ICS 33.030
CCS M21

团　　体　　标　　准

T/CAAAD 001-2021　　T/CCSA 329-2021

互联网广告数据应用和安全技术要求

Technical requirements for application and security of Internet advertising data

2021－12－28 发布　　2021－12－28 实施

中国广告协会　　中国通信标准化协会　　发 布

版权声明

邮箱： digitalad@china-caa.org IPR@ccsa.org.cn

电话： 010-59725102 010-62302847

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语、定义和缩略语 1
3.1　术语和定义 1
3.2　缩略语 2
4　互联网广告数据应用原则 3
5　互联网广告数据安全技术要求 3
5.1　通用安全要求 3
5.2　场景安全要求 9
6　互联网广告应用数据交换接口定义 10
6.1　数据交换接口定义 10
6.2　标签用数据交换接口定义 15
7　互联网广告应用数据交换升级要求 15
7.1　基本要求 15
7.2　升级流程要求 15
附录A（资料性）　互联网广告数据应用场景 17
A.1　总体技术架构 17
A.2　数据应用场景 17
附录B（资料性）　广告投放监测服务的必要信息 21
附录C（资料性）　区块链技术应用于互联网广告技术指引 22
C.1　技术简介 22
C.2　技术优势 22
C.3　技术局限 22
C.4　参考解决方案 23
参考文献 24

前　言

本文件按照GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件为互联网广告数据安全与个人信息保护系列标准之一，该系列标准的名称和结构预计如下：

a) 《互联网广告数据应用和安全技术要求》；
b) 《互联网广告数据匿名化实施指南》；
c) 《互联网广告数据分类分级指南》；
d) 《互联网广告数据流通平台技术架构》；
e) 《互联网广告隐私计算平台技术要求》；
f) 《互联网广告数据出境安全要求》。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国广告协会和中国通信标准化协会共同提出，并分别归口。

本文件起草单位：中国信息通信研究院、深圳市腾讯计算机系统有限公司、北京巨量引擎网络技术有限公司、华为软件技术有限公司、北京国双科技有限公司、利欧集团数字科技有限公司、尼洱市场研究（上海）有限公司、秒针信息技术有限公司、上海腾徽软件科技有限公司、友盟同欣（北京）科技有限公司、OPPO广东移动通信有限公司、维沃移动通信有限公司、阿里巴巴（中国）有限公司、北京快手科技有限公司、北京奇虎科技有限公司、普华永道中天会计师事务所、上海数据交易中心、北京质子云网络科技有限公司、郑州信大捷安信息技术股份有限公司、蚂蚁科技集团股份有限公司、上海亦拓广告有限公司、北京师范大学、北京小米移动软件有限公司。

本文件主要起草人：杨正军、陈婉莹、霍焰、崔妍、朱岩、王北云、李锐、黄晓林、张亚男、张贝贝、李昳婧、王红恩、欧阳书馨、吴充、周崧弢、王其武、刘力泉、范秋华、邓鸿飞、付艳艳、贾科、姚栋、落红卫、姚一楠、姜敏、张凌欣、申翔宇、李强、刘为华、马良骏、丁新勇、吴沈括、彭晋、孟小楠。

引　言

互联网广告是近20年来广告业通过对互联网技术、大数据技术、人工智能技术等综合利用，对商业价值深入挖掘而发展起来的新兴商业模式，是数据收集、加工、交换和使用密集的行业领域，特别是近年来机器学习算法和神经网络算法在广告行业的流行，使得数据更加成为广告行业的重要基础资源之一，对于数据的各种技术应用和探索也是广告行业特别关注、积极尝试和大量投资的领域。

虽然互联网广告领域对数据收集、加工、交换和使用的需求旺盛，各种技术和应用层出不穷，但是这一领域缺乏一套完整的规范和标准，广告主、媒体、用户、代理商、第三方监测机构之间在数据的收集、加工、交换和使用中的矛盾不断，数据一致性、操作规范性、商业数据安全性、个人信息保护等问题已经成为互联网广告行业在使用数据中的突出问题。

因此，有必要针对互联网广告行业的数据收集、使用、存储、传输和删除，在合法、合规的前提条件下，制定能平衡安全合规和市场需求的标准，充分发挥互联网技术的优势，增强数字行业的竞争力，发挥数据要素的商业价值。

为适应信息通信业发展对标准文件的需求，由中国通信标准化协会和中国广告协会共同组织制定该团体标准，推荐有关方面采用。有关对本文件的建议和意见，向中国通信标准化协会和中国广告协会反映。

互联网广告数据应用和安全技术要求

1　范围

本文件规定了互联网广告数据的应用原则、应用场景和安全技术要求，并给出了互联网广告数据应用数据交换接口定义和升级要求等，同时提供了技术指引建议。

本文件适用于广告主、媒体和流量平台、用户、广告代理公司、广告技术公司、广告监测公司、其他第三方组织等在互联网广告活动准备期间、执行期间以及活动结束后涉及到的互联网广告相关的数据收集、使用、存储、传输和删除等活动，其他领域的相关活动也可参照进行。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 34090.2 互动广告 第2部分：投放验证要求

GB/T 35273 信息安全技术 个人信息安全规范

T/CAAAD 002-2020 中国互联网广告投放监测及验证要求

T/CAAAD 003-2020 移动互联网广告标识技术规范

3　术语、定义和缩略语

3.1　术语和定义

下列术语和定义适用于本文件。

3.1.1

参与方 participants

在互联网广告活动过程中参与提供、接收、使用数据的单位或组织，包括数据提供方、数据接收方、数据使用方等参与主体。

3.1.2

数据提供方 data provider

在互联网广告活动过程中提供数据的单位或组织。

3.1.3

数据接收方 data receiver

在互联网广告活动过程中接收数据的单位或组织。

3.1.4

数据使用方 data user

在互联网广告活动过程中使用数据的单位或组织。

3.1.5

用户 user

使用互联网服务的人。

3.1.6

广告主 advertiser

为推销商品、提供服务或推广概念而发布广告信息的市场主体。

3.1.7

媒体 media

发布、展示广告的载体。

3.1.8

受众 audience

广告主投放广告触达并产生影响的人口群体。

3.1.9

程序化购买 programmatic buying

基于自动化系统（技术）和数据来进行的广告投放。该方式支持根据广告主定义的期望受众，系统帮其找出优选的媒体来购买受众，为广告主提出最优媒介采买计划，运用计算机软件进行自动化购买的方式执行，并按照期望的周期反馈监测结果，并对后续投放进行优化。

3.1.10

需求方平台 demand side platform

帮助广告主执行广告投放策略的平台，可以设定投放金额、单价、数量、物料等执行策略。

3.1.11

供给方平台 supply side platform

帮助媒体进行广告资源销售的平台，记录了媒体销售的广告位、物料尺寸、售卖金额、库存等信息。

3.1.12

数据管理平台 data management platform

整合各方数据并提供数据分析、数据管理、数据调用等，通过数据调用向需求方平台、供给方平台、广告主和媒体提供数据服务的平台。

3.1.13

广告交易市场 advertising exchange

联系广告主和媒体，或者需求方平台和供给方平台，组织竞价、撮合交易的市场平台。

3.1.14

广告监测 Ad monitoring

为监测和衡量广告效果、确保广告数据真实性、归因分析等目的而进行的广告相关数据监测与分析的活动。

3.1.15

广告效果 Ad effects

广告达到既定目标的程度。

3.1.16

匿名化 anonymization

个人信息经过处理无法识别特定自然人且不能复原的过程。

3.1.17

去标识化 de-identification

个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。

3.1.18

用户画像 user profiling

通过收集、汇聚、分析个人信息，对某特定自然人个人特征，如职业、经济、健康、教育、个人喜好、信用、行为等方面作出分析或预测，形成其个人特征模型的过程。

3.2 缩略语

下列缩略语适用于本文件。

ADX	广告交易市场	Advertising Exchange
API	应用程序接口	Application Programming Interface
CTR	点击率	Click Through Rate
C2S	客户端到服务器端	Client to Server

