ICS 35.240.60
L 67

中华人民共和国国家标准

GB/TXXXXX.2—XXXX

互动广告
第 2 部分：投放效验要求

Interactive advertising
Part 2:Delivery monitor requirements

点击此处添加与国际标准一致性程度的标识

（报批稿）

（本稿完成日期 2017 年 1 月 15 日）

（在提交反馈意见时，请将您指导的相关专利连同支持性文件一并附上。）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

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　发布

目　　次

前　言

GB/TXXXXX《互动广告》分为5个部分：

——第1部分：术语概述；

——第2部分：投放效验要求；

——第3部分：效果测量要求；

——第4部分：平台接口要求；

——第5部分：用户信息保护要求。

本部分是GB/TXXXXX的第2部分。

本部分按照GB/T1.1-2009给出的规则编写。

本部分由国家工商行政管理总局归口。

本部分起草单位：中国广告协会互动网络分会、腾讯科技（北京）有限公司、上海聚胜万合广告有限公司、北京奇艺世纪科技有限公司、北京秒针信息咨询有限公司、合一集团、百胜集团、内蒙古蒙牛乳业（集团）股份有限公司、华扬联众数字技术股份有限公司、工业和信息化部电子工业标准化研究院。

本部分起草人：刘曜、陈永华、段少飞、程钦召、冯惠、葛承志、龚宇、古永锵、高雅、刘胜义、刘佳、刘伟、刘研、卢振飞、李克、王佐、向维良、熊若愚、赵伟、张之彦、周平、周溯、陈永、裴跃赏。

引　　言

随着互联网和移动互联网的快速发展，互动广告已经占据了广告市场近50%的份额，成为重要的广告投放方式和渠道。但是，互动广告的快速发展也带来了许多问题和挑战：广告样式繁杂多样造成产业资源效能低化；衡量基准各说各话阻碍产业扩张与融合；数据孤岛，分类定义不能互通；参与角色多样，接口要求各自为政，导致平台和产品间合作困难。为了规范、促进互联网广告市场发展，由工商行政管理总局归口，于2015年完成了《广告法》的修订，2017年又颁布了《互联网广告管理办法》。为了充分释放互联网广告的市场效能，做强、做大互联网广告产业，使互联网成为我国参与新一轮国际竞争利器，就要规范阻碍互动广告相互之间接口协作统一的对接语言和投放执行过程中的交易形式、内容和方法，统一的数据采集方法和分类、定义以及用户数据隐私安全，统一的测量标准。本标准旨在统一规范互动广告：一是明确互动广告投放和监测等概念和维度，二是保证互动广告行业运作模式的规范性和可复制性，三是保证互动广告投放和监测的统一性。

互动广告　　第2部分：投放效验要求

1　范围

GB/TXXXXX的本部分规定了媒体广告平台、第三方监测机构在广告监测过程中应遵循的规范。

本部分适用于各类智能设备上的互动广告监测。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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/TXXXXX.1—XXXX 互动广告 第1部分:术语概述。

3　缩略语

OS	操作系统 (operating system)
IMEI	国际移动设备标识 (international mobile equipment identity)
Android ID	安卓身份标识号 (Android identity)
MAC	媒体访问控制 (media access control)
IDFA	广告标识符 (identifier for advertisers)
Open UD ID	唯一设备身份识别码 (open unique device identifier)
TS	时间戳 （time stamp）
IESID	数据交流标识 (information exchange servers ID)

4　广告监测

4.1　广告监测系统性能要求

广告监测系统性能要求见表 1。

表 1　监测系统的性能要求

项目	要求
可用性	保障线上 99.99%的可用性。
	对数据有灾备和恢复方案，避免数据丢失。
扩展性	采用服务器集群方式部署监测服务器，根据流量和业务需要，灵活增减配置。

