未成年人网络保护中的身份确认与隐私保护

■ 佟丽华
(北京青少年法律援助与研究中心,北京 100161)

【摘要】为了加强对未成年人的网络保护,我国在对未成年人的身份进行有效识别的同时,对其个人信息也进行了大量的收集,这有可能导致未成年人隐私泄露,从而引发更加严重的风险。对此,美国、欧盟等国都有着严格的关于儿童个人信息网络保护的相关规定。我国的相关立法和行业规范也应与国际接轨,这也是我国未来的发展方向。国家互联网信息办公室于 2019 年 8 月 23 日发布的《儿童个人信息网络保护规定》对我国儿童个人信息保护具有里程碑的意义。在此背景下,笔者结合国内外相关的法律政策和我国未成年人个人信息保护的立法现状及实践中存在的问题,建议国家主导建立"一站式"未成年人身份识别管理平台,区分年龄确定未成年人个人信息保护的内容,完善监护人同意制度,引导制定行业执行标准等,平衡未成年人身份识别与个人信息保护关系。

【关键词】未成年人　网络保护　身份确认　隐私保护

随着大数据分析、人工智能、机器学习等信息技术的发展,数据已成为网络世界的一种宝贵资源。以美国的 FAANG[①]和中国的 BAT[②]、TMD[③]等为代表的互联网企业,不断挖掘数据的潜在价值,为社会创造了巨大的财富。同时,对数据大范围的应用也带来了个人信息和隐私方面的安全隐患。2018 年的 Facebook"数据门"事件引发全球热议,让个人信息和数据保护一时成为热点。在未成年人网络保护过程中,我国当前立法政策的基本思路是:首先要确定未成年人的身份,在此基础上再强化对其进行特殊保护。我国在 2016 年公开征求意见的《未成年人网络保护条例》第 22 条规定,"网络信息服务提供者提供网络游戏服务的(以下称"网络游戏服务提供者"),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。"在实践中,很多互联网企业也都将人脸识别、指纹登陆、身份信息

收稿日期:2019 - 09 - 01
作者简介:佟丽华,北京青少年法律援助与研究中心主任,国务院妇儿工委办公室儿童与法律智库组组长,主要研究青少年权益保护、公益法律服务、社会组织发展等。
基金项目:本文系 2019 年共青团中央"青少年发展研究"重点项目"未成年人网络空间权益保护机制研究"(课题编号:10ZD047)、国家社科基金项目"新时代中国'两岸四地'青年认同问题研究"(课题编号:18BZZ021)的阶段性研究成果。

① FAAGN 是 Facebook、Apple、Amazon、Netflix 和 Google(Alphabet 的子公司)五家美国互联网公司的简称。
② BAT 是百度、阿里巴巴和腾讯三家中国互联网公司的简称。
③ TMD 是今日头条(字节跳动的子公司)、美团和滴滴三家中国互联网公司的简称。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

等作为加强未成年人网络保护的重要手段。但与此同时，也带来了“如何保障这些信息不会被泄露？又如何保障这些信息不会被滥用？”等一系列的问题。正如联合国儿童基金会副执行主任法图玛塔·恩达耶女士所说，未成年人在网上留下的“数字足迹”可能会导致其个人信息和隐私的泄露，对此，未成年人及其父母往往还没有意识到，就更谈不上对其所面临的风险进行有效的防范和应对了[1]。

一、我国未成年人个人身份识别及信息保护的立法与实践

国家互联网信息办公室于2019年8月23日发布了《儿童个人信息网络保护规定》，并于2019年10月1日正式施行。在此之前，我国没有专门针对未成年人个人信息保护的立法，对个人信息保护的相关规定也较为分散，而且多为原则性规定，实操性较差，在具体落实的过程中也存在很多漏洞。

（一）对未成年人身份识别的要求

为了满足未成年人网络安全保护的需求，我国立法政策在未成年人身份识别上提出了很多具体要求。根据新闻出版总署、中央文明办、教育部等八部委分别于2007年4月、2011年7月发布的《网络游戏防沉迷系统实名认证方案》和《关于启动网络游戏防沉迷实名验证工作的通知》，以及文化部2010年7月发布的《关于贯彻实施＜网络游戏管理暂行办法＞的通知》的要求，我国逐步推行网络游戏实名认证，强调网络游戏运营商应将收集的用户身份信息提交公安部门进行验证，用以识别未成年人用户，并将未成年人用户纳入防沉迷系统。