DMP	数据管理平台	Data Management Platform
DSP	需求方平台	Demand Side Platform
HTTP	超文本传输协议	Hyper Text Transfer Protocol
HTTPS	安全的超文本传输协议	Hyper Text Transfer Protocol over SecureSocket
IDFA	广告标识符	Identifier For Advertising
IMEI	国际移动设备识别码	International Mobile Equipment Identity
IP	互联网通信协议	Internet Protocol
IPV4	互联网通信协议第四版	Internet Protocol Version 4
IPV6	互联网通信协议第六版	Internet Protocol Version 6
IVT	无效流量	Invalid Traffic
JS	Java脚本	JavaScript
MD5	信息摘要算法5	Message-Digest algorithm 5
RTB	实时竞价	RealTime Bidding
SDK	软件开发工具包	Software Development Kit
SHA1	安全散列算法1	Secure Hash Algorithm 1
SSP	供给方平台	Supply Side Platform
S2S	服务器端到服务器端	Server to Server
URL	统一资源定位器	Uniform Resource Locator

4 互联网广告数据应用原则

互联网广告数据的应用原则包括但不限于：

a) 合法性原则：互联网广告数据应用的参与方应严格按照法律法规的要求开展数据使用和交换活动；
b) 完整可用原则：互联网广告数据应用的参与方应保证数据使用和交换活动中的数据完整性和可用性；
c) 安全保密原则：互联网广告数据应用的参与方应保证数据使用和交换活动中的数据安全性和保密性；
d) 透明可验证原则：互联网广告数据应用的参与方在开展数据使用和交换活动的过程中，应当记录数据使用和交换情况，实现可查看与可追溯，以验证合规性和安全性。

5 互联网广告数据安全技术要求

5.1 通用安全要求

5.1.1 总体要求

数据使用方应当遵守以下总体要求：

a) 依据《个人信息保护法》等法律法规对个人信息的定义，个人信息不包括匿名化处理后的信息；

b) 对于采用信息系统对互联网广告数据进行处理的系统，应依据等级保护相关要求对数据的传输、存储进行安全防护。

5.1.2 数据收集

数据接收方收集数据，具体要求包括：

a) 数据接收方收集数据，不应：
   1) 从非法渠道获取数据；
   2) 通过误导、欺诈、胁迫等非法方式获取数据；
   3) 隐瞒产品或服务所具有的获取数据的真实功能；
   4) 获取法律法规明令禁止获取的数据；
   5) 以其他违反法律法规的方式收集数据。
b) 数据接收方直接向用户收集数据，应当：
   1) 直接向用户收集数据时，应当遵循合法、正当、必要和诚信的原则收集数据。如涉及收集个人信息，应向用户告知收集个人信息用于互联网广告服务的目的、方式和范围，并获得用户同意。此外，应符合 GB/T 35273 第 5 章的要求规范数据收集行为；
   2) 可与用户直接交互的数据接收方，如媒体、终端设备等，宜以简洁清晰、通俗易懂的方式（可包含文字和图示）告知关键内容，同时提供完整版告知内容的链接；
   3) 不具备直接告知渠道的，如以 SDK 等形式嵌入媒体、终端设备收集个人信息的，应在媒体、终端设备的告知文本中加入本 SDK 告知条款或官方渠道链接，详细披露个人信息的收集处理情况，并向用户提供简单直观的退出或关闭的选项，媒体、终端设备应配合相关说明的披露，并且 SDK 宜在其官方渠道（网站、公众账号等）告知收集、使用个人信息的情况，并提供退出、删除机制。
c) 数据接收方间接从其他数据提供方处获取数据，应当：
   1) 间接收集数据时，数据接收方应通过合法、正当的途径，采用合法、正当、必要的方式收集数据。如涉及间接收集个人信息，应要求数据提供方说明个人信息的来源、对其个人信息来源的合法合规性进行确认，且数据接收方应了解数据提供方已获得的个人信息处理的单独同意的范围，包括授权使用的目的、方式、范围以及用户是否授权同意进一步转让、共享、公开披露等；
   2) 开展业务所需进行的个人信息处理活动超出提供方已获得的同意范围的，应重新征得用户同意；
   3) 数据接收方应对数据或个人信息的来源、共享、转让、公开批露、安全保障措施等情况通过官方渠道在隐私政策等文本中向用户进行告知。

5.1.3 数据使用

数据使用方应使用数据，具体要求包括：

a) 数据使用方使用数据，不应：
   1) 以非法用途为目的使用数据；
   2) 滥用基于互联网广告目的获得的权限、数据；
   3) 通过误导、欺诈、胁迫等非法方式使用个人信息；
   4) 使用法律、行政法规明令禁止使用的个人信息。
b) 针对受众标识的限制：应优先使用符合 T/CAAAD 003-2020 标准要求的广告标识符；
c) 使用目的限制：
   1) 不应超出与数据提供方的约定使用数据，或违反约定将数据提供给其他数据接收方；
   2) 如涉及使用个人信息，还不应超出与收集或获取个人信息时所声称或约定的目的具有直接或合理关联的范围。因业务需要，确需超出上述范围使用个人信息的，应再次征得用户授权同意。
d) 数据使用完整性要求：

1) 数据使用方应具备完善的内部权限管理策略，支持最小化原则、合理授权数据使用的权限范围；
2) 数据使用过程中，数据使用方应具备完整的用户信息访问、处理、删除的操作和记录能力，以备数据审计；
3) 数据使用的整个过程中，数据使用方应保证使用场景合理合法，不得进行滥用、篡改、非法出售和故意毁损数据等操作。

e) 数据使用安全保密要求：
1) 应对数据进行分类并根据分类采取适合的保密、脱敏等处理方法，保障敏感数据的使用安全；
2) 应对数据严格保密，建立健全数据保护制度，综合使用各类技术手段保护数据使用安全，如权限管控、访问认证/鉴权、隔离、审计、加密、脱敏等；
3) 用于数据保密应采用行业通用加密方式，应符合国家密码管理相关要求。

f) 用户画像的使用限制
1) 用户画像中对用户的特征描述，不应包含：淫秽、色情、赌博、迷信、恐怖、暴力的内容以及表达对民族、种族、宗教、残疾、疾病歧视的内容；
2) 在业务运营或对外业务合作中使用用户画像的，满足以下要求：
- 不应侵害公民、法人和其他组织的合法权益；
- 不应危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序；
- 除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人；
- 应结合用户画像所用于的目的，采取有效的数据保护措施；
- 不应以价格歧视等不正当使用数据为目的使用用户画像，损害用户正当利益；
- 在业务运营或对外业务合作中使用用户画像的，应事前进行个人信息保护影响评估，业务出现重大调整时，应重新进行评估，对评估报告和处理情况应记录，并至少保存三年。

3) 用于广告目的的用户特征组合应消除明确身份指向性，降低重标识风险，避免精确定位到特定个人，特征组合所限定的用户规模宜不少于特征组中最多特征值的 50 倍。

g) 基于不同业务目的所收集的数据的汇聚融合
1) 数据使用方应按照合法、正当的目的对基于不同业务场景所收集的数据进行汇聚融合使用；
2) 如涉及个人信息，应满足以下要求：
- 不应超出与用户或数据提供方之间明确约定的目的使用数据；
- 不应超出与用户或数据提供方之间的约定将数据提供给其他任何数据接收方；
- 应结合汇聚融合后个人信息所用于的目的，开展个人信息合规影响评估，采取有效的个人信息保护措施。

h) 委托处理数据
1) 委托方在做出委托行为之前，应当进行个人信息保护影响评估，对影响评估报告及处理情况应当记录，并至少保存三年；
2) 受委托方应严格按照委托方的要求处理数据，不得超出约定的处理目的、处理方式等处理数据。受委托方因特殊原因未按委托方的要求处理个人信息的，应及时向委托方报告；
3) 委托方应对受委托者进行监督，方式包括但不限于：通过合同等方式规定受委托者的责任和义务；对受委托者进行审计；
4) 委托方应准确记录和保存委托处理数据的情况；
5) 委托合同不生效、无效、被撤销或者终止的，受托人应当将个人信息返还个人信息处理者或者予以删除，不得保留。

