Last Updated: April 21, 2023

Advertising Exchange

See Exchange/Advertising Exchange.

Attributes/Attribute Information

Attributes are known, observed, or inferred characteristics. Examples of attributes are “male” and “visited XYZ website”. Attributes may be derived from Event Data, Bid Request Data, Client Data, Third Party Data, and Inferences/Inferred Data. Quantcast associates attributes with Pseudonymous Identifiers.

Audience

An Audience is a group of devices and/or users who are known to or are estimated to have certain common characteristics. A characteristic in common may be an Interest, such as an interest in cooking. A characteristic in common may be an Attribute, such as being male, visited a particular digital property, or viewed or interacted with a particular advertisement. One type of Audience is a group who have visited a Client’s digital property. Another type of Audience is a group who have been shown, or may potentially be shown, a Client’s advertisement.

Audience Insights

Audience Insights are data collected, or data that is inferred from data collected, about an Audience. Audience Insights are aggregated, anonymised data and are not Personal Information. An example of an Audience Insight is a report that a given audience is estimated to be 70% male and 3 times as likely to be interested in cooking compared to the general population.

Quantcast provides Audience Insights based on Event Data, Bid Request Data, Client Data, Third Party Data, and Inferred Data to Clients. Audience Insights enable Clients to better understand the audiences who engage with their content and ads.

Bid Request/Bid Request Data

A Bid Request is a request by a digital content publisher (e.g., website owner, app developer, streaming content provider, etc.) for an offer to place an ad in the publisher’s digital content. For example, when you visit an ad-supported web page, Bid Requests are sent by, or on behalf of, the publisher of the web page to multiple parties that may want to show an ad to you. Those parties can bid for the opportunity to show an ad in an auction, and one ad is selected to show on the page. Bid Requests typically go through an Advertising Exchange. This all happens via digital communication between computer servers in less than a second. The contents of the Bid Request may include information about the ad unit (the container in the digital content that will display the ad), the digital content, the device it will be seen on, and your engagement with the publisher’s digital content, so that prospective buyers can choose whether to bid and how much. For most cases, the contents of the Bid Request are defined by the OpenRTB industry standard

(https://iabtechlab.com/standards/openrtb/), though not all fields are necessarily included in every Bid Request. Bid Request Data consists of data provided in the Bid Request and will commonly consist of a Pseudonymous Identifier (if available), the content that the ad would serve in (such as the web page, app, video, etc.), the type of device the ad would be served on (i.e., your device type), the approximate geographic location of your device, the size of the ad, the auction ID, and consent information, such as TCF Signals. Bid Request Data also includes Quantcast's response to the Bid Request, such as whether Quantcast bid on the ad opportunity.

Browsing Data

Browsing Data is information collected relating to your Online activity or behaviour. Browsing Data is generated when a Pixels, Tags, or SDKs installed by a Client on its digital property loads and sends information to us. This includes the website URL of the page you are visiting, often along with a Pseudonymous Identifier, as well as fields of information that may be automatically included from HTTP Header Information, such as referral URLs (which is the URL that directed your browser to the website where an advertisement was served to you).

Browsing Data is included in Event Data.

Client Data

Client Data is Imported Data that is uploaded to the Quantcast platform by a particular advertiser Client for use on its behalf. Client Data is Pseudonymised Information, which defines groups of users. These groups might typically be based on users' Online Data or Offline Data, or other characteristics or aspects of users' relationship with the Client. The groups are then used by Quantcast to help deliver advertising campaigns to the right Audiences on behalf of the Client.

Cookie

A Cookie is a small bit of text that is sent to and saved on your computer or device when you visit a website. A Cookie is associated with a single web browser profile; each web browser and browser profile that you use on your device will have separate Cookies. Cookies allow a website to recognise a browser and are commonly used to store user preferences or identifiers, which enables us to collect and use information about browsers over time and across different internet content. Cookies enable us to understand more about users and the content they are visiting over time, which in turn can be used to improve our Clients' advertising activities and the quality of advertising you experience. The identifiers we store in Cookies are Pseudonymous Information; in other words, they cannot be linked to you as an individual without technical efforts to add additional information, which Quantcast does not have. We do not attempt to link a Pseudonymous Identifier to you as an individual, and we prohibit other parties with whom we share Pseudonymous Identifiers or Pseudonymous Information from doing the same. Browsers have controls that enable users to clear or block Cookies. See your browser help for details.

