者个人收取任何费用的；

（六）将出入境证件身份认证用于违法违规用途的；

（七）其他违反双方使用和安全保密协议的严重行为的；

（八）违反法律法规、本办法的其他行为，情节严重。

第十五条 出入境证件身份认证提供方发现使用单位使用认证业务有违法犯罪嫌疑的，应当及时报告有关部门依法查处。

第十六条 本办法由国家移民管理局负责解释。

第十七条 本办法自公布之日起试行。

3. 新加坡新《个人资料保护法令》今年 9 月 1 日生效

自 9 月 1 日起，新加坡新个人资料保护法令将正式生效，商家与业者只能在有必要时或法律规定下，向民众索取身份证号码。

个人资料保护委员会（简称，PDPC）发文告表示，业者不允许任意持有个人信息的重要资料，如身份证字号、出生证明书、外籍人士身份证、护照以及工作准证等，以杜绝个人重要信息的猖獗使用。

新加坡民众与永久居民的个人重要信息经常被广泛使用，无论是填写幸运抽奖资料、申请资料，到注册任何购买物品等。

个人资料保护委员会表示，“身份证号能够检索许多民众的个人信息，因此我们需要减少滥用身份证号码的现象。”

自周日起，身份证字号或影印本只能在法律规定下持有，例如申请电信、预约看诊服务、酒店预订登记等。

此外，身份证字号也会在必要时候，如确保个资准确无误时索取，包括进入小学学校或涉及医疗保健、财务或房地产事务的交易，确保他们是安全可信的。

业者可评估是否保留目前已登记的身份证字号，若非必要，个人资料保护委员建议应根据《个人资料保护法令》（Personal Data Protection Act，简称 PDPA）删除身份证字号。

业者若持续肆意收集或滥用消费者身份证字号，将被视为藐视个人资料保护法令，或将罚高达 100 万新元。但私人业者却反驳，可能会因为一些无聊的因素而需要登记身份证字号，如预订电影票，或租凭脚踏车或汽车。

据《海峡时报》报导，许多企业也纷纷为此早作准备，如保安公司 Prosegur Security 已随 PDPA 法为工作流程进行修订，以往他们会要求客户提供身份证字号确认身份，但如今随着修法后，他们也转而向客户要求提供手机号码或是其他国家的身份证明号码。

人力银行企业 Jobstreet 的发言人亦表示，自 6 月起，他们已不再向求职者提供身份证字号，而且也向已登记的求职者告知已删除身份证字号的讯息。[3]

[3] The Online citizen.

4. 美国旧金山颁布《停止秘密监控法令（SSSO）》（中英对照版）[4]

San Francisco Supervisor: Stop Secret Surveillance Ordinance (05/06/2019)

旧金山立法监督员：停止秘密监控法令（SSSO）(05/06/2019)

Section. 1 General Findings
(d) The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring.

第一条 一般性调查发现
（d）面部识别技术倾向于危害公民权利和公民自由，给公众带来的危害远超过好处。该技术将加剧种族歧视，并威胁我们不受政府持续监控的生活能力。

Section 2. The Administrative Code is amended by adding Chapter 19B, consisting of Sections 19B.1-19B.8, to read as follows:

第二条 《行政法典》因增加第 19B 章而修订，增加的内容包括第 19 B.1-19B.8 条，具体如下：

CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY

第 19B 章 监控技术的取得

SEC. 19B.1. DEFINITIONS.
"Face recognition technology" means an automated or semi-automated process that assists in identifying or verifying an individual based on an individual's face.

第 19B.1 条 定义
“面部识别技术”是指一个自动或半自动的程序通过，有助于基于个体面部特征识别或验证个人身份。

SEC. 19B.2. BOARD OF SUPERVISORS APPROVAL OF SURVEILLANCE TECHNOLOGY POLICY.
(d) Notwithstanding the provisions of this Chapter 19B, it shall be unlawful for any Department to obtain, retain, access, or use: 1) any Face Recognition Technology; or 2) any information obtained from Face Recognition Technology. A Department's inadvertent or unintentional receipt, retention access to, or use of any information obtained from Face Recognition Technology shall not be a violation of this subsection (b), provided that:(1) The Department does not request or solicit its receipt, access to, or use of such information; and (2) The Department logs such receipt, access to, or use in its Annual Surveillance Report.

第 19.B.2 条 监督员委会对监控技术的批准
（d）尽管有本 19B 章的规定，任何部门获取、保存、访问或使用以下内容均属违法：1）任何面部识别技术；2）通过面部识别技术获得的任何信息。部门疏忽或无意地接收、保存、访问或使用通过面部识别技术获得的任何信息不得违反本条款第（b）款规定，但前提是：（1）该部门未要求或主动获取、访问或使用上述通过面部识别技术得到的信息；（2）该部门在其年度监控报告中记录上述信息被获取、访问或使用的行为。

[4] 中文翻译：孟洁律师团队，原文链接：
https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A

5. 美国马塞诸塞州《关于面部识别和新型生物识别技术的法案（众议院第 1538 号/参议院第 1358 号法案）》（中英对照版）[5]

Massachusetts: House No. 1538/Senate No. 1358	**马萨诸塞州：众议院第 1538 号/参议院第 1358 号法案**
An Act relative to unregulated face recognition and emerging biometric surveillance technologies.	与不受监管的面部识别和新兴生物识别监控技术相关的一部法案。
Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:	参议院和众议院代表基于各自权力，共同在州立法会议制定并通过内容如下：
SECTION 1. The general court hereby finds and declares that:	***第 1 条 州立法会议特此发布声明如下：***
WHEREAS, the Massachusetts General Court finds that government use of face recognition poses unique and significant civil rights and civil liberties threats to the residents of the Commonwealth of Massachusetts.	鉴于，马萨诸塞州立法会议认为，政府机构使用面部识别技术对马萨诸塞州联邦居民的公民权利和公民自由构成了独特而重要的威胁。
WHEREAS, the Massachusetts General Court finds that face recognition technology has a history of being far less accurate in identifying the faces of women, young people, and dark-skinned people, and that such inaccuracies lead to harmful "false positive" identifications.	鉴于，马萨诸塞州立法会议认为，面部识别技术在女性、年轻人和肤色较深人群的面部识别准确性上远远落后，并且这种不准确性会导致有害的“错误识别”。
WHEREAS, the Massachusetts General Court finds that many of the databases to which face recognition technology is applied are plagued by racial disparities and other biases, which generate copycat biases in face recognition data.	鉴于，马萨诸塞州立法会议认为，许多面部识别技术应用的数据库受到了种族差异和其他歧视的困扰，这使得面部识别数据也跟着产生了偏见。
WHEREAS, the Massachusetts General Court finds that the broad application of face recognition in public spaces is the functional equivalent of requiring every person to carry and display a personal photo identification card at all times, which constitutes an unacceptable mass violation of privacy.	鉴于，马萨诸塞州立法会议认为，在公共场所广泛应用面部识别技术产生了相当于要求每个人随时携带和展示带有照片的个人身份证件同样的功能，这构成了对隐私不可接受的大规模侵犯。
WHEREAS, the Massachusetts General Court is likewise concerned about the deployment of other biometric surveillance systems, including gait and voice recognition, which raise similar concerns as face recognition.	鉴于，马萨诸塞州立法会议同样关注其他生物识别监控系统的部署，包括步和语音识别等与面部识别有相似问题的监控系统。

WHEREAS, the Massachusetts General Court finds that the public use of biometric surveillance systems can chill the exercise of constitutionally protected free speech and association.	鉴于，马萨诸塞州立法会议认为，生物识别监控系统在公共领域的使用会使受宪法保护的言论和结社自由受到抑制。
WHEREAS, the Massachusetts General Court finds that the benefits of using biometric surveillance systems, which are few and speculative, are greatly outweighed by their harms, which are substantial.	鉴于，马萨诸塞州立法会议认为，使用生物识别监控系统的好处很少，并且根据推断，相比于其所造成的实质性危害，这些好处不值一提。
THEREFORE, be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:	因此，参议院和众议院代表基于各自权力，共同在立法会议制定并通过如下内容：
SECTION 2. Chapter 4 of the General Laws is hereby amended by inserting at the end of section 13, as appearing in the 2016 Official Edition, the following:-	***第 2 条 普通法（2016 年官方版）第四章在因第十三条末尾增加以下内容，特此得以修订：***
Section 14. (a) Definitions. As used in this section, the following words shall have the following meanings:	**第十四条** (a) 定义。在本条中，以下术语有如下含义：
"Face recognition", an automated or semi-automated process that assists in identifying an individual or capturing information about an individual based on the physical characteristics of an individual's face, or that logs characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual.	“面部识别”，指一种自动或半自动化的程序，有助于识别个体或基于个体的面部身体特征捕获个人信息，或记录个体的面部、头部或身体的特征以推断其情绪、社会关系、活动或所在地。
"Other remote biometric recognition", an automated or semi-automated process that assists in identifying an individual or capturing information about an individual based on the characteristics of an individual's gait, voice, or other immutable characteristic ascertained from a distance, or that logs such characteristics to infer emotion, associations, activities, or the location of an individual; provided, however, that other remote biometric recognition shall not include recognition based on DNA, fingerprints, or palm prints.	“其他远程生物识别”，指一种自动或半自动化的程序，可帮助识别一个个体或基于个人的步法、声音或远距离获取的其他不可变特征捕获有关个人的信息，或通过记录此类特征来推断出个体的情绪、社会关系、活动或其所在的位置；但是，前提是其他远程生物识别技术不应包括基于 DNA、指纹或掌纹的识别。

[5] 中文翻译：孟洁律师团队，原文链接：https://malegislature.gov/Bills/191/H1538.pdf。

"Biometric surveillance system," any computer software that performs face recognition or other remote biometric recognition.

"生物识别监控系统"，指任何实施面部识别或其他远程生物识别的计算机软件。

"Commonwealth of Massachusetts", any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose.

"马萨诸塞州联邦"，指联邦的任何机构、执行办公室、部门、理事会、委员会、主管局、部门或机构，或其任何政府的下属分支机构，或由立法会议为服务公共目的设立的任何机构。

"Massachusetts government official", any officer, employee, agent, contractor, or subcontractor of any agency, executive office, department, board, commission, bureau, division or authority of the commonwealth, or of any political subdivision thereof, or of any authority established by the general court to serve a public purpose.

"马萨诸塞州政府官员"，指任何机构、执行办公室、部门、理事会、委员会、主管局、部门或联邦机构，或其任何政府的下属分支机构或任何由立法会议为服务公共目的而设立的任何机构的任何官员、雇员、代理人、外包人员或分包商。

(b) Moratorium on government use of biometric surveillance.

(b) 宣布政府暂停使用生物识别监控技术。

Absent express statutory authorization, it shall be unlawful for the Commonwealth of Massachusetts or any Massachusetts government official to acquire, possess, access, or use any biometric surveillance system, or acquire, possess, access, or use information derived from a biometric surveillance system operated by another entity.

如果没有明确的法律授权，马萨诸塞州联邦或任何马萨诸塞州政府官员获取、拥有、访问或使用任何生物识别监控系统，或获取、拥有、访问或使用来自由其他主体运营的生物识别监控系统的信息均属违法行为。

Statutory authorization for government use of a biometric surveillance system shall describe with particularity:

法律授权政府使用生物识别监控系统时，应特别规定以下内容：

(i) the entities permitted to use the biometric surveillance system, the purposes for such use, and prohibited uses:

（i）允许使用生物识别监控系统的实体以及允许其使用和不允许其使用的目的：

(ii) standards for use and management of information derived from the biometric surveillance system, including but not limited to data retention, sharing, access, and audit trails;

（ii）使用和管理从生物监控系统获取信息的标准，包括但不限于数据保存、共享、访问和审计跟踪;

(iii) auditing requirements to ensure the accuracy of biometric surveillance system technologies, standards for minimum accuracy rates, and accuracy rates by gender, skin color, and age;

（iii）确保生物识别监控系统技术的准确性，最低准确率标准和性别、肤色和年龄准确率的审计要求;

(iv) rigorous protections for due process, privacy, free speech and association, and racial, gender, and religious equity;

（iv）为正当程序、隐私、言论和结社自由，以及种族、性别和宗教公平而设置的严格保护机制;

and (v) mechanisms to ensure compliance.

以及（v）确保合规的机制。

c) Until such time as the General Court enacts an authorizing statute in accordance with subsection (b), the following provisions shall be in force:

（c）根据(b)项，在立法会议颁布授权法规之前，下列条款应具有效力：

(i) Admissibility. Except in a judicial proceeding alleging a violation of this section, no information obtained in violation of this section shall be admissible by the government in any criminal, civil, administrative or other proceeding.

（i）法庭采纳。除非一个司法程序指控本条违法，政府因违反本条而采集的任何信息在任何刑事、民事、行政或其他程序中均不得被当作证据采纳。

(ii) Cause of Action. Any violation of this Act constitutes an injury and any person may institute proceedings against the Commonwealth of Massachusetts for injunctive relief, declaratory relief, or writ of mandamus in any court of competent jurisdiction to enforce this Act, and shall be entitled to recover actual damages and additional damages of an amount equal to $100 for each violation, or $1,000, whichever is greater. A court shall award costs and reasonable attorneys' fees to a plaintiff who is the prevailing party in an action brought under this section.

（ii）案由。任何违反本法的行为均构成损害，任何人均可向马萨诸塞州联邦提起诉讼，要求在任何具有司法管辖权的法院执行本法案，以获取禁令救济、确认赔偿请求或强制令，并应有权要求赔偿实际损害和额外赔偿金（每次违规赔偿 100 美元或总共 1,000 美元，以较高者为准）。如原告根据本条起诉而胜诉的，法院应判处诉讼费用和合理的律师费由败诉方承担。

(iii) Training. Violations of this Act by any Massachusetts government official shall result in consequences that may include retraining, suspension, or termination, subject to due process requirements.