6) 委托方得知或者发现受托方未按照委托要求处理数据，或未能有效履行数据安全保护责任的，应立即要求受托方停止相关行为，且采取或要求受托方采取有效补救措施（如更改口令、回收权限、断开网络连接等）控制或消除数据面临的安全风险。必要时委托方应终止与受托方的业务关系，并要求受托方及时删除从委托方获得的数据；
7) 如涉及个人信息的，委托方应与受托方约定委托处理的目的、方式、个人信息种类、保护措施、双方权利义务等，并对委托方的个人信息处理活动进行监督，受托方应当协助委托方响应用户提出的相关请求；受托方在处理个人信息过程中无法提供足够的安全保护水平或者发生了安全事件的，应及时向委托方报告；
8) 未经委托方同意和用户单独告知同意，受托方不应转委托他人处理数据；
9) 宜在委托方平台进行的委托处理，非在委托方平台进行的委托处理，应满足本文件 5.1.5 数据传输要求，宜预先采用加密技术或去标识化技术使得数据对被委托方为匿名。

5.1.4 数据存储

数据使用方使用数据，具体要求包括：

a) 安全保密要求
   1) 对存储在平台的数据信息存储介质中的数据，应设置加密、备份与恢复机制，并采用数据访问控制机制来防止数据的越权访问。应提供相应的身份认证和访问控制机制，确保只有合法的用户或应用程序才能发起数据处理请求；
   2) 应采用符合国家密码管理相关要求的密码技术保证数据存储的保密性，包括但不限于鉴别数据、业务数据和个人信息等；
   3) 应使用认证系统和机制，进行权限设置、认证以及审计；
   4) 应采用加密技术或去标识化技术在数据存储过程中隐藏敏感数据。
b) 完整性要求
   1) 存储数据时应当将数据存储在存储介质中保证数据的真实性和完整性，不得篡改和伪造数据，尤其是敏感数据，应设计数据的完整性检测方案，保证可对存储数据的完整性进行检验；
   2) 数据存储应采取安全措施，及时进行备份，在数据遭遇入侵或者硬件损坏等不可抗力被损坏后，在符合一定条件时可以及时恢复；
   3) 存储数据应采取完整有效的访问控制策略，确保无权访问存储数据的个人或其他组织，不可访问或者通过其他间接手段访问或者破坏存储的数据。
c) 存储时间最小化要求
   1) 数据存储期限应为实现数据主体授权使用的目的所必需的最短时间，法律法规另有规定或者数据主体另行授权同意的除外；
   2) 超出上述存储期限后，应对数据进行删除或匿名化处理。

5.1.5 数据传输

数据提供方和数据接收方之间传输数据，具体要求包括：

a) 数据提供方和数据接收方之间传输数据，不应：
   1) 以非法用途为目的进行传输数据；
   2) 采用欺诈、诱骗、误导等非法的方式传输数据；
   3) 传输法律、行政法规、规章等明令禁止传输的数据。
b) 针对数据本身的限制：应优先使用符合 T/CAAAD 003-2020 标准要求的广告标识符；
c) 传输目的限制
   1) 不应超出与数据提供方和数据接收方之间的约定进行数据传输，以及使用传输后的数据，或超出双方的约定，将数据提供给其他任何数据接收方；
   2) 如涉及传输个人信息，还不应超出与收集或获取个人信息时所声称或约定的目的具有直接或合理关联的范围，进行个人信息传输。因业务需要，确需超出上述范围传输个人信息的，应再次征得用户单独同意。

d) 通过嵌入或接入自动化工具（如程序、脚本、接口、软件开发工具包等）进行数据传输

1) 数据提供方和数据接收方可结合业务需要，按照双方约定通过嵌入或接入自动化工具的方式进行数据传输；

2) 数据提供方（即通过嵌入或接入自动化工具提供数据的一方）：

- 应建立通过接入自动化工具提供数据的管理机制和工作流程，必要时应建立评估等机制设置接入条件，对接入的自动化工具进行尽职调查和个人信息保护影响评估；
- 数据提供方应当在向数据接收方提供个人信息前进行个人信息保护影响评估，并进行记录。
- 应与数据接收方通过合同等形式明确双方的安全责任、应实施的数据安全措施及双方法律义务与责任；在自动化工具处理数据的方式、目的、期限等发生重大变更时，如原合同没有条款说明，应对合同进行更新或签订补充协议等；
- 应向用户说明接入自动化工具的情况并明示该自动化工具由第三方提供，涉及收集处理个人信息的，应向用户告知数据接收方通过自动化工具收集处理个人信息的详细情况，并获得用户单独同意；
- 应妥善留存数据接收方接入有关合同和管理记录，确保可供相关方查阅；
- 应要求数据接收方建立响应用户请求、申诉等的机制，并妥善留存、及时更新，以供用户查询、使用；
- 应督促和监督数据接收方加强数据安全管理，发现第三方产品或服务没有落实安全管理要求和责任的，应及时通知该数据接收方，督促整改，必要时停止接入；
- 宜开展技术检测，审查该自动化工具是否存在漏洞，确保其数据收集、使用行为符合约定要求。

3) 数据接收方（即通过嵌入或接入自动化工具收集处理数据的一方）：

- 不应强迫任何单位或组织嵌入或接入可获取数据的自动化收集工具(如代码、脚本、接口、算法模型、软件开发工具包等)；
- 应与接入自动化工具的数据提供方通过合同等形式明确双方的安全责任及应实施的数据安全措施及双方法律义务与责任；在自动化工具处理数据的方式、目的、期限等发生重大变更时，如原合同没有条款说明，应对合同进行更新；
- 应制定开发者协议和隐私政策，公开个人信息收集使用规则；
- 应要求接入自动化工具的数据提供方配合向用户说明自动化工具接入及其收集处理数据的情况并明示该自动化工具由第三方提供，如涉及收集、使用个人信息的，应当要求数据接收方配合向用户告知收集处理个人信息的详细情况，并获得用户单独同意，必要时核验数据提供方的实现方式；
- 应妥善留存接入自动化工具的有关合同和管理记录，确保可供相关方查阅；
- 涉及收集处理个人信息的，应配合数据提供方及时响应用户请求、申诉等，并妥善留存、及时更新，以供用户查询、使用；
- 宜定期开展技术自检和自审等合规审计，确保其数据收集、使用行为符合规定或约定要求，如发现违规或超出约定行为，应当及时与接入产品或服务方沟通、采取措施确保合规；向接入产品或服务方提出合规建议或提供数据保护指引。

e) 完整可用要求

1) 数据提供方和数据接收方在传输数据过程中应进行身份认证，确保数据提供方和数据接收方的身份；

2) 数据传输过程中应对数据提供完整性校验；

3) 数据提供方和数据接收方应具备检测网络设备、应用系统、数据管理平台等数据在传输过程中完整性受到破坏的能力，以及数据完整性破坏后恢复数据的能力；

4) 传输数据经过的传输渠道和方式应合规合法，传输的数据如果涉及个人信息或个人敏感信息，应确保征得用户单独同意或符合法律法规规定的正当法律事由，并应告知传输敏感个人信息的必要信息以及对其权益的影响；

5) 在传输过程中，应保证数据经过处理仍具有可用性。

f) 安全保密要求

1) 传输过程中应进行身份鉴别，确保交易双方身份真实可信、不可抵赖。在通过网络传输用户个人信息数据时，宜使用安全协议，如 https；

2) 在对数据信息进行传输时，应在风险评估的基础上，采用合理的加密技术、协议。选择和应用加密技术时：

- 数据在传输过程中应加密，加密应符合国家密码管理相关要求；
- 宜根据风险评估确定保护要求，并确定加密算法的类型、属性，以及所用密钥的长度；
- 宜确定合适的保护要求，使用能够提供所需保护的合适的工具。

3) 根据数据的保密要求，在传输过程中宜使用数字签名、消息验证码等技术，以确保信息的不可否认性和完整性。使用数字签名时应符合国家政策关于数字签名的技术要求，包括且不仅限于：