There are two forms of cookies: First Party Cookies and Third Party Cookies.

A "First Party Cookie" is limited in scope to a particular website you visit ("**First Party Cookie**"). In some instances, Quantcast is able to store or access information in a First Party Cookie. If www.example.com incorporates Quantcast Pixels, Tags or SDKs into their website, and if you visit www.example.com, Quantcast may set a First-Party Cookie associated with www.example.com. In these instances, Quantcast can store a Pseudonymous Identifier in the First-Party Cookie, but because it is a First Party Cookie, Quantcast can only access that Pseudonymous Identifier in the context of your visits to that site.

A "Third Party Cookie" is a cookie associated with an internet domain that is different from the one you are visiting. For example, if you are visiting www.example.com and a Quantcast Pixel, Tag or SDK on that website is able to set a cookie associated with quantcast.com, that is a Third Party Cookie. That same cookie will be accessible to Quantcast on other sites that also incorporate Quantcast Pixels, Tags or SDKs. Quantcast uses

Pseudonymous Identifiers stored in Third Party Cookies in order to collect information across multiple websites.

Quantcast Cookies placed on your device have a maximum expiry period of 13 months (or such shorter period as described in the Privacy Policy "Information Collection" section). Each time you visit a website and a First or Third Party Cookie is placed on your device, the placement of a Cookie begins a new expiry period of up to 13 months (or such shorter period as described in the Privacy Policy "Information Collection" section). All Quantcast Cookies automatically cease providing any data to Quantcast from your browser upon expiration.

Cookie ID/Identifier

A Cookie ID is a unique string of characters that we store in a Cookie that allows us to identify a single web browser instance over time and across different web sites. Our Cookie IDs are Pseudonymous Identifiers. A First Party Cookie ID is a unique Pseudonymous Identifier relating to the First-Party Cookie set by the owner of the website you are visiting. A Third Party Cookie ID is a unique Pseudonymous Identifier relating to the Third-Party Cookie set by Quantcast.

Cookie Syncing/Matching

In the online advertising industry, Cookie Syncing/Matching generally refers to a process through which two entities who each, and separately, identify a device using their own Pseudonymous Identifier can determine which of their respective Pseudonymous Identifiers may relate to the same device. For example, Quantcast may pseudonymously identify a device as "cookie ID 123." Company B may pseudonymously identify the same device as "cookie ID ABC." Cookie Syncing/Matching enables Quantcast and Company B to recognise that their respective Pseudonymous identifiers may relate to the device that Quantcast records as "cookie ID 123".

Quantcast's Cookie Syncing activities work similarly. If you visit a website that incorporates Pixels, Tags or SDKs from Quantcast, Company B may match its own pseudonymous identifiers to Quantcast Pseudonymous Identifiers (this creates a record of matching pseudonymous identifiers for Company B). Once a match is established, Company B can reference a particular device when communicating with Quantcast, using Quantcast's Pseudonymous Identifier.

The Cookie Syncing/Matching process does not in itself result in Quantcast sharing Attributes related to Quantcast Pseudonymous Identifiers with Company B. The Cookie Syncing/Matching enables transactions between the parties at a later time; for example, in the case of an Advertising Exchange sending a Bid Request, the Bid Request can contain a previously synched Pseudonymous Identifier.

Cross-Media Matching/Linking

In the online advertising industry, Cross-Media Matching generally refers to a process through which Quantcast links identifiers across a user's consumption of various media (e.g. audio, video, websites, apps, etc) because such identifiers are known to or Inferred to relate to the same user. Matching/Linking may be undertaken for consumption of media on a single device and for consumption of media on more than one device. As an example, if you visit a digital property using your mobile phone and later visit that same digital property using a browser on your laptop or make visits to several different digital properties using a browser over a period of time, Quantcast may initially determine that these visits are made by different users and assign each device user their own profile.

