



2021年移动广告反欺诈白皮书

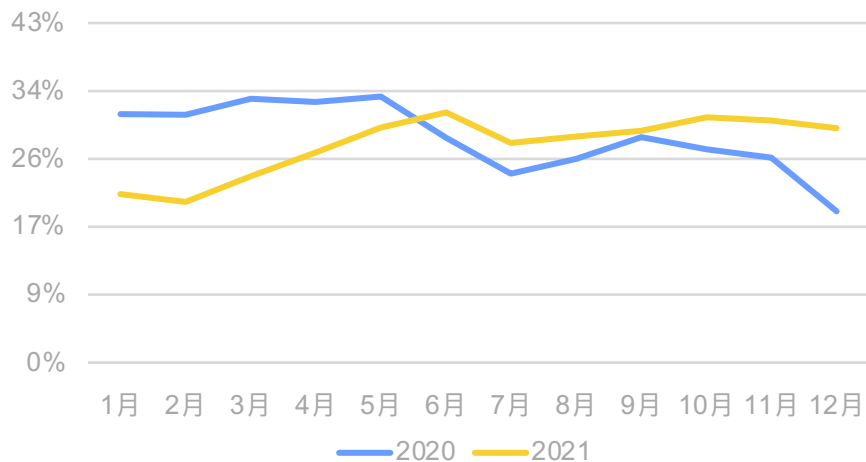


主要观点

1 2021年移动广告请求阶段异常流量占比为 27%，反欺诈形式依然严峻

2021年移动广告请求阶段的异常流量占比为 **27%**，较2020年略微减低。2021年的异常流量占比并未延续2020年9月开始的下降趋势，而是从3月开始上涨，6月达到顶峰，后一直保持在30%左右，整体反欺诈形式依旧严峻。上半年异常流量上升可能与广告主投放需求增加及公安部“净网2020”威慑力逐渐减弱有关。

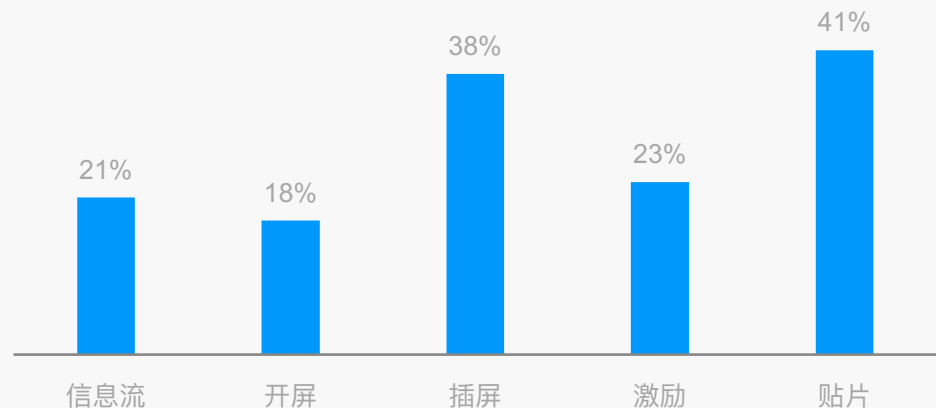
异常流量占比(按月)



来源：腾讯安全天御广告反欺诈系统，每年验证超过1万亿广告请求

从广告类型来看，插屏和贴片异常流量占比明显比其他广告类型高。插屏异常流量高主要原因是出现大量严重超出用户正常合理频次的流量；而贴片较其他广告类型有更大比例流量来自1) 高危设备的流量和2) 数据中心且不具备明确用户特征的流量。

异常流量占比（按广告类型）



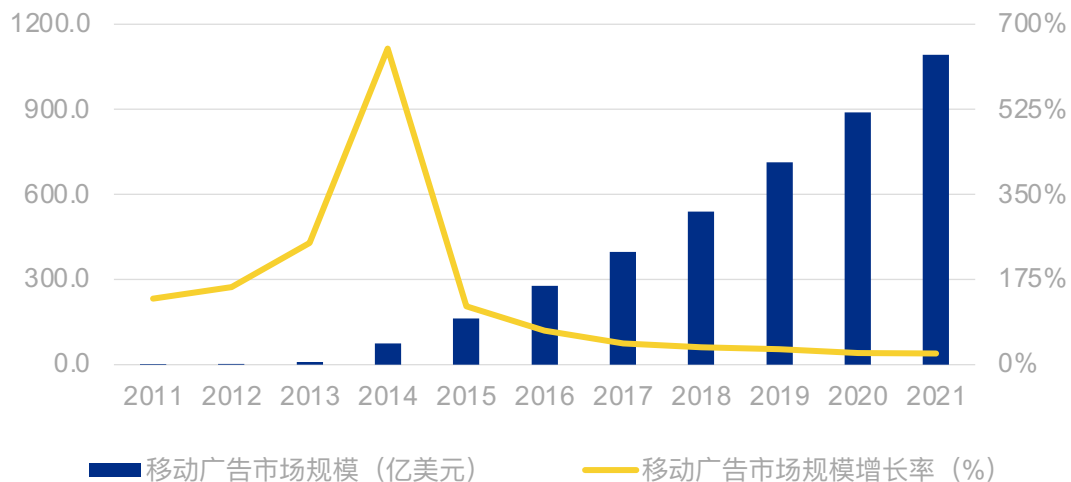
来源：腾讯安全天御广告反欺诈系统，每年验证超过1万亿广告请求

2 预计广告主因移动广告欺诈损失约 220 亿人民币

根据 eMarketer 的预测，2021 中国广告主在移动广告上的花费将达到 1093 亿美元，较 2020 年增长 23%。中国移动广告市场依旧是庞大且高速增长的市场，对于黑灰产来说也是有利可图的市场。

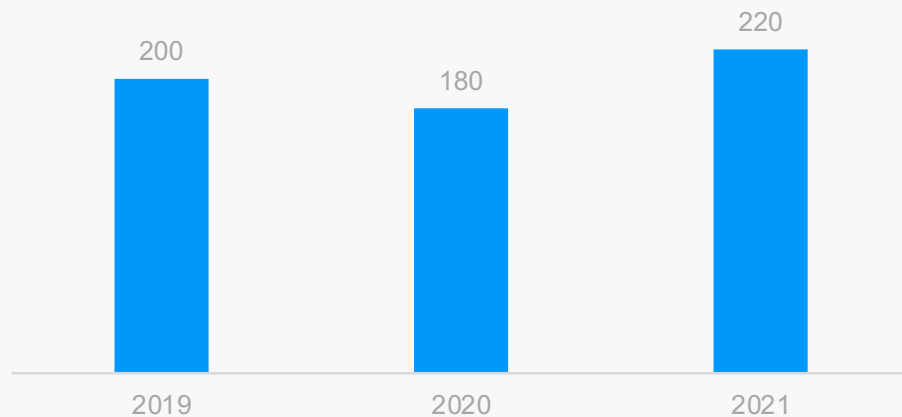
各大广告平台反欺诈团队和第三方广告反欺诈系统的使用极大程度上保护了广告主的利益，阻止〔过滤〕了大量欺诈流量进入计费环节。由于广告上下游交易环节与 KPI 错综复杂，一定比例异常流量依旧会进入曝光和点击环节，给广告主带来损失。腾讯防水墙预测 2021 年广告主因移动广告欺诈造成的损失约为 220 亿元，较去年增加 22%。