	弹性带宽配置方案，确保不发生网络堵塞。
安全性	保证服务器所在 IDC 机房的严格运维，确保控制网的安全性，避免控制网直接暴露于外网。
	未经允许，IDC 不得对服务器进行任何操作。包括：私自登陆服务器，开、关机等。
	对服务器具有 100%的控制权。
	保证机房硬件和网络的严格运维，保证硬件设备和网络正常运行，并 7*24 小时响应服务器发生的硬件或网络故障。
	IDC 需保证不对监测接入的域名进行过滤，保证服务器正常使用。

4.2 广告信息采集要求

4.2.1 信息采集参数要求

媒体客户端信息采集的参数要求见表 2。

表 2 媒体客户端信息采集的参数要求

参数	解释	使用说明
OS	客户端操作系统种类，0-Android，1-iOS，2-WP，3-Others。	判断监测请求来自哪种操作系统。
		非 Android、iOS、Windows Phone 的操作系统，OS 值统一用 3 表示。如获取不到操作系统类型，则保留空值。
IMEI	此参数仅在 Android 系统中获取使用，需要 MD5 加密。	用于识别独立访问者。 对 Android 操作系统，要求依次选用 IMEI、AndroidID、MAC。 对 Windows Phone 和其他操作系统，要求选用 MAC。 对 iOS 操作系统，要求依次选用 IDFA、OpenUDID、MAC。
AndroidID	此参数仅在 Android 系统中获取使用，需要 MD5 加密。	
MAC	用户终端的硬件地址，适用于 Android 和 iOS，字母转换大写后 MD5 加密。	
IDFA	此参数仅在 iOS 系统中获取使用，无需加密保留原始值即可。	
OpenUDID	此参数仅在 iOS 系统中获取使用，无需加密保留原始值即可。	

4.2.2 信息传输要求

广告监测信息传输应满足以下要求：

a）媒体方和监测方应采用 API 方式传输数据，通过在监测 URL 中加入宏定义的方式完成。宏定义如下：__OS__ ， __IMEI__，__MAC__ ， __ANDROIDID__ ， __IDFA__ ，__OPENUDID__ （__为连续的两个下划线），获取不到的参数保留空值。

b）在得到数据拥有方授权后，数据需求方在监测 URL 中应加入宏定义__IESID__，__IP__，_TS_，获取不到的参数保留空值。

c）IP 是数据需求方识别出的当前用户访问地址。

d）数据拥有方在得到授权之后，应开放相应的数据查询 API 接口，便于数据需求方及早发现数据差异。

4.2.3 信息保存要求

广告监测过程中采集的数据应以数据采集原始格式在媒体平台至少保存2年。向监测公司传输的数据应以数据传输原始格式在监测公司平台至少保存2年。

4.3 黑名单制度及其信息采集要求

为防止ID重复造成独立访问者识别不准确，需要精准判定独立访问者。如果ID为空或者该ID被列入黑名单，则视该ID为无效ID，不参与独立访问者的判定。黑名单信息采集应符合表3中列出的参数要求。

表 3 黑名单信息采集的参数要求

参数	原值
IMEI	非 15 位数字和字符，以及 15 位值都一样的数字和字符
ANDRIODID	9774d56d682e549c
IDFA	00000000-0000-0000-0000-000000000000

5 广告监测指标项及其计算要求

5.1 广告曝光量及其计算要求

每次广告展现，由访问者端向监测服务器发起1次HTTP请求，并携带广告活动、广告位、用户唯一标识等信息。监测服务器为收到的每次请求记录1条曝光日志。统计曝光日志的总数作为广告曝光量。HTTP请求可通过（但不限于）HTML中的<IMG>、<IFRAME>、<SCRIPT SCR>标签触发，根据实际需求，监测服务器可返回（但不限于）1x1图片、HTML、JavaScript、302跳转等。监测服务器须通过设置HTTP头等技术方式最大程度减少缓存对监测的影响。

5.2 广告独立访问者数量及其计算要求

每个访问者应具有唯一标识；统计访问者产生的曝光日志中，用户唯一标识去重后的数量作为独立访问者数量。基于浏览器网页环境的广告监测，为每个新访问者分配一个用户唯一标识，并使用第三方Cookie存储此标识；基于应用环境的广告监测，使用设备ID（或广告追踪匿名ID）作为用户唯一标识。当ID无法获取时，使用IP地址、User-Agent等能表示数据唯一性的信息作出判断。