（iii）培训。任何马萨诸塞州政府官员违反本法案的，依据正当程序要求，将导致可能包括再培训、停职或开除的后果。

二、监管动态

1. 网信办：重点做好加强数据安全管理和个人信息保护

2019 年国家网络安全宣传周 9 月 16 日开幕，为了帮助民众更好地相关的情况，中央网信办副主任、国家网信办副主任刘烈宏先生，中共天津市委常委、宣传部部长陈浙闽先生介绍 2019 年国家网络安全宣传周有关情况。

国家网络安全的形势与进展

党的十八大以来，以习近平同志为核心的党中央高度重视网络安全工作，提出了一系列新思想、新理论、新论断、新战略，形成了习近平总书记关于网络强国的重要思想，为做好网络安全工作提供了根本遵循和强大动力。在习近平总书记关于网络强国的重要思想指引下，国家网络安全工作取得了积极进展，以《网络安全法》为核心的法律法规和政策准体系框架基本建立，国家网络安全保障体系不断完善，网络安全能力和水平不断提升，为保障国家安全和经济社会的发展发挥了重要作用。

说到风险，随着网络信息技术的持续演进，互联网对整个经济社会发展的渗透、驱动作用越来越明显，带来的风险挑战也在不断扩大。网络安全威胁和风险日益增多，地下黑产、电信网络诈骗等各类违法犯罪活动时有发生，数据安全和侵犯个人隐私问题日益凸显。针对关键信息基础设施的有组织高强度网络攻击愈加明显，特别是网络空间与现实世界安全问题不断交织，网络安全问题向现实世界传导，现实世界的安全问题也不断向网络空间蔓延，网络安全问题日益成为影响国家安全、社会稳定和人民群众切身利益的重大战略问题。

国家网络安全新的举措

做好新时代的网络安全工作，要深入贯彻落实习近平总书记关于网络强国的重要思想，重点做好以下几方面的工作：

一是加强数据安全管理和个人信息保护。加快出台数据安全管理办法、个人信息出境安全评估办法等相关法规制度和标准规范。深入开展 App 违法违规收集使用个人信息专项治理，依法严厉打击针对和利用国家大数据资源和个人信息的违法犯罪活动。

二是强化关键信息基础设施的保护。加快出台关键信息基础设施安全保护条例，落实运营单位主体责任和保护部门的监管责任，统筹开展网络安全检查，强化网络安全态势感知，监测预警和应急处置能力建设。

三是培育扶持网络安全技术产业做大做强。我们正在加强网络安全技术产业的规划和整体布局，完善支持网络安全技术产业发展的政策措施，培育一批具有国际竞争力的网络安全企业。

四是持之以恒抓好网络安全人才培养。加强网络空间安全学科专业建设，实施好一流网络安全学院建设示范项目，加快建设国家网络安全人才与创新基地，形成人才培养、技术创新、产业发展的良好生态。

五是积极推动网络空间国际治理。在习近平总书记全球互联网治理体系变革“四项原则”、构建网络空间命运共同体“五点主张”指引下，深化与各国和相关国际组织的务实合作，深入开展网络安全的对话互动，共同应对网络安全的威胁与挑战，携手构建网络空间命运共同体。[6]

[6] 国务院新闻办网站。

2. 教育部等八部门发布《关于引导规范教育移动互联网应用有序健康发展的意见》

教育移动互联网应用程序（教育 APP，以下简称教育移动应用）是指以教职工、学生、家长为主要用户，以教育、学习为主要应用场景，服务于学校教学与管理、学生学习与生活以及家校互动等方面的互联网移动应用。近年来，教育移动应用快速发展、广泛应用，在提高教学效率和管理水平、满足学生个性化学习需求和兴趣发展、优化师生体验等方面发挥了积极作用。但一些学校出现了应用泛滥、平台垄断、强制使用等现象，一些教育移动应用存在有害信息传播、广告丛生等问题，给广大师生、家长带来了困扰，产生了不良的社会影响。为引导和规范教育移动应用有序健康发展，更好地发挥教育信息化的驱动引领作用，现提出以下意见。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，深入贯彻党的十九大精神，全面落实全国教育大会精神、全国网络安全和信息化工作会议精神，根据《中华人民共和国教育法》《中华人民共和国网络安全法》等国家有关法律法规，围绕落实立德树人根本任务，积极发展“互联网+教育”、办好网络教育，全面深化“放管服”改革，实施包容审慎监管，引导教育移动应用健康有序发展，为广大师生营造健康、有序、安全的网络空间和学习环境。

（二）基本原则

科学施策、分类引导。正确处理政府与市场、管理与服务、安全与发展的关系。分类引导不同教育阶段和类型、不同用户群体、不同功能用途的教育移动应用，构

建良好教育生态。

问题导向、标本兼治。围绕群众反映强烈的问题，从供给侧和需求侧两端进行规范。开展专项行动治理乱象，建章立制规范管理，提质增效支撑发展，综合施策打好组合拳。

多方参与、协同联动。以构建常态化的治理体系为关键，建立政府管理、企业履责、专家献策、学校把关、家长监护、社会监督、行业自律等多主体参与、职责明晰的综合协同治理体系。

（三）工作目标

全面治理教育移动应用乱象，补齐监督短板，规范全生命周期管理，提高开发供给质量，营造优良发展生态，促进教育移动应用有序健康发展。2019 年底，完成教育移动应用备案工作。开展教育移动应用专项治理行动，群众反映强烈的问题得到有效缓解。2020 年底，建立健全教育移动应用管理制度、规范和标准，形成常态化的监管机制，初步建成科学高效的治理体系。

二、提高供给质量

（四）建立备案制度。教育移动应用提供者应当在取得 ICP 备案（涉及经营电信业务的，还应当申请电信业务经营许可）、网络安全等级保护定级备案的证明、等级测评报告后，向机构住所地的省级教育行政部门进行教育业务备案，登记单位基本信息和所开发的教育移动应用信息。已备案的教育移动应用提供者上线新应用前，应当在备案单位更新相关信息。教育部制定备案办法，明确备案流程和内容，依托国家教育资源公共服务平台为备案登记工作提供信息化支撑，汇总各省级教育行政部门备案信息，并向社会提供查询渠道。

（五）加强内容建设。教育移动应用提供者呈现的内容应当严格遵守国家法律法规，符合党的教育方针，体现素质教育导向，呈现的广告应当与提供的服务相契合。以未成年人为主要用户的教育移动应用应当限制使用时长、明确适龄范围，对内容进行严格把关。鼓励以高校师生为主要用户的教育移动应用增强优质网络教育资源供给能力，成为加强网络思想政治工作的有效载体。具备论坛、社区、留言等功能的教育移动应用应当建立信息审核制度。面向各教育阶段实施培训的教育移动应用应当对提供服务的主体进行审核、登记，其中：在校外线上培训机构实施学科类培训的人员应当取得教师资格证；聘用外籍人员实施培训的应当审查教学资质、学历和能力，并严格落实国家相关要求。

（六）规范数据管理。教育移动应用提供者应当建立覆盖个人信息收集、储存、传输、使用等环节的数据保障机制。按照“后台实名、前台自愿”的原则，对注册用户进行身份信息认证。收集使用个人信息应当明示收集使用信息的目的、方式和范围，并经用户同意。收集使用未成年人信息应当取得监护人同意、授权。不得以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得收集与其提供服务无关的个人信息，不得违反法律法规与用户约定，不得泄露、非法出售或非法向他人提供个人信息。

（七）保障网络安全。教育移动应用提供者应当落实网络安全主体责任，采取有效措施，防范应对网络攻击，保障系统的平稳、安全运行。教育移动应用和后台系统应当统一落实网络安全等级保护要求。应用商店等移动应用分发平台提供者应当加强教育移动应用上架审核管理，建立开发者真实身份信息登记制度，对教育移动应用开展安全审核，及时处理违法违规教育移动应用。鼓励教育移动应用提供者参加网络安全认证、检测，全面提高网络安全保障水平。

三、规范应用管理

（八）落实主体责任。教育行政部门和学校是本单位自主开发的教育移动应用的主管单位和选用第三方教育移动应用的责任单位，应当加强统筹管理，明确职能部门归口，将教育移动应用、公众号和小程序等移动互联网平台纳入本地区、本单位的重要议事日程予以部署。按照“谁主管谁负责、谁开发谁负责、谁选用谁负责”的原则，建立健全教育移动应用管理责任体系，切实维护广大师生和家长的切身利益。

（九）建立推荐机制。省级教育行政部门应当根据地方实际，会同网信等职能部门探索本地区教育移动应用的推荐机制，按照公平、公正、公开原则，组织开展教育移动应用的评议，形成推荐名单并向社会公开，同时报教育部。推荐名单应保证质量，并保持动态更新。鼓励通过第三方评估，组织对教育移动应用的合法合规、功能性能、安全保障等方面进行检测，对教育移动应用呈现的内容进行检查，为推荐工作提供技术支撑。

（十）健全选用机制。教育行政部门和学校应当制定教育移动应用的选用制度。选用应当充分尊重教职工、学生和家长的意见，并严格选用标准、控制数量，避免造成不必要的负担。确定选用的教育移动应用应当报上级教育行政部门进行备案。未经教育行政部门、学校集体决策选用的教育移动应用，不得要求学生使用。中小学学习类教育移动应用应当落实教育行政部门和学校的“双审核”制度；各省级教育行政部门可根据地方实际结合推荐制度简化审核流程。

（十一）规范进校合作。教育行政部门和学校应当规范教育移动应用的进校管理。作为教学、管理工具要求统一使用的教育移动应用，不得向学生及家长收取任何费用，不得植入商业广告和游戏。推荐使用的教育移动应用应当遵循自愿原则，不得与教学管理行为绑定，不得与学分、成绩和评优挂钩。对于承担招生录取、考试报名、成绩查询等重要业务的教育移动应用，原则上应当由教育行政部门和学校自行运行管理。确需选用第三方应用的，不得签订排他协议，或实际由单一应用垄

断业务。鼓励高校联合省级教育行政部门、招生考试机构、教育部“阳光高考”平台优化公共服务。

（十二）促进整合共享。教育行政部门和学校应当创新教育资源供给模式，探索通过国家数字教育资源公共服务体系，汇聚优质教育资源，集成各类应用，使网络学习空间成为教育移动应用的主要入口。面向师生提供管理和服务的教育移动应用应当整合为“互联互通、业务协同、信息共享”的综合性教育移动应用。鼓励教育移动应用将收集的机构、师生信息与国家基础数据库进行统一校验，并统一汇聚至国家教育基础数据库。

四、健全监管体系

（十三）加强行业规范。教育移动应用提供者应当自觉接受社会监督，设置便捷的投诉举报渠道，及时处理投诉。应用商店等移动应用分发平台提供者应当落实监督责任，健全资质核验、内容审核，配合进行适龄提示管理，并将教育业务备案作为上架应用商店的重要条件。鼓励移动终端提供者为家长监护提供技术支撑，提供未成年人监管功能。积极发挥行业协会的作用，制定行业公约，建立行业信用评价体系和服务评议制度，促进行业规范发展。

（十四）建立协同机制。建立多部门协同联动的监管机制。教育行政部门牵头负责教育移动应用治理工作，负责统筹协调，指导和监督学校落实主体责任，会同相关部门开展联合治理。网信部门、电信主管部门、公安部门依据职责重点做好教育移动应用提供者、应用商店等移动应用分发平台提供者、移动终端制造商的监管工作。新闻出版部门重点做好教材、教辅等网络出版物的监管工作。民政部门重点做好教育类民办非企业单位的登记管理工作。市场监管部门重点做好线上盈利性教育机构的登记管理，依法查处违规收费，虚假、违法广告等行为。公安部门重点做好打击整治相关违法犯罪活动。

（十五）拓展监督渠道。教育行政部门应当加强与有关职能部门、专业机构、行业协会和企业的合作，通过技术检测和人工查看相结合的方式，建立常态化的监测预警通报机制。通过家长委员会，满足家长对学校教学管理工作的知情权、评议权、参与权和监督权。引导家长履行监护责任，通过加强家庭交流互动、设置移动终端限制等方式，引导学生正确使用教育移动应用。教育行政部门应当全面掌握教育动态，及时受理投诉建议，主动回应社会关切，切实解决群众痛点难点问题。

（十六）加强考核问责。省级教育行政部门应当建立教育移动应用的选用退出机制、负面清单和黑名单制度，推动将黑名单信息纳入全国信用信息共享平台，按有关规定实施联合惩戒。教育督导部门应当将教育移动应用治理情况纳入对下级政府履行教育职责督导评估和对学校的综合督导评估。教育行政部门应当将教育移动应用治理纳入网络安全责任制等相关考核。对责任不落实、措施不到位的教育行政部门和学校予以约谈、通报。对因失职、渎职造成严重后果的，依法依规对相关负责人严肃问责。

五、加强支撑保障

（十七）加强组织领导。教育行政部门和学校应当将引导规范教育移动应用工作纳入重要议事日程，建立由教育行政部门牵头，宣传、“扫黄打非”、网信、电信、公安、民政、市场监管等部门共同参与的部门协同机制，制订工作方案，明确职责分工、时间节点、实施路径和保障措施。建立本地区的教育移动应用重点任务台账，统筹协调校外线上培训机构治理等重点工作，监督指导各项任务落实到位。

（十八）健全制度规范。教育行政部门应当完善教育移动应用的备案、推荐、选用、监督检查等制度，构建覆盖全生命周期的管理机制。健全教育移动应用评估、监测、检查、防护等技术规范，推进教育移动应用治理制度化、规范化、标准化。组织行业专家和相关企业共同完善教育移动应用的标准，规范程序开发、运行管理

