Media Rating Council, Inc.

420 Lexington Avenue
Suite 343
New York, NY 10170

Tel: (212) 972-0300
Fax: (212) 972-2786
www.mediaratingcouncil.org

Originally Authored January 2024

Published Final April 24, 2024

To: Digital Measurement Vendors Subject to MRC Audit

From: George Ivie, Laris Oliveri and Ron Pinelli

Re: 2024 IVT Interim Updates

Abstract:

Through the course of MRC's audit activities of digital measurement services, observations of emerging Invalid Traffic (IVT) threats as well as dynamic aspects of the measurement environment have led to the need to update and enhance IVT requirements in the following key areas:

-Privacy implications on IVT [applicable to all digital vendors; GIVT and SIVT]
-Domain and inventory mismatch and Bundle ID Spoofing in Connected TV (CTV) [applicable to SIVT digital vendors]
-Property-level considerations [applicable to SIVT digital vendors]

The following represents a discussion of these key areas, references to existing related requirements and incremental updates to these requirements **(updated requirements in bold**).

Background:

On October 27, 2015 the Media Rating Council (MRC) issued the final *Invalid Traffic Detection and Filtration Guidelines, Version 1.0* and in June 2020 MRC updated these former Guidelines by issuing the final *Invalid Traffic Detection and Filtration Standards Addendum (IVT 2.0)*. The standards can be found here:

https://www.mediaratingcouncil.org/sites/default/files/Standards/IVT%20Addendum%20Update%20062520.pdf

Privacy Implications on IVT [applicable to all digital vendors; GIVT and SIVT]:

MRC's position is that privacy regulations are not a barrier to be engineered around, but hard and fast requirements that must be adhered to and considered when designing measurement methodologies. MRC Standards are not intended to, and do not provide measurers with reasons or permission to deviate from privacy requirements. While MRC's measurement requirements and related auditing is not intended to directly assess privacy compliance, data collection, processing and transmission processes are encouraged to adhere to applicable privacy regulations and requirements. Measurers should consider whether proper permissions and access rights are present including whether they clearly state in their privacy policies why they are collecting information and how it may be used and shared.

Measurement organizations are encouraged to consider and comply with additional industry and regulatory guidelines and requirements in this area where applicable. Localized privacy regulations must also be considered. Privacy regulations as they emerge should be monitored and evaluated by the measurement organization as soon as known to the extent they impact measurement. Future browser and identification restrictions are likely to continue to evolve and MRC will make efforts to stay abreast of and consider these throughout, as well as to update measurement Standards as warranted.

Specifically, as it relates to IVT detection and filtration, MRC has evaluated all aspects of the IVT 2.0 Standards and excerpted any current requirements that may be impacted by current and prospective future privacy restrictions and changes, primarily centered around user level attributes such as IP address. Limited or no IP address and less granular User Agent (UA) string may impair list-based approaches, particularly current Specific Identification, Data Center GIVT approaches and Activity Based techniques requiring session or user level analysis. The following provides excerpts of current IVT requirements that may be impacted by privacy and signal availability :

IVT 2.0 Excerpts:

1.1.2 Categories of IVT and Associated General Requirements

This addendum establishes two categories of IVT. The first, referred to herein as "General Invalid Traffic" or GIVT, consists of traffic identified through routine means of filtration executed through application of lists or with other standardized parameter checks. Key examples are:

- *Known invalid data-center traffic (determined to be a consistent source of invalid traffic; not including routing artifacts of legitimate users or virtual machine legitimate browsing);*
- *Bots and spiders or other crawlers (except those as noted below in the "Sophisticated Invalid Traffic" category);*
- *Activity-based filtration using transaction-level data and parameters from campaign or application data;*
- *Non-browser user-agent headers or other forms of unknown browsers;*