5.3 广告点击量及其计算要求

每次广告点击，由访问者端向监测服务器发起1次HTTP请求，并携带广告活动、广告位、用户唯一标识等信息。监测服务器应为收到的每一次请求记录1条点击日志。统计点击日志的总数作为点击量。

5.4 广告独立点击者数量及其计算要求

统计访问者产生的点击日志中，通过用户唯一标识进行去重后得到的数量。

5.5 触达次数及其计算要求

指定时间周期内，观看过某广告的N次及N次以上的访问者人数，称为“N+触达”。“1+触达”即“独立访问者人数。N+触达的计算方法与独立访问者计算方法一样，即统计访问者产生的曝光日志中出现N次及N次以上的用户唯一标识的数量。

5.6 互联网毛评点及其计算要求

计算指定时间周期内广告曝光量与总体互联网人口的比值。中国总体互联网人口应参照中国互联网络信息中心（CNNIC）发布的相关统计数据。

5.7 点击率的计算要求

点击率是点击数量除以有效曝光量得出来的。　　即点击量与曝光量的比值。

6 异常流量排查

6.1 异常流量排查方法

6.1.1 通过行为频率与其关联性来监测。通过统计监测日志中访问者的曝光、点击等行为，分析行为频率、行为间关联性等，发现流量异常。例如，某访问者短时间内在某广告上产生大量曝光或点击日志记录，明显偏离正常访问行为；某访问者产生点击前无对应曝光日志记录。

6.1.2 通过分析流量来源来监测。通过统计监测日志中的 Referer、User-Agent 等信息，分析流量来自的页面 URL、请求所采用的浏览器类型、版本等，发现流量异常。例如，曝光或点击日志的 Referrer 信息中出现广告主与媒体约定范围外的媒体、频道或页面的 URL；曝光或点击日志的 User-Agent 信息中出现广告主与媒体约定范围外的操作系统或浏览器信息。

6.1.3 通过分析流量分布来监测。通过统计监测日志中的 IP、时间或访问者的操作系统、浏览器等信息，分析它们的分布情况，发现流量异常。例如，在未做 IP 地址精确定向的广告投放中，点击或曝光日志集中于同一地址或地址段；在未做时间定向的广告投放中，点击或曝光日志集中在一天中的某时段内产生；在未针对操作系统、浏览器做定向的广告投放中，点击或曝光日志的操作系统、浏览器的分布明显偏离一般人群。异常流量监测要求请**见*附录 A**

6.2 异常流量排查流程

根据公开、对等、透明的原则，通过对相关数据的排查，发现异常流量来源。监测方、媒体方、代理公司中的任意一方发现异常流量后，可向委托方提出启动异常流量排查申请，并将收集到的数据发送给委托方。委托方收到申请后，可委托代理公司成立异常流量调查小组，对异常流量进行调查，以代理公司名义向委托监测方提交调查报告。具体流程见图1