- 应充分保护私钥的机密性，防止窃取者伪造密钥持有者的签名；
- 应采取保护公钥完整性的安全措施，例如：使用公钥证书；
- 应确定签名算法的类型、属性以及所用密钥的长度；
- 用于数字签名的密钥应不同于用来加密内容的密钥。

g) 数据提供方宜对数据接收方收集处理数据的行为进行审计，发现超出约定行为，应及时通知该数据接收方，督促整改，必要时停止接入；

h) 在数据传输过程中，应有完整的数据处理的相关记录，用于数据验证和核查。

5.1.6 数据删除

数据使用方使用数据，具体要求包括：

a) 数据使用目的达成后，应对数据进行删除或匿名化处理；

b) 涉及个人信息， 符合以下情形，个人信息主体要求删除的，应及时删除个人信息：

1) 数据使用方违反法律法规规定，收集、使用个人信息的；

2) 数据使用方违反与个人信息主体的约定，收集、使用个人信息的。

c) 数据使用方违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，数据使用方应立即停止共享、转让的行为，并通知第三方及时删除；

d) 数据使用方违反法律法规规定或违反与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，数据使用方应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

5.1.7 安全事件处置

参与方应具备安全事件处置能力，具体包括：

a) 应制定数据安全事件应急预案；

b) 应定期(至少每年一次)组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程；

c) 发生数据安全事件后，数据使用和传输主体应根据应急响应预案进行以下处置：

1) 记录事件内容，包括但不限于：发现事件的人员、时间、地点，涉及的数据及规模，发生事件的系统名称，对其他互联系统的影响，是否已联系执法机关或有关部门；

2) 评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；

3) 按照有关规定及时上报，报告内容包括但不限于：涉及用户的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式；

4) 当法律法规变化或事件处置情况有变化时，应及时更新应急预案。

5) 安全事件告知

除采取措施能够有效避免信息泄露、篡改、丢失造成危害的以外，发生或者可能发生个人信息泄露、篡改、丢失的，应当立即采取补救措施，并通知履行数据或个人信息保护职责的部门和个人：

1) 应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的用户。难以逐一告知用户时，应采取合理、有效的方式发布与公众有关的警示信息；
2) 告知内容应包括但不限于：安全事件的内容和影响；已采取或将要采取的处置措施；用户自主防范和降低风险的建议；针对用户提供的补救措施；数据处理者的联系方式。

5.2 场景安全要求

5.2.1 场景描述

场景描述可参考附录A。

5.2.2 程序化购买

程序化购买场景中数据安全要求如下：

a) 在任一方接入程序化购买平台之前，各方应签订数据安全协议，规定各方的数据安全责任和义务；
b) 在程序化购买过程中，供给方平台(SSP)和广告交易市场（ADX）应对信息收集过程向用户进行充分披露，并保存相应的证据。广告投放服务（Ad Serving）和需求方平台（DSP）可要求供给方平台（SSP）和广告交易市场（ADX）提供相应的授权证明；
c) 在程序化购买过程中，数据提供方应该只传递最小必要的已授权用户信息，不能泄露用户的固定唯一标识符。各方在程序化购买过程中使用加密手段来保护用户固定唯一标识符的，应该确保来自同一用户或设备的信息可识别。应优先使用符合 T/CAAAD 003-2020 标准要求的广告标识符；
d) 在程序化购买过程中，各方应使用数字签名、唯一时间戳等多种手段确保交易关键信息不被篡改、不可抵赖；
e) 在程序化购买过程中，各方产生的交易记录应安全保存，以备各方审计；
f) 在程序化购买过程结束后，各方均应遵照数据安全协议约定执行。

5.2.3 广告监测

广告监测场景中数据安全要求如下：

a) 如果媒体/广告主植入监测公司的 SDK，监测公司应将 SDK 收集数据所需要的权限告知媒体/广告主，并取得媒体/广告主授权同意；
b) 媒体/广告主应在隐私政策中预先将广告监测可能索要的权限向用户进行告知，并取得用户授权同意；
c) 媒体、广告主应在隐私政策中将广告监测需要收集的数据，以及收集数据的目的、方式、范围向用户进行告知，并取得用户授权同意；如果媒体/广告主使用监测 SDK 的，还应将监测 SDK 名称向用户告知；
d) 监测方应当在其隐私政策中明确告知用户可以撤回收集、使用其个人信息同意授权的方法。若用户撤回同意后，监测公司后续不得再处理相应的个人信息；撤回同意不影响撤回前基于同意的个人信息处理；
e) 监测公司不得收集与提供广告投放监测服务无关的个人信息，符合本条要求收集的数据类型和用途，可参考附录 B；
f) 监测公司的数据收集、存储、处理、计算系统应满足以下要求：
   1) 广告监测数据应以数据传输原始格式分别在媒体平台及监测公司系统中至少保存 2 年，如果有法律法规对数据保存时间另有规定，应以法律法规的规定为准；
   2) 若广告主、媒体或相关方应个人信息主体请求，要求监测公司删除原始监测数据，应出示个人信息主体要求删除个人信息的证明；

注：根据GB/T 35273的定义，此处“删除”是指在实现日常业务功能所涉及的系统中去除个人信息的行为，使其保持不可被检索、访问的状态。

   3) 监测公司应在媒体配合下，遵循数据安全要求对的数据进行收集，应保证数据准确、完整地传输、存储、处理、计算。

5.2.4　广告效果评估

广告效果评估场景中数据安全要求如下：

a)　数据收集：此过程中通过技术手段收集广告监测数据与广告互动效果数据信息，如果涉及到个人信息，市场研究公司或媒体方应在信息收集前向个人信息主体说明信息收集类型及用途，并应获得个人信息主体授权同意后方可进行；

b)　数据处理：此部分包含数据存储，数据传输及数据计算，市场研究公司与数据处理方应该建立严格的审批与数据安全管理机制，防止用户信息泄露及随意扩大商业用途，宜预先采用加密技术或去标识化技术使得数据对市场研究公司与数据处理方为匿名；

c)　报告产出：移动互联网广告效果评估报告仅以聚合报告形式呈现给广告主。

5.2.5　异常流量排查和反作弊

异常流量排查和反作弊场景中数据安全要求如下：

a)　识别异常流量的安全性要求

判定为异常的原始数据均应保留至少2年，识别为无效的流量应做好标记，以备需要复核时提供判定依据。

b)　无效流量复核时安全性要求

对判定结果复核时，监测机构、媒体、广告主三方应提取异常数据样本或全部复核，样本提取应遵守最少够用的原则，各方负有对涉及的数据和判定依据保密的义务。

c)　无效特征提炼的安全性要求

通过数据分析完善反作弊算法，应对新型的作弊手段，新的算法规则应该严格保密，在企业内部数据的存储、访问上都应该设置严格的权限机制。

d)　制作、管理和使用行业公共无效流量定义数据的要求

行业协会组织成员企业制作无效流量定义名单数据时，允许使用移动设备和智能电视等用于广告用途的识别标识的之未加密原始数据值、加密数据值等多种数据格式，以满足甄别无效流量的目的。数据提供、加工、使用的各方应本着最小化的使用场景原则使用数据，并限制上述数据仅在本企业内使用。应用区块链技术实现安全技术要求的先进技术指引可参考附录C。

6　互联网广告应用数据交换接口定义

6.1　数据交换接口定义

6.1.1　概述

在广告交易参与方之间的网络连接基本协议采用HTTP/HTTPS协议，并且开启长连接模式，用于减少连接的处理时间。

多个参与方应该根据业务需要减少交换接口连接的超时时间，超时时间不大于100毫秒。

多个参与方数据交换接口应该采用HTTP POST方式，用于满足大量数据请求的场景。

多个参与方数据交换接口的请求与响应的应用层数据格式应该约定为Protobuf格式，具体的字段描述详见本文件6.1.2和6.1.3节。请求和响应消息内容的MIME类型填写为：Content-Type: application/x-protobuf

6.1.2　交易请求

6.1.2.1　总章

交易请求按照协议格式封装请求数据，数据包含DSP报价依赖的交易基本信息（交易请求信息、广告位信息、曝光信息、交易信息、格式信息）、受众信息（用户信息、设备信息、地理位置信息）以及展示环境信息（网站信息、移动应用信息、视频信息、私有交易），通过对象来封装。