中国移动广告市场规模（亿美元）



来源：eMarketer

广告主因移动广告欺诈导致的损失（亿元）



来源：根据移动广告规模，结合腾讯安全天御广告反欺诈的异常流量占比及内部买量等数据进行预测和估算

3 欺诈流量的识别和防御变得更困难

作为常规数据载体的IMEI和 IDFA 获取越来越困难，基于IMEI 和 IDFA 规则的反欺诈覆盖率将随之下降，以IMEI和IDFA为key的属性数据也将失去意义，给欺诈流量的识别带来困难。

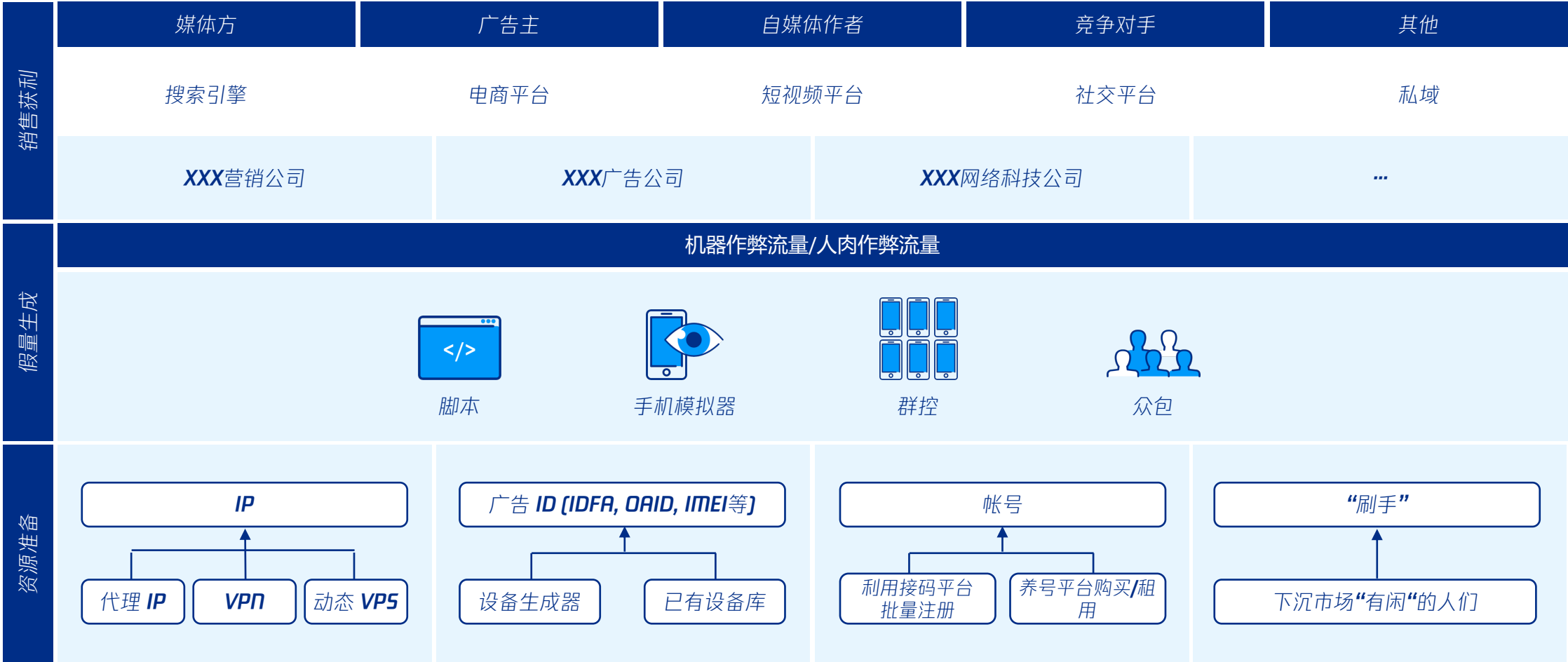
媒体使用聚合 SDK 会将一个用户的广告请求切成多份，并交互到各个广告平台，每个广告平台只能获取到部分不连续的请求行为数据，由于数据不完整，一些明显的行为异常可能都会被掩盖掉，导致异常流量的识别更加困难。

4 缺乏整体惩治体系，一些有作弊行为的媒体很难受到惩罚

目前国内缺乏对作弊媒体整体的打击体系，如果一个媒体在投放平台 A 出现作弊行为，被A平台惩罚，媒体可以将流量切给 B 平台，或者 C 平台，继续作弊，直到找到那个“最宽容”的广告投放平台。即使被所有平台封禁，还可以换个壳继续卖低质量〔作弊〕广告流量。

广告黑灰产业链概述

相较于正常用户流量，广告黑灰产能够获利的本质就是绕过各种资源限制，低成本批量制造假量，并形成稳定的销售渠道〔客户〕。经过多年的发展，广告黑灰产已经形成了一个上下游分工明确、配合密切的产业链。腾讯防水墙根据多年和广告黑灰产对抗的经验，将广告黑灰产产业链分为：资源准备->假量生成->销售获利三个环节，下面是黑灰产产业链结构图的流程示意：



图：黑灰产产业链结构图 来源：腾讯防水墙

1 资源准备

IP 地址、广告ID (IDFA, OAID, IMEI等) 是一个正常的移动广告请求的必备要素。如果需要伪造下载等后链路数据, 还需要大量的账号资源支持。因此IP地址、广告ID和账号是广告作弊的核心资源。

IP 地址

IP地址是网络接入的载体, 是有限资源, 且每个IP都有较容易获取的公共属性数据, 不易被伪造, 因此黑灰产通过VPN、代理及VPS混拨等方式隐藏真实访问IP, 通过不停切换IP出口制造全国用户访问的假象。

- VPN代理: 用户通过VPN去访问其他网站, 可实现跨城市的IP网段切换。这种方法较容易被防御。
- 代理 IP: 用户通过代理IP访问其他网站, 可以掩盖流量的真实来源。代理IP可切换的资源较VPN更多, 但也容易被发现和防御, 维护成本高。
- VPS混拨: 远程在VPS云服务器上架设多根网线, 软件实现多线混拨, 远程控制VPS服务器拨号。VPS混播IP池资源丰富, 可以实现跨城市切换, 而且速度快、稳定性好, 是目前黑灰产团伙使用的主流IP切换模式。

广告 ID

目前被广泛使用的是IDFA、OAID和IMEI。黑灰产主要通过设备号生成器或者购买广告ID库来批量获得广告ID。通过设备号生成器生成ID较容易被识别, 但从广告ID库获取的ID需要结合后续表现才能被识别。