等环节，提高教育移动应用的服务质量和保障水平。

（十九）提升信息素养。教育行政部门和学校应当组织管理和技术人员培训，将规范教育移动应用管理作为重要内容，切实提高管理水平和保障能力。同时，应当加强宣传引导和教育，以开学教育、网络安全宣传周等活动为契机，培养在校师生科学的使用习惯；通过家长会、家长学校、专题报告等形式，促进家长树立正确的用网观念，全方位地提高广大师生、家长的信息素养。

（二十）落实工作保障。教育行政部门应当加强对教育移动应用管理的经费支持，保障备案推荐、监测评估、监督检查等重点任务开展。教育行政部门和学校应当利用国家教育资源公共服务体系和国家教育管理公共服务平台为教育移动应用治理工作提供信息化支撑，探索“政府统筹引导、企业参与建设、学校购买服务”的教育移动应用供给机制，提供优质的教育资源和应用服务。[7]

[7] 中华人民共和国教育部。

3. 中国信通院发布《人工智能数据安全白皮书（2019 年）》

当前，数据作为驱动本轮人工智能浪潮全面兴起的关键要素，数据安全已成为人工智能安全的关键。与此同时，人工智能应用也为数据安全治理带来新机遇。如何应对人工智能场景下的数据安全风险并促进人工智能在数据安全领域中的应用，日渐成为人工智能安全治理的重要议题。

本白皮书从人工智能数据安全的内涵出发，首次提出人工智能数据安全的体系架构，内容包括人工智能数据安全概述、人工智能数据安全风险、人工智能数据安全应用、国内外人工智能数据安全治理动态、人工智能数据安全治理建议五大板块。在系统梳理人工智能数据安全风险和安全应用情况的基础上，总结了国内外人工智能数据安全治理现状，研究提出了我国人工智能数据安全治理建议。[8]

[8] 中国信通院，《人工智能数据安全白皮书（2019 年）》

4. 2019 年国家网络安全宣传周在天津举办

2019 年的国家网络安全宣传周将于 9 月 16 日-22 日举行。

这已经是连续举办的第五届，主题是“网络安全为人民，网络安全靠人民”。作为一个网络大国，我国的网络安全也成了一个大问题。层出不穷的病毒、防不胜防的黑客，盗取数据、破坏电脑，给个人带来麻烦，让企业遭受损失，也对国家安全构成了极大的威胁。“没有网络安全就没有国家安全”，习近平总书记的论断，为网络安全各项工作提供了根本遵循。党的十八大以来，在习近平总书记关于网络强国的重要思想指引下，网络安全保障能力和水平不断提升。

自 2014 年起，由中央网信办牵头，联合中央宣传部、教育部、工业和信息化部、公安部、人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等十部门，共同主办国家网络安全宣传周，开展网络安全进进社区、进农村、进企业、进机关、进校园、进军营、进家庭等活动，以 2018 年国家网络安全宣传周为例，线下直接参与人数达到了 1.7 亿人，发放宣传材料 3700 万份，发送公益短信 10 亿余条。

安全是发展的前提，发展是安全的保障。众多业内人士指出，虽然网络安全领域，成就明显，但安全与发展要同步推进，网络安全是动态而不是静态的，随着 5G、人工智能等信息技术的快速发展，网络安全领域会面临着更多、更新、更复杂的挑战，网络安全事业依然任重道远。[9]

[9] 网信中国。

三、相关案例

1. 荷兰 DPA 称某知名电脑操作系统远程收集用户数据，或违反隐私法

据路透社报道，荷兰数据保护局（DPA）今日表示，某知名电脑操作系统远程收集操作系统家庭版和专业版用户的数据，这可能违反了荷兰的隐私保护法。

事实上，荷兰 DPA 早在 2017 年 10 月就曾表示，该操作系统违反了该国的数据保护法。在使用默认设置时，销售该操作系统的公司不断收集有关应用程序的使用记录。

荷兰 DPA 表示，虽然销售该操作系统的公司按照要求在去年对相关设置进行了而调整。但在测试这些调整后的隐私保护措施时，又发现了新的问题。

荷兰 DPA 称：“测试发现，销售该操作系统的公司还远程收集用户的其他信息。因此，销售该操作系统的公司还是潜在地违反了隐私保护法。”

荷兰 DPA 还表示，已将这一发现转交给爱尔兰数据保护机构，因为销售该操作系统的公司在爱尔兰设有欧洲总部。

销售该操作系统的公司对此表示，公司始终致力于保护用户隐私。最近几年，销售该操作系统的公司已针对个人和小企业用户对该操作系统的隐私功能进行了改进。

销售该操作系统的公司说：“有机会进一步改进我们为用户提供的工具和选择，我们也很高兴。”

早在2017年1月，瑞士数据保护机构“瑞士联邦数据保护与信息委员会”曾表示，经调查发现，该操作系统因自动上传用户隐私信息而违反了瑞士的数据保护法。[10]

[10] 新浪科技。

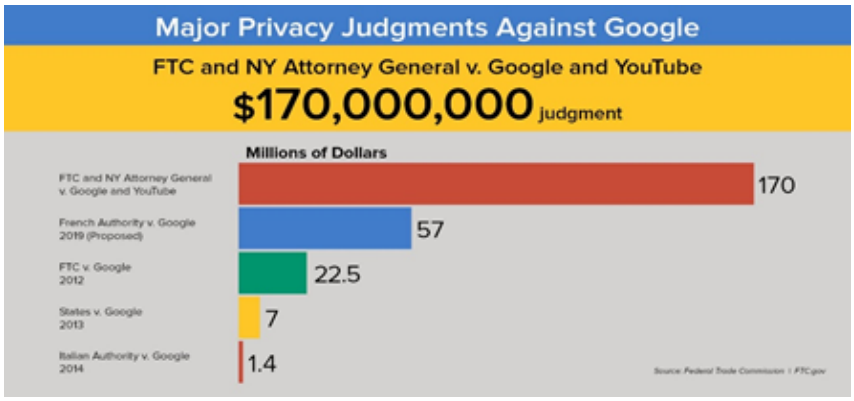
2. FTC 官方报道：谷歌和 YouTube 因涉嫌违反 COPPA 支付 1.7 亿美元

9 月 4 日美国联邦贸易委员会（FTC）网站上正式发出和解声明，大概一周时间。FTC 的官方报道中文翻译请见下文。

案件概述

Google 及其子公司 YouTube 将支付 1.7 亿美元以和解联邦贸易委员会（FTC）和纽约总检察长关于 YouTube 视频共享服务未经父母同意非法收集儿童个人信息的指控。

该和解要求谷歌和 YouTube 向 FTC 支付 1.36 亿美元，并向纽约州支付 3400 万美元，因其涉嫌违反儿童在线隐私保护法案（COPPA）的规则。自国会于 1998 年颁布法律以来，1.36 亿美元的罚金是目前美国联邦贸易委员会在 COPPA 案件中处以的最高的罚金数额。



（图片来自 FTC: Google and YouTube Will Pay Record $170 million for Alleged Violations of Children's Privacy Law）

在针对这些公司的指控中，美国联邦贸易委员会和纽约总检察长指控 YouTube 违反了 COPPA 规则，通过用于跟踪互联网用户的永久性标识符形式收集儿童频道观众的个人信息，且没有预先通知父母并征得他们的同意。根据指控，YouTube 通过使用通常称为 cookies 的标识符向这些频道的观众提供有针对性的广告，从而赚取了数百万美元。

COPPA 规则要求针对儿童受众的网站和在线服务当收集 13 岁以下儿童的个人信息前，告知其信息被收集和使用的情况并获得其父母的同意，包括为了向用户推送个性化广告而使用永久性标识符技术来追踪其用户的互联网浏览习惯。此外，广告提供方等第三方，在有意识地直接从以儿童受众的网站和在线服务中收集个人信息时，也应受到 COPPA 的约束。

FTC 主席 JoeSimons 说："YouTube 向其企业用户宣扬其在儿童用户中的受欢迎程度，但当涉及到遵守 COPPA 规则时，该公司却拒绝承认其平台的部分内容明确针对儿童用户。YouTube 违反法律是没有理由和借口的。"

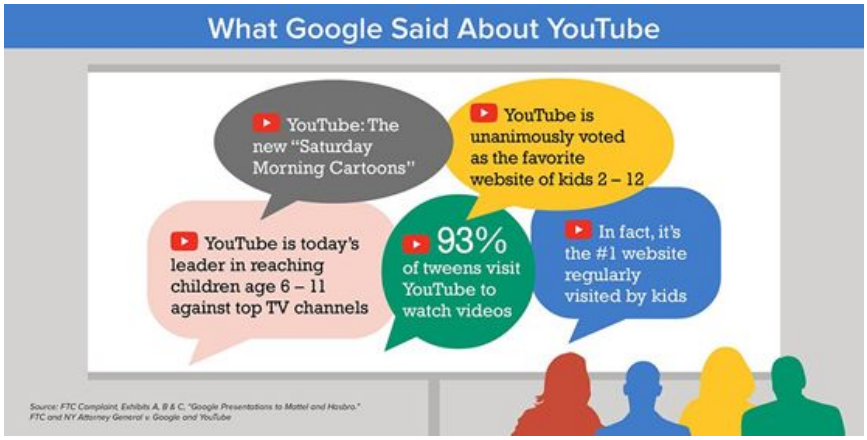
YouTube 平台允许 Google 账户持有者（包括大型商业实体）创建"频道"（channels）来展示其内容。根据指控，符合条件的频道所有者（channelowners）可以选择允许 YouTube 向用户投放针对其浏览行为的广告，从而为频道所有者和 YouTube 带来收入。

在指控中，美国联邦贸易委员会和纽约总检察长声称，虽然 YouTube 声称其网站针对一般受众和用户，但 YouTube 的一些个人频道（例如由玩具公司经营的频道），都是针对儿童用户的，因此必须遵守 COPPA。

该指控指出，YouTube 平台知道自己有许多针对儿童受众的频道。YouTube 在为热门儿童产品和品牌制造商进行的推广演示中，将自己打造成儿童广告投放的

首选。例如，谷歌和 YouTube 告诉芭比娃娃和 MonsterHigh 玩具制造商 Mattel，“在接触 6-11 岁儿童的受众上，YouTube 是当今能与顶级电视频道抗衡的引领者”，并告诉 Hasbro（MyLittle Pony 和 Play-Doh 的制造商），“YouTube 是孩子们定期访问网站的第一名”。

部分频道所有者会告诉 YouTube 和 Google，他们频道的内容是专门针对儿童的，但在其他情况下，YouTube 自己的内容评级系统会自行识别频道内容是否是专门针对儿童的。此外，根据指控，YouTube 会人工审核其 YouTube 平台上的儿童内容，并将其归入 YouTube 儿童版 App（YoutubeKids）的功能。尽管 YouTube 是知悉其平台上有专门针对儿童的频道，但 YouTube 仍在这些频道上投放了个性化广告。根据指控，它甚至告诉一家广告公司，它的平台上没有 13 岁以下的用户，因此其平台上的频道不需要遵守 COPPA。



（图片来自 FTC: Google and YouTube Will Pay Record $170 million for Alleged Violations of Children's Privacy Law)

与 FTC 达成和解

除了罚款之外，拟达成的和解还要求 Google 和 YouTube 开发、实施和维护一套系统，该系统内允许频道所有者识别他们在 YouTube 平台上投放的专门针对儿童的内容，以便 YouTube 确保它符合 COPPA 的规定。此外，Youtube 必须通知频道所有者他们所投放的专门针对儿童的内容可能受 COPPA 规则的约束，并为服务于 YouTube 频道所有者的员工提供有关遵守 COPPA 规则的年度培训。

和解还禁止谷歌和 YouTube 违反 COPPA 规则，并要求他们在收集儿童个人信息前，告知将会收集哪些个人信息并获得可验证的父母的同意。

FTC 以 3-2 投票批准了指控并且约定将其提交终审裁定。Simons 主席和 ChristineS. Wilson 委员就此事发表联合声明，而 NoahJoshua Phillips、RohitChopra 和 Rebecca Kelly Slaughter 委员则分别发表了声明。

指控和拟议的和解令已提交至美国哥伦比亚特区地方法院。（注：FTC“有理由相信”法律已经或正在被违反，并且 FTC 认为程序符合公共利益。）在地区法院法官批准和签署后，和解令具有法律效力。

FTC 感谢乔治城大学公共代表研究所所代表的消费者团体联盟，该组织提交了一份请求，对此事件提供了宝贵信息。[11]

[11] 作者：孟洁律师团队，与 FTC 和解已正式达成：谷歌和 YouTube 因涉嫌违反 COPPA 支付 1.7 亿美元。

3. HiQ 诉 LinkedIn 案二审宣判：抓取公开数据合法

案件概述

2019 年 9 月 9 日，美国第九巡回上诉法院公布了 HiQ 诉 LinkedIn 一案二审判决，认定自动抓取可公开访问的数据不违反《计算机欺诈和滥用法案》（CFAA）。

对许多研究人员、记者和公司而言，该判决免除了出版商反对访问公开信息可能带来的巨大法律风险。这是对 CFAA 适用范围的一个重要限定，为美国法院和国会进一步遏制滥用 CFAA 铺平道路。

CFAA 适用中存在的问题

CFAA 是 1986 年在联邦层面制定的反黑客法，对任何访问连接到互联网的计算机“未经授权”或“超出授权访问权限”的人可以施加刑事和民事责任。然而法案没有定义“没有授权”，如何在互联网背景下解释其含义是众所周知的难题。HiQ 案件只是关于 CFAA 的一系列备受瞩目的第九巡回法院判决中的最新案例，其中上诉法院经常在将 CFAA“限制在其最初目的”和“采用更广泛的解释”之间摇摆不定，这些解释可能会使广泛存在且无害的在线行为成为犯罪行为。