1.1.4 Data-center Traffic (previously part of interim guidance)

The filtration of invalid data-center traffic contemplates the availability and use of industry lists in order to promote consistency amongst vendors. While measurement organizations are strongly encouraged to utilize available industry lists, there may be limitations to these lists (e.g. the TAG Data Center IP list is limited to traffic from data-center IP addresses where human traffic is not expected to originate and excludes mixed data-center IPs). In lieu of or in addition to the use of such industry lists, measurement organizations must seek alternate means to develop filtration rules for this type of invalid traffic. While impression-level granularity in filtration is preferred, as a starting point, the MRC is requiring filtration of invalid data-center traffic originating from IPs associated to the three largest known hosting entities: Amazon AWS, *Google and Microsoft. This means filtration of IPs within those of known hosting entities determined to be a consistent source of invalid traffic not including routing artifacts of legitimate users or virtual machine legitimate browsing.*

3.2 General Data Analysis

A measurement organization shall establish and maintain a function that assesses and researches the attributes of the data it collects and reports. A part of this research-oriented function is to provide input into new methods of invalid traffic detection and alerting as well as the efficacy of existing employed methods at removing material invalid traffic.

This general data analysis function shall contain the following areas, which are considered useful to the invalid traffic detection process:

- *Data Attribute & Pattern Analysis*

Data quality and completeness is a critical element of invalid traffic detection and filtration and accordingly this function must be independent from data collection and charged with ensuring business partners and other sources of traffic data are complete and fully populated to facilitate application of internal controls and detection processes. Data completeness for events or transactions shall include elements such as device information, user information (cookies, IP address, user agent string [as complete as possible, unmodified], and relevant ad serving information (ad serving sources, placement and campaign information, site information, application information, referrer information, etc.). The objective is to ensure the full record is received, not partially or fully lost or otherwise not corrupted.

The objective of measurement organizations and their business partners shall be to ensure transparency with respect to where the ad is served from, the device type and the user agent receiving the ad. This information shall be captured in ad serving transactions and maintained across business partner information transfer. The following fields shall be captured by the measurement organization, where possible/applicable (current or future data collection restrictions to measurement related to user identification and privacy requirements may preclude collection of one or more of these fields; while MRC believes current privacy requirements allow effective IVT telemetry in all required areas, should future requirements arise that consistently limit IVT capabilities across vendors, MRC will reassess requirements accordingly):

- *IP Address (X-Forwarded-For especially in instances of traffic routing or use of proxies such as in a corporate structure, for OTT or Server Side Ad Insertion [SSAI])*
- *MAC Address*
- *User Agent (full user agent string, browser and OS)*
- *Cookie/Unique Identifier or Mobile ID Field^^*
- *App Identifier (iOS IFA [numeric or bundle], Google AID, Windows AID)^^*
- *Mobile Telephone Number (can be partially obscured for PI reasons)^^*
- *Referrer Site Information, if applicable*
- *Device ID, Device Type^^*

^^ The above list includes specific fields for mobile devices, although many of the general fields also apply to a mobile environment.

General Note 2: Personal Identifying Information (PII) legal requirements and restrictions or browser restrictions may dictate eliminating one or more of these fields from retained records or altering the content of fields for identity protection purposes. In these cases deviations must be supported by the measurement organization's privacy policy and must be available for review by auditors. Differential collection by browser or environment due to data collection restrictions should be considered, disclosed as a limitation where applicable along with any related impact and be periodically studied with regard to the impact on IVT effectiveness. Auditable evidence of this periodic study shall be retained for inspection. As discussed throughout this document, measurement organizations should take steps to mitigate false positive/negative IVT identification and should take care to not erroneously invalidate traffic with missing information due to privacy constraints without direct IVT signals and instead consider this unmeasurable for IVT (not valid by default).

Measurement organizations are expected to comply with legal and business contractual requirements within the countries they operate; accordingly if a formal (legally dictated) privacy restriction in a country prevents the capture and tracking of certain of the fields stated above, these can be excluded. In all cases, documentation of legal limitations, by country, shall be maintained by the measurement organization. The MRC Staff will attempt to collect these data collection restrictions across measurement organizations to understand the consistency of interpretations as well as build an understanding of regional differences in laws.