If, however, Quantcast finds there is sufficient commonality between the Pseudonymous Identifiers associated with the consumption of media, Quantcast will assess that those identifiers may be joined as they are likely to emanate from the same user. This assessment is"probabilistic"– in other words, it uses statistical techniques to determine that the identifiers to be matched have a higher likelihood of relating to the same device and/or user.

Data Management Platforms and Data Providers

Data Management Platforms and Data Providers provide Third Party Data to Quantcast, or provide a platform through which Clients can provide Client Data to Quantcast. These companies either directly licence first and third party Audience Segment Data from different sources (such as Online Data and Offline Data) to businesses or provide a platform through which Clients can collect, organise, and activate such data for Quantcast's use in connection with the Solutions. We share Pseudonymous Identifiers with Data Management Platforms/Data Providers in order to sync/match identifiers to effectively integrate with their services (see Cookie Syncing/Matching).

Device ID/Identifier

A unique string of characters that can be used to identify a device set by the developer of the device's operating system (e.g., a mobile phone, tablet, TV, or console). Device Identifiers (or "**Device IDs**") serve a similar purpose as Cookies and can be used to provide personalised advertising. A Device ID is a Pseudonymous Identifier.

A Mobile Advertising ID (or "**MAID**") is a Device ID assigned to a mobile device by the mobile device operating system. Typically, the device user can reset or turn off the ID via the device's settings. A MAID is referred to as the IDFA (ID for Advertisers) on iOS devices and GAID (Google Ad ID) on Android mobile devices.

Device Configuration/Device Information

Information about a device or its configuration, transmitted from the device, and typically associated with a Pseudonymous Identifier. The information includes browser, app, or other information about the device (such as device type, screen size and resolution, date and time, and language), which also may include a User Agent. Some Device Information is derived from HTTP Request Header Information.

Event Data

Information collected relating to your Online activity/behaviour, which may include Personal Information in Pseudonymous Identifiers, Imprecise/Approximate Location Information, HTTP Request Header Information, Device Information, Browsing Data and TCF Signals. Event Data is generated when a Pixel, Tag, or SDK installed on a Client's digital property loads and sends information to us. Event Data can also be collected from ads, when you view or click on an ad which contains a Tag.

Exchange/Advertising Exchange

A marketplace platform that facilitates automated, real-time, auction-based buying and selling of ad inventory (which are spaces available on sites and apps to display ads). An Advertising Exchange receives Bid Requests from digital publishers and forwards them to advertisers, or to entities like Quantcast who act on behalf of advertisers. Advertisers, or their agents, respond to Bid Requests with a bid amount and an advertisement to provide to a user if they win the auction.

First Party Cookie

See Cookie.

HTTP Request Header Information

HTTP headers are defined by internet standards and contain a number of data fields designed to facilitate communication and interoperability on the internet. On the web, your web browser controls which headers are sent and what the contents are. We receive the headers when a request is sent over the internet to our system, such as when a Pixel loads in your web browser. We also might receive information that has been derived from the HTTP headers from another party, such as in a Bid Request. We use a subset of the header fields for purposes described in the Privacy Policy, which includes:

- IP Address
- Cookie (if available)

User Agent, which is a string (a line of text) identifying the device type, browser type, and version that the user is using to access the web server ("User Agent")

- Date, which includes the precise time of access
- Referral URL, which is the web page you were on when the request was sent
- TLS Session ID, which identifies a particular session of communication between the browser and the server
- Content-Language, which is the languages of the intended audience for the enclosed content

Detailed documentation related to HTTP header information can be found online in a general search for "HTTP header information fields".

IAB Transparency & Consent Framework ("TCF")

The IAB Transparency & Consent Framework, or "TCF," is a standardised industry program active in countries governed by the GDPR, and designed for notifying users about data Processing by companies involved in digital advertising on sites and apps that users visit, and for establishing a legal basis for that Processing.