美国许多早期案例中的一个关键问题是公司和网站是否可以通过 CFAA 的未授权访问概念来执行其计算机使用政策，如服务条款或公司计算机政策。2012 年，第九巡回法院在美国诉诺萨尔案中作出了一项强有力的判决，法院拒绝将 CFAA 解释成一项全面的互联网监管任务清单，并把 CFAA 的重点聚焦于黑客攻击，“认为违反公司或网站的使用条款不能引起法律责任。否则，任何使用互联网的人几乎都会面临刑事责任，例如违反社交媒体网站的服务条款，甚至禁止谎言用户档案。

可惜的是，第九巡回法庭在后来的两个判决中混淆了自己确定的规则，即诺萨尔案和 Facebook 诉 Power Ventures 案。在诺萨尔案中，法院认为“未经授权”不仅限于规避技术访问机制（如密码障碍），并得出结论认为：使用其他人的有效登录凭据可能违反了法案。然后，在 Power Ventures 案中，法院作出判决：一个数据聚合器在获得用户同意的情况下，有权使用用户的密码访问 Facebook 帐户，但一旦 Facebook 发出停止和终止信件并阻止了 Power Ventures 的地址之后，如果该数据聚合器继续爬取数据时，则违反了 CFAA。

HiQ 和 LinkedIn 之间的争议

第九巡回法院在 Nosal II 案和 Power Ventures 案中的错误判决导致后续法院在进行判决时进一步滥用 CFAA。HiQ 的业务模式涉及利用公开的 LinkedIn 数据来创建企业分析工具，以确定员工何时可以离开另一家公司，或者公司应该为员工进行哪些培训。也许是因为它打算开发自己的产品以与 HiQ 竞争，LinkedIn 发出了停止信函，声称它将实施技术措施以阻止 HiQ 访问该网站并依赖 Power Ventures 案进一步争辩访问此公开信息将违反 CFAA。HiQ 主动提起诉讼，并在加州地方法院获得初步禁令，初步认为自动获取公开信息可能并不违反 CFAA 。

一审裁定

2017 年，一审法院作出裁定，认定基于反不正当竞争法（UCL）和联邦计算机欺诈与滥用法案（CFAA），原告 HiQ 已提出足够重要的实体法问题；基于公共利益的考量，法院将颁发预先禁令。禁令内容如下：

“1. 被告 LinkedIn 公司及其职员、代理人、雇员和律师禁止采取以下行为：

(1) 阻止 HiQ 访问、复制或使用 LinkedIn 网站的公开数据信息 (也就是

LinkedIn 会员设定的公开数据信息，即不仅对 LinkedIn 会员，而且对他人，包括那些可能通过谷歌、必应、其他服务器或直接链接访问 LinkedIn 网站的人，也可见的数据信息)；（2）屏蔽或设置任何法律或技术障碍阻止 HiQ 访问这些成员的公开资料的障碍。如果 LinkedIn 已经实施了防止 HiQ 访问这些公共数据信息的技术，在本裁定下达 24 小时之内必须移除。

2. 被告 LinkedIn 公司及其律师、代理人、雇员和律师应撤回 2017 年 5 月 23 日和 2017 年 6 月 24 日向 HiQ 送达的禁止通知函，并不得再以本禁令有效期内规定的原因为由，向 HiQ 发出进一步的禁止通知函。

3. 该禁令立即生效。

4. 该禁令无需任何担保，因为被告未证明其可能会因此禁令遭受任何损害。”

一审裁决作出后，LinkedIn 提出了上诉。

二审辩论及判决要点

在上诉中，EFF、搜索引擎 DuckDuckGo 和互联网档案馆一起提交了一份“法庭之友”文件，敦促法院承认爬虫是一种常见的技术手段，应当支持公益研究以及其他有益用途。既然人工誊写是合法合理的，那么作为一个技术问题，网页抓取只是机器自动化的网页浏览、访问和记录相同的信息，这有什么实质差别呢？

2019 年 9 月 9 日，美国第九巡回上诉法院对“HiQ 诉 LinkedIn 案”做出判决，认定 HiQ 公司从 LinkedIn 上抓取公开的个人信息数据的行为并未违反《计算机欺诈和滥用法案》，维持一审法院做出的对 HiQ 公司有利的裁决。[12]

[12] 数据法盟。

4. 国内某知名大数据公司涉嫌侵犯公民个人信息被查

9 月 6 日，推特网友 TonyStark 爆料称，杭州西湖分局集结 200 余名警力，对涉嫌侵犯公民个人信息的国内某知名大数据公司进行统一抓捕。截止目前抓获涉案人员 120 余名，冻结资金 2300 余万元，勘验固定服务器 1000 余台，扣押电脑 100 多台，手机 200 余部。案件正在进一步侦办中。

随后，杭州市公安局西湖区分局向 21 世纪经济报道记者证实，该公司的相关人员已经被经侦大队带走调查。据报道，多位业内人士认为，该公司被查可能是爬虫催收类业务出现了问题。

公开资料显示，该公司成立于 2016 年，总部位于杭州，在北京、广州、深圳设有分支机构，是国内专业的大数据智能风控服务供应商

据官网介绍，该公司凭借不断更新的用户授权数据和数亿级数据调用，结合机器学习和精准模型服务，为 2000 多家银行、保险机构、消费金融、互联网金融客户提供风险分析、反欺诈、多维度用户画像、授信评分等金融全生命周期风险管理服务。

不过，早在 2017 年，该公司就疑似被曝出开发使用恶意爬虫。金融科技类自媒体“一本财经”曾撰文称，当时现金贷行业流行一个“风控奇招”——用一款被称为“同业爬虫”的产品，直接将其他现金贷平台的放款额和风控数据扒出来，相当于别家替你做了风控。

该公司工作人员介绍，只需提供其他现金贷平台的用户名和密码，同业爬虫就可以爬取用户的基本信息、银行卡信息、职业、联系人、贷款记录、理财信息等，成功率在 85%以上。

此外，该公司还开发了支付类爬虫、社交平台爬虫等产品。比如某支付类爬虫只需要扫描一下登录“二维码”，后台就可爬取用户的真实姓名、手机号、收货地址、近一年的购物信息，甚至详细到每笔交易的金额。而社交平台爬虫则可以获取用户关注的账号、交易记录等信息。

该事件爆发后，据 21 世纪经济报道调查，一批大数据公司随之关闭了类似的爬虫服务。[13]

[13] 隐私护卫队

5. 国内热门 AI 换脸 App ZAO 回应被工信部约谈：将确保用户个人信息安全和数据安全

9 月 4 日，工信部表示，因国内热门 AI 换脸 App ZAO 用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工业和信息化部网络安全管理局对 ZAO 某一关联公司相关负责人进行了问询约谈。对此，ZAO 团队回应表示，将严格按照法律法规和各主管部门的要求，按照更加严格的标准，全面加强内容管理、完善各项管理机制，确保用户个人信息安全和数据安全。

表示将加强内容管理、完善管理机制

ZAO 表示，App 上线以来，我们和各主管部门保持着积极顺畅的沟通。非常感谢大家对于新技术新应用的关注，我们也在第一时间回应了大家的核心关切，将严格按照法律法规和各主管部门的要求，按照更加严格的标准，全面加强内容管理、完善各项管理机制，确保用户个人信息安全和数据安全。

工信部则表示，2019 年 9 月 3 日，针对媒体公开报道和用户曝光的 ZAO App 用户隐私协议不规范，存在数据泄露风险等网络数据安全问题，工业和信息化部网络安全管理局对 ZAO 某一关联公司相关负责人进行了问询约谈，要求其严格按照国家法律法规以及相关主管部门要求，组织开展自查整改，依法依规收集使用用户个人信息，规范协议条款，强化网络数据和用户个人信息安全保护。同时，要进一步加强新技术新业务安全评估，切实采取有效措施，积极防范自有业务平台被利用实施电信网络诈骗等风险隐患。工业和信息化部网络安全管理局将进一步加大工作力度，指导督促相关企业切实履行法律责任，认真做好网络数据和用户个人信息安全保护、行业电信网络诈骗防范治理等工作。

此前其用户协议引争议

此前，不少用户则更关注 ZAO 的隐私保护问题。用户注册时必须要提供的手机号码等信息，再加上人脸验证，让人很容易想到银行卡、支付宝等金融类 APP 才有的面部识别。再加上仔细看过该 App 的用户协议，不少用户的心里就更加打鼓。

ZAO 的用户协议中规定：“如果您把用户内容中的人脸换成您或其他人的脸，您同意或确保肖像权利人同意授予 ZAO 及其关联公司全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利，包括但不限于：人脸照片、图片、视频资料等肖像资料中所含的您或肖像权利人的肖像权，以及利用技术对您或肖像权利人的肖像进行形式改动。”另外，还规定“在您上传及/或发布用户内容以前，您同意或者确保实际权利人同意授予 ZAO 及其关联公司以及 ZAO 用户全球范围内完全免费、不可撤销、永久、可转授权和可再许可的权利，包括但不限于可以对用户内容进行全部或部分的修改与编辑……以及对修改前后的用户内容进行信息网络传播以及著作权人享有的全部著作财产权利及邻接权利。"

有用户质疑，“这是什么意思？是说我只要上传了照片，你们就可以拿我的照片和视频去做任何事了吗？而且还可以随意修改？”

目前，该协议已经被修改，不过核心与此前的并无二致。“在您上传及/或发布用户内容时，您同意或者确保实际权利人已经同意授予 ZAO 及 ZAO 用户全球范围内免费的、可以对用户内容进行部分的修改或编辑（如将短视频中的人脸换成另一个人的人脸等）以及对修改或编辑前后的用户内容进行信息网络传播的权利；在您使用 ZAO 提供的技术服务在 ZAO 内把用户内容中的人脸换成您或其他人的脸时，您同意或确保肖像权利人已经同意授予 ZAO 使用 ZAO 的技术服务对您的或其他人的人脸进行处理，但仅为与用户内容合成为新的内容”。

“换脸”的玩法对于不少用户来说还比较新，不过，这一功能由于可能引发一些不良问题已经为业界所担忧。此前，在国外曾出现过，有网站利用“换脸”技术，将一些色情低俗视频的主角替换为国外的女明星，合成效果十分逼真，从而引发伦理争论，也影响到到普通人的生活。

知微数据的创始人&CEO 于霄表示，这类 App 的面部数据采集，不能等同于一般的公共区域视频监控、支付宝/银行的面部采集、一般的美颜软件。数据掌握在大还是小平台，是否将身份数据和面容数据打通，采集的粗糙或者精细，都直接决定的风险级别。目前的情形已经越来越危险，别说掌握在盈利为目的的小平台，即使是超级大平台这几年数据泄漏的案例层出不穷。

于霄认为，和密码不同，人脸、声纹等生物特征是无法改变不可再生，一旦被盗用，会产生极为可怕的社会后果。很多先进技术，早期并不是被一些良性积极的创新孵化成熟的，恰恰是具有暴利特征且监管防控缺失的犯罪产业有最大的应用热情，他们执行力奇高，为追逐暴利不择手段。这类数据基本可以说，一次泄漏，终身有效。

北京志霖律师事务所副主任、中国政法大学知识产权中心研究员赵占领认为，这一技术被滥用，或者是被那些不法之徒及有恶意的人使用，便等于打开了潘多拉的魔盒。以后，我们可能会有更多机会看到某个公众人物“出演”的色情电影、某个官员“发表”敏感言论的视频、某个企业家“从事”违法犯罪行为的画面……诸如此类的视频可能不断突破公众的想象力。而令人担忧的是，这些视频一经传播，短时间内会带来极大的震撼，给相关受害人造成的伤害也将迅速扩大，造成的社会影响有时又来不及迅速消除。

他表示，技术本身是中立的。因此，如何关上 AI 技术打开的潘多拉魔盒，关键不在于禁止新技术，不是因噎废食，而是要对滥用技术从事的违法犯罪行为进行

规制。同时，应该通过更多的手段让民众知晓这种行为带来的危害性和严重性，使这种技术得到善用。同时让民众更重视自己的隐私保护，让一些好事之徒没有可乘之机。[14]

[14] 北京青年报。

6. 17 万"人脸数据"公开售卖被下架当事人对此一无所知

近日，在网络商城中有商家公开售卖“人脸数据”，数量达 17 万条。网络商城运营方已认定涉事商家违规，涉事商品已被下架处理。

网售人脸数据，每个人有多张照片

在商家发布的商品信息中可以看到，这些“人脸数据”涵盖 2000 人的肖像，每个人约有 50 到 100 张照片。此外，每张照片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。

此外，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。商家在商品说明中称，数据中并不提供所涉及人物的人名和身份证号等信息，也不得用于违法用途。

商家称，其售卖的人脸样本中，一部分是从搜索引擎上抓取的，另一部分来自境外一家软件公司的数据库等。该商家称，从发售至今，他已多次卖出这些数据。其表示，自己平时从事人工智能的相关工作，因此收集了很多人脸数据，发售出来“也就是挣个饭钱”。

该商家售卖的数据包中确实包括 2000 个文件夹，每个文件夹里都有数十张照片和相应的数据文件。一些照片属于知名演艺界人士，也有一部分照片来自医生、教师等市民群体，还有部分照片为未成年人。然而，对于这些数据，当事人对此一无所知。

认定商家违规，网络商城运营方予以下架

北青报记者就网售的人脸数据情况向网络商城平台运营方进行了举报，经运营方核实，确认该商家销售的人脸数据不符合平台的销售规则，平台运营方称将立即进行相应的处理。截至 9 日下午，该商品已被下架。[15]

[15] 北京青年报。

7. 国内某快递公司管理不严，导致个人信息全部泄露

近日，有多名受害者透露自己经常收到一些货到付款的快递，一般金额都为一百元至一百五十元不等，在他们把钱交上去的那一刻，就已经被骗了，包裹内可能仅仅是一个几块钱的 led 太阳能灯。