4.1.3 Data Analysis and Discovery Functions

Additionally, the following data analysis and discovery functions are strongly encouraged for SIVT Process measurement organizations:

- *Indirect Detection Techniques – alternatives to be considered for inclusion but are not limited to:*

Using device or parameter-based fingerprinting, as permitted depending on privacy circumstances

4.2 Analysis of Specific Production Traffic or Campaign Data

The following techniques shall be employed by the measurement organization to the extent necessary to filter material General Invalid Transactions:

- *List or Parameter Based Detection*
    - *Traffic that Does Not Originate from Known Browser Types*
        - *Non-Browser User-Agent Header*
    - *Activity-Based Detection and Removal Techniques – Based on transaction-level data and parameters from campaign or application data; traffic is removed when thresholds or other negative evaluation criteria are met*
        - *Continuous; Full Coverage of Monetized Traffic*
        - *Speed of Transactions*
        - *Repeat Transactions*
        - *Interval Testing*
        - *Outlier Identification*

        - *Missing Values, Missing UAs, etc.*
        - *Transaction Protocol Verification*
        - *Inconsistencies in Transaction and Browser/Agent Parameters*

4.2.2 Mobile In-App and OTT Controls (In-App content previously part of interim guidance)

Mobile in-app and OTT specific SIVT considerations shall include (but not be limited to) where known:

- *Presence of proxy traffic or routing artifacts that may obfuscate origination information or limit the granularity of data collected for purposes of IVT determination. The potential disproportionate presence of proxy or data center traffic in OTT traffic (due to the delivery models present) may not only lead to false positives (valid traffic filtered), but also inhibit the ability to collect certain parameters or originating information necessary to effectively evaluate traffic for validity. OTT measurement organizations shall consider these aspects of OTT traffic when applying invalid traffic detection and filtration techniques to it and consider false positives as required (proxy and data center traffic must be known to be invalid in order to be filtered, otherwise it must be treated as unknown and not included in the numerator of the decision rate discussed below for purposes of IVT).*

Measurement organizations applying SIVT detection and filtration techniques must also consider mobile applications and OTT discretely in setting parameters or determining heuristics used should they represent a material portion of measured and filtered traffic. Mobile in-app and OTT SIVT specific considerations must include (but not be limited to) where known:

- *Presence of proxy traffic or routing artifacts that may obfuscate origination information or limit the granularity of data collected for purposes of IVT determination as discussed above and as a means to collect originating and more granular data (such as X-Forwarded-For data).*
- *Differentiation of parameters or heuristics by device such as:*
    - *Device type/operating system*
    - *Device status (stock/jail-broken) where known and applicable*
- *Differentiation of parameters or heuristics by user such as:*
    - *Population or content of collected user information, or lack thereof*
    - *Inconsistent user parameters*

Valid app installs must be tied to corresponding valid impressions and clicks directly measured and subject to unique identifiers. In addition, specific activity-based logic shall be applied to the relationship between impressions, clicks and installs including the time between them (short, illogical durations may be a signal of invalid activity) as well as to post-install activity (non-use or deinstallation may also be a signal of invalid activity). Invalid installs may be tied to generation of invalid impression and click activity through hidden ads, redirects and routed traffic and must be considered regardless of the reporting of app installs when measuring application activity.

4.3 Removal of Internal "Unnatural" Activity

Measurement organizations shall have procedures to segregate all internally generated activity (that of the measurement organization and the organization under measurement) which does not represent legitimate advertising consumption or otherwise valid internet traffic – for example: software testing; tag testing by publisher, agencies and advertisers; corporate mandated transactions that may drive traffic unnaturally high, offline scanning or other contracted site governance techniques, etc. These activities are considered invalid traffic for advertising commerce purposes if material, but are allowed to be removed prior to impression counting (prior to invalid traffic measurement and reporting) with appropriate support.

Development and testing environments shall be logically segregated from or clearly distinguished in production environments as to not commingle test and production transactions. Such traffic may be excluded from impressions altogether with support and mechanism to do so (dedicated IPs/campaign IDs and contractual or other evidential support for the activity). Publishers should provide a mechanism to identify and segregate this traffic or otherwise declare it to measurement organizations as well as ad servers, as absence of these mechanisms precludes measurement organizations from doing so. Excluded test impressions may be separately reported (distinguished in some manner) to help reconcile and minimize discrepancies.