The TCF is designed to be used on digital properties, such as websites and apps. The TCF incorporates a consent dialog that displays when users visit a website or app, giving them information about vendors, the data they collect, and the purposes for which they collect it. It also offers an opportunity for users to give or change their permissions for such data collection and use.

The TCF allows Quantcast to work with publishers of websites and other digital properties in a consistent manner using standardised technical specifications to:

(a) provide a link to Quantcast's Privacy Policy, as well as transparency about Quantcast's Processing of Personal Information, the specific purposes for which Quantcast Processes Personal Information, and Quantcast's legal basis for such Processing, directly on the website or other digital property accessed by the user;

(b) allow the user, in a granular manner, to express their consent or refusal to consent, to Quantcast's (i) use of Cookies, and (ii) the purposes of Quantcast's Processing, which are the reasons why Quantcast Processes the personal data of users ("TCF Purposes"), including where Quantcast relies on the user's consent for such Processing directly on the website or other digital property that the user is accessing;

(c) allow the user to object to Quantcast's Processing of Personal Information (for purposes where Quantcast relies on legitimate interests) directly on the website or other digital property accessed by the user.

Using the TCF allows publishers of websites or other digital properties to provide information about Quantcast's Processing to users in

a consistent manner. The user-facing disclosures presented by these digital properties are sourced from information that Quantcast has registered with the TCF's "Global Vendor List", a publicly accessible, machine-readable repository of information about TCF-compliant vendors, like Quantcast. This information includes Quantcast's Privacy Policy URL, the purposes for which it Processes Personal Information, and its legal basis for each of these purposes. As the description of these purposes and minimum standards for disclosures are standardised across all TCF participants, Quantcast knows how operators of websites or other digital properties using the TCF are making disclosures about Quantcast and can have confidence in such disclosures.

In addition, the TCF enables publishers of websites or other digital properties to create and send to Quantcast a standardised technical signal that indicates (A) whether Quantcast's transparency disclosures were provided to a user; (B) whether or not the user has consented to Quantcast's Processing and/or each purpose for which Quantcast sought the user's consent; and (c) whether the user objected to Quantcast's Processing and/or any purposes for which Quantcast Processes Personal Information on the basis of its legitimate interests (the "**TCF Signal**").

TCF Signal is collected via Quantcast Tags if the digital property on which the Tag is implemented has also implemented a TCF-compatible Consent Management Platform, which is a company or organisation that centralises and manages transparency for, and consent and objections of, the user ("**CMP**") . In addition, TCF Signal is received by Quantcast as part of the Bid Requests it receives from Advertising Exchanges. Quantcast is able to read the standardised TCF Signal and will only Process Personal Information for purposes to which the user has consented (where consent is the legal basis) or not objected (where legitimate interests is the legal basis) in order to provide the Solutions.

Read more about the TCF here https://iabeurope.eu/transparency-consent-framework/

Imported Data

Imported Data is uploaded to the Quantcast platform or provided to us via an Application Programming Interface ("**API**"). Imported Data is Pseudonymised Information, which may include information relating to your Online data or Offline data or other information that Clients or partners have about you. For examples of Imported Data provided to Quantcast, see Client Data or Third Party Data.

Imported Data (Client)

See Client Data.

Imported Data (Third Party/Segment)

See Third Party Data.

Imprecise/Approximate Location Information

Typically, in digital advertising we distinguish between precise and imprecise geolocation information.

Precise geolocation usually comes from GPS coordinates from mobile devices, and can have precision up to about one metre. Quantcast does not use precise geolocation data and we request that Clients, partners, and third parties refrain from sending precise geolocation to us. If a party inadvertently sends it, we do not use it in the Solutions and it is removed from our systems within 30 days.

Imprecise geolocation is lower precision, and refers to a general

geographic area, for example a country, region, city or division of a metropolitan area, and/or some combination of these, and is often derived from GPS coordinates or from IP Addresses.

