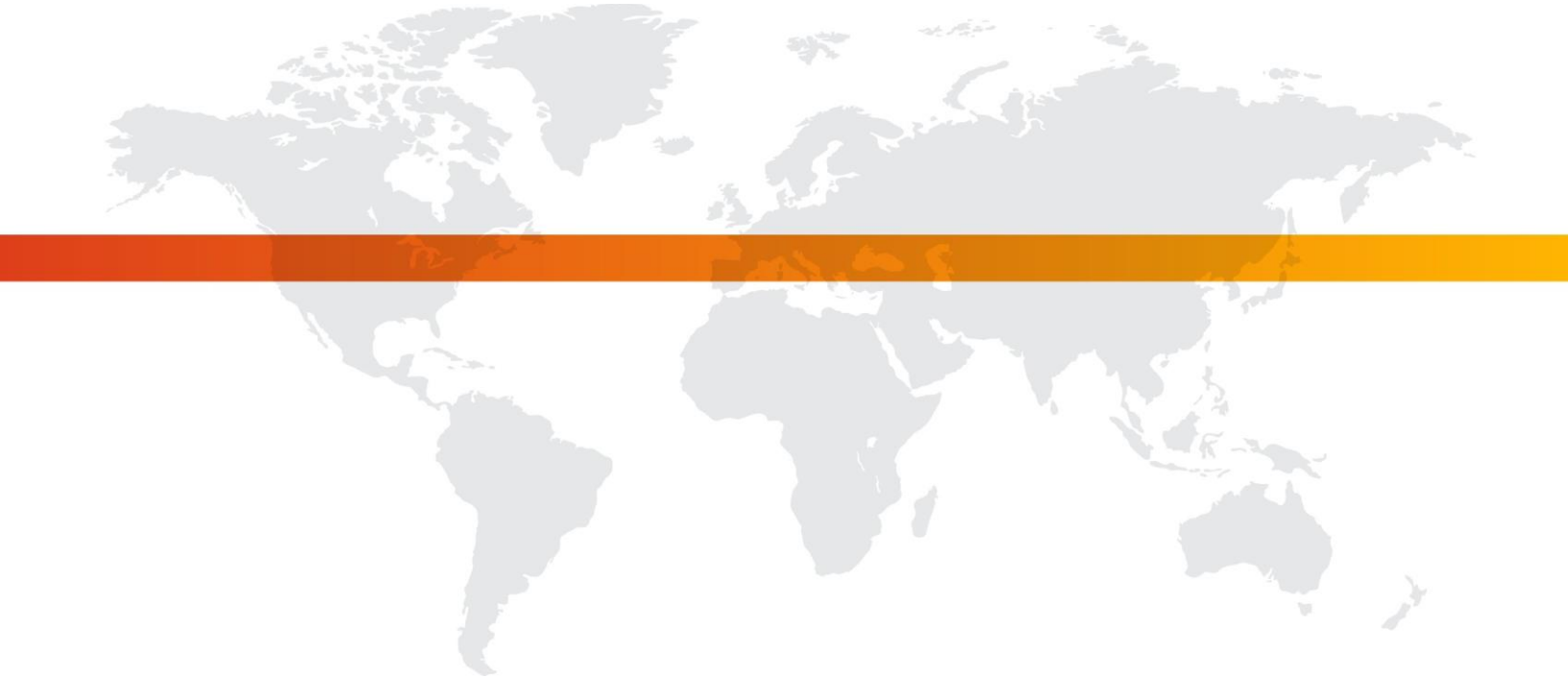
comscore

Description of Methodology

Comscore Direct

March 2021

Version 1.33



Summary of Changes

Version 1.33 March 22, 2021	Added disclosure related to IVT Decision Rates as required by MRC's IVT 2.0 Standards.
Version 1.32 March 15, 2020	Updated to include disclosures related to iOS updates (forking to iOS/iPadOS) Added discussion of Chrome SameSite attribute treatment to assure 3rd party cookies can be set. Updated example UI reporting.
Version 1.31 March 18, 2019	Sample Traffic Review update to current period
Version 1.30 November 19, 2018	Updated Comscore branding/logo
Version 1.29 June, 2018	Remove reference to MRC Accreditation given Census tagging, collection and processing will be addressed in Media Metrix® going forward.
Version 1.28 April, 2018	Added disclosures related to Unique Cookie limitations
Version 1.27 September, 2016	Updated reissuance policy incorporating backward looking assessments for invalid traffic
Version 1.26 July, 2016	Updated disclosures related metric labeling and Invalid Traffic (frequency/granularity of reporting, partner qualification and auditing)
Version 1.25 September, 2015	Update to reflect Minimum Reporting Standard for Unique Cookies
Version 1.24 August, 2015	Updated references to Page Views to Pages to assure readers do not interpret this as viewability measurement.
Version 1.23 August, 2015	Updated language referencing Invalid Traffic in lieu of Non-Human in line with the Public Comment version (5.0) of MRC's Invalid Traffic Guidelines. Also note Direct's assertion that General IVT Filtration is reflected in reported data whereas Sophisticated IVT is identified/filtered downstream in the Media Metrix® process.
Version 1.22 July, 2014	Updated to reflect accreditation of Unique Cookies (p.2), alerting for publishers who have not supplied internal IP addresses for filtration (p.8), enhancements to highlight Unknown Domains and drive understanding of their importance (p.6) and declare the threshold for restatement of reported results (p.11).
Version 1.21 July, 2013	Application reporting added (p.3), data caching limit updated (p.5), additions to data validation protocol (p.5).
Version 1.1 October, 2012	Incorporated enhancements to publisher internal traffic filtration (p.7).

