I. Introduction

TRUSTe's TRUSTed Data Program Requirements apply to companies who help in the optimization or serving of an online advertisement. These Program Requirements set the standard for responsible third party data collection practices by **Ad Companies** addressing **Online Behavioral Advertising** (OBA). This provides Ad Companies who lack a direct relationship with an **Individual** a way to demonstrate they use data collected from web sites or mobile applications, or data received from different sources in a manner that respects an Individual's preference.

The Trusted Data Program Requirements are based upon a philosophy of notice and choice that gives Individuals control over the use of their information for OBA purposes. This is accomplished by providing:

- Notice - in a contextually relevant manner; and
- Choice – easy access to a preference mechanism for persisting and honoring an Individual's OBA preferences

OBA practices and technologies, along with Individual preference management controls continue to evolve rapidly. Accordingly, TRUSTe may continue to refine and evolve the Trusted Data Program Requirements based on the changing requirements of global OBA compliance frameworks.

The Trusted Data Program is a single program that sets forth requirements consistent with regulatory guidelines such as the Federal Trade Commission's Self-Regulatory Guidelines on OBA, and self-regulatory frameworks such as the Digital Advertising Alliance's (DAA) OBA, multi-site, and mobile principles, and the European DAA and DAA Canada OBA Principles. In addition, Ad Companies certified under these program requirements will be certified to a standard consistent with the Network Advertising Initiative's 2013 Code of Conduct and Mobile Application Code.

Terms defined in Section III of these Program Requirements are bolded the first time they appear in this document.

II. Minimum Program Requirements

Participants wanting to be certified under the TRUSTed Data Program agree to comply with the following Program Requirements:

A. Transparency and Notice

1. Consumer Education

    a. Participant must provide Individuals access to educational information provided by industry self-regulatory organizations about behavioral advertising.

    b. Educational information must be accessible through preference management tools and through the Participant's website.

    c. Educational information must include at least the following information:

        i. Description of what is behavioral advertising;

        ii. How the Participant collects, uses, and stores behavioral advertising data; and

        iii. How the Individual can exercise their preference.

2. Enhanced Notice

Participants, depending on their role in the ad ecosystem, must provide **Clear and Conspicuous** enhanced notice regarding OBA data collection, use, and choice practices. To provide this enhanced notice, Participants shall make available access to easy-to-find-and-use preference management tools that include a universal choice mechanism as follows:

    a. **Ad Networks**, **Ad Servers**, and **DSP**s shall provide notice and access to preference management tools through an in-ad notice via an **Icon**, "Ad Preferences", or similarly labeled button, or direct link.

    b. The following information shall be accessible from the Icon, "Ad Preferences" or similarly labeled button, or direct link, and shall include the following:

        i. What data is collected, either through active or passive means, and how the data is used with respect to OBA; and

        ii. The means by which the Individual can express their privacy preference with respect to OBA and instructions.

        iii. Description of the effects of exercising a privacy preference.

        iv. How the Individual's **Device** was identified if using **Device Recognition Technology**.

    c. If more than one Ad Company is involved in the ad chain, the Participant, if the Participant is not directly serving the ad to the Individual, will verify that the Ad Company directly involved provides enhanced notice and access to preference management tools.

d. Enhanced notice may be provided through the app or Web page where data is collected if there is an arrangement with the First Party.

e. Enhanced notice is not required if data is only collected or received for the following purposes:

i. Operations and systems management including:

1. intellectual property protection;

2. compliance, public purpose, and consumer safety;

3. authentication, verification, fraud prevention, and security;

4. billing or product or service fulfillment; or

5. Ad Reporting or Ad Delivery.

f. Market research or product development including the analysis of the characteristics of a group of consumers or market, and product performance to improve existing or develop new products using de-identified data that has been de-identified in such a way that an Individual cannot be re-identified.