账号

账号是广告后链路作弊必不可少的资源。黑灰产团伙主要通过批量注册或从养号平台购买的方式来获取账号。批量注册离不开提供电话号码和手机验证码的平台——接码平台。一台电脑加上一个能够插入大量手机卡的猫池, 即可组成一个简易的接码平台。平台使用者只需要调用对应的API接口就可以完成手机号和验证码的自动获取。接码的单价一度维持在0.1元*左右, 但是随着国家“断卡”行动的执行, 多个卡商和接码平台被查处, 目前接码单价已经涨到0.2元*左右。

黑灰产也会直接通过购买/租用养号平台的社交账号来制造广告后链路数据, 不过成本更高。养号平台的账号通常会直接用于网络诈骗, 部分账号也会用在收益高的效果广告作弊中。养号平台的账号大多通过盗号、批量注册、低价收购等方式获得。养号平台同时还提供账号的批量解绑、换绑、找回密码、解冻等服务。2020年被查封的特大养号平台——果平台就是一个典型的例子, 该平台拥有2亿多的社交账号。

*来源: 公开资料整理

2 假量生成

脚本刷量

黑灰产通过设计一个机器脚本来模拟人的浏览、点击等行为，再借助 IP 和广告 ID 等资源即可伪造一条广告流量。脚本刷量成本最低，但相对也容易被识别。爬虫本质上也是一种脚本，通过模拟人的行为去浏览页面，并将里面的内容记录下来，一些爬虫行为会被统计为有效曝光，损害广告主的利益。

模拟器刷量

模拟器是能在电脑上模拟整个手机行为的一个软件。黑灰产会通过多开多个手机模拟器，然后通过电脑操作多个手机进行刷曝光、点击、点赞等来获利。

群控〔设备农场〕刷量

群控可以用一台电脑控制上百部手机，实现上百部手机同时同步操作。群控可批量浏览、点击广告从而达到刷量的效果。群控也可被用在点赞、关注、薅羊毛等场景。

众包刷量

流量需求方将需求打包成各个微小的任务下发到个人去完成而产生流量。由于众包刷量都是真人刷出来的，成本最高，众包下发的任务必须是可执行和验证〔截图〕的，所以通常会用在APP注册、伪造转化数据等效果广告作弊上。

3 假量获利

国内广告主普遍压力较大，品牌广告主希望采购单价越来越便宜和品效合一，效果广告主则希望ROI越来越高。出于行业竞争、个人业绩压力等因素，加之广告上下游交易环节与KPI错综复杂，从广告主原始需求传导到中下游时，动作已变形，一些假量就以各种名义被“采买”进来。这是假量获利的主要途径之一。

一些自媒体创作者为了让自己发布的内容进入榜单，或者获取更高额的内容平台〔新闻、视频等〕费用，采购刷量服务将自己的内容的播放量、点赞量刷高。这也是假量获利的另一主要途径。

广告欺诈案例介绍

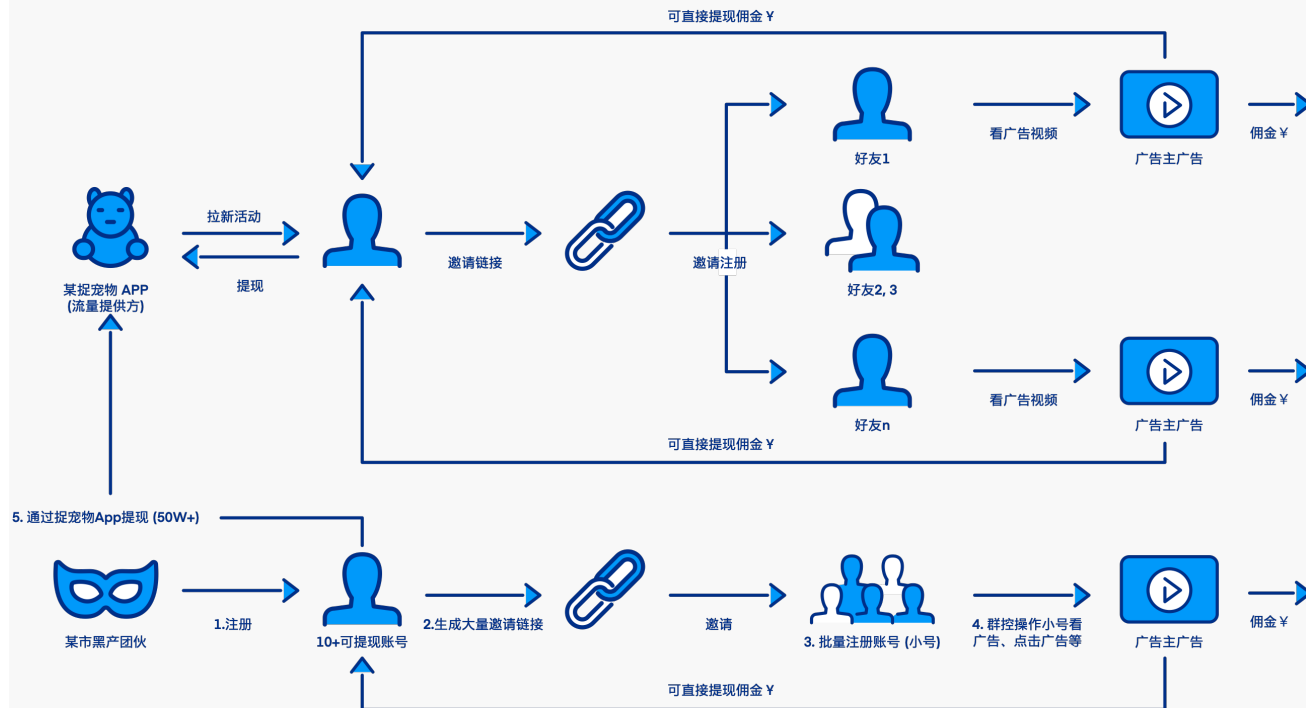


从防水墙发现的广告欺诈案例来看，虚假流量的产生原因很多，利益链也较复杂。以下列举了2021年发生的一些案例，便于读者对广告欺诈有个整体的认识。

1 拉新是假 提现才真

某捉宠物游戏APP想出了一个可提现的拉新方案：1) 现有用户可将邀请注册链接分享给好友，好友注册成功后即可成为该邀请人的下级。2) 下级观看广告视频后，上级可分得佣金，上级的佣金可直接提现。3) 单日佣金有上限，每个下级单日最多能让上级获利XX元。

因为可以直接提现，这个APP很快被黑产盯上。黑产团伙1) 首先注册了十余个可提现的账号，2) 利用提现账号生成大量注册邀请链接。然后3) 批量注册了大量的社交账号〔小号〕，小号通过邀请链接成为提现账号的下级。最后4) 再通过脚本+群控的方式，控制数千个小号观看、点击广告视频等赚取看广告佣金，这样提现账号就有源源不断的下线佣金进来。该捉宠物游戏APP被黑产团伙恶意提现数十万元，广告主损失惨重。