揽件的快递员透露：这件事还和国内某一较为知名的快递有关系，是因为郑州某电商公司有一批货物实在卖不出去，就动起了歪脑筋，联系了当地该快递物流公司某营业部老板开始“行动”，他们利用公司里面的全部资源开始大面积发快递，并且开始全网进行“99 元货到付款”等手段进行诈骗，而他们的想法就是利用被害人贪便宜、马虎大意等心理进行敲诈。

通过仔细调查发现，除该营业部老板以外，其他多个区域经理为了自己营业部的发货量，也与其公司进行了勾结，将全国使用过该快递的用户信息都纳入囊中，累计发货案值已经超出了 1200 万，并且共有五万多条公民个人信息被泄露。

目前此案涉及的所有犯罪分子都已经被缉拿归案，其中包含 6 名快递员，而他们也因为涉嫌侵犯公民个人信息罪和诈骗罪被刑事拘留。[16]

[16] 商业侦查眼。

8. 人脸识别已进校园 数据立法还有多远

9 月开学季，许多高校在新生报到期间都引进了人脸识别系统，新生到校不再需要复杂的报到流程，只要通过人脸识别系统便可以轻松完成报到。同时，为方便考勤，在上课的教室内，学校也安装了人脸识别系统。但人工智能的功能远不止于此。据了解，通过人脸识别系统，上课期间学生发呆、玩手机等行为都可以被感知。此事引发了舆论的广泛争议，一些网友称此举有侵犯学生隐私和尊严之嫌。

对此，9 月 5 日，教育部科学技术司司长雷朝滋在接受采访时说，人脸识别进校园，既有数据安全也有个人隐私问题，“教育部已经开始关注这个事情，正组织专家论证研究。对学生的个人信息要非常谨慎，能不采集就不采，能少采集就少采集”。[17]

[17] 法制网。

9. 实测 30 款儿童 APP：9 款存隐私规范瑕疵

一、13 款儿童 APP 索取位置权限，快乐小鸡、小盒学生强制索权

9 月 3 日至 9 月 8 日，记者经测试 30 款儿童 APP 发现，有 2 个 APP 涉及强制授权，6 个无隐私协议，2 个有隐私协议但没有监护人授权。由于有的 APP 同时存在两个问题，最终一共有 9 款 APP 在隐私规范上存在瑕疵。

在强制授权上，绝大多数儿童 APP 均能做到对收集的信息进行明示提醒并给用户提供可拒绝选项。如宝宝玩英语索取相机和录音权限，被拒绝后提示“需要这些权限才能让程序正常运行”，少儿趣配音在文件访问权限被拒绝后提示“拒绝将会导致 APP 无法正常使用”，不过上述 APP 在拒绝授予权限后，仍可打开。

从 APP 要求索取的权限来看，30 款儿童 APP 中有 13 款索取了地理位置权限，地理位置是儿童 APP 最爱收集的涉敏感权限。快乐小鸡在安装之时就索取了储存与地理位置权限，用户若选择拒绝就无法安装。而小盒学生则在安装之后首次打开时提示索取存储、位置、电话、拍照、麦克风权限，若拒绝就无法使用。对比来看，小盒学生有较为完善的隐私协议并要求填写“你或者爸爸妈妈的手机号”，快乐小鸡则较为简单，没有隐私协议。

根据 APP 专项治理工作组发布的《APP 申请安卓系统权限机制分析与建议》，APP 不应采用“一揽子打包”“默认打开”“强制捆绑”“私自更改”“频繁打扰”等方式征得用户同意获取权限，如“在 APP 安装时一次性申请多项或所有危险权限的授权，并在打开 APP 后权限均为默认开启状态”。

需要注意的是，根据《网络安全法》第四十一条规定，网络运营者不得收集与其提供的服务无关的个人信息。但对于儿童类 APP 中何种信息属于“与其提供的服

务无关”，目前尚未有明确的标准出台。此前，全国信息安全标准化技术委员会曾发布《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》，依据个人信息收集最少够用的原则以及不同种类 APP 的业务范围，对地图导航、网上购物、餐饮外卖等 16 类 APP 收集个人信息的范围给出了参考，但目前尚无针对儿童 APP 的明确标准。

二、6 款儿童 APP 无隐私协议，8 款未设置监护人同意选项

《儿童个人信息网络保护规定》强调，APP 在收集、使用、转移、披露儿童个人信息时，应当征得儿童监护人的同意。目前，在测试中，共有 8 款 APP 在隐私条款或运行界面中没有监护人同意的设置。

其中，有 6 款 APP 直接没有隐私条款的设置，包括可可宝贝、人教版小学英语、宝宝爱连线、小企鹅乐园、快乐小鸡、DIY 史莱姆制造者。其中，人教版小学英语或为配合教程使用的辅助 APP，而宝宝爱连线、DIY 史莱姆制造者等为功能较为单一的游戏类 APP，不过可可宝贝获取了电话、照片等敏感权限，却没有隐私条款，存在的隐私规范瑕疵较大。

此外，少儿趣配音与晓黑板 2 款 APP 虽然具备隐私政策，但没有监护人授权的选项。因此共有 8 款儿童 APP 没有“征得监护人同意”的设置。

测试的 30 款儿童 APP 中，监护人同意的表述大部分都写在隐私协议中，如宝宝玩英语在其隐私政策中表示，“若您是 18 周岁以下的未成年人，请在您的父母或监护人的指导下仔细阅读本《隐私政策》，并在征得您的父母或监护人同意的前提下提交您的个人信息。”而少数 APP 具备家长设置儿童使用时间，以及通过算术题验证的方式验证家长身份等。

对于儿童类 APP“监护人同意”选项的设置方式，早教类 APP 从业者表示，在实际操作中，“征得监护人同意”的规定“较为死板”，“一般小孩子玩的 APP 都是家长给下载好的，手机也是家长的，再在 APP 里写一则隐私协议并标注‘监护人同意’也就是为了合规，即便写了，也怀疑家长会真正阅读。”她认为，一些规则较为简单的儿童游戏 APP 的界面设计“非常简单，并不收集儿童信息，但再强行放置一个隐私协议或家长需知，有些没有必要，通过做算术题或者填成语的方式验证家长身份比在隐私协议中标明家长需知更加能确保 APP 收集信息的行为真正被监护人而不是儿童知晓。”

三、综合类 APP 保护儿童信息陷困境

目前，对 APP 用户年龄最精确的统计方式是直接统计 APP 注册用户的年龄信息，但多个专家表示，对于儿童，这种方法无法做到。

实际上，绝大多数 APP 都不可避免的有儿童用户，此时如何判断用户为儿童是一大难点。“例如我们可以统计手机注册用户的年龄，但 14 岁以下的儿童基本没有手机，都是使用大人的，此时 APP 也不知道对方的真实身份，因此难以统计。”

四、收集儿童信息以判断儿童身份或增加问题

2017 年发布的《未成年人网络保护条例（送审稿）》第二十二条规定，网络信息服务提供者提供网络游戏服务的，应当要求网络游戏用户提供真实身份信息进行注册，有效识别未成年人用户，并妥善保存用户注册信息。国家鼓励网络游戏服务提供者根据国家有关规定和标准开发网络游戏产品年龄认证和识别系统软件。

我国未成年人网络保护立法政策的基础是身份识别，为了加强对未成年人的网络保护，首先强化了对其个人信息的收集，通过收集其各种信息以确认其是未成

年人，千方百计避免未成年人虚报年龄以逃避特殊保护。但在收集儿童信息方面，必须提出的问题是:这个收集信息的过程也许就成为侵害未成年人隐私权的过程，就埋下了未成年人隐私权受到严重侵害的风险。

在此次30款儿童APP测试中并未发现有游戏APP要求对儿童进行信息注册。目前，在实名注册方面做得较为完善的游戏 APP 包括王者荣耀、和平精英等，但这些 APP 的主要用户为成年人，而对于这批用户，腾讯采取一定的算法来进行识别，比如查看用户的游戏时长以及操作习惯等，对判断为未成年人的用户，也会采取相对应的措施。

不过，通过收集注册信息来判断儿童身份或许会带来负面影响。如 2011 年韩国国会通过了《未成年人保护法》，规定 0 点至 6 点之间，互联网游戏运营者不得向不满 16 周岁的未成年人提供互联网游戏服务。但根据韩国产业研究 2014 年的“文化产业全球竞争力提高方案”报告，推行游戏宵禁制度之后，青少年每日玩游戏的时间虽然减少了约 16 到 20 分钟，但这项制度也使 40%的青少年通过盗用身份证号码的方式玩游戏，从而导致他们可能更多地接触面向成人的游戏。另外未满 16 岁的未成年人需要监护人的同意才能注册游戏账号，因此游戏公司需花高额费用建构个人信息收集系统，用于收集监护人的个人信息。

目前未成年人网络保护问题上存在多重视角，政府希望通过推动立法、制定政策，不仅督促企业承担更多责任，也希望家长、学校发挥起有效作用；越来越多企业在承认自身要承担更多责任基础上，也希望政府、家长、学校要积极履责。因此对此问题，亟需多方共治。[18]

[18] 新京报。

四、环球解读

1. 针对隐私信息管理的国际标准 ISO/IEC 27701 的简要解读（三）

国际标准化组织（ISO）与国际电工委员会（IEC）发布 ISO/IEC27701，旨在明确建立、实施、维护和持续改进隐私信息管理系统（Privacy Information Management System, "PIMS"），并提供相关指南，为相关处理者和控制者提供了与 PIMS 相关的指导。本文将着力于讨论 ISO/IEC27701 在适用上与其他国家标准和各国国内立法上的兼容性，以为中国企业适用该标准时需注意的问题。

一、各国均有隐私保护立法，国际也有 ISO/IEC27001，为何还要制定 ISO/IEC27701？

ISO/IEC27701 出台前，ISO/IEC27001 作为国际上公认的信息安全管理体系标准，在隐私保护方面仅较为概括地提出了信息安全管理体系的基本要求。ISO/IEC27002 虽为组织内启动、实施、保持和改进信息安全管理的措施提供指南。但两部标准一方面未能区分从 PII 控制者和 PII 处理者二者不同的角度来实现和满足不同国家和地区的隐私保护法律法规的要求，另一方面每一项内容的讨论并不深入，并没有提供足够的操作指引。因此，新标准 ISO/IEC27701 隐私信息管理体系应势而生，助力企业为保护用户隐私和个人信息合规管理提供了更多相关指南。

对于需要在全球多国进行经营和数据合规的企业而言，ISO/IEC27701 进一步解决了两个问题：

1. 降低企业在全球多法域的合规实践难度和工作负担

各国数据保护法规种类繁多，企业面临的合规工作不仅繁琐，且负担较大。而 ISO/IEC27701 通过参考在世界范围内有较大影响力的欧洲《通用数据保护条例》

（General Data Protection Regulation，“GDPR”）对主要的隐私保护规则进行了有效整合并提供了较为详细的操作指南。具体而言，ISO/IEC27701 在附表 C 提供了 ISO/IEC 27701 和 GDPR 第 5 条至第 49 条的对应情况，并为作为 PII 控制者或 PII 处理者不同角色的企业提供了具有操作性、受国际认可的数据收集、处理的指南。尽管企业在各国进行数据合规时仍需要结合各国的数据保护法律法规，ISO/IEC27701 通过引入 PIMS 框架和对主要合规行为的具体指引，大大降低了企业的合规难度，试图采用一套标准适用于全球多法域的数据合规。

2. 帮助企业与共同控制者、处理者（第三方）建立法律纽带约束各方行为

不同于中国的数据保护法规仅规制了个人信息控制者的责任和义务，ISO/IEC27701 则是对 PII 控制者、PII 处理者的责任与义务均作出了详细规定，并要求各方之间构建合同纽带，约束双方对数据处理的行为。

具体而言，ISO/IEC27701 第 7.2.6 条要求 PII 控制者与任何代表 PII 控制者处理 PII 的处理者签订协议，确保协议中涉及 ISO/IEC 27701 中对 PII 处理者的相关要求，具体而言：

（1）PII 控制者应当根据安全风险评估的结果以及 PII 处理者处理 PII 的类别和体量，在合同中要求 PII 处理者实施附录 B 中规定的适当的控制措施。在默认情况下，附录 B 中规定的所有控制措施均应被视为“适当”。

（2）如果 PII 控制者决定不要求 PII 处理者实施附录 B 中的某项控制措施，

则应当提供合理理由。

ISO/IEC27701 第 7.2.7 则规定，PII 控制者应与任何 PII 共同控制者签订协议确定处理 PII（包括 PII 保护和安全要求）的各自角色和责任，包括：

（1）PII 共享的目的/PII 共同控制者关系；

（2）作为 PII 共同控制者关系一部分的组织（PII 控制者）的身份；

（3）根据协议共享和/或转让和处理的 PII 类别;

（4）处理操作概述（如转让、使用）；

（5）各自角色与职责的描述；

（6）实施 PII 保护的技术和组织安全措施的责任；

（7） PII 泄露时的责任确定（例如，谁将在何时互相通知信息）；

（8）PII 的保存和/或删除条款；

（9）未能遵守本协议的责任；

（10）如何履行对 PII 主体的义务；

（11）如何向 PII 主体提供包含 PII 共同控制者之间协议的核心内容的信息；

（12）PII 主体如何获得其有权接收的其他信息；以及

（13）为 PII 主体提供的联系方式。

通过加强 PII 控制者与 PII 共同控制者、PII 控制者与 PII 处理者的法律纽带，建立起较为全面的隐私保护体系，从而减轻或避免企业因第三方不当收集、处理个人信息而招致的损失。

3. 帮助企业的合规证明

随着越来越多的隐私保护立法的生效，企业面临的另一压力则是证明企业已进行了相关合规工作。ISO/IEC27701 在两方面对于企业合规的证明提供了帮助：

一是要求企业对 PII 收集、处理的全过程进行记录；

二是提供了认证服务，通过提供认证展示遵守相关的隐私要求。

具体而言，ISO/IEC27701 要求企业对 PII 收集、处理的全过程进行记录。根据第 7.2.8 条的规定，组织应当建立并维护 PII 处理记录，包括 PII 类别描述、PII 主体类别描述、收集、处理每一项信息的目的和方式、采取的去标识化等技术安全措施、委托处理、隐私影响评估报告等情况的详细记录，并维持记录的准确性，从而为企业证明自身合规保留客观证据。