自2012年起，《全国人民代表大会常务委员会关于加强网络信息保护的决定》（2012年发布）、《网络安全法》（2016年通过，2017年实施），以及国家互联网信息办公室发布的相关规章等逐步要求“信息发布、即时通讯等服务”，通过“后台实名、前台自愿”的方式获取用户的真实身份信息。2017年的《未成年人网络保护条例（送审稿）》中专门要求网络游戏服务提供者“有效识别未成年人用户，并妥善保存用户注册信息”。中国网络视听节目服务协会于2019年1月发布的《网络短视频平台管理规范》也明确要求，网络短视频平台应采用“用户画像、人脸识别、指纹识别”等新技术手段以落实账户实名制。

从上述所介绍的法律政策的具体要求可以看出，我国未成年人网络保护立法政策的基础是身份识别，也就是说，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，以便于给他们提供特殊保护。但这个收集信息的过程极有可能成为侵害未成年人隐私权的过程，或者就此埋下未成年人隐私权受到严重侵害的隐患。尤其是在互联网企业高度全球化的背景下，中国未成年人的信息往往被大量外国企业轻易收集，这有可能会成为影响国家安全的重大风险之一。

（二）未成年人个人信息保护立法现状及规定

第一，法律。对于未成年人个人信息保护，《未成年人保护法》第39条规定“任何组织或者个人不得披露未成年人的个人隐私”，这仅仅做了原则性的规定。另外，在其他立法中也仅有一些涉及有关个人信息的一般性规定，如在《网络安全法》《消费者权益保护法》等法律中要求，网络运营者在收集、使用用户的个人信息时，必须“公开收集、使用规则”，“明示收集、使用信息的目的、方式和范围”，“并取得用户的同意”。但这些规定都过于笼统，对于如何在实践中落实并没有明确的指引。

第二，部门规章。《儿童个人信息网络保护规定》作为儿童个人信息保护的专门性规定，填补了这一领域的空白。该《规定》对儿童的范围、网络运营者在收集、使用、转移、披露儿童个人

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

信息过程中的义务进行了全面规范，比如，“网络运营者应当设置专门的儿童个人信息保护规则和用户协议，并指定专人负责儿童个人信息保护。”“网络运营者收集、使用、转移、披露儿童个人信息的，应当以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意”。这些内容都对网络运营者提出了明确的要求。

第三，其他规范性文件。工业和信息化部信息安全协调司2011年2月指导起草的《信息安全技术个人信息保护指南》第5.1.4条规定，“个人信息管理者不应要求未满16周岁的未成年人提交个人信息，当发现信息提交者未满16周岁时，应给出明确提示并停止收集行为，为提供必要服务确需收集其个人信息的，应征得其监护人的同意”；全国信息安全标准化技术委员会2012年11月出台的《信息安全技术公共及商用服务信息系统个人信息保护指南》第5.2.7条规定，“不直接向未满16周岁的未成年人等限制民事行为能力或无行为能力人收集个人敏感信息，确需收集其个人敏感信息的，要征得其法定监护人的明示同意”；2017年12月发布的国家标准GB/T352273－2017《信息安全技术—个人信息安全规范》第5.5条c项规定，“收集年满14周岁的未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满14周岁的，应征得其监护人的明示同意”。这些文件的规定相对较为全面，但仅具有一般的行业约束力和指导性价值，不具有法律强制力，难以得到有效执行。

总体来说，在我国个人信息保护立法相对不完善的情况下，《儿童个人信息网络保护规定》的出台具有里程碑意义，将使儿童个人信息网络保护工作有法可依。但也存在一些问题，比如对那些满14周岁不满18周岁的未成年人个人信息如何保护？如何避免孩子滥用监护人的同意权？父母提出撤回同意或请求删除孩子个人信息是否方便？父母或其他监护人怎样了解网络运营者超出目的范围或必要期限收集、存储、使用、转移、披露儿童个人信息？很多具体制度还都有待在执行中不断完善。