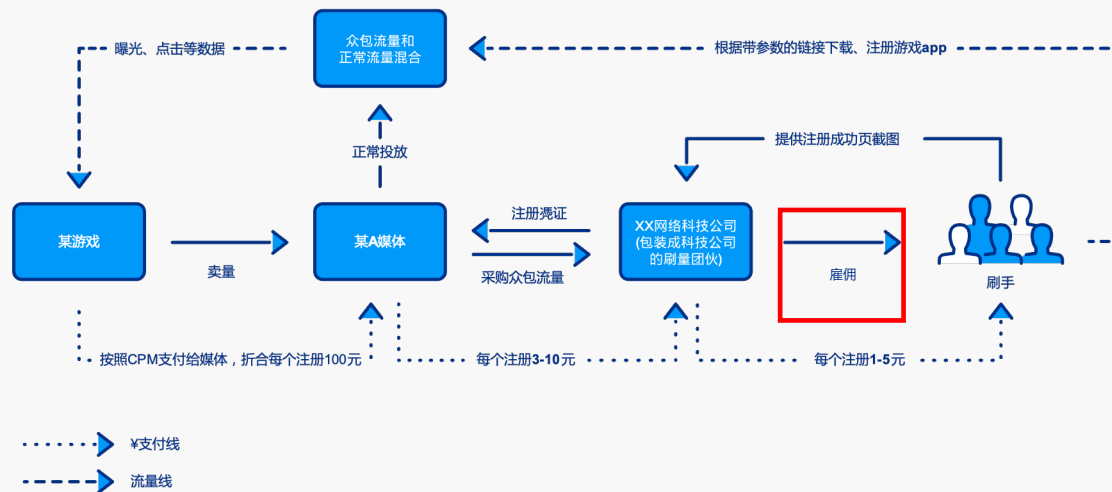


*来源：腾讯监测发现

2 真注册假流量 广告费用打水漂

某游戏在买量过程中发现来源于A媒体的流量，点击率、下载率都很正常，但是用户次日活跃、三日活跃和付费转化率数据很差。

防水墙深入挖掘后发现A媒体的转化流量可能掺杂了大量B刷量公司的假流量，防水墙情报团队接触了B公司，并“购买”了B公司的众包下载量，购买的下载量在后续行为甚至IP段都和A媒体的异常流量高度一致。购买一个B公司带凭证的众包注册需要约4元*，但游戏公司支付给A媒体的一个注册用户的平均成本在100元*以上，广告主损失的是刷量成本数十倍的真金白银。