Interim Updated Requirements [applicable to all digital vendors; GIVT and SIVT]:

The above IVT requirements may necessitate reliance on the ability to obtain and analyze IP address and UA as well as "user" level analysis of activity (such as cookies, fingerprinting or other individual identifier processes or proxies). All measurement organizations (GIVT and SIVT) must periodically assess (at least annually) IVT detection capability reliance on IP address, UA and user-level analysis and the impact privacy-related changes, signal availability and signal granularity have on the ability to make IVT determinations by incorporating privacy considerations into required periodic IVT risk assessment processes to determine whether IVT detection avoidance that may be disguised as limitations of signal availability due to privacy is present and has an impact on IVT risks as well as assess whether detection capabilities require changes to IVT techniques, approaches and analyses to account for this risk. Measurement organizations must retain evidence and results (such as meeting minutes, desk review documentation, related data analyses, legal review input, etc.) for audit purposes related to consideration and inclusion of privacy considerations within required periodic IVT risk assessments.

If material impairments in IVT capabilities arise (material as defined within MRC IVT standards relative to reported metrics or particular signals or filters), measurement organizations must research the impact these impairments have (and generally disclose these limitations to measurement users) as well as actively research alternative approaches to comply with existing requirements where possible.

MRC will continue to assess IVT requirements and the feasibility of compliance with the changing privacy landscape and consider updating these requirements with the objective of seeking to avoid reducing the rigor of IVT detection and filtration and also work within the industry to highlight challenges that privacy initiatives raise for IVT measurement and to

research how these initiatives may be adapted to minimize the impact and risks to IVT measurement organizations.

To that end, the MRC encourages audited organizations to raise concerns and report industry changes that may limit or challenge adherence to existing IVT requirements as they are currently written so that we may consider in future updates. Based on this, the MRC may proactively and periodically conduct reviews of expected signal availability and their impact on current IVT guidance. Finally, evolving Privacy-centric environments may result in different degrees of availability of signals for different entities, depending on their placement in the ad ecosystem and their relationships with other entities. As a result, some signals that are available for IVT purposes may be sourced from entities with greater or lesser access than others. Measurement organizations should differentially consider carve-outs and signal sharing exceptions vs. general signal availability in their risk assessments with regard to privacy impacts on IVT and consider differential approaches and disclosures (see further discussion on decision rate below).

Further, Section 2.4.1 of IVT 2.0 requires the computation and disclosure of an IVT decision rate:

Computed as recorded impressions where the vendor was able to collect sufficient information and signals as designed/intended to be collected and used to make an IVT determination; divided by the total number of impressions (or respective transactions, if applied to something other than impressions) intended for measurement and reporting by the same measurement organization. Impressions without sufficient information to make an IVT decision must be reported as such and must not contribute to IVT metrics or rates.

In situations where differential detection capabilities are present and vendors may not be able to make a full IVT decision, this traffic must be reported as unknown and not included in the numerator of the decision for purposes of IVT reporting and not assumed to be valid or invalid unless supported to be without material false positives or negatives. The data fields required to consider an impression recorded where the vendor was able to collect sufficient information and signals as designed/intended to be collected and used to make an IVT determination may vary depending on vendor methodology and environment, but must be empirically supported and demonstrable through auditable evidence.

Interim Updated Requirements [applicable to all digital vendors; GIVT and SIVT:

The IVT decision rate was designed to actively disclose to measurement end users differential levels of IVT detection capabilities as well as to assist in identifying inventory sources where IVT determinations are unable to be made (unknown). However, limitations in signal availability due to privacy may unfairly understate true measurement organization capabilities or inventory source quality, but also may enable bad actors to evade IVT detection. To address these issues, this interim update further requires all measurement organizations to evaluate their IVT decision rate by source and reason and differentiate levels of unknown IVT due to privacy restrictions in aggregate, and by source where material and possible. Finally, SIVT measurement organizations should make reasonable attempts to determine if limitations in signal availability or granularity represent legitimate compliance with privacy requirements or are attempts to evade IVT detection and differentiate this in reporting where possible or otherwise generally disclose

it, including considering known and supported attempts to evade IVT detection as IVT (not unknown).