（三）存在的主要问题

从目前大型互联网企业的通行做法来看，在身份识别和个人信息保护方面还存在以下问题。

第一，在身份识别方面难以有效落实。我国在网络游戏方面的实名认证要求比较严格，在网络游戏注册环节一般都会有实名认证程序，甚至会进行人脸识别，但仍存在未成年人使用监护人或其他成年人身份信息注册的情况，从而逃避防沉迷系统的限制。而在其他网络平台，用户只需填写手机号码即可注册，一般不会要求用户提供年龄信息，对用户年龄的识别主要基于用户主动提供以及人工审核判断。这是互联网行业内的普遍做法，虽然这种做法能够满足目前我国法律关于一般网络使用行为的实名认证要求，但对未成年人账号的识别不够主动且不全面。互联网企业完全被动地依赖未成年人提供的年龄信息，且后续一般不会通过其他更有效的审核手段来判断用户真实年龄，使得用户识别机制对未成年人形同虚设。

第二，在个人信息保护方面未能建立有效保护。互联网企业主要按照2017年12月国家标准化管理委员会发布的《信息安全技术—个人信息安全规范》的规定及其提供的隐私政策模板开展未成年人个人信息保护工作。企业在用户注册环节一般会同时向用户提供用户服务协议和隐私政策两份文件。（1）在文件内容上，一般对企业收集、使用、存储个人信息等行为有着十分全面的描述，也赋予了用户很多保护其个人信息的权利。但是，这两份文件一般都很冗长，对成年人而言，阅读起来都会有一定难度，对于未成年人来说难度就更大了，他们几乎是不阅读的。（2）在文件的同意方式上，一般设置为主动勾选同意或默认勾选，否则用户无法使用相关服务。在隐私政策中一般都有关于未成年人个人信息保护的特殊规定，包括要求未成年人和父母共同阅读该政策并取得父母的同意；如果发现未经监护人同意而搜集了未成年人个人信息，

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

将设法尽快删除相关信息等。但实际上，企业不会主动设法联系未成年人的监护人。未成年人很可能在监护人不知情的情况下提供了大量的个人信息。

可见，我国互联网企业的做法更主要的是满足了相关规定形式上的要求，并没有采取具体的实质性措施，难以真正实现对未成年人的有效识别以及个人信息的有效保护。目前美国和欧盟等发达国家的普遍做法是：通过制定较为完善的法律法规来保护未成年人个人信息，这是值得我们借鉴的。

二、美国和欧盟儿童个人信息保护模式

从世界范围来看，发达国家的普遍做法是通过制定较为完善的法律法规来保护未成年人个人信息，比如，美国于1998年通过了《儿童网络隐私保护法》（以下简称“COPPA”），并于2013年7月修订了相应规则；欧盟于2018年5月实施了《一般数据保护条例》（以下简称“GDPR”）。美国和欧盟均对儿童个人信息保护作出了严格的规定。

（一）美国儿童隐私保护模式

COPPA确定的重要原则就是，要求特定网站和网络服务运营商在收集、使用或透露不满13岁儿童个人信息前应履行“通知并取得同意”义务，即通知儿童父母并取得父母同意的事先义务。联邦贸易委员会（以下简称“FTC”）负责儿童网络隐私保护的执法。FTC在判断一个网站或一项网络服务是否针对儿童时，不仅以其运营者的主观意愿或单方面宣称为准，还会结合其他多种客观元素，进行综合判断。这些客观因素主要由该网站或该项网络服务的主题、内容、语言、广告以及实际观众构成[2]。

在不同网络服务运营者的识别用户年龄义务上有明确区分。针对儿童的网站和网络服务运营者，必须将全部用户都视作儿童，必须认真履行对父母“通知并取得同意”的义务[3]。针对普通用户的网站和网络服务运营者，则仅在“实际知晓”某用户为儿童（如接到父母投诉）时才需对其父母履行“通知并取得同意”义务，或删除该用户的个人信息，而不需主动调查用户年龄[4]。对于被判定为“针对儿童”、但不以儿童为“主要观众”的网络运营者，COPPA允许其在收集其他个人信息前首先通过“年龄信息收集屏”①来区分儿童用户和非儿童用户，并向那些自我识别为儿童的用户履行对其父母“通知并取得同意”的义务[5]。