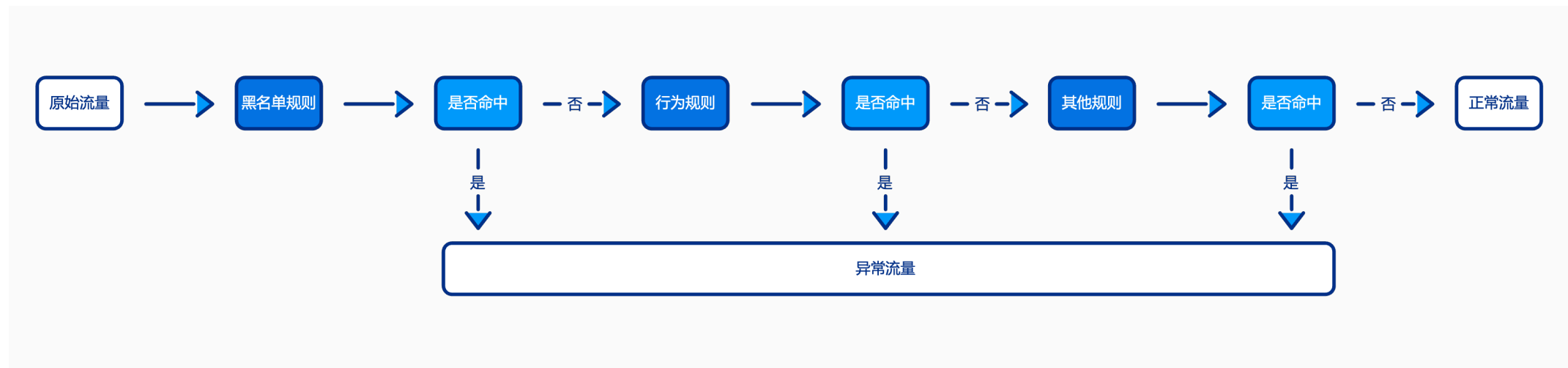
*来源: 腾讯监测发现

广告反欺诈方法介绍



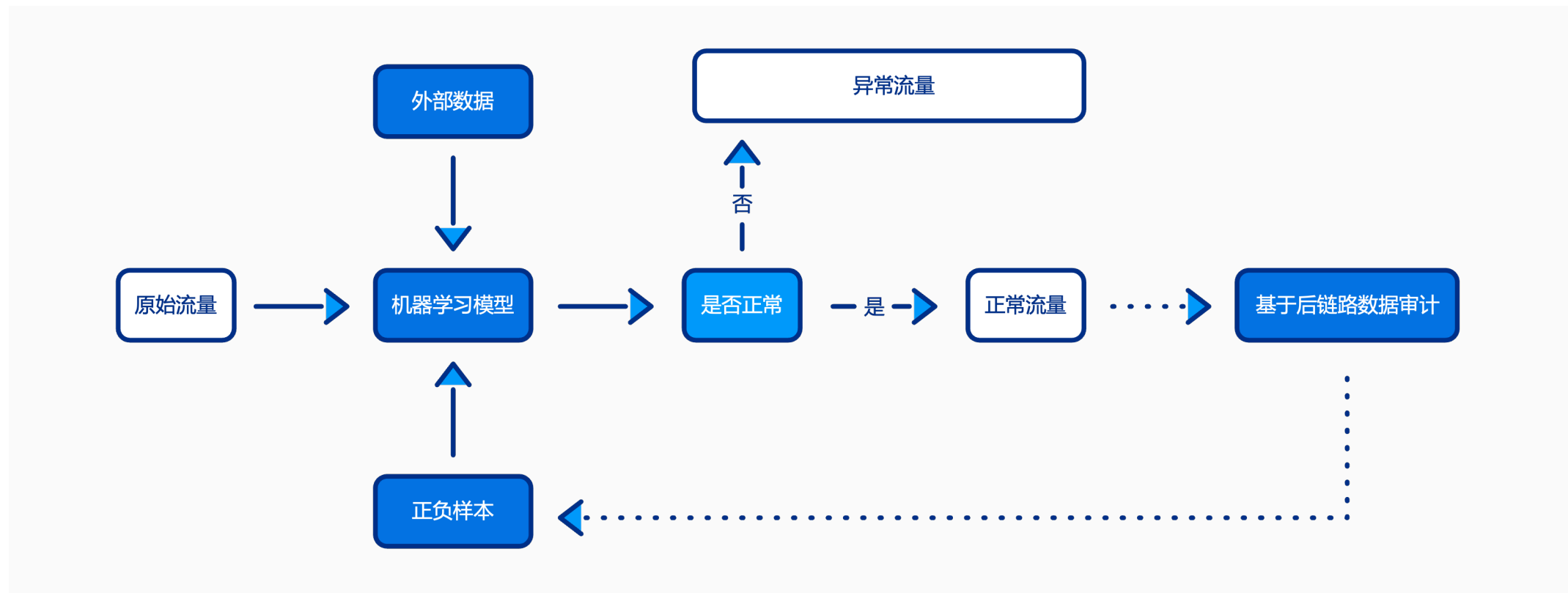
基于规则的反欺诈方案

基于规则的反欺诈方案通常简单有效，可以识别出大量的一般无效流量〔GIVT〕。利用行业经验和大数据分析，通过黑名单和统计分析进行人机识别和爬虫识别等，比如通过规律请求和黑名单，可识别出部分群控设备。基于规则的反作弊方案的缺点是需要大量的基础数据，比如代理IP、IDC IP、设备黑名单、设备行为等。另外规则不宜设置过多和过于复杂，否则容易导致规则之间冲突和事后归因困难。



基于机器学习和AI的反欺诈方案

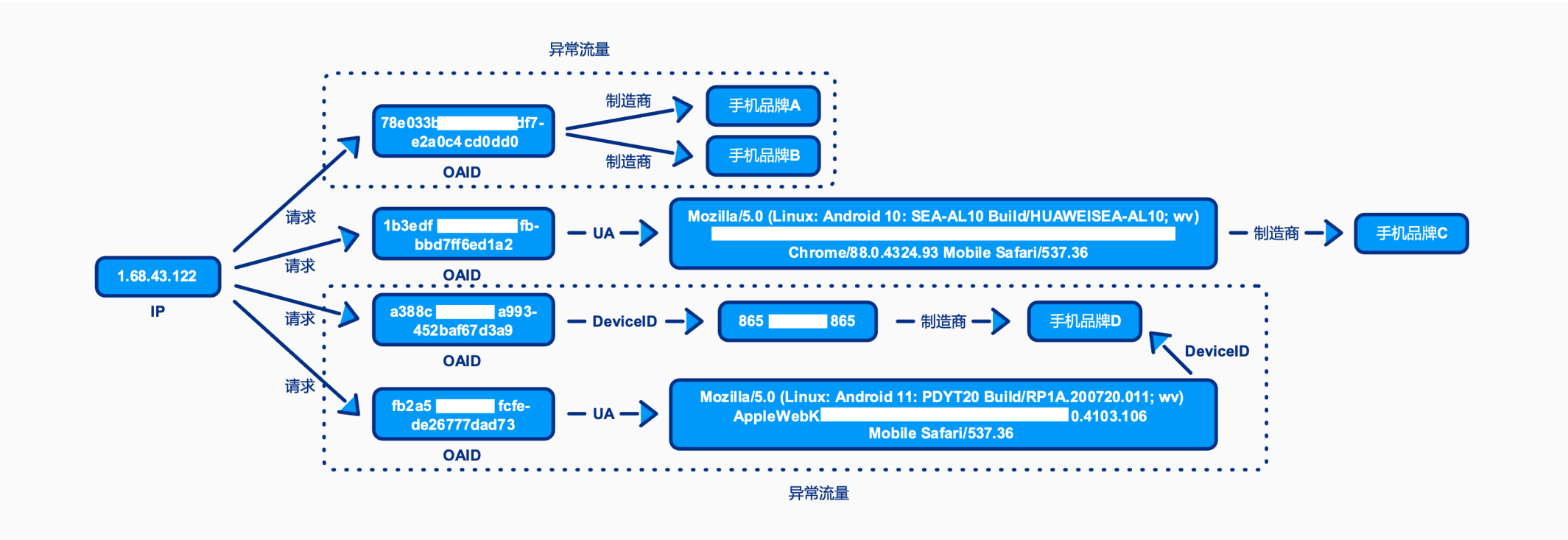
基于机器学习和AI的反欺诈方案是通过机器学习和AI模型来判断广告欺诈的一种方法。模型需要多维度的输入及大量的正负样本训练模型，当模型的准确率和召回率达到一定平衡的时候，就可以将该模型部署在反欺诈系统中对于广告请求进行识别。基于机器学习和AI的反欺诈方案能够识别复杂、难发现的复杂无效流量[SIVT]，缺点是可解释性较差，对正负样本的质量和数量要求很高。如果在请求阶段使用该方法，则需要考虑时延的问题，请求阶段的反作弊通常时延要控制在10ms以内。



基于图算法的反欺诈方案

图在数学中用 $G=(V,E)$ 表示，其中 V 表示节点的集合， E 表示边的集合。图算法在图的基础上刻画节点与边的各种特征，较其他算法更容易挖掘出孤立性和聚集性。在反作弊场景中，可以将IP、设备号、设备品牌、设备型号、useragent等作为节点，他们之前的关系作为边先建立一个图库，然后再采用Graph Embedding聚类的方式通过种子广告请求对恶意请求进行召回。

随着个人信息保护法的健全，设备指纹信息逐步离散化，传统的广告反欺诈方法和模型会更加困难，而通过图可以将个体的多种二部关系整合，并进一步扩散出更多有价值的线索，提供高效可达的鉴别效果。



中国广告反欺诈和国外的差异



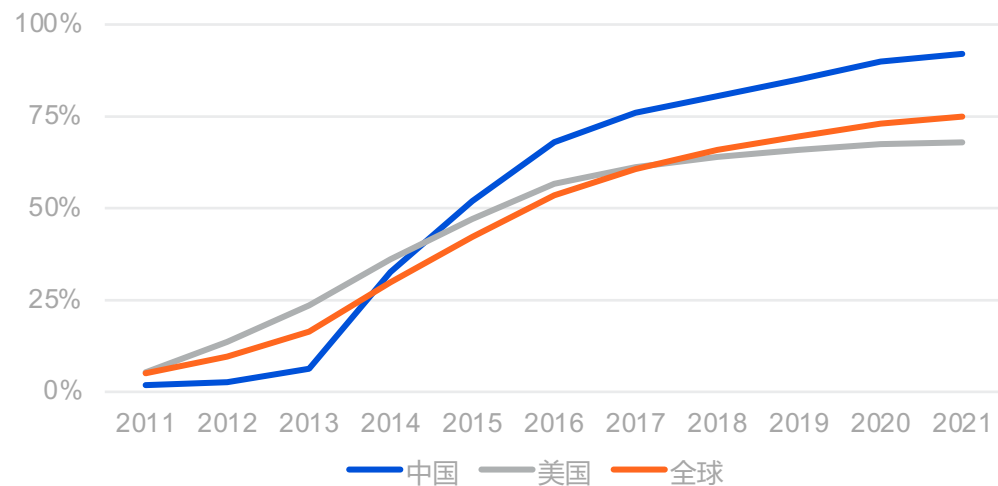
中国广告反欺诈和国外的差异

腾讯安全发现中国的广告反欺诈和国外有比较大的差异，主要体现在三个方面：广告市场、行业标准和成熟度。

市场的差异

首先，中国数字媒体以移动广告为主，而国外PC端流量还占据不可忽视的份额。国内反欺诈方案多是基于移动广告新建的SaaS方案，国外反欺诈方案更多是从PC反欺诈方案延续过来的，还有很多基于JavaScript的方案。