This may also involve processes to notify or warn publishers or other entities being measured of abnormally low IVT decision rates where appropriate and where a relationship between the measurement organization and these entities exist in order to allow these entities to enable signals where permissible with privacy requirements, taking care to avoid enabling reverse engineering or revealing sensitive information to suspected bad actors or unknown entities. Measurement organizations should consider existing Discrepancy Resolution requirements (Section 4.4.1 of the IVT Addendum) as part of these processes.

Domain and Inventory Mismatch and Bundle ID Spoofing in CTV [applicable to SIVT digital vendors]:

IVT 2.0 Excerpt:

1.1.2 Categories of IVT and Associated General Requirements

The second category, herein referred to as "Sophisticated Invalid Traffic" or SIVT, consists of more difficult to detect situations that require advanced analytics, multi-point corroboration/coordination, significant human intervention, etc., to analyze and identify.

Key examples are:

- *Domain and App misrepresentation: App ID spoofing, domain laundering and falsified domain / site location;*

Interim Updated Requirement [applicable to SIVT digital vendors]:

Current IVT requirements for SIVT include situations of domain or app misrepresentation whereby property IDs are spoofed, laundered or falsified. However, this current requirement does not explicitly dictate that SIVT measurers actively consider disclosed property IDs (such as domain, sub-domain and app ID) pre-bid or in bid values and compare them to the IDs where ads are delivered, this does not include considerations of inventory type nor does this current requirement consider CTV bundle IDs (strings of characters used by advertisers and ad platforms to identify specific apps on CTV platforms). GIVT measurement organizations are encouraged to determine if such activity can also be included within GIVT processes such as protocol validation or inconsistencies in transaction and browser/agent parameters where applicable.

SIVT measurement organizations are encouraged to obtain and consider bid information where possible. To the extent that an SIVT measurement organization receives pre-bid property ID information (either directly or through declared bid information), the SIVT measurement organization should have processes to consider the reliability and accuracy of this information and if deemed reliable, compare and reconcile this to the property ID information of where the ad is served where available. If this information does not match or reconcile, or is otherwise obfuscated or missing, the SIVT measurement organization should consider whether this traffic should be considered SIVT due to domain or app

misrepresentation. SIVT measurement organizations should have formal processes to determine if this mismatch represents a legitimate situation (such as due to properly disclosed referral or affiliate traffic) or is due to error (such as spelling, syntax or format), but illegitimate mismatch or situations where there is evidence of falsified property ID (such as in situations where properties are meaningfuly different from each other) should be deemed SIVT. For errors or missing values not deemed SIVT or in cases where bid information is not deemed fully reliable, SIVT measurement organizations are encouraged to separately report this as well as to discuss these occurrences with publishers where they have a direct relationship in order to help rectify these situations. Measurement organizations should consider existing Discrepancy Resolution requirements (Section 4.4.1 of the IVT Addendum) as part of these processes.

Further, SIVT measurement organizations should also consider mismatches in inventory or placement type (e.g., display vs. video, in-stream vs. accompanying content vs. interstitial vs. standalone per IAB placement definitions or onsite vs. offsite) as part of IVT determination. To the extent that an SIVT measurement organization receives pre-bid inventory type or placement information, the measurement organization must compare and reconcile this to the inventory or placement type of the ad served where available. If this information does not match or reconcile, the SIVT measurement organization must consider whether this traffic should be considered SIVT due to inventory misrepresentation. Illegitimate mismatch or situations where there is evidence of intentionally falsified inventory or placement type should be deemed SIVT.

Finally, CTV Bundle ID should be included in the existing requirements for App misrepresentation and spoofing for SIVT measurement organizations that measure CTV, including whether the ID is a legitimate CTV App. Non-CTV Apps misrepresented as CTV should be considered SIVT.

SIVT measurement vendors are also encouraged to make use of available telemetry such as through ads.txt or app-ads.txt in their IVT considerations under this requirement for all of the above considerations.