General Overview

comScore, Inc. (Comscore) provides audience measurement of internet sites and services through multiple methodologies, including: panel-based measurement, direct measurement and Unified Digital Measurement (UDM). This description of methodology covers the direct measurement methodology termed Comscore Direct (Direct). The Direct methodology obtains measurement information through the use of a measurement tag, placed on the participating publisher's site pages by the publisher, which is requested from the measurement server, which is hosted by a third-party content delivery network (CDN) vendor. These tags utilize a JavaScript process, and are backed up by image calls included within NOSCRIPT tags in order to measure activity generated from a browser or application that does not execute JavaScript.

Comscore reports Direct audience and traffic measures, including metrics pertaining to websites, distributed content, ad and video content, presenting counts and other audience reported data (Unified Digital Measurement) by month (selected calendar month) or custom date range; and geography.

The measurement process is census based, not-sample based; therefore, there are no universe estimates or statistical projections of the data. The measurement methodology is based on all activity recorded (subject to filtration procedures).

Client-initiated Counting

The IAB Guidelines define a page impression as "measurement of responses from a web server to a page request from the user browser, which is filtered to remove robotic activity and error codes prior to reporting, and is recorded at a point as close as possible to opportunity to see the page by the user".

For AD campaign measurement, the IAB Guidelines indicate that measurement should occur "at a point as late as possible in the process of delivery of the creative material to the user's browser – therefore closest to the actual opportunity to be seen by the user." Client-initiated counting (where client refers to the user's browser), which is required by the IAB Guidelines, relies on the browser to initiate the measurement requests, subsequent to the initial page request, that result in the counting of user activity. Therefore, the measurement requests are not processed and logged by the servers during the initial page request, but rather as part of a subsequent set of requests or communications (transactions) initiated by the browser.

There are several different accepted methods for performing client-initiated counting specified in the Ad Campaign Measurement & Audit Guidelines based on the requirement that "the count must happen after the initiation of retrieval of underlying page content".

"Permissible implementation techniques include (but are not limited to) HTTP requests generated by <IMG>, <IFRAME>, or <SCRIPT SRC>."

Publishers that participate in the Direct measurement methodology implement Comscore measurement tags onto the pages of their sites or within their flash-based content such as videos and widgets. Therefore, the actual implementation of the client-initiated measurement tag is the responsibility of the publisher, and not Comscore.

When the browser or application renders Direct tagged content, the browser will encounter the Comscore measurement tags and make the designated call to a third-party vender, who manages the data collection

servers. In response to the measurement tags, the data collection servers record the activity and return an invisible (transparent) pixel to the browser or application. Measurement of the user activity occurs when the data collection server acts upon the request, records the activity, and returns the transparent pixel.

Comscore's primary measurement methodology uses a JavaScript function included via a <SCRIPT SRC> tag. Additionally, an <IMG> tag is used to allow for measurement of JavaScript incapable browsers or internet applications. Both of these implementations are specifically identified as permissible implementations within the Ad Campaign Measurement & Audit Guidelines. Under this implementation, the following series of events occurs while the browser renders the complete web page:

1. The user's web browser requests the web page content from the publisher's web content server, which includes a small, initial portion of the Direct JavaScript measurement code (Beacon JavaScript);
2. The user's browser executes the Beacon JavaScript, which makes a request to the measurement servers;
3. The measurement servers receive the request and return the full Direct JavaScript measurement tag (web beacon);
4. The user's browser executes the full Direct JavaScript measurement tag, which in turn sends the full measurement data records to the measurement servers, by making a request to the measurement servers;
5. The measurement server records the activity and then delivers a '204 No Content' server code (server request complete).

The Beacon JavaScript file that is returned, as noted in Step 3 above, is designed to be cached for up to seven days. In the event that the user has accessed Direct measured content during the prior seven days, and the browser has cached the Beacon JavaScript file, Steps 2 and 3 are not required, allowing the browser to construct the full measurement data record and send the request (Step 4) to the measurement servers.

Additionally, in the event that the browser is not JavaScript capable (either incapable or disabled) the code contained within the page itself (Step 1) also includes a direct call to the measurement servers that will be sent if the JavaScript is not executed. This allows for measurement even if the user's browser does not execute JavaScript.

In the event that the user requesting the Direct measurement tag does not provide cookie information, the measurement tag request will result in a "302 redirect" response by the measurement server to attempt the assignment of a cookie to the subsequent measurement call. This attempt to assign a cookie will add an additional step to the sequence of events outlined above.