对象的描述和对应的章条见表1。

表1 对象和章节对应关系

对象	章节	描述
交易请求（Bid Request）	6.1.2.2	最高层对象，包含所有交易相关信息
曝光信息（Impression）	6.1.2.3	曝光中创意的要求信息
广告位信息（Banner）	6.1.2.4	曝光所处的广告位的属性、媒体设置等信息
用户信息（User）	6.1.2.5	广告受众的属性、兴趣等信息
设备信息（Device）	6.1.2.6	广告最终展现所在的设备的系统、型号等信息
网站信息（Site）	6.1.2.7	广告最终展现所在的网站信息，适用于网页广告
移动应用信息（App）	6.1.2.8	广告最终展现所在的移动应用信息，适用于移动应用广告
视频信息（Video）	6.1.2.9	广告最终展现所在的视频广告信息
私有交易（PMP）	6.1.2.10	PMP广告请求传输的广告活动参数
地理位置信息（Geo）	6.1.2.11	广告受众/设备的位置信息
原生信息（Native）	6.1.2.12	原生请求内容
交易信息（Deal）	6.1.2.13	广告交易价格等信息
格式信息（Format）	6.1.2.14	广告展示格式

6.1.2.2 交易请求 BidRequest

字段	类型	必填	缺省值	说明
consentObtained	bool	是	False	交易请求信息中所包含个人信息的收集是否获得用户同意，True为同意，False为不同意，后续的信息处理可据此字段做相应调整
id	string	是		标识竞价请求的唯一ID，由ADX提供
impressions	Impression array	是		曝光对象数组，至少包含一个对象
user	User	否		用户对象，包含使用设备的人类用户或广告受众的细节信息
device	Device	否		设备对象，包含展示广告的用户设备的细节信息
site	Site	否		网站对象，包含媒体网站的细节信息
app	App	否		应用程序对象，包含媒体App的细节信息
test	bool	否	False	测试标识，值为true时，该次请求为测试流量，不会真实展现，但DSP还是需要完成正常的处理流程并返回

6.1.2.3 曝光信息 Impression

字段	类型	必填	缺省值	说明
impression_id	string	是		在交易请求中这个曝光的唯一标识,是程序化交易系统基本的曝光流水号，如果采用整数，建议使用64位整数
banner	Banner	否		普通曝光对象
video	Video	否		视频广告对象
native	Native	否		原生广告对象
pmp	Pmp	否		私有市场广告对象
tagid	string	是		广告位id
imptype	int32	是		定义广告曝光类型，比如来自图形广告、原生广告或者视频广告等;也可以定义为来自某种特定的交易模式，比如实时竞价交易，私有化交易等定义

6.1.2.4 广告位信息 Banner

字段	类型	必填	缺省值	说明
format	Format array	否		允许的尺寸信息，建议填写
width	int16	否		像素宽，未填写format信息时建议填写
height	int16	否		像素高，未填写format信息时建议填写

6.1.2.5　用户信息 User

字段	类型	必填	缺省值	说明
id	string	否		ADX提供的用户id
buyeruid	string	否		买家提供的映射到ADX的用户id，id和buyeruid至少提供一个
yob	int32	否		出生年份
gender	string	否		性别，M-男，F-女，O-其他
keywords	stirng	否		关键词，逗号分隔

6.1.2.6　设备信息 Device

字段	类型	必填	缺省值	说明
ua	string	否		浏览器useragent
ipv4	string	否		ipv4地址
ipv6	string	否		ipv6地址
devicetype	int16	否		定义设备类型
make	string	否		设备制造商
model	string	否		设备型号
os	string	否		操作系统
osv	string	否		操作系统版本
hwv	string	否		硬件版本（例如iphone中的5s）
height	int16	否		高
width	int16	否		宽
ppi	int16	否		每英寸像素数，像素密度
pxratio	float	否		物理像素和独立像素比例
js	int	否		是否支持js，0-否，1-是
geofetch	int	否		支持banner中js代码获取地理位置信息，0-否，1-是
language	string	否		浏览器语言
carrier	string	否		运营商
geo	Geo	否		地理位置信息
connectiontype	int16	否		定义用户端设备联网方式
didmd5	string	否		硬件设备号，md5 hashed
didsha1	string	否		硬件设备号，sha1 hashed
dpidmd5	string	否		平台设备号，md5 hashed
dpidsha1	string	否		平台设备号，sha1 hashed
macmd5	string	否		Mac地址，md5 hashed
macsha1	string	否		Mac地址，sha1 hashed
macsha256	string	否		Mac地址，sha256 hashed
idfa	string	否		IDFA
oaid	string	否		OAID
caid	string	否		CAID

6.1.2.7　网站信息 Site

字段	类型	必填	缺省值	说明
id	string	否		ADX指定id
name	string	否		网站名称
domain	string	否		网站域名
cat	string array	否		网站分类
page	string	否		页面url
ref	string	否		Referrer url
keywords	string	否		逗号分隔的关键词

6.1.2.8　移动应用信息 App

字段	类型	必填	缺省值	说明
id	string	否		ADX置顶app ID
name	string	否		移动应用App名称
bundle	string	否		平台定义的应用唯一标示(Android中的 包名，IOS中的 numeric ID)
ver	string	否		版本号
storeurl	string	否		应用商店中的安装地址
keywords	string	否		逗号分隔的关键词

6.1.2.9 视频信息 Video

字段	类型	必填	缺省值	说明
mimes	string array	否		支持的内容Mime类型
minduraion	int16	否		最短时间（秒）
maxduration	int16	否		最长时间（秒）
protocols	string array	否		支持的协议
width	int16	否		播放器宽度
height	int16	否		播放器高度

6.1.2.10 私有交易 PMP

字段	类型	必填	缺省值	说明
private_auction	bool	是	True	True私有交易，False公有交易
deals	Deal array	否		Deal列表

6.1.2.11 地理位置信息 Geo

字段	类型	必填	缺省值	说明
lat	float	否		纬度（-90.0 ~ 90.0）
lon	float	否		经度（-180.0 ~ 180.0）

6.1.2.12 原生信息 Native

字段	类型	必填	缺省值	说明
request	string array	否		原生请求内容

6.1.2.13 交易信息 Deal

字段	类型	必填	缺省值	说明
id	string	是		Deal id
bidfloor	float	否		最低价格

6.1.2.14 格式信息 Format

字段	类型	必填	缺省值	说明
width	int16	否		像素宽（和比例尺寸选填一种）
height	int16	否		像素高
wratio	int16	否		比例尺寸的相对宽度
hratio	int16	否		比例尺寸的相对高度
width_min	int16	否		比例尺寸的最小像素宽

6.1.3 交易响应

6.1.3.1 交易响应信息 BidResponse

字段	类型	必填	缺省值	说明
id	bool	是		对应的交易请求id
seatbids	SeatBid array	否		Seatbid数组，至少一个
bidid	string	否		交易者产生的本次交易的唯一id

6.1.3.2　交易席位 SeatBid

字段	类型	必填	缺省值	说明
bids	Bid array	是		交易数组，至少一个
seat	string	否		本次出价的交易者座位id

6.1.3.3　交易信息 Bid

字段	类型	必填	缺省值	说明
id	string	是		交易者产生bid id，用于日志/跟踪
impid	string	是		对应请求中的imp id
price	float	是		交易价格
nurl	string	否		交易成功通知url
adm	string	否		交易成功后传输的创意内容，支持宏替换
adid	string	否		交易成功后的预加载广告id
dealid	string	否		对应的deal id
imptrackers	string array	否		曝光监测地址数组
clicktrackers	string array	否		点击监测地址数组

由于交易响应时返回的创意内容部分结构差异较大，故此处未列，可参考IAB的OpenRTB Dynamic Native Ads API Specification。

6.1.4　交易响应校验规则

交易响应返回的内容包含很多需要校验的内容，多个参与方确保以下原则基础上可自行设立：

a)　字段内容合法检测；
b)　竞价者 id 检测；
c)　创意类型检测，返回的创意符合请求中的要求；
d)　id 检测，返回的各个 id 与请求中的对应 id 一致；
e)　内容审核，创意内容遵守相关要求。其中预加载创意可以事先审核，后加载可以抽样审核。

6.1.5　交易胜出通知

宏替换是实时竞价交易中常用的参数返回方法，采用${macro_name}的形式，以下列举常用宏：

a)　点击宏：

宏名称	说明
user_id	用户id
request_id	请求id
imp_id	曝光id
adid	广告id
price	价格
ip	Ip地址
timestamp	时间戳
oaid	oaid

b)　价格宏：

价格属于敏感信息，在回传时应该先进行加密。

c)　自定义宏：

宏名称	说明
data	用户数据回传，内容可由用户自行定义，采用base64编码

6.1.6　第三方监测应用

在本文件6.1.3.3的定义中已经包含了可以添加第三方监测的字段（imptrackers, clicktrackers），只需要将确认的第三方监测地址添加进去，由媒体方在曝光或者点击发生后向该地址发送请求即可。