Property-level considerations [applicable to SIVT digital vendors]:

Section 4.2 of IVT 2.0 requires all digital measurement organizations to include *"Known Dangerous or Fraudulent Sources, Based on Specifically Identified Blocking Lists"* as part of list or parameter-based detection. Further, IVT 2.0 Section 1.1.2 includes the following SIVT requirements:

- *Incentivized human invalid activity: self-directed activity to benefit self or harm others and directed activity;*
- *Manipulated activity: Forced new browser window opening, forced tab opening, forced mobile application install (mobile re-direct), forced clicking behavior, tricking users to click / accidental clicks, clickjacking (UI redress attack) and hijacked measurement events;*
- *Hidden/stacked/covered/transparent/invisible or otherwise intentionally obfuscated ad serving such as Z-order stacking, banner stuffing, transparent ads and background cycling and pop-under with auto-close (specific to ads);*

- *Adware and Malware that conduct deceptive actions including ad injection and unauthorized overlays;*
- *Misappropriated (pirated or stolen) content (where used to purposefully falsify traffic at a material level);*

While existing IVT 2.0 requirements have required SIVT measurement organizations to detect and filter the above activities at an impression level, these have not included more holistic requirements to consider the property or source itself. There are instances where a property or inventory source may have a high degree of IVT, with some legitimate traffic making up the minority of traffic.

Such as is the case with “Made for Advertising” and “Made for Arbitrage” properties or MFAs. MFA’s have long been discussed in the media industry with various definitions as low-quality properties with very little to no content and high ad density. These properties also often include incentivized or purchased traffic, manipulated activity, hidden or stacked ads, adware/malware and misappropriated content, which are invalid activities as defined by MRC, but may also have a degree of valid traffic.

While IVT 2.0 requirements preclude labeling valid traffic as invalid solely based on the inventory source (a false negative), MRC believes property-level IVT reporting would provide additional data to help inform ad delivery practices and IVT avoidance.

Interim Updated Requirement [applicable to SIVT digital vendors]:

In addition to IVT filtration requirements at an impression level, SIVT measurement organizations should consider including properties exhibiting high degrees of SIVT as well as those with a high degree of incentivized or purchased traffic, manipulated activity, hidden or stacked ads, adware/malware and misappropriated content as part of possible known dangerous or fraudulent sources, to enable specifically identified blocking or inclusion lists where available at a user’s discretion. To facilitate this, measurement organizations must report the percentage of invalid activity of total activity where an IVT decision can be made along with the IVT decision rate for reported metrics on a property-level (domain, sub-domain and App ID) subject to minimum thresholds of activity defined and empirically supported by measurement vendors to prevent reverse engineering, in addition to reporting impression level filtration to enable measurement users to use this information to make decisions about what properties ads are served to (through exclusion or inclusion thresholds or lists).

These requirements pertain only to IVT as defined by MRC and should be delineated by GIVT vs. SIVT where reported at an impression level. These requirements do not include that more subjective aspects of site or content quality/design are included in the above consideration nor do they mandate blocking at a property level for IVT or suspected MFAs without user specification. Further, it is encouraged that measurement organizations contribute to and make use of commonly available industry lists of known dangerous or fraudulent sources or MFAs based on IVT definitions where available or if they become available in the future, for consistency and comparability.

This may also involve processes to notify or warn publishers or other entities being reported as having high IVT (as part of MFA designations or otherwise) where appropriate

or where a relationship between the measurement organization and these entities exist in order to allow these entities to enable signals where permissible with privacy requirements, taking care to avoid enabling reverse engineering or revealing sensitive information to suspected bad actors or unknown entities. Measurement organizations should adhere to existing Discrepancy Resolution requirements for IVT reporting (Section 4.4.1 of the IVT Addendum), which apply to customers and non-customers, as part of these processes.

Adoption Process:

The MRC has produced this interim guidance based on input from our membership, industry trade organizations and an IVT Update working group and until such time as there is a formal standards update that incorporates it, this interim guidance is considered authoritative. This interim guidance should be applied by measurement services in the MRC accreditation process as part of initial accreditation audits or the next planned recurring accreditation audit after the date of publication of these interim updates. If the timing of these audits where this interim guidance takes effect is imminent, MRC will discuss a grace period for adoption on a case by case basis and may periodically update the marketplace regarding compliance with these requirements across audited services.

Please contact Ron Pinelli at MRC (rpinelli@mediaratingcouncil.org) or Laris Oliveri (loliveri@mediaratingcouncil.org) with any questions.