在验证方式上也有具体的要求。在已经识别出该用户是儿童之后，COPPA要求网络服务运营者取得“可验证的父母同意”，即在现有技术背景下，通过合理方式来验证儿童父母的身份[6]。目前经FTC确认的合理验证方式包括：由儿童父母签署同意书、使用网络支付系统、拨打免费电话、视频通话、提供身份证并与政府数据库核对（核对后立即删除身份信息）、回答一系列个性化问题、提交一张带照片的身份证明和一张不同的照片并经人脸识别技术核对，等等。为了避免监护人在受到强迫的情况下做出同意的选择，COPPA规则要求运营者为儿童父母提供仅同意收集和使用儿童个人信息、但不同意向第三方透露儿童个人信息的选项[7]。此外，COPPA还规定了儿童父母对儿童个人信息的查阅权、撤回同意并要求删除权[8]。对2019年2月14日以后违反COPPA的行为处罚也是很严厉的，最高可被处以42 530美元/次的民事罚款。

为了给行业更多的自我管理空间，COPPA规则允许行业组织等起草自我管理性质的COPPA规则的合规指南，这些指南经报FTC批准后被称为“安全港”项目，网站或网络服务经营者只要遵守了经FTC批准的安全港项目指南，即被视为符合了COPPA规则的要求。这些指南能

① 年龄信息收集屏（age－screen），通常是指用户登陆网站时会出现一个页面，提示用户填写年龄信息。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

为网站或网络服务经营者在具体执行中提供具体的指引。

美国这一模式对儿童信息保护提出了较高要求，但也存在缺陷。对于被判定为针对儿童又不以儿童为主要观众的网站来说，儿童可以轻易通过谎报年龄的方式规避“年龄信息收集屏”，后续因“实际知晓”而附带的“通知和取得同意”义务对运营者的防规避责任要求较低，这些运营者可以通过消极不作为的方式避免“实际知晓”。也就是说，美国法律并未规定身份识别，儿童年龄主要是通过其主动申报。这种模式的优点是能够更好保护儿童及其监护人的个人隐私权利，避免为了识别身份而过度搜集儿童及其监护人个人信息，其缺点是容易放纵儿童通过谎报年龄的方式上网，难以有效落实对儿童的其他网络保护内容。

（二）欧盟儿童个人信息保护模式

欧盟 GDPR 在引言和正式条款中有多处针对儿童个人信息保护的内容，其中第 8 条专门规定对处理儿童个人信息的同意①问题。

在同意年龄上，GDPR 允许欧盟各成员国在 13 – 16 周岁的范围内自主决定同意年龄的下限。截至 2019 年 1 月，德国、荷兰和爱尔兰选择了 16 周岁，法国和希腊选择了 15 周岁，意大利和西班牙选择了 14 周岁，英国、比利时、丹麦和瑞典则选择了 13 周岁[9]。

在监管对象上，GDPR 第 8 条的规定适用于直接向儿童提供的信息社会服务，在实际判断中既要考虑网络经营者主观表示的服务对象是否包括 18 周岁以下的儿童，也要考虑网站内容、营销方式等客观证据[10]。但在具体实施上，比如在英国，会将不设 18 周岁年龄限制的网络服务视为“直接向儿童提供的”[11]，但 GDPR 没有 COPPA 中“实际知晓”这一相对较低的适用标准，因此，相比 COPPA 而言，GDPR 在监管对象范围上的要求更严。

在年龄识别上，欧洲数据保护委员会（以下简称“EDPB”）认为，网络经营者必须通过合理的努力、结合现有技术和行为的内在风险性来验证用户的年龄以及儿童父母的身份，选择与该行为的性质和风险性相适应的验证方法，避免在年龄验证过程中过度处理用户个人信息[12]。GDPR 并没有具体列出一些可行的验证儿童父母身份的方法。EDPB 认为，可信赖的第三方验证服务有助于减少个人信息控制者自身需处理的个人信息数量[13]。另外，GDPR 还允许网络运营者为了追求“正当利益”，在未经儿童父母同意的情况下处理儿童个人信息，但强调应顾及儿童的利益、基本权利和基本自由[14]。