此外，依据 ISO/IEC27701 介绍的内容，如满足 ISO/IEC27701 的要求，适用该标准的企业可以生成有关如何处理 PII 的书面证明，且可以要求 ISO 就相关证明进行独立认证，从而帮助企业提供合规证明，提高隐私合规的透明度。

二、ISO/IEC27701 是否与 ISO/IEC 的其他国际标准构成冲突？是否考虑了兼容性？

ISO/IEC27701 与 ISO/IEC27001 和 ISO/IEC27002 的关系可以通过以下图片简单展示：

如前所述，ISO/IEC27701 对于 ISO/IEC27001 和 ISO/IEC27002 的扩展体现在两个方面：

一是对于 ISO/IEC27001 和 ISO/IEC 27002 构建的 ISMS 提出更高的要求；

二是明确区分了 PII 控制者和 PII 处理者并对这两种不同的角色提出了特别的指南。ISO/IEC 27701 的 PIMS 并不是针对 ISMS 的推倒重建，而是对于现有的 ISMS 进行提升。故对于已经实施了 ISO/IEC27001 和 ISO/IEC27002 的 ISMS 的企业而言，则仅须对新规定的部分进行实践操作，即可实现 ISO/IEC 27701 规定的 PIMS 的要求。

三、ISO/IEC27701 是否与与各国隐私保护立法构成冲突？是否考虑了兼容性？

ISO/IEC27701 相较于以往的国际标准的亮点之一是在附表 C 给出了 ISO/IEC 27701 条文与 GDPR 的对应关系。例如：

1. ISO/IEC27701 第 5.4.1 条关于信息安全风险评估和信息安全风险处置对应 GDPR 第 32 条对于组织处理数据的安全要求。

2.ISO/IEC27701 第 6.6.2 条关于用户访问权限的规定对应 GDPR 第 5（1）（f）项关于数据处理过程中应采取措施避免数据未经授权被处理的规定。

但需要提示的是，附表一方面仅展示了 ISO/IEC27701 与 GDPR 的对应关系，对于其他国家法律的对应关系仍是空白；另一方面该附表没有涵盖所有的 GDPR 条款，ISO/IEC27701 对于儿童数据等作为特殊类型个人数据则没有规定。正如 ISO/IEC27701 在多个条文中多次强调的，企业在具体适用标准时，还需要结合并遵从各国国内立法进行解释和实践。

四、结论

ISO/IEC27701 作为 ISO/IEC27000 系列最新推出的标准，整体规范上侧重于框架上的构建，对于各国建构完善的隐私保护体系提供思路。一方面，是对原有 ISO/IEC27001/27002 的延伸规定，另一方面，又提出了新的合规指引。同时，对于世界主要立法均有规定的部分，进行了详细规定，可以减轻企业合规负担；但是，因各国文化、社会观等情况不同，需要“因地制宜”实施的部分例如特殊类型的数据，仅作概括或较少规定，留给各国细化的空间。正如 ISO/IEC27701 中反复提醒的，企业在某一国家进行数据合规时，仅仅按照 ISO/IEC27701 的要求构建 PIMS 或获得 ISO 认证，并不能保证该合规措施完全符合当地法律法规规定，企业仍需关注各国的立法动态，参照当地国家的法律法规和商业惯例确定具体的要求，比如对未成年人年龄的限制等，对合规工作进行相应地调整。[19]

[19] 作者：孟洁律师团队。

2. 《网络生态治理规定（征求意见稿）》要点评析

2019 年 1 月，国家互联网信息办公室（下称“网信办”）启动为期 6 个月的专项行动，对各类网站、移动客户端、论坛贴吧、即时通信工具、直播平台等重点环节中的淫秽色情、低俗庸俗、暴力血腥、恐怖惊悚、赌博诈骗、网络谣言、封建迷信、谩骂恶搞、威胁恐吓、标题党、仇恨煽动、传播不良生活方式和不良流行文化等 12 类负面有害信息进行整治，集中解决网络生态重点环节突出问题，意在促进网络生态空间更加清朗。

基于上述行动，2019 年 9 月 10 日（即昨日），网信办发布了《网络生态治理规定（征求意见稿）》（下称“《规定》”），并向社会公开征求意见。《规定》是我国第一部整治网络生态问题的专门性规定，体现了网信办在今年及以往网络生态专项整治行动[2]中积累的丰富经验，具有颇多亮点。下文就拟对《规定》中的要点问题进行简要评析。

一、多类别主体协同共治

根据《规定》第二条，本规定所称网络生态治理，是指政府、企业、社会、网民等主体，以网络信息内容为主要治理对象，以营造文明健康的良好生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。本条明确提出政府、企业、社会、网民等都是网络生态治理的主体，各自需要在网络生态治理中承担不同的责任。具体而言，《规定》第二至五章分别列举了网络信息内容生产者（如遵纪法律与公德）、网络信息内容服务平台（如审查信息内容）、网络信息内容使用者（如违规举报）以及网络行业组织（如行业准则）等在网络生态治理中应当承担的权利和义务。

此外，根据《规定》第三条，国家网信部门负责统筹协调网络生态治理和相关

监督管理工作。国家新闻出版部门和国务院教育、电信、公安、文化、市场监督管理、广播电视等有关主管部门依据各自职责做好网络生态治理工作。以上与专项整治行动中国家网信办负责人强调的“谁主管谁负责，谁主办谁负责”的原则[3]一脉相承，既充分发挥了多方主体积极参与、共同治理的优势，也强调了不同政府部门在网络生态治理方面共同具有监督管理的职责。

二、界定规制主体的具体类别

《规定》主要针对网络信息内容生产者、网络信息内容服务平台、网络信息内容服务使用者的行为进行了规制。

根据《规定》第四十一条，网络信息内容生产者是指制作网络信息内容的组织或者个人，即在网络上发布消息的组织或个人。网络信息内容服务平台是指提供信息内容复制、发布、传播等服务的网络信息服务提供者，例如微博、微信、抖音等互联网平台。网络信息内容服务使用者是指使用网络信息内容服务的组织或者个人，例如网络群组、论坛社区版块的建立者和管理者同样也属于网络信息内容使用者的范畴。

随着网络技术的发展，提供网络信息内容的平台、使用网络信息内容的主体都日益增多，生活中能够接触到网络的任何个人或组织通过接发消息都可能成为网络服务的生产者或使用者。《规定》警示我们在提供或使用网络信息内容时，需始终注意遵守行为规范，维护网络生态的清明有序。

三、治理对象主要包括违法信息与不良信息

《规定》第六、七、十一、十二、二十二条等大量条款规定，网络信息生产者、网络信息内容服务平台、网络信息内容服务使用者在各自义务范围内，都不得从事

与违法信息、不良信息相关的行为。除了规定利用互联网制作、复制、发布、传播诸如违背宪法、危害国家安全等信息构成违法行为外，《规定》第七条还特别对构成“不良信息”的类型进行了说明，其所列举的每一项都是对生活中典型乱象的回应。

《规定》第六条 网络信息生产者禁止制作含有下列内容的违法信息：

（一）违反宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损害国家荣誉和利益的；

（四）歪曲、丑化、亵渎、否定英雄烈士及其事迹和精神的；

（五）宣扬恐怖主义、极端主义，煽动民族仇恨、民族歧视，破坏民族团结的；

（六）破坏国家宗教政策，宣扬邪教和封建迷信的；

（七）散布虚假信息，扰乱经济秩序和社会秩序的；

（八）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（九）侮辱或者诽谤他人，侵害他人名誉、隐私和其他合法权益的；

（十）含有法律、行政法规禁止的其他内容的。

《规定》第七条 网络信息生产者不得制作含有下列内容的不良信息：

（一）带有性暗示、性挑逗、性诱惑的；

（二）展现血腥、惊悚等致人身心不适的；

（三）宣扬炫富拜金、奢靡腐化等生活方式的；

（四）过度炒作明星绯闻、娱乐八卦的；

（五）使用粗俗语言、展示恶俗行为、宣扬低俗内容的；

（六）调侃恶搞自然灾害、重大事故等灾难的；

（七）煽动人群歧视、地域歧视等的；

（八）使用夸张标题，内容与标题严重不符的；

（九）对未成年人身心健康造成不良影响的；

（十）其他含有危害社会公德等破坏网络生态内容的。

例如，规定第七条第（一）项“带有性暗示、性挑逗、性诱惑的”是对色情、低俗的主播/直播等现象的规制；第（二）项“展现血腥、惊悚等致人身心不适的”则是呼应了 2019 年 8 月发生的某明星直播割手指的事件；第（三）项“宣扬炫富拜金、奢靡腐化等生活方式的”针对的是用户在微商、社交网络等宣传“一夜暴富”“喜提 XX”等炫富行为；第（六）项“调侃恶搞自然灾害、重大事故等灾难”则是针对国内发生自然灾害时某些用户在社交网络中造谣干扰试听的现象等等，体现了网信办对于社会热点的密切关注以及整治乱象的力度与决心。

此外，违法行为诸如恶意泄露热点新闻当事人/明星艺人个人隐私、人肉搜索、散布谣言以及前段时间引起热议的“流量造假”等网络侵权、网络暴力行为，也都将受到《规定》的规制。

四、进一步强调未成年人保护义务

根据《规定》第十三条，网络信息内容服务平台应当加强以人工编辑、机器算法等方式推荐、呈现信息环节的管理，营造积极健康的版（页）面生态。包括但不限于以下重点环节：（十二）以未成年人为服务对象的网络信息内容服务。该条款进一步强调针对向未成年人提供网络信息内容服务应该健康、积极、正面。

值得注意的是，根据《规定》第十四条，（本规定）鼓励网络信息内容服务平台开发适合未成年人使用的模式。 网络信息内容服务平台提供网络游戏、网络文学、网络动漫、网络直播、网络音视频及其他各类服务时，应当采取措施防止未成年人接触违法和不良信息。半个月前，网信办刚刚正式发布《儿童个人信息网络保护规定》，体现了对儿童权益的重点特别保护，9 月 10 日推出的《规定》在此基础上进一步具体指出，鼓励网络信息内容服务平台开发适合未成年人使用的模式（如儿童版/青少年版等），对网络信息内容提供者在儿童或未成年人保护方面提出更明确要求，体现了国家对于儿童或未成年人健康、安全使用网络服务的持续关注和保护力度。

五、强调网络信息内容服务平台的个人信息保护义务

根据《规定》第十五条，网络信息内容服务平台采用个性化算法推荐技术推送信息的，应当建立体现主流价值导向的推荐模型，建立健全人工干预机制，建立用户自主选择机制。这也是与今年五月份出台的《数据安全管理办法（征求意见稿）》的精神一脉相承。

第十八条进一步提示网络信息内容服务平台应当在首页、账号页面、信息内容页面等显著位置设置便捷的投诉举报入口，公布投诉举报方式，细化网络生态违法和不良信息举报分类，及时受理处置公众投诉举报并反馈处理结果。

个性化推送、用户投诉举报等制度在《信息安全技术 个人信息安全规范（征求意见稿）》（2019.6.21）及其他法规中均有体现，这反映出在网络生态中的个人信息保护领域，《规定》与我国个人信息保护的法律体系相适应。

第十七条强调网络信息内容服务平台应当完善用户服务协议，明确用户相关权利义务，并依法依约履行相应管理职责。值得注意的是，虽然制定用户服务协议已是实践中常见合规措施，但在法规中明确要求网络信息内容服务平台向用户提供用户服务协议并进行签署的尚属首次。这与个人信息保护法律法规方面要求制定单独成文的隐私政策，正好构成相互呼应。

第二十五条规定网络信息内容服务使用者不应通过人力或者技术手段实施流量造假、流量劫持以及虚假注册账号、批量买卖账号、操纵用户账号等行为。第十七条第二款规定网络信息内容服务平台应当在平台内部建立用户账号信用档案，依据账号的信用等级提供相应服务。我们理解，如果网络信息内容服务使用者有第二十五条禁止的行为，网络信息内容服务平台可以通过对其提供分级服务，中止、终止提供服务等方式予以处罚，这些都可以在用户服务协议中与用户进行约定。

六、首次提出“网络生态治理负责人”和“网络生态治理工作年度报告”

根据《规定》第九条，网络信息内容服务平台应当设立网络生态治理负责人，配备与服务规模相适应的工作人员，并加强教育培训；第十九条，网络信息内容服务平台应当编制网络生态治理工作年度报告，包括网络生态治理工作情况、网络生态治理负责人履职情况、社会评价情况等内容。

《规定》参考了《网络安全法》第二十一条要求网络运营者设置网络安全负责人以及第三十四条要求关键信息基础设施的运营者设置安全管理负责人等规定，对网络信息内容服务平台对平台上发布内容的监管提出了更高的要求，但目前尚

未对网络生态治理负责人以及工作年度报告的设定细节（如负责人的数量、资质等）作出规定，有待我们持续关注网信办此方面的后续细化措施。至于该网络生态治理负责人由企业内部的哪个部门选派，是否可以与 “网络安全负责人”、“个人信息保护负责人”、和“数据保护官”设置为同一人，可以根据企业内部的实际情况进行决策。

七、多方共同配合监管，被规制主体承担责任多样化

《规定》第七章集中对被规制主体违反《规定》需要承担责任做出规定。首先，对于网络信息服务生产者，如果其生产违法、不良信息，将会受到与网络信息内容服务平台具体订立协议的制约，例如被平台警示整改、限制功能、暂停更新、关闭账号，被平台要求及时消除违法信息内容等。同时，其不当行为还会被保存记录并向有关主管部门报告，由有关主管部门依法采取相应措施。