移动广告支出占数字媒体支出比例



*来源: eMarketer, 腾讯防水墙整理



国外广告反欺诈通常包括品牌安全 [Brand Safety] 和 可见性曝光 [Viewability], 而在国内则鲜有提及。因为:



品牌安全 [Brand Safety]

需要追踪广告曝光的页面、抓取曝光页面的内容、识别页面上是否存在损害品牌的色情、暴力、宗族歧视等不良内容, 而追踪广告曝光页面在移动端是不能实现的。国内有部分反欺诈厂商通过对APP或广告内容进行分类来给客户提供品牌安全的服务。



可见性曝光 [Viewability]

国内大多由广告平台的反欺诈系统负责完成, 由于各个广告平台的曝光统计标准不一样, 曝光统计的结果也会有些差异。

中国数字媒体经历了高速的发展, 并从PC端快速转移到了移动端。但不可否认的是在数字媒体高速发展中, 广告监测、反欺诈、可见性曝光验证等并没有得到足够的重视, 异常流量泛滥、曝光统计口径混乱时有发生, 这些问题已经开始影响整个广告行业的健康发展。



遵循标准的差异

国外广告主通常使用媒体评级委员会 [Media Rating Council, MRC] 制定的标准对广告投放媒体进行资格认证。MRC成立于1964年，是一个国际性非盈利组织，其制定的广告测量标准主要包括：

- 品牌安全验证指南 (Brand Safety Ad Verification Guidelines)
- 无效流量检测和过滤标准 (Invalid Traffic Detection and Filtration Standards)
- 广告曝光可见性测量标准 (Viewable Ad Impression Measurement Guidelines)

等24种。这些标准大多都会有对应的认证。

MRC的标准非常权威，标准认证严格而复杂，有的认证可能要几年的时间。国外大的媒体和第三方反欺诈公司会在网站的特定位置是否通过了MRC的相关认证。对于媒体来说经过了MRC的相关认证是信用的保证，通常也能够卖出更高的价格；对于广告反欺诈机构更是如此，通过MRC的无效流量相关认证几乎是从业的必要门槛。



国内广告标准分国家标准和团体标准，都是非强制执行，而在认证方面今年刚启动了“数字广告可见性验证”

国家标准：国家标准依据的是中华人民共和国国家质量监督检验检疫总局、中国国家标准化管理委员会 于2017年7月31日发布的《互动广告国家标准》，该标准包括：

序号	标准号	标准名称	状态	发布日期	实施日期
1	GB/T 34090.1-2017	互动广告 第1部分：术语概述	现行	2017/7/31	2018/2/1
2	GB/T 34090.2-2017	互动广告 第2部分：投放验证要求	现行	2017/7/31	2018/2/1
3	GB/T 34090.3-2017	互动广告 第3部分：效果测量要求	现行	2017/7/31	2018/2/1

团体标准：团体标准由中国广告协会发布，目前实施的标准有：

序号	标准号	标准名称	状态	发布日期	实施日期
1	T/CAAAD 003—2020	移动互联网广告标识技术规范	现行	2020/12/10	2021/1/1
2	T/CAAAD 002—2020	中国互联网广告投放监测与验证要求	现行	2020/12/10	2021/1/1

参照国外IAB Tech Lab的成功经验，中国广告协会与中国信息通信研究院联合成立了“互联网广告技术实验室”[CDA Tech Lab]。CDA Tech Lab与2021年11月正式启动了“数字广告可见性验证”测评工作，验证数字广告投放过程中媒体、监测方等是否按照标准要求进行广告可见性曝光统计和测量。这是国内的第一个广告相关认证，标志国内广告行业向更先进的管理范式迈出了一步。



反欺诈市场成熟度的差异

美国是全球最大的广告市场，其广告反欺诈服务也同样比较成熟和发达。美国广告反欺诈公司DoubleVerify和IAS都已上市，市值均超过30亿*美金。DoubleVerify2020年在美国市场销售额达2.44亿美金，IAS 2020年在美国市场的销售额也超过1亿*美金。

*来源：腾讯防水墙根据公开材料整理

作为全球第二大广告市场的中国，从事广告反欺诈的公司只有秒针、RTBasia、腾讯安全天御等。这些公司没有一家因为广告反欺诈业务而单独上市，年销售额和DoubleVerify、IAS等也相距甚远。此外，国内反欺诈公司在广告反欺诈上的投入也很难和国外反欺诈巨头相比。

公司名称	DoubleVerify	IAS
成立年份	2008年	2009年
总部所在地	纽约	纽约
员工数	633	651
是否上市	是 [US: DV]	是 [NASDAQ: IAS]
市值	55.36亿美金	36.45亿美金
年收入	2.44亿美金 [2020年]	2.41亿美金 [2020年]
认证	MRC SIVT检测和过滤认证	MRC SIVT检测认证

趋势和展望



1 国家继续大力打击虚假流量黑产，促进广告行业正本清源

2021年10月，国家发布了《反电信网络诈骗法〔草案〕》，该法案已经明确禁止制造、销售、提供或者使用“批量网络地址自动切换系统〔IP切换系统〕”，同时对电话卡、物联网卡、金融账户、互联网账号的开办和注册进行了明确规定，加大滥用以上账号的惩戒力度。预期草案通过审议施行后，将给广告反欺诈行业带来积极影响。