在同意条件上，GDPR 对其有着非常细致、明确的要求：（1）同意应是自愿给出的，如果被认定为强迫同意，个人信息控制者将可能面临高额罚款。（2）同意应是具体的，应明确信息处理的目的，且以满足该目的必要性为限[15]。（3）同意应是在完全知情基础上的，应明确同意范围且条款简洁清晰。GDPR 特别强调，向儿童提供的信息尤其应采用简洁、透明且易于辨认和接触的形式，并使用儿童可以轻易理解的清楚而平白的语言[16]。（4）同意应是清晰明确的，应通过清晰的确认行为作出[17]。

在信息管理上，GDPR 对于个人信息主体的权利和个人信息控制者的义务有着非常全面的规定。个人信息主体可行使包括但不限于以下权利：（1）撤回同意权，即有权在任何时候、通过与要求同意时同等容易的方式撤回同意并要求删除其个人信息[18]；（2）查阅权，即有权查阅其被处理的个人信息，并获取被处理的个人信息副本[19]；（3）被遗忘权，即有权要求删除经儿童父母同意或授权而处理的个人信息[20]；（4）个人信息可移植权，即有权要求将那些经其同意而被以自动方式收集的个人信息以通用的电子格式从某一个人信息控制者处转移至另一个人信息

① 这里的“同意”，是指对于儿童用户，个人信息控制者必须经他们的父母同意或授权后才能处理他们的信息，文中简称“同意”。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

控制者处[21]。

在个人信息使用上，由于儿童的成熟度和理解力较低，更容易在网络环境中受到剥削，EDPB 认为，那些足以影响儿童选择和行为的纯自动化判断都有可能对儿童产生较大影响，因此，通常情况下应避免对儿童进行“用户画像”，并用于行为定向广告等营销目的。

在违法处理上，GDPR 明确允许公民和社会组织针对个人信息控制者的违规行为提起侵权诉讼，寻求损害赔偿。而行政罚款金额可高达违规者全球年收入额的 4% 或 2000 万欧元，以二者较高一项为准，远高于 COPPA[22]。

与 COPPA 的“安全港”项目相仿，GDPR 也规定了行为准则和认证机制。经监管机构批准后，行业组织可以通过行为准则实施行业自我管理，认证机构可以提供 GDPR 合规认证、个人信息保护标识等服务[23]。

欧盟的 GDPR 是一部全面的个人信息保护立法，没有专门规定儿童父母的权利。但在个人信息主体的权利和个人信息控制者的义务等方面，均有着远比 COPPA 更细致、更充分、更严格的要求，并注入了更多新的理念。GDPR 尤其在对同意的四项要求（即同意是自愿给出的、具体的、在完全知情基础上的、清晰明确的）上比 COPPA 规则中的一次性“通知并取得同意”等标准更为严格。GDPR 明确了网络经营者验证儿童年龄及其父母身份的义务，同时，强调了在验证过程中要避免过度处理个人用户信息，并对侵害隐私权规定了严重的法律后果。

互联网时代对于个人信息安全隐患的担忧成为世界范围内的主要社会和政治议题。我国应与国际趋势相呼应，应有与国际标准接轨的立法和行业规范。为此，本文针对我国的立法与实践中存在的问题，在借鉴域外相关立法与成功经验的基础上，兼顾未成年人个人信息保护和身份识别的双重需求，提出未成年人网络保护工作的具体建议。

三、具体建议

（一）国家主导建立“一站式”未成年人身份识别管理平台

为了更好地平衡未成年人身份确认与隐私权保护两者之间的关系，建议国家立法明确规定，由国家网信部门主导建立“一站式”未成年人身份识别管理平台，凡是需要确认未成年人身份的，都由这个平台统一收集和管理。该平台由国家建设，避免出现各个互联网企业为了识别身份而大肆收集未成年人及其监护人个人信息的情况。同时明确，该平台只负责身份识别，不负责对这些信息的储存及分析。

（二）区分年龄确定未成年人个人信息保护的内容

在未成年人保护领域，年龄是个复杂的问题。根据联合国 1989 年通过的《儿童权利公约》以及我国《未成年人保护法》（2012 年修订）的规定，国际范围内的“儿童”以及我国法律中的“未成年人”都是指不满 18 周岁的人，这是全球公认的需要特殊保护的年龄阶段。我国在民事法律中规定不满 8 周岁为无民事行为能力人、满 8 周岁不满 18 周岁为限制民事行为能力人，满 16 周岁以自己收入为主要生活来源的可以被视为完全民事行为能力人。