6.1.7　唯一标识符（ID）映射

在互联网广告交易过程中，参与方之间交换同一个用户的数据，需要通过唯一标识符（ID）映射，使得在不同参与者数据体系内的数据可以打通交换。在符合本文件5.1要求的前提下，建立唯一标识符（ID）映射的流程如下：

a） 客户端 ID 映射：

用户加载网页代码时候，同时加载多个参与方的代码，互相调用映射接口传输ID信息。

b） 服务端 ID 映射：

用户加载网页代码时候，由服务端转发携带ID的请求，由一个参与方服务器告诉其他参与方相关ID信息。

6.2 标签用数据交换接口定义

6.2.1 概述

在互联网广告交易中，各参与方有信息交换需求，例如人口统计信息、标签信息、消费记录等等，这些信息不能直接进行交换，必须在符合本文件5.1章要求的前提下，通过制定标签数据接口，进行交换。

6.2.2 标签用数据交换接口定义基本原则

接口定义的基本原则应符合以下几点：

a） 安全性，传输上采用安全的模式，数据内容要求加密，接口访问应有版本认证机制；

b） 接口定义支持版本向前向后兼容；

c） 交换数据带有核对标识，用于核对和追溯；

d） 协议应采用序列化高效、可压缩、传输量小的文件格式，用于适应大量数据传输。

6.2.3 协议格式

数据交换协议格式可以约定为protobuf或者thrift。详细字段可以由具体的各参与方自行决定，但至少应包括以下字段：

字段名称	类型	说明
id	string	唯一id，用于跟踪 / 日志 / 核对本条记录
ver	string	版本
sndid	string	在发送方的受众用户id（符合加密规范）
rcvid	string	在接收方的受众用户id（符合加密规范）
timestamp	int64	记录生成时间戳

7 互联网广告应用数据交换升级要求

7.1 基本要求

互联网广告应用数据交换升级涉及媒体，代理，广告主，第三方监测等多个参与方，在升级时各方要遵循相同的规则，做到各方在升级前后数据交换仍能顺利进行。

a） 数据格式升级应做到向前向后兼容；

b） 升级时间点各方应尽量保持一致，如果有时间差，可利用第一条做到兼容；

c） 对于升级内容，在升级前应通知到各方，并得到认可，如有异议可暂缓升级；

d） 多方交换场景中，各参与方推荐或者自荐产生一位执行者，具体执行升级流程。

7.2 升级流程要求

互联网广告具体升级流程如图1所示，具体要求如下：

a） 各参与方提出数据交换升级需求；

b） 由执行者整理需求，向各参与方提交数据交换升级要求；

c） 各参与方确认后反馈给执行方（应包含各参与方升级所需时间），如果有反对意见则返回第二条继续执行；

d) 执行者确定最终升级时间和升级资料并告知各参与方；
e) 各参与方按照约定升级；
f) 各参与方升级完成汇报；
g) 执行方检查升级结果并汇报。

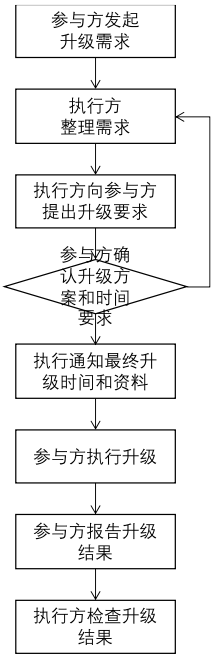
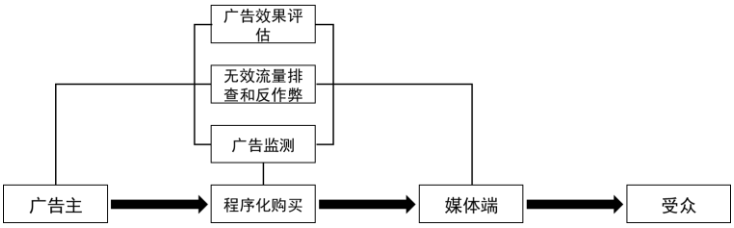


图1　升级流程

附　录　A
（资料性）
互联网广告数据应用场景

A.1　总体技术架构

互联网广告数据应用场景一般包括程序化购买、广告监测、广告效果评估、无效流量排查和反作弊等场景。涉及的实体包括广告主、媒体、受众，实体间的关联如图A.1所示。



图A.1 互联网广告实体关系图

A.2　数据应用场景

A.2.1　程序化购买

程序化购买主要涉及到以下各方：

a) 广告主：广告活动发起方；
b) 媒体方：广告活动实施方；
c) 平台方：包括供给方平台 SSP、广告交易市场 ADX、需求方平台 DSP、广告投放服务系统 Ad Serving、第三方数据管理平台 DMP、第三方无效流量过滤服务平台、三方监测系统等，按照各自平台分工，协助广告主与媒体进行广告过程。

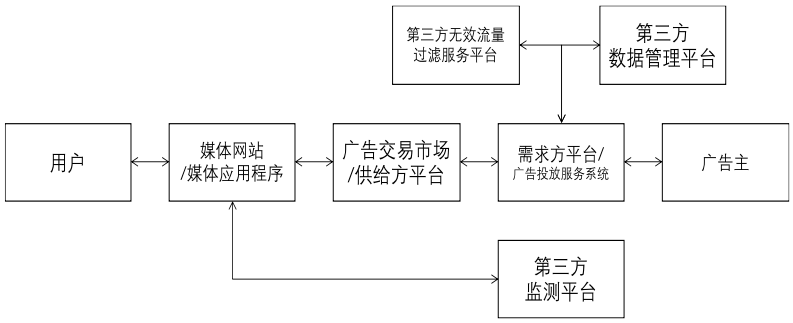
在程序化购买场景中，采用开放式实时竞价协议规范（OpenRTB）。实时竞价过程是指用户在访问媒体网站或媒体应用程序上的广告位置时，该广告位置接入的供给方平台SSP或者广告交易市场ADX会根据OpenRTB将广告请求数据封装在竞价请求中，并发送给多个对接的需求方平台DSP或广告投放服务系统Ad Serving，广告请求数据通常包括：用户信息、设备信息、地域信息、媒体信息等，各DSP或Ad Serving根据自身的竞价策略决定是否参与竞价，并将结果回复。

在实时竞价过程中，如广告主需要使用第三方数据管理平台（DMP），在使用前置机情况下，DSP或Ad Serving系统在竞价决策过程中会向第三方DMP前置机发送设备标签查询请求，请求中携带设备信息，第三方DMP前置机回复该设备命中的标签情况。

在实时竞价过程中，如广告主需要使用第三方无效流量过滤服务平台，DSP或Ad Serving平台在竞价决策过程中会向第三方IVT过滤服务前置机发送本次流量IVT查询请求，请求中携带本次请求中的设备信息、IP信息等，第三方IVT过滤服务前置机回复本次流量的IVT得分情况。

ADX或SSP收到回复后，根据竞价规则将获胜的DSP回复的广告展示给用户。

广告展示给用户以及用户点击广告事件后，在C2S模式下，用户的客户端向DSP、Ad Serving或第三方监测系统发送广告展示通知、广告点击通知，在服务器端到服务器端S2S模式下，用户客户端向ADX或SSP上报广告曝光量、广告点击事件后，再由ADX或Ad Sercing的服务器端向DSP、Ad Serving发送广告展示通知、广告点击通知。