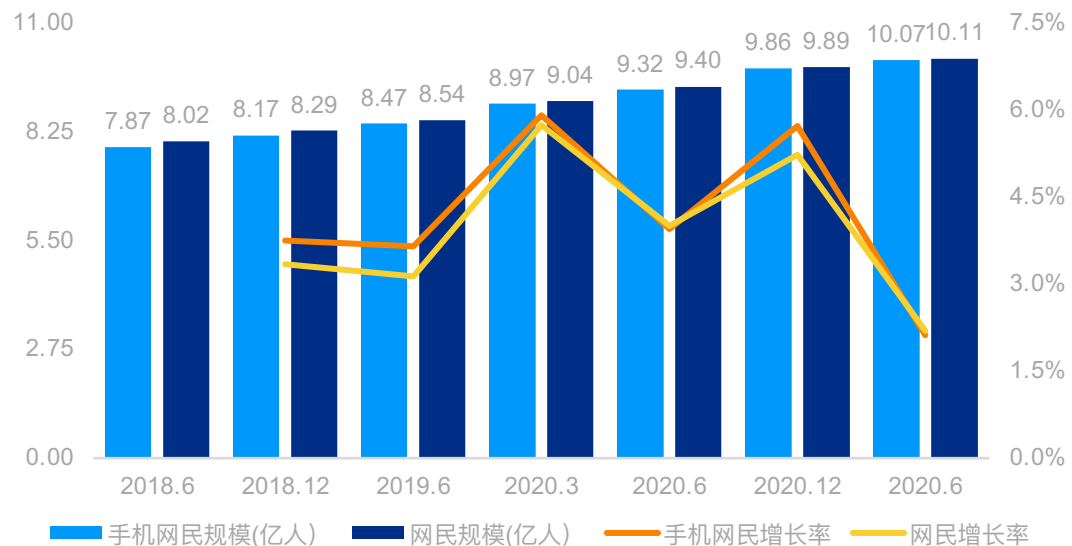
11月，国家出台了《互联网广告管理办法〔公开征求意见稿〕》，该法案表示，以启动播放、视频插播、弹出等形式发布的互联网广告，应当显著标明关闭标志，确保一键关闭，不得以欺骗、误导方式诱使用户点击广告。法案明确表示用户“一键关闭”互联网广告，可以有效避免用户因误点击广告关闭键而产生无效流量。

12月，中央网信办部署开展“清朗·打击流量造假、黑公关、网络水军”专项行动。整治批量购买粉丝、增加“僵尸粉”“达人粉”，组织水军制造虚假阅读量、评论量、转发量、点赞量、下载量、曝光量等问题。进一步加强对虚假流量的打击。

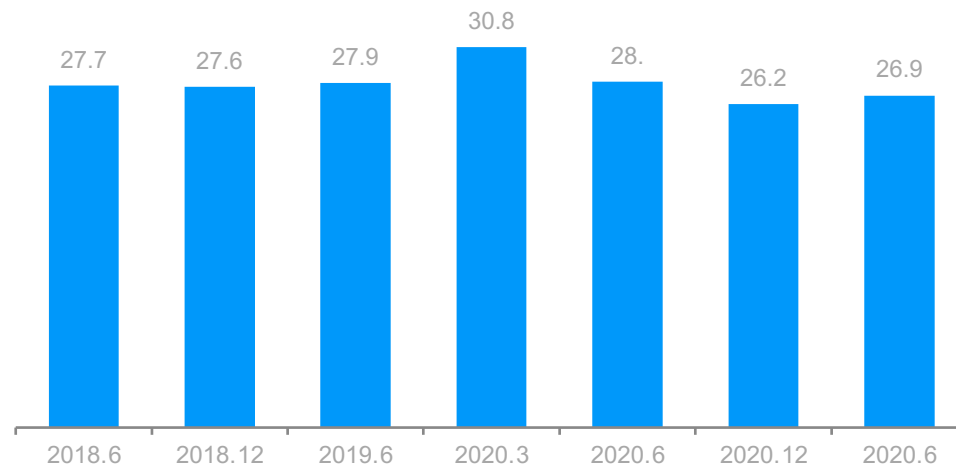
2 互联网人口红利趋缓，移动广告市场越来越卷 低质量和异常流量有上涨的趋势。

根据中国互联网络信息中心 [CNNIC] 的数据，整体网民和手机网民增速放缓，人均上网时长也不再增长，一直维持在27小时左右，互联网人口红利趋缓。

网民规模和增长率



中国网民人均每周上网时长（小时）



从防水墙的监测数据来看，越来越多媒体开始增加广告位、增加广告请求频次以获得更高的广告收入，甚至有些媒体利用更隐蔽的技术手段，掺杂机器人曝光和点击来获得更高的广告收入。在互联网人口增长趋缓，用户上网时长停滞的背景下，单纯增加广告位或掺假量不但会导致低质量和异常流量的上涨，损害广告主利益，同时也会影响用户的体验。

3 更多先进的算法和工程学技术将会被用到反欺诈系统中来

《个人信息保护法》和苹果ATT方案的实施，短期内会给广告反欺诈行业带来更严格的要求，一些基于规则的反欺诈方案的识别能力会下降。广告反欺诈需要采取更先进的算法比如XGboost〔知名机器学习算法〕、Graph Embedding〔图嵌入算法〕等，通过一些弱相关因子来识别异常流量。

复杂算法的使用会增加异常流量的识别时间。主流请求阶段的移动广告反欺诈方案对时延要求很高，通常需要10毫秒以内识别出异常流量并将结果反馈给广告主和广告平台。10毫秒时延对于算法运算速度、部署环境、内存分配等工程学提出了更高的要求，将倒逼工程学的升级和创新来满足市场需求。

4 希望CDA Tech Lab考虑引入Sellers.json和Ads.txt两项技术规范，增加广告行业透明度

Sellers.json和Ads.txt是由美国的IAB Tech Lab*推出的两项技术规范。两项技术已被证明在提高广告行业透明度、打击广告欺诈方面是非常有效的。希望CDA Tech Lab可以考虑引入以上技术规范，以增进广告主和媒体之间的信任，打击恶意转包等欺诈现象。

Sellers.json

给广告主看的一个透明文件，目的是增加广告主对于SSP的信任，尤其是在实时竞价和程序化购买场景中。形式是一个包括子媒体ID、名称、域名、采购类型等的json文件。

```
{
  "contact_email": "adops@advertisingssystem.com",
  "contact_address": "Advertising System Inc., 101 Main Street, New York, NY 10101",
  "version": "1.0",
  "identifiers": [
    {
      "name": "TAG-ID",
      "value": "28cb65e5bbc0bd5f"
    }
  ],
  "sellers": [
    {
      "seller_id": "1942009976",
      "name": "Publisher1",
      "domain": "publisher1.com",
      "seller_type": "PUBLISHER"
    },
    {
      "seller_id": "1397382429",
      "name": "Exchange1",
      "domain": "exchange1.com",
      "seller_type": "INTERMEDIARY"
    },
    {
      "seller_id": "20000000",
      "name": "Seller And Intermediary, Inc",
      "domain": "sellerandintermediary.com",
      "seller_type": "PUBLISHER"
    },
    {
      "comment": "NorthAmerica O&O inventory",
      "seller_id": "20000001",
      "name": "Seller And Intermediary, Inc",
      "domain": "sellerandintermediary.com",
      "seller_type": "PUBLISHER"
    },
    {
      "comment": "APAC O&O inventory",
      "seller_id": "20000002",
      "name": "Seller And Intermediary, Inc",
      "domain": "sellerandintermediary.com",
      "seller_type": "INTERMEDIARY"
    },
    {
      "comment": "Non O&O inventory",
      "seller_id": "101010101",
      "name": "Hybrid Seller",
      "domain": "hybridseller.com",
      "seller_type": "BOTH"
    },
    {
      "comment": "Sells both O&O and other sellers' inventory",
      "seller_id": "00000001",
      "seller_type": "INTERMEDIARY",
      "is_confidential": 1
    },
    {
      "seller_id": "EB_0001",
      "name": "Passthrough Publisher",
      "domain": "passthroughpublisher.com",
      "seller_type": "PUBLISHER",
      "is_passthrough": 1,
      "comment": "direct buyer/seller of this inventory must establish an account relationship with Passthrough Publisher"
    }
  ]
}
```