其次，对于网络信息内容服务平台，其承担责任的形式更为多样化。除了一般可能触发法律规定的行政、刑事责任外，其在复制、发布、传播不良信息，不按主流价值观干预个性化算法推荐，不按《规定》订立用户服务协议、建立用户信用档案等情形下，还可能被网信等有关主管部门依职责进行约谈。“约谈”虽不是正式的行政责任形式，但是现今已经越来越多地被运用到司法实践之中，不得不引起我们高度的重视。

再次，网络信息服务使用者违反《规定》责任，根据不同行为的性质，可由其他相应的法律、行政法规进行处罚。

值得注意的是，根据《规定》第四十条，网信部门还将会同其他部门建立健全网络信息服务严重违规失信联合惩戒机制。该机制可以对严重违反《规定》的前述三类被规制主体采取限制从事网络信息服务、网上行为限制、行业禁入等惩戒措施。

另根据《规定》第二十九条，行业组织也有可能通过其评价奖惩机制对规制主体施加影响，例如对会员单位的不当行为进行惩戒等，这一点可能同样需我们谨慎对待。[20]

[20] 作者：孟洁、颜婷婷.《环球评论丨《网络生态治理规定（征求意见稿）》要点评析

3. FTC/纽约州诉谷歌/YouTube 的和解令全文翻译及关键点提要

视频网站 YouTube 及其母公司 Google 因为违反《儿童在线隐私保护法》而支付了总共 1.7 亿美元的民事罚款。据联邦贸易委员会和纽约司法部长在美国联邦华盛顿哥伦比亚特区地方法院提起的诉讼，YouTube 通过其网站上的视频和频道页面，有意且违法地收集了 13 周岁以下儿童的个人信息，并使用这些信息投放有针对性的广告而实现获利。但 YouTube 最终与原告 FTC 和纽约司法部长达成和解，并将分别支付 FTC 和纽约州 1.36 亿美元和 3400 万美元。这是自《儿童在线隐私保护法》在 1998 年颁布以来，联邦贸易委员会在儿童隐私法案中处以的最高罚款金额。

除去创纪录的罚金数额，此次和解的引人注目之处还有其创新地针对 YouTube 平台命令了禁止令。和解要求 Google 和 YouTube 开发、实施和维护一套系统，在该系统内能使频道所有者识别他们在 YouTube 平台上投放的内容为专门针对儿童的内容，这不仅是 FTC 第一次将 COPPA 用于一个针对有广泛受众且拥有大量儿童内容的平台，也是 FTC 向其他拥有全年龄用户的内容平台所传达的信号：即 FTC 不会犹豫地将目标转移到更广泛的内容平台上，并采取强有力的措施来保护儿童的在线隐私。网站已经不再能靠定性自己为“针对广泛、全年龄受众”而避免自己被 FTC 针对，只要他们对自己的平台或服务中有针对儿童提供的内容且可以证明是实际知情（actual knowledge）的，他们就可能会因为违反 COPPA 及其规则而被 FTC 处罚。

虽然针对何为“实际知情”，法律上一直有所争议。YouTube 声称，因自己不生产针对儿童的内容，所以其对儿童用户使用平台的情况没有达到“实际知情”，但 FTC 认为 YouTube 的广告和营销活动，包括其内容分级体系已经证明了 YouTube 了解自己平台上有内容是针对儿童提供，并且有儿童用户在使用其平台。FTC 的

和解中同时规定了 YouTube 平台上的频道所有者同样可能受到 COPPA 规则的限制，一旦他们指认自己提供儿童导向的内容，他们就需要遵守 COPPA 的规则，例如关闭评论和通知功能、不准使用永久标识符来追踪儿童用户、以及接受 COPPA 培训等。

这份和解令对一些关键定义给出了很好的解释，比如何为“清晰而醒目”地告知，对通过视频或者音频形式进行交流作出了区分；对于“收集”儿童个人信息，将“请求、促使或鼓励儿童在线提交个人信息”与“被动跟踪儿童的在线行为”都囊入；对设立专门的儿童网站或在线服务以及实际知悉网络运营者所有服务中只有一部分是针对儿童的，都算为“针对儿童的在线服务”。另外，对于禁令的要求也分几个不同的层次，有要求被告开发系统以识别平台上的频道投放了儿童内容以及要求向员工提供 COPPA 培训的命令，也有针对收集儿童个人信息需要向父母告知并获得其可验证的同意，以及需要在平台的每一区域设置显著链接以明示收集使用儿童个人信息做法的命令，并且还命令被告先前已经收集的儿童个人信息不得再批露、使用和受益。可谓逻辑清晰，层层递进。此外，除了命令被告向两位原告进行巨额赔偿以外，还规定了被告需要对今后一年中的合规运营情况向 FTC 和纽约州进行报告，需要做记录保存并且需要受到合规监控。该合规监控既可以由 FTC 和纽约州代表对被告的相关人员进行直接约谈，也可以由 FTC 和纽约州代表假扮消费者或者供应商对其进行无感监控且无需事先通知被告。我们将所有我们认为的重点内容，在和解令中用蓝色或者红色进行了重点提示，以供大家快速阅读与参考。

有人指出，FTC 的此项政策会对 YouTube 这样的拥有大量内容的平台和内容提供者造成巨大的合规风险和困难。但也有专家指出，此次和解会促使更多行业领导者和类似的平台做出内容审核和筛选机制的改变，以规避自己被 FTC 处罚的风险，从而带来好的转变。由此看来，接下来平台运营方和内容提供方将如何指认自

己的内容是否专门为针对儿童提供的可能会成为下一个争议焦点，FTC 将以何种方式和强度来实施此项政策也会给整个行业带来更多改变。

以下为和解令的中文翻译：[21]

美国联邦哥伦比亚特区地方法院

联邦贸易委员会，)

与)

由纽约州司法部长)

LETITIA JAMES 代表纽约州人民，)

原告，)

)

vs.) 案号：19-cv-02642

)

GOOGLE LLC，) 永久禁止令及

特拉华州有限责任公司，) 民事处罚判决

与)

YOUTUBE, LLC，)

特拉华州有限责任公司，)

被告，)

[21] 作者：孟洁律师团队。《【重要参考文件】FTC/纽约州诉谷歌/Youtube 的和解令全文翻译及关键点提要》

原告，联邦贸易委员会（“FTC”或“委员会”）和纽约州人民（“纽约州”）（统称“原告”）提出了他们的指控，请求永久禁令、民事处罚和其他补救方法（“指控”）。依据《联邦贸易委员会法案》（简称“《FTC 法案》”）第 13（b）和 16(a)(1)条，《儿童在线隐私保护法案》（简称“《COPPA》”）第 15 U.S.C. §§6502(c)，6504(a)(1)和 6505(d)，以及 FTC 通过的《儿童在线隐私保护规则》（“《规则》”或“《COPPA 规则》”）16 C.F.R. 第 312 部分。被告已放弃传票和指控的送达。原告和被告达成通过永久禁令和民事罚款，解决他们之间有关这一诉讼程序的所有争议事项。

因此，法院命令如下：

调查发现

1. 本法院对此事项拥有管辖权。

2. 指控指出，因被告对儿童个人信息的收集，未能在其在线服务平台上发布隐私政策并提供有关其信息收集和使用情况的清晰、易懂和完整的通知；且被告未能直接通知儿童父母关于此类信息收集和使用的情况；且被告未能在收集、使用或披露儿童个人信息

之前获得可验证的父母同意，因此被告违反了《COPPA 规则》、《FTC 法案》第五章以及第 15 U.S.C. §45 条。

3. 除本命令中所明确规定的事项外，被告既不承认也不否认指控中的任何说法。仅针对本指控目的而言，被告承认对于建立管辖权所必要的事实。

4. 被告放弃根据《司法平等法案》第 28 U.S.C.§2412 条可能拥有的本命令下达之日起，关于本指控的任何主张，并同意承担己方的诉讼费和律师费。

5. 被告和原告放弃上诉或对本命令的效力另行提出挑战或质疑的所有权利。

定义

为满足本命令目的，以下定义适用：

A. “**频道所有者**”是指，将视频上传到 YouTube 服务平台的个人或实体。

B. “**儿童**”或“**儿童们**”是指，未满 13 周岁的个人或群体。

C. “**清晰而醒目**”是指，要求该披露**很难被错过**（即容易引人注意）并且易于普通消费者理解，包括以下所有方式：

1. 在任何仅通过视频或音频的交流中，必须以该交流所呈现的相同方式进行披露。 在同时通过视频和音频（例如电视广

告）进行的交流中，即使要求批露的呈现方式仅为一种，也必须以视频和音频同时进行交流的方式进行批露。

2. **视频信息的披露，通过其大小、对比度、位置、出现的时长和其他特征呈现的，必须从任何附带的文本或其他视觉元素中脱颖而出，以便容易被注意、阅读和理解。**

3. **音频信息的披露，包括电话或流媒体视频，必须以一定的音量、速度和节奏，足以使普通消费者能够轻松听到和理解。**

4. 在使用交互式电子媒介（如互联网或软件）的任何交流中，披露是必不可少的。

5. 披露必须使用普通消费者可以理解的词汇和语法，并且每一种语言中的表达都要求体现该等披露。

6. 披露必须符合其可被接收的每一种介质的要求，包括所有的电子设备和面对面的交流。

7. 披露不得与交流中的任何其他内容相对立、互相减损或相互抵触。

8. 当代表或销售针对特定受众时，例如儿童、老人或绝症患者时，“普通消费者”是指该群体中的理性成员（reasonable members）。

D. **“收集”**是指，通过任何方式收集儿童的任何个人信息，包括但不限于：

1. 请求、促使或鼓励儿童在线提交个人信息；

2. 使儿童能够以可识别的形式公开个人信息。如果运营者在信息公开之前采取了合理措施删除了儿童帖子中所有或几乎所有的个人信息，并且从其记录中也删除了此类个人信息，则该运营者不会被认为收集了儿童的个人信息；

3. 对儿童的在线行为进行被动跟踪。

E. **"合规日期"**是指，**本命令生效后四个月**。

F. **"内容"**是指，在 YouTube 服务上找到的任何视频或频道页面。

G. **"被告"**是指，特拉华州有限责任公司 Google LLC 和特拉华州有限责任公司 YouTube，LLC 及其继承人和受让人。

H. **"删除"**是指，移除个人信息，使其成为不以可恢复的形式，并且无法在正常业务过程中被恢复。

I. **"披露"**是指，就个人信息而言：

1. 运营者出于任何目的，公开以可识别的形式向儿童收集个人信息，除非运营者仅向为网站或在线服务提供支持的内部运营人员提供此类信息；

2. 通过任何方式，以可识别的形式公开运营者向儿童收集的个人信息，包括但不限于通过互联网公开发布、通过网站、个人主页或页面、笔友服务、电子邮件服务、留言板或聊天室等在线服务收集个人信息。

J. **"互联网"**是指，包括设备和操作系统软件在内的无数计算机和电信设施的统称，这些设备和操作系统软件构成了采用传输控制协议/互联网协议（或此类协议的任何历史或演进版本的协议）进行互连的全球网络，并在全球网络中通过有线、无线电或其他传输方式传递各种信息。

K. **"获得可验证的父母同意"**是指，做出任何合理的努力（考虑到现有技术），以确保在收集儿童个人信息之前，他们的父母：

1. 接收到运营者对个人信息收集、使用和披露情况的通知；

2. 根据现有技术，使用合理的计算方法授权任何对个人信息的收集、使用和/或披露，以确保提供同意的人是儿童的父母。

L. **"在线联络信息"**是指，能直接联系到在线人员的电子邮件地址或任何其他本质上相似的标识符，包括但不限于即时消息用户标识符、互联网协议语音（VOIP）标识符或视频聊天用户标识符。

M. **"运营者"**是指，经营互联网网站或在线服务网站，以及从该网站或在线服务的用户或访问者处收集或维护个人信息或代表其收集或维护此类信息的任何人。同时，包括通过该网站或在线服务，销售产品或服务的任何人。此类网站或在线服务是为了商业目的，包括在不同国家间或与一个或多个境外国家；在美国或哥伦比亚特区内，或任何该等区域与另一区域或任何国家或境外国家之间；或哥伦比亚特区与任何国家、区域或境外国家之间，进行商业活动而运营。该定义不包括任何被《FTC 法案》（15

U.S.C.§45）第 5 节豁免的非营利实体。在下列情况下，*代表*运营者*收集*或*维护*个人信息的行为包括：

1. 由运营者的代理商或服务提供商收集或维护；
2. 运营者通过允许其他人直接从该等网站或在线服务收集用户个人信息而获利。

N. **"父母"**包括法定监护人。

O. **"人"**是指，任何个人、合伙企业、公司、信托、财产、合作社、协会或其他实体。

P. **"个人信息"**是指，在线收集的有关个人的可识别信息，包括：

1. 名字和姓氏；
2. 家庭或其他实际地址，包括街道名称和城市或城镇名称；
3. 在线联系信息；
4. 与在线联系信息功能相同的屏幕或用户名；
5. 电话号码；
6. 社会保障号码；
7. 永久标识符，可用于跨时间和跨不同网站或在线服务来识别用户。此类永久标识符用于除支持网站或在线服务内部运营之外的功能。这种永久标识符包括但不限于 cookie 中保存的