As noted above, during the five steps of the process, the web browser renders the Direct measurement tag and makes the designated call to the measurement server. In response to the measurement tag (web beacon), the measurement server records the activity and returns a '204 No Content' server code to the browser. Measurement of the user activity occurs when the measurement server acts upon the Direct measurement tag request, records the activity, and returns a server code indicating successful completion of the request.

Comscore generates the tag HTML text for the Direct publisher and includes instruction on copying the tag and placing the JavaScript in the header of the page. This approach, while different than the recommended IAB bottom of the page approach, is an acceptable practice for generating the census based pages metric reported in Direct.

In addition, Comscore has developed an integrated measurement solution with Omniture, such that clients of both Omniture and Comscore can participate in Comscore Direct measurement without implementing an additional Comscore tag on their content pages. Refer to the Data Collection and Accumulation Process for additional details.

Data Collection and Accumulation Process

Due to the highly automated nature of the Direct methodology, certain errors in data collection, accumulation and processing may go undetected unless sufficient controls are in place to monitor the systems and analyze the reported results. Additionally, due to the reliance on the publishers to implement the tags properly, controls should be in place to detect publisher errors in implementing the tags to prevent errors in the reported results.

As previously discussed, Comscore utilizes a third-party to serve and log the initial measurement call, which parses the initial record utilizing a pre-determined format by Comscore. All valid record entries (e.g. 200 type event) are cached on the server for one minute (or up to 56kb of data), and pushed to the third-party storage system. No additional modifications, formatting, stripping or validation of data is performed by the third-party. Comscore servers search for files on the third-party storage servers in half-hour cycles and pull the files for processing and aggregation. Data on the third-party storage servers are deleted after the files are downloaded to Comscore servers.

Comscore performs the following data validation procedures to determine the completeness of the files:

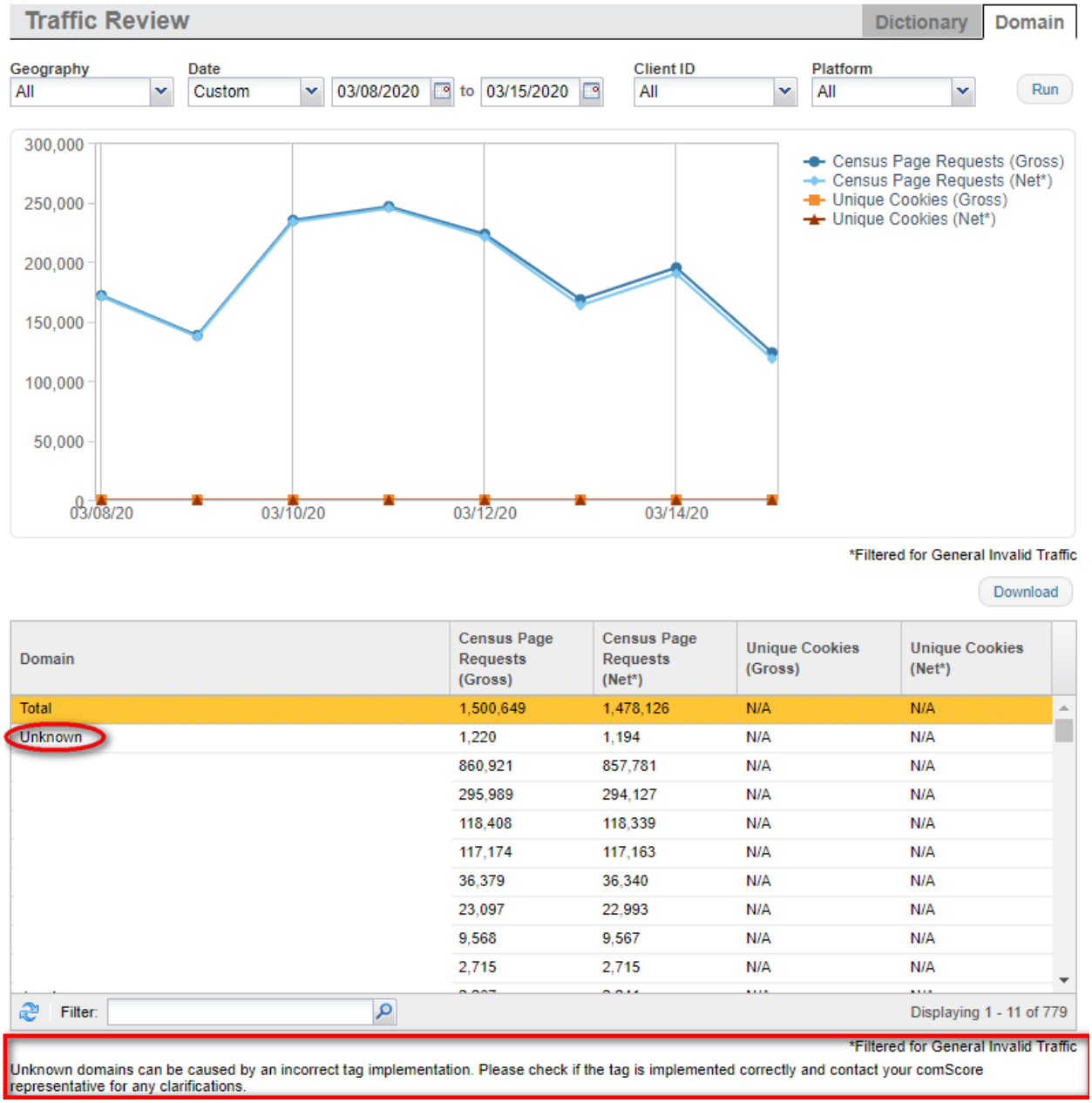
1. Comparison of the files downloaded to expected (manifest file);
2. Utilization of file checksums within file header;
3. Utilization of relational database between downloaded and processed files;
4. Unique file name (third-party server region, associated box and timestamp relating to half-hour data pull);
5. Confirmation of deleted third-party server files through the return of a “complete” http header.
6. Daily report to compare record counts downloaded to expected