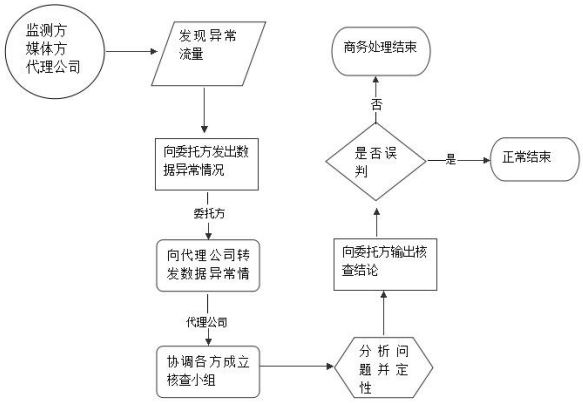

图1　异常流量排查流程图

附录 A：异常流量监测要求

A.1 异常流量监测字段

在异常流量监测中首先要甄别出常规异常流量监测字段，找出这些非人类和非有效用户产生的多余、重复或无法识别的数据流量字段。如表A.1所列

表 A.1　数据流量常规监测字段

序号	字段	描述	是否必须
A.1.1	事件类型	描述业务或转化的信息，例如曝光、点击等	是
A.1.2	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
A.1.3	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
A.1.4	IP	用户端 IP 地址，不能为直接用户访问时以外的 IP	是
A.1.5	请求方式	HTTP 协议中的请求方式，如 GET、POST 和 HEAD 等	是
A.1.6	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
A.1.7	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
A.1.8	预加载 HEADERS	如 X-MOZ/FireFox,X-Purpose/Safari 等	否
A.1.9	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
A.1.10	广告页面 URL	在可获取广告所在页面 URL 的前提下可用	否
A.1.11	设备信息		否
A.1.12	运营商		否
A.1.13	应用程序标识符	主要适用于移动 APP	否
A.1.14	位置信息		否
A.1.15	请求状态码	HTTP 请求返回的状态码，如 200、302、400 等	否
A.1.16	视频/音频广告完成百分比	包括开始、播放完成百分比和结束阶段信息	否

A.2 异常流量分类

异常流量分为一般异常流量和复杂异常流量。

A.2.1 一般异常流量：通过常规过滤方法能够识别的流量。

1) 机器人和爬虫或其它伪装成合法用户的流量数据以及非浏览器用户代理头或其它形式的未知浏览器带来的流量。

2) 超出频次、时间间隔等目标设定的流量数据。

3) 通过隐藏/堆叠/覆盖或其它方式导致用户无机会看到正常广告内容的流量。

4) 已知的来自数据中心的流量(指明显具有非人类访问广告所在的特定网络 IP 或 IP 段所产生的流量来源）。

5) 预获取或浏览器预览的广告流量。

6) 已知的来自高危或者作弊来源流量。

7) 基本信息缺失或不一致的流量（基本信息至少应包含事件类型、广告系列 ID、时间戳、IP、请求方式、用户代理 UA 字段）。

A.2.2 复杂异常流量

无法直接通过监测字段识别出来的异常流量,需要多维度的高级分析才能识别的重大人为干预产生的流量。包含（但不限于）以下检测点：

1) 劫持设备以及设备中的会话；

2) 非法劫持广告创意和操纵流量；

3) 内容盗用、伪造、虚假展示；

4) 恶意修改、插入或删除 cookie 内容以改变用户访问记录；

5) 操纵或伪造位置数据以及相关属性。

6) 无效代理流量（即来自中间代理设备的无效流量，包括通过代理设备操纵流量计数、创建/传输非人类流量或无法通过协议验证的流量）。

A.3 异常流量的检测要求

广告测量机构必须应用对“一般异常流量”的检测和过滤。测量机构需要输出一般异常流量过滤之前的流量总量，在后续对流量的统计分析中，一般异常流量应当被过滤。

广告投放流程中的各环节的参与机构（包括但不限于媒体、供给方平台、广告交易平台、需求方平台、测量机构、广告主等）均有责任在其所参与的流程中对异常流量进行必要的检测和过滤，同时积极合作推动广告投放过程在各环节被完整监控、可追溯。