Inferences/Inferred Data

Inferences, or Inferred Data, is information that is inferred from data that we have collected about a device, such as Event Data, Bid Request Data, Client Data, or Third Party Data. Our inferences are made using algorithms that estimate the likelihood that the user of a device has particular interests or characteristics. The Inferences are then associated with a Pseudonymous Identifier as part of a set of device Attributes.

For example, if a device frequently visits sports websites, it might be inferred that there is some probability the user of that device likes sports. Similarly, if a device frequently visits an airline provider's website, it might be inferred that there is some probability a user of that device likes to travel. Other Inferences include things such as Interests, income range, gender, age, marital status, and other socio-economic information.

Inferences associated with any individual device have a high degree of uncertainty. Inferences become more accurate when used to estimate the characteristics of a large group of devices, like an Audience.

Interests

Interests are known, observed, or inferred non-demographic characteristics. Interests are associated with Pseudonymous Identifiers to characterise particular interests of users. Examples of Interests include "cooking" and "outdoor activities". Interests may be derived from Event Data, Bid Request Data, Client Data, Third Party Data, and Inferences/Inferred Data.

IP Address

An IP ("**Internet Protocol**") Address is a unique numerical label corresponding to a computer or device. Computers use IP Addresses to identify each other and know where to send information over the Internet. For example, when you open a web page in your browser a request is made to a server for the web page content. The server knows where to send the content based on the IP Address contained in the request. Computers or other devices are assigned an IP Address from the network the device is on. A device's IP Address may change over time or as a device changes locations. Also, an IP Address can refer to multiple devices, for example if the devices are behind an internet router.

An IP Address that has been hashed, or encoded using a cryptographic hashing function to obfuscate the email, is treated as a Pseudonymous Identifier.

Labels/Label Data

Labels, or Label Data, are descriptors associated with Pseudonymous Identifiers to denote particular groups of users that can be subsequently used to index all Pseudonymous Identifiers associated with that label. An analogy would be applying a "label" to messages in an email inbox - you might decide to label messages from work as "Work", family members as "Family," and so on. These labels then help you readily index and recall particular categories of email.

Labels processed by Quantcast are:

- Labels from Data Management Platforms and Data Providers : these are category Labels (e.g., male, female, age 21-24) acquired from third party data partners relating to a Pseudonymous Identifier;
- Custom-Client Data Labels: these are custom category labels set by Clients corresponding to a device associated with the identifier visiting their digital property (e.g., byline of the news article accessed by the user) or product name (of the product accessed by the user).
- Inferred Data Labels: these are inferred category Labels about a user using a device associated with a Pseudonymous Identifier, e.g., inferred age, inferred gender, inferred interest.

Example Labels are “male” and “visited XYZ website”. Labels may be inferred information (see Inferences/Inferred Data) or may be Imported Data (see Client Data and Third Party Data).

Log Data

Log Data is an industry term that is generally used to refer to data collected from interactions with computer systems, and is used differently by different companies. For purposes of describing our Processing, we use more precise terms, such as Pseudonymous Identifiers, Event Data, Bid Request Data, Client Data, Third Party Data, and/or Inferences/Inferred Data, which are all types of data that can be subsumed within the general industry term “Log Data”. Some elements within Log Data, when isolated from the Pseudonymous Identifiers, will not qualify as Personal Information. For example, a single time zone and publisher URL without an associated Pseudonymous Identifier would not qualify as Personal Information.

Online Data

Data relating to a user’s interaction with digital media including websites, apps and streaming media services.

Offline Data

Data relating to a user’s real-world purchases and/or activity.

Panel

A Panel is a set of individuals who have consented to participate in market research and share information about themselves, their preferences and interests for purposes of research and market analytics.

This information can then be used as the basis for learning or making inferences about a larger population. For example, if a number of people on a Panel share that they visit a particular news website, and of those people, most of them are male and over the age of 50, we might extrapolate from that and say that most of the audience for that website is male and over 50.