Additionally, Comscore has developed an automated quality control process whereby Comscore makes scripted scheduled calls to Comscore’s CDN vendor. The calls received from third-party CDN vendor are identified and segregated for comparison with the original scripted request. Other procedures have been implemented to ensure that the CDN vendor is passing all of the data to Comscore and any material differences are investigated.

Although publishers implement the Comscore measurement tags on their own sites, Comscore provides a self-check tool to Direct publishers to determine if the tags were properly implemented on their web site (i.e., the self-check tool is in place to assist the developers so they can make sure that the beacons are firing correctly). Upon successful completion of this process, the user is informed that “Comscore will report counts as soon as they are received, usually within a day.”

Currently, Comscore’s Product Management Group assists clients with the implementation of the Direct measurement methodology through such procedures as training in the functionality of the user interface and obtaining and implementing the tags. Comscore currently is striving for a client “self-serving” implementation approach; however, Comscore’s intent is to continue to provide customer support for large clients with complex implementation procedures.

Comscore reporting in the User Interface includes a capability to report Unknown domains where traffic is detected with incomplete identifying information. This can be indicative of implementation errors so it is important to monitor for this and follow up if the level of traffic so reported is material. See below for an example:



As indicated above, Comscore has developed an integrated measurement solution with Omniture. With this integrated dual measurement enabled, the Omniture tag will reside within the content and when loaded, the browser will make the designated Omniture measurement call to Omniture measurement servers. In response, the Omniture measurement server will issue a 302 redirect to Comscore's data collection servers, which will then respond with the pixel. This process requires the publisher to provide certain Comscore Direct account information to Omniture so that Omniture can form the correct Comscore Direct measurement tag (URL) and redirect the browser to that URL.

The Omniture redirect is designed to result in the browser making a request to Comscore Direct's measurement servers in the same manner as a Comscore Direct tag. This request is similar to a Comscore Direct tag request, and is made to the same front-end CDN vendor servers. The differences in the request are primarily related to "form" such as the names of parameters within the URL; the "function" in terms of the data captured and reported in the URL string is consistent between the two measurement sources.

Once the request is logged in the Comscore Direct measurement servers, a transformation process is employed to cause the Omniture records to become equivalent to Comscore Direct records, and then all subsequent processing is identical. That is, post-transformation, both Omniture and Comscore Direct measurements are comingled and processed together using the same processes and through the same processing pipeline.

Data Editing Procedures

In accordance with the applicable industry guidelines, Comscore has implemented several measures to reasonably assure that data is scanned and filtered for non-qualifying activity, including the removal of incomplete and malformed tag requests. The remainder of this description of methodology document addresses specific IAB Guidelines and related Comscore procedures.

Invalid Traffic

Invalid traffic includes robots, spiders, crawlers and agents executing programmatic activity on the customer's websites. The activity is comprised of programs making requests for web pages on the website and recursively following the links on the page to other pages within the website. This activity may include system monitoring tools designed to ensure the website is functioning properly and content indexing or retrieving processes such as those used by search engines to populate their databases.

These utilities do not represent human web site traffic and can create significant overstatement if not identified and excluded from reported traffic counts. IAB Guidelines require procedures to identify and exclude this traffic using both specific identification procedures as well as activity based analyses. Additionally, as no process can identify and exclude 100% of this traffic, we disclose this fact to users of the reported data.

Comscore utilizes a dual pass specific identification approach for filtration of robotic activity. User agents are compared to a list of known robot user agent strings and to a list of known valid browser user agent strings. Any log entries that include a known robot user agent string are filtered as are log entries that do not contain a known browser user agent.

This specific identification filtration approach involves maintaining: (a) a list of known browsers and removing activity not associated with a known browser; and (b) a list of known robots, spiders and non-human agents and removing their activity. This identification is generally made on the basis of the user agent string and the IAB publishes both of the aforementioned lists for use by publishers. Comscore's has a manual process in place to obtain the current IAB lists and upload them to the processing servers.

Additionally, as a subcomponent of the IAB Guidelines requirements related to specific identification of invalid traffic, a robot instruction file (robots.txt) should be used to instruct compliant robots not to follow links pointing to the measurement servers. A robot instruction file is included in the root directory of Comscore's measurement servers.