Ads.txt

Authorized Digital Sellers [授权数字卖家]，IAB Tech Lab指定了一种txt的标准，供媒体列出其授权的数字卖家，以打击欺诈和虚假域名。Ads.txt文件被要求放在网站根目录下[便于被爬虫爬取]，写明授权售卖系统名称、媒体ID、账号类型或合作类型、授权ID等信息。

2019年针对移动端媒体IAB Tech Lab发布了app-ads.txt标准。app-ads.txt是ads.txt的拓展，标准要求应用商店在app介绍页发布三个HTML<meta>标签，三个<meta>分别存放app开发者的网址[为了放app-ads.txt]；app的bundle id；app的应用商店id，样例如下：

HTML meta tags in App stores 示例图

```
<meta name="appstore:developer_url" content="https://www.path.to/page" />
<meta name="appstore:bundle_id" content="com.example.myapp" />
<meta name="appstore:store_id" content="SKU12345" />
```

来源：IAB Tech Lab Authorized Sellers for Apps (app-ads.txt) Final specification version 1.0

图：HTML meta tags in App stores 示例图 来源：IAB Tech Lab Authorized Sellers for Apps (app-ads.txt) Final specification version 1.0

5 希望国家、协会、广告主、媒体和反欺诈机构共同努力 建立一个更透明、健康的广告生态

广告是一个由广告主、媒体、广告平台、第三方监测机构、国家机关、用户一起组成的一个生态。随着互联网人口红利趋缓，移动广告市场也将进入存量时代，行业需要变得越来越透明，让假量、欺诈媒体无处可躲，让行业生态更健康。

腾讯安全

腾讯安全作为互联网安全知名品牌，致力于成为产业数字化升级进程中的安全战略官，依托20多年业务安全运营及黑灰产对抗经验，凭借行业知名安全专家、完备安全大数据及AI技术积累，为企业从“情报-攻防-管理-规划”四维构建安全战略，并提供紧贴业务需要的安全实践，守护政府及企业的数据、系统、业务安全，为产业数字化升级保驾护航。

腾讯防水墙

腾讯防水墙，专注业务安全服务。基于腾讯十多年的安全大数据，用先进的人工智能技术、实时计算引擎，从黑产情报、实时AI营销风控模型、事后追踪等环节，全方位感知并解决营销等风控问题，帮助业务避免活动受损。防水墙能力通过腾讯安全天御对外接入。

名词解释 - 部分词汇出自《MMA中国MarTech词典》

国际移动设备识别码 | IMEI, International Mobile Equipment Identity

用于识别每一部独立的移动通信设备。

匿名设备标识符 | OAID, Open Anonymous Device Identifier

一种非永久性设备标识符，可在保护用户个人数据隐私安全的前提下，向用户提供个性化广告。

苹果广告标识码 | IDFA, Identifier For Advertising

Apple 公司为iOS移动设备提供的用于追踪用户的广告标识码。

IP地址 | IP address

IP地址 [Internet Protocol Address] 是指互联网协议地址，又译为网际协议地址。IP地址是IP协议提供的一种统一的地址格式，它为互联网的每一个网路和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。

软件开发工具包 | SDK, software development kit

在APP开发时候的标准的模块化软件开发工具包，在开发APP时只需要植入标准SDK就能实现部分功能，而不需要从零开始写源代码。

设备号 | Device ID

消费者移动设备 [手机和Pad]的唯一ID,包括了基于通讯模块的IMEI、Apple 设备的IDFA和安卓操作系统设备的安卓ID等。

无效 [异常] 流量 | Invalid traffic

在广告投放中，由于各种原因造成非真人消耗了广告费用。原因有两大类：1.使用技术手段恶意造成的广告损耗，例如利用群控软件控制大量设备进行广告点击；2.由于互联网的复杂环境，非恶意造成的无效流量，例如网络爬虫在获取数据的时候对广告资源造成的消耗。

一般无效流量 | GIVT, General invalid traffic

一种无效流量的甄别标准，行业通用的利用技术和数据手段，对无效流量进行甄别的解决方案。

复杂无效流量 | SIVT, Sophisticated invalid traffic

一种无效流量的甄别标准。针对通用的GIVT标准无法识别的高阶异常流量，通过更实时，更高阶的算法分析进行识别，但是需要产生额外的成本。

机器人流量 [或非人类流量] | Bot traffic [or non-human traffic]

一种无效流量，由人工恶意的利用软件造成虚假流量，以骗取广告预算为最终目的。

反作弊 | Anti-Fraud

通过技术手段，识别虚假流量、僵尸网络等作弊行为。

可见性曝光 | Viewable ad

广告创意出现在浏览器的可见窗口页面的活跃标签上，并且满足设定的曝光条件 [如像素露出面积的百分比和连续有效曝光的时长。] 展示类广告至少50%露出后持续播放1s既满足可见性曝光，视频类广告至少50%露出后持续播放2s即满足视频可见曝光标准。

品牌安全 | Brand Safety

当广告出现的页面上，还会存在广告之外的其他内容，为了避免这些内容对于品牌的可能性伤害，需要对存在黄赌毒，明星绯闻，诋毁等内容的页面进行屏蔽，避免广告出现在这些页面上。

归因 | Attribution

一种效果评估的算法逻辑，当有很多种因素会推动消费者形成最终购买的时候，通过算法来衡量这些因素的重要程度。例如一个消费者在购车前分别在5个媒体看过汽车类广告，通过归因算法可以获得5个媒体推动消费形成最终购买的价值比率。

广告监测 | Ad Tracking

通过独立第三方工具跟踪广告投放的真实效果，涵盖曝光、点击、转化等环节，用于品牌和媒介进行广告结算和效果论证。

后链路 | Post-click Chain

泛指受众在点击广告后，进入落地页/销售页面后的所有行为环节。

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，也被称为“甲方”，“品牌主”等。

互动广告协会 | IAB, Interactive Advertising Bureau

成立于1996年，旨使媒体和营销行业能够在数字经济中蓬勃发展，目前有超过650家会员。IAB在北美、南美、非洲、亚洲、亚太地区和欧洲都会分会，制定全球性的解决方案，推动数字广告产业的发展。

IAB技术实验室 | IAB Tech Lab

IAB技术实验室成立于 2014 年，是一个非营利组织，旨在与全球成员社区合作开发基础技术和标准，以促进数字媒体生态系统的增长和信任。研究内容覆盖品牌安全和广告欺诈解决方案；广告id、数据和消费者隐私；广告体验和衡量标准；程序化购买有限性等。

媒体评估委员会 | MRC, Media Ratings Council

MRC是目前全球最权威的广告媒体协会，成立于1964年，旨在建立广告媒体测量的行业标准并通过审计和认证业务促进企业遵守其适用的行业标准。