Another way to use Panel data is to compare Panel results to the estimates that we have made using our algorithms in order to score the effectiveness of our algorithms. So, if our algorithm predicted for the same news website that most of the audience is under 30, we would learn that our algorithm might be wrong.

Personal Information

Personal Information refers to information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, to you, your browser, or your device. We use the term “personal information” to refer to information that is subject to protection under data protection and privacy laws and regulatory regimes around the world. Depending on the jurisdiction, such information may be referred to as “personal data.”

The Personal Information Processed by Quantcast is limited to Pseudonymised Identifiers. Quantcast does not Process Personal Information that directly identifies you as an individual, and that can be used to directly identify you without technical efforts to add additional information, which Quantcast does not have.

Pixels, Tags, and SDKs

Pixels, Tags, and SDKs are computer code embedded in a website that we use to enable the Solutions. We tend to use the terms Pixels, Tags, and SDKs interchangeably. Clients that use the Solutions can put them on their sites, in their apps, or in their ads in order to send us information that is then used in the Solutions. When a Pixel, Tag, or SDK loads and calls our servers, we receive HTTP Header Information, along with other information that is configured by the Client who is using the Solutions. That information includes IDs from partners, so we know which partner the data is coming from.

Pixels, Tags, and SDKs include:

- Sync Pixels: These are used to exchange and match Pseudonymous Identifiers between companies that participate in the digital advertising market. By matching, they can synchronise these identifiers to deliver and measure ads.
- Tags or Pixels in ads: When a digital ad loads on a page, it can include a Tag or Pixel that we use on behalf of Clients to gather information about where and when the ad was served. This can help to measure ad performance, to ensure ads are shown where intended, and to learn in order to improve ad effectiveness.
- Tags or Pixels on publisher Clients’ web pages: For publisher Clients that use the Solutions, they can put our Tags on their sites. The information we collect then enables the Client to learn about their audience, and it enables us to build models for better targeting ads.
- Tags or Pixels used by advertiser Clients: When advertiser Clients use our Tags or Pixels, they send us information so we can learn about their customers in order to help them better target their ads.
- SDKs: SDKs are bits of computer code that mobile app publisher Clients incorporate into their apps, enabling them to send us information. Similar to Pixels or Tags, the information enables us to offer the Solutions as described in our Privacy Policy.

Probabilistic Identifier

A Probabilistic Identifier is a Pseudonymous Identifier which we create by combining Pseudonymous Identifiers (such as IP Addresses) with Bid Request Data and/or Event Data using non-deterministic, statistical methods to estimate the likelihood that a group of devices may be used by the same user or household, if applicable law or rules allow. For example, we might be able to determine that because a mobile phone and a TV are on the same network, they are likely in the same house. We can then use that information to select and measure ads. Unlike using Cookie IDs, this approach is not 100% accurate and could identify one or many devices.

Process

Refers to any operation or set of operations performed upon Personal Information or sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Pseudonymous Identifiers

Pseudonymous Identifiers are unique values that distinguish your browser profile(s) or device(s). Pseudonymous Identifiers cannot be linked to you as an individual without technical efforts to add additional information, which Quantcast does not have. We do not attempt to link Pseudonymous Identifiers to you as an individual, and we prohibit other parties with whom we share Pseudonymous Identifiers from doing the same.

Pseudonymous Identifiers are important in digital advertising because they help distinguish browsers or devices over time across different contexts. This is useful for example, to limit the number of times that we show the same ad to one device, to measure the performance of ads, and to target and select personalised ads.