Comscore Direct provides selected General IVT identification/filtration (Robots & Spiders, Invalid Browsers, Internal traffic) and Outliers (Sophisticated IVT) identification/filtration in the production or reported metrics. More comprehensive Comscore-identified General and Sophisticated IVT filtration of census data is supported downstream in the Media Metrix® process. Following provides additional information related to the Direct filtration process:

- **Granularity and Frequency of Invalid Traffic Processes**
  vCE invalid traffic identification and filtration operates at the individual impression level. Invalid traffic is identified in hourly processing.

- **Partner Qualification**
  Comscore employs internal partner qualification controls in order to assure advertisers and publishers accessing its data represent legitimate businesses rather than being intentionally engaged in driving invalid traffic.

- **Auditing Invalid Traffic Processes**
  Comscore invalid traffic processes are subject to ongoing internal validation/quality assurance processes as well as external auditing, including via the Media Rating Council and the Audit Bureau of Circulations (ABC UK).

Activity-based filtration

Activity-based identification is directed at identifying automated agents or other simulated human activity which may not be identified through dual pass specific identification filtration processes. Typically, this involves conducting certain types of pattern analyses, looking for behavior that is likely to identify invalid traffic, such as an excessive volume of activity.

Comscore performs activity-based filtration on a periodic basis and activity that exceeds the established thresholds is automatically removed from the measurements. Periodic assessments are also performed to ensure that the established thresholds continue to be effective.

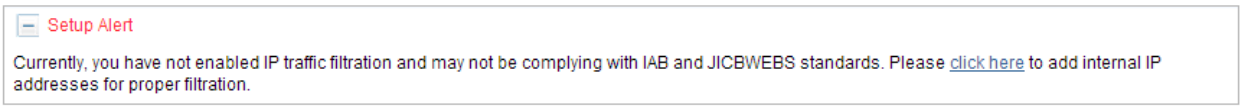
Internal Traffic

Internal visitors accessing their company's site from their business computer network can skew measured statistics. IAB Guidelines require that if company-internal traffic is material to reported metrics and does not represent exposure to ads or content that is qualitatively similar to non-internal users, such traffic should be removed from the reported results. Additionally, nonhuman traffic originating from the company network (e.g., internal robots or monitoring tools) should be excluded.

Comscore has a mechanism in place that allows it to evaluate their internal traffic and the impact it has on the Census Pages metric reported in Direct. The internal traffic is evaluated for its impact on the reported metrics and if it is deemed to be material Comscore has the ability to exclude this traffic from the reported Census Pages metric. Internal traffic classified as immaterial will be allowed to contribute to the Direct Census Pages metric.

Additionally, publishers can proactively exclude website traffic, by IP, from Comscore reporting. All submissions are conducted through Comscore Direct's self-service portal. To exclude website traffic from Comscore reporting, users are required to log into Comscore Direct and navigate to the Setting feature located in lower right hand navigation menu. Users can create a custom filter, from this feature, by entering a specific IP address or a range of IP addresses to exclude from Comscore reporting. Submissions will be removed from Comscore reporting within 24 hours after submission receipt.

Comscore has also implemented an alerting feature in the interface whereby clients who have NOT submitted their internal IPs are reminded to do so.



Invalid Traffic Decision Rate

MRC's V2.0 Invalid Traffic Standards (June 2020) introduces required reporting of a new "decision rate" metric to help users understand the degree to which traffic has been subject to IVT detection/filtration processes. This is particularly important where the measurement service employs sampling, excludes certain traffic from those processes, including due to insufficient signals and so forth:

> *"IVT measurement organizations shall take steps to disguise and vary scripts and tags to avoid detection and prevent reverse engineering if possible. Bad actors may attempt to avoid or obfuscate detection by returning manipulated information, downloading a tag without payload return, preventing interaction with a tag, patching scripts or bypassing an intermediary and making direct requests. As a result, in addition to taking steps to secure and protect tags, measurement organizations must actively report IVT "decision rates" (or an alternate and descriptive name) or situations where insufficient signals are collected to make an IVT decision.*
>
> *This decision rate shall be 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. Decision rates can be reported on both the basis of tracked ads and impressions, but it is not expected that downstream metrics such as viewability would include impressions without sufficient information to make a GIVT decision (differential GIVT and SIVT reporting of decision rates for downstream metrics is permissible) and the panel reporting exception described herein applies to the decision rate as well. The decision rate shall also be reported by media type and environment (desktop/web, in-app and OTT) and shall be presented for GIVT and SIVT distinctly if different. MRC may consider decision rates, much like viewability measured rates, when making accreditation decisions based on benchmarking across audited vendors.*
>
> *Further, measurement organizations must differentiate between degrees of detection capabilities (when a decision can be made or when varying tags such as SDKs, scripts or pixel tags are applied and differential signals are collected) and empirically support the effectiveness of each across environments. Limitations of each technique (such as instances where certain normally collected and utilized fields are not available) shall be actively disclosed and quantified to client users where applicable and appropriate and considering reverse engineering concerns discussed throughout this document. 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.