图A.2 程序化购买实体关系图

A.2.2　广告监测

广告监测主要涉及到以下各方：

a)　广告主：广告主一般作为数据使用方，使用监测公司收集的数据，对于部分需做归因分析的广告监测场景，广告主亦可能提供数据；

b)　媒体：媒体支持监测数据发送服务，一般需要在广告位支持集成监测代码；

c)　广告监测公司：监测公司作为数据收集方，与媒体&广告主进行监测对接，通过不同集成方式进行监测数据接收，并在广告事件发生后收集事件信息、进行处理。

广告监测的一般场景为：在广告活动开始前，广告主或者代理公司向媒体、广告投放公司以及广告监测公司提供广告活动排期，广告监测公司根据排期出具监测代码，媒体或者投放方对不同广告点位添加对应的监测代码。在广告活动进行过程中，每当有曝光或者点击等需要监测的行为发生时，由媒体向监测公司发送一条监测请求。监测公司根据收到的监测请求记录曝光、点击等指标，并根据收集到的数据进行处理生成报告和服务。

广告监测场景中的数据来自媒体（对于部分需做归因分析的广告监测场景，广告主亦可能提供数据），由监测公司进行收集。应用数据过程一般是：

a)　监测公司根据广告主排期出具监测代码，并由媒体集成在广告位上，监测代码集成方式包括SDK、JS、监测链接等；

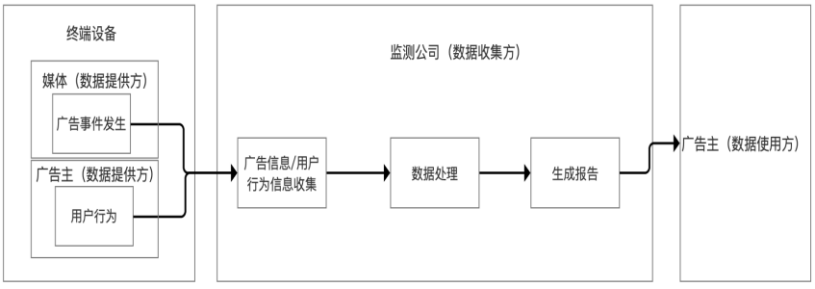
b)　广告主的客户端/站点集成监测公司的归因分析代码用以收集用户行为信息，集成方式包括SDK、监测链接等；

c)　执行广告投放，在广告投放过程中，每当有曝光或者点击等需要监测的行为发生时，监测公司收集广告信息；

d)　监测公司根据收集到的信息记录曝光、点击等指标，并根据收集到的数据进行处理、生成报告，报告提供给广告主。

e)　监测公司收集广告主的客户端/站点上的用户行为信息（例如，用户激活/注册），并根据收集到的数据进行处理、生成报告，报告提供给广告主。

上述过程中，b）、e）在需要做归因分析的广告监测场景才发生。



图A.3 广告监测实体关系图

A.2.3　广告效果评估

广告效果评估主要涉及到以下各方：

a) 广告主：互联网广告效果评估的发起者，以获取广告效果评估报告为项目目的并依此来优化其广告营销策略；

b) 平台方：通常为媒体平台或数据平台，根据市场研究公司的要求协助完成移动互联网广告效果评估所需数据的收集；

c) 市场研究公司：依据广告主要求设计及执行移动互联网广告效果评估项目。

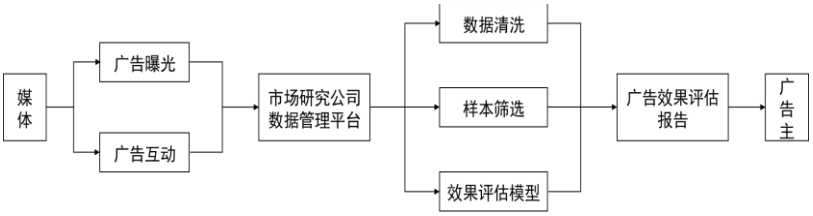
移动互联网广告的效果评估，需要以用户感知为中心，以用户对广告的逐步接受过程为依据，评测他们在每个阶段被广告影响的程度，从而形成完整的对移动互联网广告效果的评估体系。其实施过程简要描述如下：

a) 广告监测数据收集：在广告活动开始前，市场研究公司依照广告主提供的广告投放排期生成监测链接，并交由媒体或平台方依照广告投放排期在其广告版位上部署。在广告活动进行过程中，每当有曝光或者点击等需要监测的行为发生时，由媒体或数据平台向监测公司发送监测请求；

b) 广告互动效果相关数据收集：通过技术手段（包括但不限于加码监测，在线调研，数据合作及多种数据收集方式综合完成等）获取用户对移动互联网广告或广告品牌的响应、认知变化等数据；

c) 数据存储：市场研究公司对接收到的广告监测数据及广告效果相关数据进行清洗后，按照广告曝光、点击、互动、品牌认知、品牌推荐等进行分类存储；

d) 数据处理及报告产出：市场研究公司的监测系统会对广告监测数据和广告互动效果数据通过反作弊算法过滤掉无效流量，然后通过用户标识进行匹配，匹配成功即为一个有效转化样本，进而结合收集到的所有有效数据综合评估及产出本次广告效果评估报告。



图A.4 广告效果评估实体关系图

A.2.4　异常流量排查和反作弊

异常流量排查和反作弊主要涉及到以下各方：

a) 广告主：监测活动发起方，在监测公司集成 SDK/代码，在监测单元下生成监测短链代码，部署监测链接到媒体方的广告投放计划下。同时，广告主选择监测公司是否回调转化数据给媒体；

b) 媒体方：支持监测数据发送服务。媒体方需要保证监测代码和广告信息对应无误，在移动端需要支持代码或者 SDK 的监测方式并保证正确装载监测代码；

c) 监测公司：通过不同集成方式，提供监测短链和监测数据接受服务，与媒体方进行监测接口对接。

异常流量是指各方在开展广告业务过程中，通过技术方式识别出来的存在问题的非常规流量，这些问题可能是由于伪造流量，或机器人、爬虫等行为导致。无效流量指对识别出来的异常流量进行复核，被各方共同认定为不应被正常统计的广告流量。无效流量的定义应符合GB/T34090.2或者T/CAAAD 002-2020的相关规定。

涉及到应用数据的过程主要有：

a) 异常流量识别

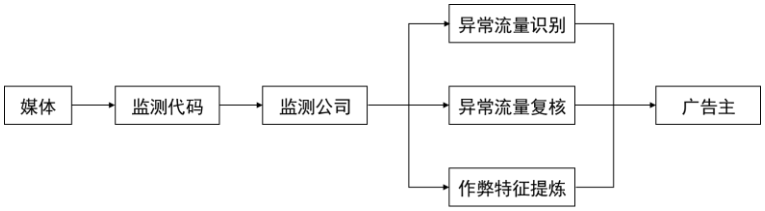
各方均有义务基于行业认可的标准，识别异常流量和反作弊。

b) 异常流量复核

判断为异常的流量，在媒体或广告主需要对判定结果复核时，需要监测机构、媒体、广告主三方在数据安全规范的条件下进行，提取异常数据样本或全部复核。

c) 作弊特征的提炼

对新型的作弊手段，各方均有可通过数据分析，提炼出共性特征，完善现有反作弊规划或丰富黑名单库。



图A.5 异常流量排查和反作弊实体关系图

附 录 B
（资料性）
广告投放监测服务的必要信息

在广告监测场景中监测公司不得收集与提供广告投放监测服务无关的个人信息。
表B.1列出广告投放监测服务收集的必要数据示例。

表B.1 一般无效流量监测字段

序号	字段	说明	是否必须
1	事件类型	描述业务或转化的信息，例如曝光、点击等	是
2	广告系列 ID	包括广告活动、媒体、广告位等信息，至少包含广告唯一 ID	是
3	时间戳	格林威治时间 1970 年 01 月 01 日 00 时 00 分 00 秒(北京时间 1970 年 01 月 01 日 08 时 00 分 00 秒)起至现在的总秒数	是
4	IP 地址	用户端 IP 地址，不能为直接用户通过接入互联网服务商所获得的互联网 IP 地址以外的 IP	是
5	请求方式	HTTP 协议中的请求方式，如 GET、POST 和 HEAD 等	是
6	用户代理信息	网页为包含浏览器和操作系统的 User-Agent 完整字符串，PC 客户端（如视频客户端）和移动 App 应含有 App 名称、App 版本及操作系统等基本信息	是
7	COOKIE/设备唯一标识符	用户的唯一标识，需满足网页端可读写 COOKIE 或移动端可获取到设备唯一标识的情况下可用	是
8	预加载 HEADERS	如 X-MOZ/FireFox,X-Purpose/Safari 等	否
9	适用的 OpenRTB 属性	投标唯一标识、广告位类型、请求安全协议标识符等	否
10	广告页面 URL	当广告展示在网页、移动网页或任何通过浏览器使用 http 或 https 协议可以访问的页面时	是
12	App 程序完整包名	仅当广告展示在移动 APP 内部时	是
13	位置信息	需注明所使用的坐标系规格	否
14	请求状态码	HTTP 请求返回的状态码，如 200、302、400 等	否
15	视频/音频广告开始播放的标志	仅当视频/音频广告需要被用户点击然后开始播放的场景	是