客户编号、互联网协议（IP）地址、处理器或设备序列号或唯一设备标识符；

8. 包含儿童图像或声音的照片、视频或音频文件；

9. 足以识别街道名称、城市或城镇名称的地理位置信息；

10. 运营者在线从儿童处收集并与定义中所描述的标识符相结合的有关该儿童或者该儿童的父母的信息。

Q. **“个人信息的发布”**是指，向任何第三方共享、出售、出租或转让个人信息。

R. **“支持网站或在线服务的内部运营”**是指

1. 为满足以下目的所采取的必要行为：

a) 维护或分析网站或在线服务的运营；

b) 进行线上交流；

c) 对网站或在线服务的用户进行身份验证或个性化推送；

d) 在网站或在线服务上提供插入式广告或限制广告的频率；

e) 保护用户、网站或在线服务的安全性或完整性；

f) 确保对法律、法规的遵守；或

g) 满足《COPPA 规则》第 312.5(c)(3)和(4)条所允许的儿童的请求（详见附录 A）；

2. 只要第 1(a) – (g)所列出的这些活动所收集的信息未被用于或披露于与特定个人相联系（包括通过行为广告）、汇聚成一个特定人的画像以及任何其他目的。

S. **"第三方"**是指，任何一个人不是：

1. 通过网站或在线服务收集或维护个人信息的运营者；或
2. 为网站或在线服务内部运营提供支持且不使用或不披露其信息受《COPPA 规则》（详见附录 A）保护的人。

T. **"针对儿童网站或在线服务"**是指，**针对儿童的商业性网站或在线服务或者网站或者在线服务中的一部分是针对儿童的。**

1. 在确定网站或在线服务或其中一部分是否针对儿童，FTC 将考虑其主题、视觉内容、动画人物的使用或者以儿童为导向的活动和奖励、音乐或其他音频内容、模特的年龄、童星的出现或能吸引到儿童的名人、网站或在线服务的语言或其他特征，以及出现在网站和在线服务上的广告宣传是否针对儿童。FTC 还将考虑受众的构成情况这些有力且可靠的据实证据和目标受众的证据。
2. 当网站或在线服务实际知悉它会从其他针对儿童的网站或在线服务平台直接收集个人信息时，该网站或在线服务平台会被认为以儿童为目标受众。

3. 根据本定义第（1）段所规定的标准针对儿童提供服务，但不以儿童为主要受众的网站或在线服务，**如果符合以下情况，则不应视为针对儿童：**

   a) 在收集年龄信息之前，不收集任何访客的个人信息；

   b) 在未遵守《COPPA 规则》的通知和父母同意条款（详见附录 A）之前，防止收集、使用或披露自称未满 13 周岁的访问者的个人信息。

4. 网站或在线服务不应仅仅因为它通过使用信息定位工具（包括目录、索引、引用、指针或超文本链接）引用或链接到针对儿童的商业性网站或在线服务而被视为针对儿童提供服务。

U. **"YouTube 服务"**是指，由普通 YouTube 用户生成的视频共享平台，目前位于 www.youtube.com 和 YouTube 移动应用程序，消费者可以在其中查看视频或上传视频进行分享。

命令

I. 关于 YOUTUBE 服务中针对儿童提供特定内容的禁制令

不迟于合规日期前，被告和被告的官员、代理人、雇员和律师以及所有其他处于或参与到同样团体的、接受到本命令实际通

知的，无论直接或间接参与运营 YouTube 服务平台的所有人员，均受到永久限制和禁止：

A. 未能开发、实施和维护一套系统，该系统允许频道所有者识别他们在 YouTube 平台上投放的专门针对儿童的内容。该系统内应包括清晰而醒目的通知，即 YouTube 服务中所投放的专门针对儿童的内容可能受《COPPA 规则》16 C.F.R. 第 312 部分（附录 A）的约束。当这些内容是专门针对儿童时，频道所有者有义务指出该等内容；

B. 未能为运营和维护频道所有者的其员工提供有关遵守《COPPA 规则》16 C.F.R.第 312 部分（附录 A）所要求的年度培训。

II. 关于从儿童处收集个人信息的禁令

不迟于合规日期前，被告和被告的官员、代理人、雇员和律师以及所有其他处于或参与到同样团体的、接受到本命令实际通知的，无论直接或间接参与运营 YouTube 服务平台的所有人员，均受到永久限制和禁止：

A. 未考虑现有技术，未做出合理的努力确保儿童的父母在被告收集、使用或披露儿童个人信息前收到直接的通知，包括通知儿童的父母其之前经过同意的收集、使用和披露行

为发生了任何重大变化。除非《COPPA 规则》16 CFR 第 312 部分（附录 A）提供了此类通知的例外情况；

B. 未能在其主页、登陆页面、其网站和在线服务的页面，以及在收集儿童个人信息的网站和在线服务平台的每一个区域发布一个醒目且明确标识的链接，以通知其针对儿童个人信息收集和使用的相关做法。除非《COPPA 规则》16 CFR 第 312 部分（附录 A）提供了提供此类通知的例外情况；

C. 在收集、使用或披露儿童个人信息之前未能获得可验证的父母同意，包括针对儿童的父母之前经过同意的收集、使用和披露行为发生了任何重大变化，除非《COPPA 规则》16 CFR 第 312 部分（附录 A）提供了获得可证实的父母同意的例外情况；和

D. 违反《COPPA 规则》16 C.F.R.第 312 部分（附录 A）。

III. 关于使用先前收集的个人信息的禁令

在合规日期的九十（90）天内，被告的官员、代理人、雇员和律师以及所有其他处于或参与到同样团体的人员在收到本命令实际通知的情况下，不得披露、使用或受益于之前从频道所有者指明针对儿童提供内容的频道中所收集的个人信息，只要上述指

明发生在合规日期的六十（60）天之内。但是，如果政府机构要求，或法律法规或法院命令要求可以披露此类个人信息的除外。

IV. 民事处罚和其他罚款：

进一步命令：

A. 作为民事处罚，被告须赔偿原告 FTC 一亿三千六百万美元（136,000,000 美元）的赔偿金，各被告承担相应的连带责任。

B. 被告须支付原告 FTC 一亿三千六百万美元（136,000,000 美元），按照被告的约定，被告律师仅出于向 FTC 付款的目的代管此款项。此款支付必须在本命令生效后三十（30）天内按照委员会代表先前提供的指示通过电汇方式转账。

C. 被告须赔偿原告纽约州三百四十万美元（34,000,000 美元），以对纽约州人民进行损害赔偿、救济或其他赔偿，各被告承担相应连带责任。

D. 被告被命令通过纽约州司法部支付原告纽约州三千四百万美元（34,000,000 美元）。此款支付必须在本命令生效后三十（30）天内按照原告纽约州代表提供的指示通过电汇进行。

V. 附加罚款条款

进一步命令：

A. 被告放弃对根据本命令转让的所有资产的法律上及衡平上的权利和所有权益，并且不得寻求任何资产的归还。

B. 为执行本命令中任何付款或金钱赔偿的权利而由 FTC 或纽约州或代表 FTC 或纽约州提起的任何后续诉讼程序中，指控所声称的任何事实，将被视为真实的，无需进一步证实。

C. 指控中声称的事实，对构成由 FTC 或纽约州根据《破产法》第 11 节第 (a)(2)(A)条提起的诉讼被维持原判所具有的所有要素是必需的，以及本命令将为此目的具有禁止反言的效力。

D. 根据第 31 U.S.C.§7701 的规定，被告承认，其必须向委员会提交纳税人识别号码用于收集和报告本命令产生的任何拖欠金额。

VI. 命令确认书

进一步命令，被告须承认接收到本命令：

A. 每个被告在本命令生效后七（7）天内，必须在会受伪证处罚的宣誓后向 FTC 和纽约州提交收到此命令的确认书。

B. 在本命令生效后的五（5）年内，每个被告必须将本命令的副本交付给：（1）所有负责人、高级职员、董事和有限责任公司的经理和成员；（2）对本命令第 I 部分和第 II 部分的主要内容有监督责任的所有员工、代理人和代表；（3）“合规报告”一节中规定的任何结构变更产生的任何商业实体。现职人员对确认书的提交必须在本命令生效后的七（7）天内完成。对于其他人员，确认书的提交需要在他们承担职责前完成。

C. 对于交付本命令副本的每个被告个体或实体，被告必须在本命令生效后的三十（30）天内获得这些个人或实体关于签收本命令的确认书（签名+日期）。

VII. 合规报告

FTC 还命令被告及时向委员会和纽约州提交下列材料：

A. 在合规日期后一年，每个被告在做出会受伪证处罚的宣誓后，必须提交一份合规报告。在此报告中，每个被告必须：

1. 识别主要的实际地址、邮政地址、电子邮件地址和电话号码，作为指定联系方式，以便 FTC 和纽约州代表与该被告进行联系；

2. 通过被告的姓名、电话号码、实际地址、邮政地址、电子邮件地址和互联网地址，识别被告在运营 YouTube 服务或从 YouTube 服务中收集、使用和披露儿童个人信息的所有业务。

3. 描述与运营 YouTube 服务直接相关的每个业务，包括所提供的商品、服务、广告、营销和销售方式；

4. 详细说明被告是否以及如何遵守本命令的每个部分；

5. 提供发布在 YouTube 服务平台上、或以其他方式适用于 YouTube 服务平台、或发送给 YouTube 服务平台用户的任何隐私声明的每个有实质差异版本的副本；

6. 详细说明用于跟踪 YouTube 服务儿童用户的方法（如有）（包括用于被动跟踪的方法和用户控制或选择退出的方法），以及为避免跟踪儿童而采取的措施；

7. 详细说明通过 YouTube 服务收集、使用和/或披露儿童个人信息之前获得可验证家长同意的方法；

8. 详细说明家长如何审查通过 YouTube 服务平台收集其子女个人信息的方法，和拒绝允许 YouTube 服务平台进一步使用或维护其子女个人信息的方法；

9. 提供根据本命令获得每份命令的确认书副本，除非先前已提交给 FTC。

B. 在本命令生效后十（10）年内，每个被告必须在发生以下任何变更的十四（14）天内，于会受伪证处罚的宣誓后，提交一份合规通知。变更包括：（1）任何已确认的联系方式；或（2）该被告或被告直接或间接拥有任何所有者权益或可直接或间接控制可能影响本命令项下产生的合规义务的任何实体的结构，包括:设立、合并、出售或解散从事本命令项下任何行为或做法的任何子公司、母公司或关联方。

C. 每一被告必须向委员会和纽约州提交由该被告提起的或针对该被告提起的任何破产申请、资不抵债程序或类似程序的通知，在其归档后十四(14)天内提交。

D. 根据本命令向委员会和纽约州提交的任何会受伪证处罚的宣誓书必须真实准确，并符合美国法典第 28 编第 1746 条的规定，例如结尾陈述为:“本人在美利坚合众国法律项下声明上述内容真实正确，并受伪证罪处罚。签署

日期:____年___月___日，并提供签字人的全名、职务(如适用)和签字。。

E. 除非委员会代表另有书面指示，根据本命令向委员会提交的所有文件必须通过电子邮件发送至 DEbrief@ftc.gov 或通过隔夜快递（不包括美国邮政）发送至：美国宾夕法尼亚州西北方向 600 号宾夕法尼亚大道 600 号，华盛顿特区 20580 号，联邦贸易委员会消费者权益保护局负责执行事务的副主任。主题行必须始于：FTC v. Google LLC and YouTube, LLC, FTC File No. 1723083.

F. 除非纽约州代表另有书面指示，根据本命令向纽约州提交的所有文件必须通过电子邮件发送至 ifraud@ag.ny.gov 并通过隔夜快递(而非美国邮政)发送至:纽约自由街 28 号，纽约 10005 号，纽约州司法部长办公室互联网和技术局局长。主题必须始于: FTC v. Google LLC and YouTube, LLC, FTC File No. 1723083。

VIII. 记录保存

进一步命令，被告必须在本命令生效后十（10）年内创建特定记录，并对每条记录保存五（5）年。具体而言，与运营 YouTube 服务相关的每一被告必须创建并保留下列记录:

A. 会计记录：所有销售的商品和服务的收入；

B. 人事记录：对于提供服务的每个人，无论是作为雇员还是其他人，该人员的姓名、地址、电话号码、职称或职位、服务日期和终止的理由（如适用）；

C. 证明完全遵守本命令各项规定所需的所有记录，包括向 FTC 和纽约州提交的所有材料；

D. 所有与未经授权收集、使用或披露与 YouTube 服务互动的儿童个人信息的消费者投诉记录，以及任何回复；

E. 每个被告通过 YouTube 服务收集儿童个人信息而创建、维护或以其他方式提供的有实质差异的表格、页面或屏幕的副本，以及每份实质上不同的文件的副本，该文件包含关于收集、使用和披露通过 YouTube 服务收集的儿童个人信息的做法的陈述。每个网页副本都应附有在线发布材料的网页 URL。电子副本应包括用于在互联网上呈现信息的所有文本和图形文件、音频脚本和其他计算机文件；以及

F. 与推广或销售 YouTube 服务有关的每个不同的广告、其他营销材料、电话营销脚本或与儿童个人信息收集相关的其他陈述的副本。

IX. 合规监控

为监督被告遵守本命令之目的，兹进一步命令:

A. 在收到委员会或纽约州代表的书面请求后十四（14）天内，每个被告必须：提交额外的合规报告或其他要求的信息，这些信息必须在受伪证处罚下宣誓；出庭作证；出示供检查和复制的文件。委员会和纽约州还被授权在不经法院许可的情况下，利用《联邦民事诉讼规则》第 29、30 条 (包括电话证词)，第 31、33、34、36、45 和 69 条所规定的任何程序得到证据。

B. 对于与本命令有关的事项，FTC 和纽约州有权直接与每一被告联系。每一被告必须允许 FTC 和纽约州的代表约谈同意接受约谈的任何雇员或与被告有关联其他人员。被约谈人可以有律师在场。

C. FTC 和纽约州可以使用所有其他合法手段，包括通过其代表冒名为与被告或任何与被告有关联的个人或实体的消费者、供应商或其他个人或实体，而无需身份证明或事先通知。根据 FTC 法案第 9 节和第 20 节，美国法典第 15 编第 49、57b-1 条，本命令的任何规定不得限制 FTC 合法使用强制程序。

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