As an illustrative example, for a campaign of 100 total Rendered Impressions, if a measurement vendor receives full information to make an IVT determination for 80 of those rendered impressions, receives partial information and can make an empirically supported IVT determination for 5 rendered impressions, receives partial information and cannot make an empirically supported IVT determination for 5 rendered impressions and receives no information for the remaining 10 rendered impressions, it should be reported as:

100 Rendered Impressions (intend for measurement and reporting)
85 Recorded Impressions (80 full + 5 partial)
15 Unknown (5 partial + 10 no information)

Decision Rate = 85 Recorded Impressions / 100 Rendered Impressions = 85%

In the above example, only the 85 recorded impressions must be used for resultant GIVT metrics and rates as well as downstream metrics such as viewability (differential GIVT and SIVT reporting of decision rates for downstream metrics is permissible).

If a measurement organization has a decision rate of 100% across all measured traffic, this can be generally disclosed in reference materials without the need for discrete reporting, with appropriate support. *It is not necessarily always desired or required to have 100% signal collection to have effective IVT defenses and the decision rate is designed to be informational to users of measurement data. It is important that steps are taken to educate users related to this metric and its meaningfulness. There is also a risk of assisting bad actors by highlighting lack of coverage of certain properties or inventory types and as a result, reporting of decision rates should be limited to users of reported data that have been subject to Business Partner Qualification."*

Comscore brings a wide variety of detection/filtration methods to bear across the totality of its measurement methodologies. However, we do not disclose the details of our detection methodology beyond standard industry treatments to protect the security of those methods. **Across the totality of our methods, Comscore applies IVT detection to 100% of all traffic.** This includes:

- Impressions sourced from user agents on the IAB's Robots & Spiders lists are filtered out as they reflect activity from known non-valid sources.
- Impressions sourced from Invalid Browsers (not on the IAB's known browser list) are also filtered out.
- Comscore Internal traffic filtration addresses identification and exclusion of impressions sourced from Comscore's own corporate IPs. To date, this activity is immaterial as demonstrated in data provided to the Media Rating Council.
- Activity Outliers exceeding established thresholds (again, not disclosed for security purposes).
- Additional impression level filters applied in Direct, Media Metrix Desktop, Mobile Metrix and vCE products.
- Non-Essential Domains are removed from Media Metrix and Mobile Metrix as described in the discussion of the Client Focused Dictionary.
- The three-second rule addresses double-tagging and similar issues, applied to all page impressions counts.

Certain GIVT or SIVT filters may entail the use of identifiers which may not be available in cases where telemetry from selected users or devices is limited. Additionally, some filters may rely on JavaScript tags, limiting their ability to be applied to pixel-tagged pages or ads. However, these limitations only impact the application of individual detection methods to the affected content or advertising. In all cases, every impression is subject to Comscore's established detection methods. Selected filters also depend on the use of Comscore SDKs and/or may be platform-specific (e.g., mobile SIVT filters apart from desktop). Again, this yields a 100% decision rate.

Note that Direct filtration reflects a subset of the full array of invalid traffic detection methods employed in the actual application of traffic collected via Direct as part of the full Media Metrix Desktop product. Similarly, Mobile Metrix brings to bear filters that are not currently applied in Direct reporting. This to assure that Direct remains effective in helping users to understand census intake in line with the reporting by their own site analytics.

Prefetch

The IAB Click Measurement Guidelines require the removal of self-announced prefetch activity. Mozilla based prefetchers should set an X-MOZ HTTP header to a value of "prefetch." Prefetch ad requests should be blocked using a "403 denied" return code, to encourage counting clicks only upon direct user request for the ad and the required ad interaction.

Comscore has a mechanism in place that allows it to tabulate and evaluate the impact self announced prefetchers on the Census Pages metric that is reported in Direct. The prefetch traffic is evaluated for its impact on the reported metrics and if it is deemed to be material Comscore has the ability to exclude this traffic from the reported Census Pages metric. Prefetch traffic classified as immaterial will be allowed to contribute to the Direct Census Pages metric.

Caching

Caching of the measurement transaction (such as an ad call or measurement tag) may result in an undercounting of impressions and related traffic, if the browser identifies the measurement transaction request in its cache and serves the result without making the call to the measurement server. IAB Guidelines require the use of techniques to reduce the impact of caching on reported data. Additionally, as no process can eliminate all caching, publishers should fully disclose their cache busting techniques and indicate certain amounts of caching may persist even with these techniques in place.

Comscore utilizes HTTP cache-control headers (i.e. cache-control, expiry and pragma) in addition to the use of a Unix timestamp appended to the tag URL for JavaScript generated tags. This random number is designed to create a unique tag that the browser, or any intermediate network or proxy cache would not have previously requested and cached.

Abandonment

Comscore Direct does not count the event until after the page content is delivered, which is in compliance with the IAB Guidelines. Regardless of the placement of the tag, it is possible that abandonment may have the effect of over counting as the user may abandon the page content before the page is displayed by the browser.

Auto-Refreshed Pages

Using site-initiated auto-refresh, a web page can automatically reload itself without the involvement of the user. This potentially results in page impressions that are not viewed by a human. Comscore has studied

the impact of autorefresh on reported results for sites using an auto-refresh command. If deemed material, the traffic should be filtered and reported separately (i.e., estimates with and without refresh activity).

The IAB Guidelines further state that if the content is such that it is likely to be minimized or kept in the background (e.g., Internet Radio) the traffic should be excluded from reported estimates.