A.3.1 测量机构需要建立的制度和措施

1) 建立对数据和数据应用的规定和控制措施，包括对于异常流量鉴别的常规分析。

2) 保证数据完整性的方法，抽样方法的误差分析（如果使用了抽样方法）。

3) 采用多种方式（系统自动和人工等）研究分析异常流量。

4) 定期应用报告结果改进检测方法。

A.3.2 异常流量检测的业务流程和报表输出要求

1) 测量机构根据收集到的数据，计算输出过滤前的流量总量

2) 针对一般性异常流量进行过滤

3) 在过滤掉一般性异常流量的基础上，输出指标和报表同时甄别复杂异常流量

A.3.3 一般性异常流量过滤方法

1) 基于名单和参数的过滤

2) 不能获取浏览器用户代理信息的流量

3) 已知的来自数据中心流量

4) 已知的来自高危或者作弊来源的流量

5) 爬虫或高度嫌疑爬虫流量

6) 基于行为的检测和过滤

7) 明显异常的高速、连续重复请求

8) 含有非法或异常参数及字符

9) 基础信息缺失或不一致

A.3.4 异常流量举证

异常流量的举证由广告主或者媒体发起，需广告主授权，测量机构方可提供异常流量证据。为了保护异常流量的具体检测方法和阈值，异常流量举证由测量机构采取抽样的方法提供，样本中包含的字段需要由举证发起方和测量机构共同协商，建议包含以下信息：

1) 事件类型（描述业务或转化的信息，例如曝光、点击等）

2) 时间戳

3) IP 地址

4) 用户代理标识（或浏览器、操作系统信息）

5) 广告活动、媒体、广告位信息

A.4 异常流量审计要求

A.4.1 提交审计的材料说明

测量机构申请关于本标准的认证需要提供以下文档和说明：

1) 关于保证数据完整性的说明

2) 关于检测一般异常流量的方法说明

3) 关于检测复杂异常流量的方法说明（如果提交了此审计项）

4) 异常流量相关的内部政策和流程（例如根据异常流量情况改进检测方法的数据分析情况和记录）

5) 业务合作伙伴检查的政策流程

6) 审计公司要求的为了理解系统、制度和流程的其他文件

A.4.2 合作伙伴检查要求

测量机构有时候会接触业务合作伙伴来满足测量要求，这里的业务合作伙伴是指和测量机构有合作关系且在广告行业中充当一定角色的机构。为了促进整个产业链的健康发展，测量机构需要有规则和流程来保证选择的业务合作伙伴符合相关法律法规和行业标准并且充分理解异常流量的检测和过滤。

这些规定和流程应该满足以下需求：

1) 业务合作伙伴是否合法（例如是否有国家机关颁发的相关证件，是否有固定地址电话联系人等，是否有相关行业机构认证等）

2) 业务合作伙伴是否有不良行为记录（例如被行业黑名单记录）

3) 业务合作伙伴的产品是否有异常流量相关的功能

4) 业务合作伙伴是否出于逃避异常流量检测的目的来寻求合作

5) 对于业务合作伙伴，需了解其相关业务流程，以及其取得的相关第三方审计认证（如果有）

6) 对于重要的业务合作伙伴（即影响异常流量检测过程的合作伙伴）需要提供独立的审计认证，证明这些业务伙伴符合本标准；如果本标准对业务合作伙伴不适用，需保留对应的记录用于今后检查和审计。

A.5 异常流量报告要求

异常流量报告，至少需要包含一般性异常流量部分。一般性异常流量的报告输出需包含且只能包含如下内容：

A.5.1 基于名单和参数的过滤

1) 机器人和爬虫或其它伪装成合法用户的流量。

2) 无法获取浏览器用户代理信息、非浏览器用户代理信息或其它形式的未知浏览器带来的流量。

3) 已知的来自数据中心、高危作弊来源、预加载且没有指定触发时间的流量。

A.5.2 基于行为的检测和过滤

1) 明显异常的高速、连续或重复请求

2) 含有非法或异常参数及字符、基础信息缺失或不一致

3) 隐藏/堆叠/覆盖或以其它方式不可见的广告投放的数据（在可见曝光相关统计中过滤）

注 1：一般性异常流量报告需包含上述分类的具体流量分布。

A.5.3 复杂异常流量报告

可选择性包含复杂性异常流量部分。

1） 复杂性异常流量的报告输出需包含且只能包含的内容

2） 劫持设备以及设备中的会话；

3） 非法劫持广告创意和操纵流量；

4） 内容盗用、伪造、虚假展示；

5） 恶意修改、插入或删除 cookie 内容以改变用户访问记录；

6） 操纵或伪造位置数据以及相关属性。

7） 不包含在上述内容中的其他复杂性异常流量

注 2：复杂性异常流量报告需包含上述分类的具体流量分布。

注 1：