附　录　C
（资料性）
区块链技术应用于互联网广告技术指引

基于对技术发展的探索，以及响应党中央对区块链技术的使用号召，在本文件内探讨可行的基于区块链与分布式存储技术的解决方案。本附录主要目标是，为本文件正文中如数据收集（5.1.2）、数据使用（5.1.3）提供强制技术执行的可能性解决方案；为数据存储（5.1.4）、数据传输（5.1.5）等部分提供更安全和高效的技术可能性解决方案；为交易请求（6.1）部分提供了安全的可能性解决方案。

考虑到区块链技术的成熟程度和各企业技术水平差异，本附录仅提供技术概念和可能性方案以及给出相应的过渡性方案。

C.1　技术简介

C.1.1　什么是区块链技术

区块链是一项信息技术领域的术语，是一串使用密码学方法相关联产生的数据块，从本质上讲，它是一个去中心化的共享数据库，存储器中的数据和信息，具有“不可伪造”、“全程留痕”、“可以追溯”、“公开透明”、“集体维护”等特征。基于这些特征，区块链技术奠定了坚实的“信任“基础，创造了可靠的“合作”机制，具有广阔的运用前景。

C.1.2　什么是智能合约

智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议，在区块链内制定合约时使用，目的是提供优于传统合约的安全方法，并减少与合约相关的其他交易成本。智能合约中内含了程式码函式，可以与其他合约进行互动、做决策、储存资料及传送资产等功能。区块链上所有的用户都可以看到基于区块链的智能合约。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

C.2　技术优势

C.2.1　不可篡改性

区块链是一个分布式的不可篡改的数据存储系统,新的数据产生时,需要区块链中所有节点的审核。同时，区块链的非对称加密技术，通过私钥进行数字签名，并通过私钥产生的公钥对签名进行认证，任意单一节点都不能修改已有记录。哈希算法是区块链中保证交易信息不可篡改的单向密码体制，无法通过输出散列的内容推断出任何与原文有关的信息。通过哈希算法，可对一个区块的所有交易信息进行加密，并把记录内容压缩成一串数字和字母组成的字符串，这个字符串无法反推出原来的内容。基于输出散列与输入原文一一对应的特性，哈希算法可以被用于验证信息是否被修改。确保在数据传输过程中所有记录的安全性。

C.2.2　可溯源性

区块链是一个分散的数据库，将数据分散存储在互相链接的各个节点上，不受单一服务器控制。分散数据库记录了区块链上的每一次操作记录，天然适合解决数据记录与溯源问题。

C.2.3　安全自治性

区块链的智能合约即一段预先编写并对各方公开的代码，此代码在部署之后会基于预先设定的程序与相关条件在区块链上全自动执行，其中无法进行人为干预。这样大大降低了由于人为疏忽或黑客攻击造成的数据泄漏问题。另外，因为合约代码完全公开，既降低了代码审计成本，又提升了业务流程的标准性。

C.3　技术局限

当前区块链项目，在信息吞吐量、网络延迟、容量和带宽、能耗及商业应用等不同方面指标体现出区块链技术仍存在局限性。尤其目前公有区块链并不适合企业使用。区别于公有链，行业联盟链是指有

若干个行业机构共同参与管理的区块链，每个机构都运行着一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送,并且共同来记录交易数据。尽管行业联盟链具备部分去中心化、可控性强、数据私密、交易速度快等优点，仍存在无法与传统企业技术融合、流通效率低等弊端。并且，行业联盟链在技术上也落后于公有链及其生态的迭代速度。

C.4 参考解决方案

基于技术局限性的考虑，当前区块链技术在广告行业的应用讨论更多集中在在广告投放前（例如目标用户人群分析等）与广告投放后（例如投放历史数据沉淀等）。而广告投放执行期间使用区块链技术则需等待该技术进一步发展。

C.4.1 数字身份加密

在本文件5.1.3 e)数据使用安全保密性中已经说明对数据的加密脱敏的要求。区块链本身基于密码学技术可以妥善加密敏感数据，并且在使用中确保安全性同时可以生成加密Hash作为匹配依据。

C.4.2 数据收集与隐私防护

区块链技术可以在数据应用环节中，进行最细颗粒度的权限控制与记录。并且过程中会产生相应的不可篡改的痕迹。收集数据的同时区块链的加密技术能够确保传输中的安全性。在区块链权限控制系统的普及之下，用户可以更好的掌控自己数据的被使用情况以及随时控制自己数据开放程度。

C.4.3 数据传输与隐私防护

利用区块链技术可以更快捷有效的进行数据传输，同时加强隐私防护。在数据上链过程中，通过打通Hash唯一标识符，串联起多方数据，以统一标准在智能合约中进行数据匹配，完成数据传输。基于智能合约，在完成数据传输或调用的过程中，数据将留下不可篡改的调用痕迹，个人信息和敏感信息可用而不可见，从而达到数据使用（5.1.3）的保密要求。

C.4.4 自动化反作弊

基于区块链技术可优化本文件5.2.5中对异常流量的排查和反作弊。可以安全的自动化打通多数据源，并且可以给予预设的代码进行作弊检验。又由于数据可以通过Hash关联，使得各方数据可以串联验证用户行为真实性。

C.4.5 数据存储

为确保数据的可用性和永续性（5.1.4中的多项要求），并同时享受到区块链技术带来的安全与可信环境，则需引入新型的分布式存储技术来解决区块链存储效率低，成本高的弊端。例如，可以使用IPFS（星际文件存储协议）存储广告监测数据，并将唯一永久可用的IPFS地址放置到区块链事务中，而不必将数据本身放在区块链中。

C.4.6 过渡方案以及推进过程与建议

目前行业内已有基于区块链的尝试性解决方案，主要为投放准备期的数据传输协同，投放后的数据确权上链与加密存储。

例如，为加强广告行业区块链系统中多方参与者数据的隐私防护，需要对上链的用户数据进行加密保护。在需要进行隐私求交的场景下，可以通过部署安全可靠的可信计算环境与加密信道执行计算，并接受其他各方参与者的审计。可信计算环境中隐私求交计算求出的明文数据后，进行签名，并将签名信息上链，可供参与方用来核验数据的真实性。

但由于行业各方在区块链技术储备上各不相同，整体推进速度受限，目前在本文件附录A中的前置机（A.2.1给出方案）解决方案依然是很好的过渡性方案。在行业推进过程中会逐步向区块链方案过度。

参 考 文 献

[1]中华人民共和国网络安全法
[2]中华人民共和国广告法
[3]中华人民共和国数据安全法
[4]中华人民共和国个人信息保护法
[5]电信和互联网个人信息保护规定
[6]互联网广告管理暂行办法
[7]国家网络安全事件应急预案
[8]APP违法违规收集使用个人信息行为认定办法
[9]数据安全管理办法（征求意见稿）
[10]《网络数据安全管理条例（征求意见稿）》
[11]OpenRTB Dynamic Native Ads API Specification
（https://iabtechlab.com/wp-content/uploads/2016/07/OpenRTB-Native-Ads-Specification-Final-1.2.pdf）。
[12]https://developers.google.com/ad-exchange/rtb/response-guide/decrypt-price#encryptionscheme

团体标准

互联网广告数据应用和安全技术要求

T/CAAAD 001-2021　　T/CCSA 329-2021

*

中国广告协会

地址：北京市朝阳区西大望路甲 12 号通惠国际传媒广场 2 号楼 4 层
邮编：100124
电话：010-59725102
网址：www.china-caa.org

中国通信标准化协会

地址：北京海淀区花园北路 52 号
邮编：100191
电话：010-62302735
电子版发行网址：www.ccsa.org.cn