Comscore has a mechanism in place that allows it to tabulate and evaluate the impact of auto-refresh on the Census Pages metric that is reported in Direct. Traffic that is identified as auto-refresh traffic is tabulated and disclosed as separate line item in the Traffic Audit Report Tab of Direct.

Technology Issues

In addition to the measurement issues discussed previously, other technology issues may impact the accuracy of impression counting and related metrics. These could include the use of blocking software or tools which prevent the browser from making request of specific domains or for specific image sizes, content formats that cannot be measured by the methodology, browser settings that impact the counting process, and page requests from non-PC devices (although this activity may be filtered out unless the device is using a known browser user agent). To the extent these and other technological issues impact the accuracy of audience measurement, Comscore discloses these potential limitations with an explanation of the potential impact of this activity.

Blocking software or tools (including certain firewalls) that are configured to prevent the browser from making requests to the measurement servers may result in undercounting of audience metrics if the user is generating activity on a Direct site but not requesting the pixel from the measurement servers. Similarly, certain tools also allow users to block images based on dimensions, such as standard advertising image sizes or one-by-one images (pixels), which may also result in undercounting of audience metrics if the tools identify the pixel as a one-by-one image prior to making the request of the measurement servers.

Comscore's Direct methodology allows for measurement of any HTML content served to a device that is supports JavaScript or image tags, as well as flash components that include the Comscore Direct ActionScript. If a publisher were to create content such as widgets that are neither HTML nor flash based, they may be under counted as the Direct methodology would not be supported.

Comscore site/page measurement tags include a JavaScript function as well as an HTML image tag embedded within <NOSCRIPT> tags to allow for measurement of both JavaScript capable and JavaScript incapable browsers or internet applications. If a user were to utilize a JavaScript incapable browser (either disabling JavaScript or an older browser that does not support JavaScript) and also disable image rendering, under counting may occur as both the JavaScript and image pixel methodology would be disabled.

Certain browsers allow users to generate Internet activity through multiple tabs within the same browser session, as well as, open additional browser windows. Additionally, users may generate activity across multiple browsers during a session (i.e. simultaneously running Internet Explorer and Firefox). Comscore's procedures do not identify in-focus and out-of-focus events. That is, if the user simultaneously loads two different publisher pages in a multi-tab browser, Comscore would identify a Page for each page loaded regardless of whether the page was "in-focus" or "out-of-focus".

Certain types of page content utilizing RIA/AJAX technologies allows for portions of the page to be reloaded, refreshed or altered without updating the entire page; therefore, the underlying page beacon is not requested. As such, only one Direct Filtered Tag Request will be counted.

Limitations Impacting Unique Cookie Counts

Comscore Direct reports raw and filtered Unique Cookies in Traffic Reviews and the Traffic Audit Report. These counts can be impacted (under or overstated vs. a true measure of computer usage) due to cookie rejection (leading to undercounting) and cookie deletion (inflating counts vs. a more persistent identifier). Use of multiple browsers on a given computer generates multiple cookies, similarly inflating counts. Cookie sharing by multiple users of a given computer appear as if there is only one user. However, counting shared cookies as opposed to individual users conflates persons measurement as in Media Metrix whereas Direct census counts are not intended to represent persons measurement. Finally, mobile devices often to not support cookies and certain browsers (e.g., Safari may reject cookies by default), resulting in undercounting.

Limitation Related to Apple iOS Update

With Apple's deployment of an iOS operating system update on September 24, 2019, Apple iPad browsing on tablets with the new iPadOS operating system mimicked MacOS browsing, eliminating the distinction between Mac and iPad Safari user agents, thus impacting census measurement for browser traffic originating from iPads.

With the release of iPadOS, iPhone and iPad forked to separate OS versions. Apple now mimics a MacOS Safari user agent (UA) string when users are viewing content in full-screen mode on the iPadOS Safari browser. This change did not apply to iPad Mini devices, nor was it applied when the user has two or more apps in view regardless of the iPad model.

Please see the demo from WWDC 19 for more specifics on the changes Apple implemented: https://developer.apple.com/videos/play/wwdc2019/203.

With this change, Apple forced the market, including all first-party analytics platforms (Google Analytics, Adobe Analytics, etc.) to classify most iPadOS Safari browser traffic as Desktop with this release, and made the browser indistinguishable from a Mac browser by all officially supported methods. This update has no impact on mobile app traffic or measurement.

Because Apple is mimicking Mac Safari browser profiles for most iPadOS browser use cases, classification shifts from iPad to Mac have occured in our Census records. This shift will not involve any modifications to existing census data collection or processing. Pending an industry solution, we have not modifed our methodologies nor our Panel collection and processing.

We are working with industry bodies to facilitate development of new approaches to address this limitation. For the long-term, this may impact broader industry guidelines around the classification of tablet and convertible devices. Comscore will continue to pursue solutions as appropriate.