We may incorporate any one of the following types of information in a Quantcast Pseudonymous Identifier:

- Third Party Cookie ID: see Cookie ID.
- First Party Cookie ID: see Cookie ID.
- IP Addresses.
- Hashed email addresses, which are email addresses that have been encoded using a cryptographic hashing function to obfuscate the email.
- Device ID.
- Application ID: an ID that is unique to your mobile device and a particular app on your device.
- Application Session ID: like an application ID, except that it is reset periodically (e.g., many browsers reset these after 30 minutes of inactivity).
- Exchange User ID: an ID that is sent to us with a Bid Request that identifies the device or browser where an ad is to be shown.
- Probabilistic Identifier.
- Publisher User ID: digital publishers that use the Solutions can send us an ID to use in the Solutions. The digital publisher hashes or encrypts an identifier available to it. The resulting ID is pseudonymous because it does not directly identify you, but it would be consistent across different publishers, so the Publisher User ID can be used to match data.
- TLS Session ID: when you visit a website URL that starts with “https” instead of “http”, that means you have an encrypted connection between your browser and the site. If one of our Pixels, Tags or SDKs loads on the site, that call to our server will also be encrypted. The Session ID identifies a particular session of communication between the browser and the server.

Pseudonymous/Pseudonymised Information

Pseudonymised Information is Personal Information that has been Processed in such a manner that the information can no longer be attributed to a specific user without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal information is not attributed to a specific user.

Segment Data

Segment Data is imported data that is uploaded to the Quantcast platform or provided to us via an API by Clients or Third Party Data Partners. Segment Data is Pseudonymised Information, which may include Online Data and/or Offline Data as well as Attributes, Inferences, or Interests inferred from that data. This category of information is typically called “Segment Data” because it identifies groups of users who fall into advertising segments (e.g., “auto buyers,” “shoe shoppers,” or “women 25-35”). These segments represent groups of users that share (or that are inferred to share) one or more certain characteristics in common (e.g., a client may want to advertise to a segment of “male shoppers who are interested in sports fashion”). These groupings are created by using the intersection of different segments (in the example given, an audience that is simultaneously in the “male”, “shopper”, and “sports fashion” segments). A segment may be identified with a Label (in which case it is referred to as “Label Data”).

Software Development Kit (SDK)

See Pixels, Tags, and SDKs.

Tag

See Pixels, Tags, and SDKs.

TCF

See IAB Transparency & Consent Framework.

TCF Purpose/TCF Special Purpose

The TCF has standardised certain Purposes, Special Purposes and Special Features and the descriptions of data processing activity in the digital advertising industry. Through this standardisation, the digital advertising industry can ascribe consistent meanings for the permissions that data subjects give via the TCF. This also ensures a consistent experience for users because they then do not have to read and understand an entirely different set of Purposes, Special Purposes and Special Features for each website they visit.

Because of the benefits of standardising the purposes across the industry, we use the TCF to establish the legal basis to Process Personal Information and use the Purposes, Special Purposes and Special Features in our Privacy Policy to describe much of our data processing activity.

For detailed descriptions of TCF “Purpose” or TCF “Special Purpose”, see IAB Transparency & Consent Framework.

Third Party Cookie/Cookie ID

See Cookie.

Third Party Data

Third Party Data is Imported Data that is uploaded to the Quantcast platform or provided to us via API by third party Data Management Platforms and Data Providers. Third Party Data may include Segment Data.

Training Data

Training Data is Pseudonymous Information that we receive from Clients and third party data providers, where the actual Attributes or Interests of the underlying users are known (even though their actual identities are not known to Quantcast). The Training Data is segmented across various Interests and Attributes, such as shopping interests (e.g., automotive, technology, or restaurants), business and occupation (e.g., management, IT professional or retail), media interests (e.g., cinema, video games, TV), income range, age, marital status, and other socio-economic information and used for data modeling purposes. We use the Training Data to train statistical models to make Inferences. When our systems subsequently receive Event Data relating to a user, we can infer whether the Event Data displays characteristics similar to the Training Data. If the Event Data displays characteristics that are similar to the Training Data, we can infer from that the likely Attributes and Interests of the user to whom the Event Data relates. These Inferences are then used to deliver advertising and provide aggregated, analytical reporting to our Clients.

URL (Uniform Resource Locator)

A URL, also known as a web address, is a reference to a unique web resource that specifies its location on a computer network. Most commonly, a URL points to a web page. URLs can also point to a document, image, video, etc. URLs often use plain text, such as www.quantcast.com; in that case, the domain name must be processed by a Domain Name Server in order to convert the domain name into an IP Address.