在刑法中拐骗儿童罪和拐卖儿童罪中的“儿童”是指不满 14 周岁。2019 年 8 月发布的《儿童个人信息网络保护规定》中规定“儿童”为不满 14 周岁，这显然是一个反复斟酌的结果，其主要目的就是要加强对不满 14 周岁儿童信息的特别保护，但又不可避免地忽视了对满 14 周岁不满 18 周岁未成年人个人信息的特别保护。对于指纹、人脸等生物信息，年满 14 周岁的未成年人显然也需要特别保护。所以，建议全面加强对不满 18 周岁未成年人个人信息的保护，认真研究各个年龄阶段需要保护的信息内容，区分不同年龄确定要特别保护的重点内容。

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

(三)完善监护人同意制度

如前所述,目前大部分互联网企业都制定了隐私政策,并规定了监护人同意的内容,但在执行过程中更多的是流于形式,相关规定无法得到有效执行。鉴于此,笔者建议,在未成年人个人信息保护的后续执行机制中增加监护人同意的条件及方式的规定。《儿童个人信息网络保护规定》中,增加了收集、使用不满十四周岁儿童的个人信息应当征得监护人明示同意的规定,并采纳了与 GDPR 近似的对于同意的要求,即"告知""具体""清楚、明确"和"基于自愿"。但是,该《规定》并没有对儿童用户的识别和父母同意的验证方式作出规定。建议参考美国和欧盟的相关规定,以"合理性"和"现有技术水平"作为标准,采取多途径、全方位的验证模式,包括邮件、传真、金钱交易凭证、视频连线、身份证等,把监护人同意制度真正落到实处。

(四)引导制定行业执行标准

目前我国已对儿童个人信息保护做出了专门规定,应有具体的执行标准使之得到有效落实。如果没有具体的执行要求,仅仅依靠单个企业自身力量,可能会出现执行不到位,或执行成本太高影响企业积极性的情况,最终难以使《儿童个人信息网络保护规定》得到有效落实。我们也应借鉴美国和欧盟在个人信息保护方面的安全规则,由大型互联网企业或已有的行业组织牵头起草关于保护未成年人个人信息的可行性具体措施,并提交网信部门审核、备案,作为行业执行标准,这样既能够实现行业自我管理,也能够达到对未成年人个人信息保护的目的。

结语:网络保护关系到未成年人的各项权利。如果单纯依靠主动申报年龄,虽然有助于保护未成年人的个人隐私,但显然淡化了对其他权利的保障;如果为了加强对其他权利的保障而过度强化身份识别,又不可避免导致隐私权受到侵害。因此,从国家立法的角度,如何破解身份识别和隐私保护之间的两难命题?这是当前我们必须直面的问题。个人信息的保护不仅是未成年人网络保护的重要内容,也关系到国家安全。如何构建科学的制度以平衡、全面保护包括隐私在内的未成年人各项权利,还需要我们作出更多的努力。

[参 考 文 献]

[1]《凝聚青春微梦想传递校园正能量》,https://www.qunfenxiang.net/marketing/1097.html

[2] [7] [8] Children's Online Privacy Protection Rule,https://www.ftc.gov/system/files/2012-31341.pdf

[3] [4] [5] Complying with COPPA: Frequently Asked Questions,March 20,2015,https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[6] Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,June,2017,https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

[9] The Changing Patchwork of the Child's Age of Consent for Data Processing across the EU,https://www.betterinternetforkids.eu/en_US/web/portal/practice/awareness/detail?articleId=3017751

[10] [12] [13] [15] [17] Guidelines on Consent under Regulation 2016/679,July,2018,https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

[11] What are the Rules about an ISS and Consent? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-are-the-rules-about-an-iss-and-consent/

[14] What do We Need to Consider When Choosing a Basis for Processing Children's Personal Data? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-do-we-need-to-consider-when-choosing-a-basis-for-processing-children-s-personal-data/

[16] [18] [19] [20] [21] [22] [23] The General Data Protection Regulation(GDPR),https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

(责任编辑:王建敏)

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net