Cookie Collection – Chrome SameSite

Comscore tags transmit all browser cookies previously set on the scorecardresearch.com domain for use in the Unified Digital Measurement methodology. The most common cookies set and collected on the scorecardresearch.com domain are:

Cookie Name	Description

UID	This cookie contains an anonymous unique id that is generated on the Akamai servers that serve the scorecardresearch.com domains.
UIDR	This cookie contains a timestamp corresponding with the last time the UID cookie was set (or refreshed).
NO_COOKIE	This cookie is set when a user has performed an opt-out for tracking.

When a tag call is received that does not contain expected scorecardresearch.com cookies (e.g., because a user has recently cleared cookies from their browser), Comscore will attempt to set those cookies via 302 Redirect. On browsers such as Chrome 80+ that default cookie sets lacking a SameSite attribute to SameSite=lax, the 302 Redirect cookie set will also include cookie attributes SameSite=None and Secure so that third-party cookies may be set over HTTPS. The latest tags distributed via Comscore Direct default all tag calls to HTTPS.

Pre-Issuance Inspection Procedures

Comscore's pre-issuance checks are designed to ensure that all Census Pages and Unique Cookie data loaded into the Comscore Direct reporting interface (Direct) is comprehensive of the time period of data that is reported. This includes systematic checks to ensure that all expected files for the different reporting periods have been received and loaded into Direct before being made available for querying by the user.

In addition to these systematic completeness checks Comscore also has a review process for the monthly Census Pages and Unique Cookie metrics reported in Direct. For the monthly time period, Comscore will reviews the Census Pages and Unique Cookie metric by client in order to determine if any unusual data fluctuations are caused by potential anomalies. Clients meeting a predefined daily unique cookie or Census Pages threshold are evaluated in this process.

Month over month increases or decreases exceeding a predefined threshold in the average daily Unique Cookie or Census Pages metrics are classified as potential anomalies. Any change exceeding the predefined threshold that is not a function of the entity tagging more or fewer pages and/or events since the prior month will be flagged for further investigation. Variances classified as legitimate are allowed to flow through Direct without any additional modifications.

Re-issuance Procedures

Comscore has a Direct Census Pages and Unique Cookie reissuance policy in place for those instances where a site's traffic fluctuations exceeding a predefined threshold (5%) cannot be attributed to changes in tagging coverage or newly inplaced or updated invalid traffic filters for which data/signals did not previously exist. If the investigation uncovers an error impacting the Direct Published Unique Cookie or Census Pages by more than a predefined threshold, Comscore will reissue the corrected data in Direct. Any other Census Pages or Unique Cookie errors brought to Comscore's attention through internal analysis or external client analysis within a month of the data's original release will be reissued in Direct if it is determined that the error impacted the reported metric by more than the predefined threshold. Errors brought to our attention after one month of the data's original release will be evaluated by management on case by case basis in order to determine the proper course of reissuance action.

In the event that Comscore discovers new sources of Invalid Traffic where data/signals previously existed or adjustments to improve existing filters within the past month have a material (greater than 5%) impact on net filtered audience metrics across 15% or more of the reported entities, Comscore will reprocess/reissue reported data.

Data Processing and Software Quality Assurance

Internet audience measurement is highly automated and therefore requires sufficient program change controls to avoid systematic errors.

Comscore's change management process tracks all changes to production systems, and includes requirements for segregation of duties, QA testing and approvals prior to implementation of new functionality into the production environment. In addition, Comscore has appropriate access control procedures in place to limit access to data, servers and related databases to authorized users.

Data Retention

Comscore maintains the raw log files from the third-party storage servers for forty-five days and the parsed log files for ninety-days. This is required by our clients in our Service Level Agreements. Comscore has made the required compromises in this area in order to accommodate the audit requirements that are part of yearly accreditation process.

Computation of Reported Results

The Direct report consists of the following metrics delivered monthly through an online reporting system:

- Census Page Requests (Gross) – The sum of all tag requests seen for a domain or entity.
- Robotic Traffic – The number of tag request attributed to invalid activity including: robots, spiders, crawlers and agents.
- Census Page Requests (Net*) – The “Census Page Requests (Gross)” filtered for certain General Invalid Traffic (robots & spiders, invalid browsers and internal traffic) as well as activity outliers (Sophisticated Invalid Traffic)).
- Multi Event Traffic – The number of census tag request requested within three seconds of a previous one for the same user.
- Estimated Auto-Refresh Events – The estimated fraction of Pages due to auto-refresh rather than user initiated request.
- Estimated Auto-Refresh Interval – The frequency in which a page auto-refreshes.
- Unique Cookies (Gross) – The unduplicated count of unique cookie IDs from the Comscore cookie database.
- Unique Cookies (Net*) – The unduplicated count of unique cookie IDs corrected for filtered for invalid traffic as outlined above.

Minimum Reporting Standard

Comscore has established a minimum standard of at least 6 unique cookies for reporting purposes to assure reported metrics are reflective of actual traffic as opposed to likely “noise” in the measurement process. The related data is fully retained in the reporting database such that reports run over a longer period where unique cookies do exceed this minimum will be reported.

The Direct accredited reports are delivered monthly through an online reporting system. The monthly reports are based on the following parameters:

Day	00:00:00 - 23:59:59 GMT
Time Zone	Tag requests are logged and reported in Greenwich Mean Time (GMT)
Month	Calendar month