3. Privacy Statement

a. Participants shall provide a Clear and Conspicuous **Privacy Statement** on their online properties, including its Web site, regarding their privacy practices around OBA, or multi-site or **Cross-App Data** collection.

b. Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe in its sole discretion that states Participant's data practices and is in conformance with these Program Requirements including, but not limited to:

i. The scope of the Privacy Statement including data collected for OBA or non-OBA purposes;

ii. What types of data, including **Personally Identifiable Information (PII),** are collected, either through active or passive means;

iii. The type of entity(ies) including **Service Providers**, that assist Participant in collection and use of the data;

iv. How the collected data will be used, including whether the data is used for OBA or non-OBA purposes;

v. Whether collected data is tied to or otherwise linked to PII;

vi. Whether the collected data is shared with **Third Parties**, including Service Providers, what types of Third Parties the data is shared with, and if those Third Parties use the data for targeted advertising purposes;

vii. A general description of the techniques and technologies the Participant uses to collect data about Individuals online or offline behavior, or app or Web usage activity including but not limited to the use of cookies, pixels, Device Recognition techniques, or LSO's;

viii. Whether the Participant supplements the data it collects with data from Third Party sources, the types of data it receives, and types of Third Party sources it receives data from;

ix. How Individuals can exercise their preferences, including the ability to withdraw consent, regarding the collection or use of data for OBA purposes, and obtain access to privacy preference management tools;

x. How Individuals can request access to **Contact Information** or **Sensitive Information** for the purpose of correcting inaccuracies, updating it, or to request deletion;

xi. How long collected data is retained;

xii. General statement regarding the types of security measures in place to protect collected data;

xiii. As applicable, a statement of the Participant's compliance with self-regulatory frameworks such as the DAA or NAI;

xiv. That collected data is subject to disclosure pursuant to judicial or other government subpoenas, warrants, orders, or if the Participant mergers with or is acquired by a Third Party, or goes bankrupt;

xv. How the Individual will be notified of any **Material Changes** in the Participant's OBA data collection or use policies, and practices;

xvi. How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address;

xvii. Effective Date of Privacy Statement;

xviii. If required, a statement of participant in the TRUSTe program, that Participant complies with these Program Requirements, and the scope of that participation; and

xix. Information on how to contact TRUSTe to express concerns regarding the Participant's Privacy Statement or privacy practices.

c. Access to the Privacy Statement shall be Clear and Conspicuous, and at a minimum be accessible from the homepage of the Participant's Web site.

d. Participant shall treat all collected data in accordance with the posted Privacy Statement in effect at the time of collection unless the Individual otherwise has given **Express Consent**.

4. Foreign Language Privacy Statement
    a. If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe shall use ISO 9001 certified translation services or tools to verify that Participant's Foreign Language Privacy Statement is an accurate translation of Participant's English language Privacy Statement.

    b. Participant shall ensure that its privacy practices are the same, and that the Foreign Language Privacy Statement provides materially the same description of Participant's privacy practices as Participant's English Language Privacy Statement.

    c. Participant must notify TRUSTe of any Material Changes to its Foreign Language Privacy Statement and submit changes to TRUSTe for review and approval.

    d. Participant shall only link to it TRUSTe certified English language privacy statement from its TRUSTe certified English language online properties.

B. Individual Control

1. Participants will provide Individuals the ability to exercise choice or withdraw previously given Express Consent with respect to the collection and use of data for OBA.

    a. Opt-out choice needs to be provided for:

        i. Use of non-PII or **Pseudonymous Data** for OBA;

        ii. Use of PII to be merged with non-PII on a going-forward basis for OBA purposes; or

        iii. Use of **Persistent Device Identifiers** for OBA.

    b. Express Consent needs to be obtained for:

        i. Use of PII merged with previously collected non-PII;

        ii. Use of **Precise Geo-location Data**; or

        iii. Use of Contact Information or Sensitive Information.

    c. **Personal Directory Data** shall only be used for OBA if the **First Party** partner has obtained authorization through providing Clear and Conspicuous notice and obtaining Express Consent from the Individual.

        i. Participant shall ensure First Party has authorization from the Individual to authorize the Participant to collect Personal Directory Data.

        ii. Participant shall ensure the First Party offers a mechanism for the Individual to withdraw consent for further collection and use of Personal Directory Data.

2. Participant will persistently honor the Individual's preference.

3. An Individual's preference will be applied as broadly as possible across different technology platforms (e.g. mobile browser and apps where technically feasible, and in general accordance with user expectations).

4. In cases when additional steps are required by the Individual to exercise a preference, the Individual shall be provided Clear and Conspicuous notice at each step on how to do this.

5. Privacy preference management tools will be intuitive, reliable, and easy for Individuals to use. It will list the Participant along with other parties that collect and use data for OBA purposes, and allow Individuals to opt-out of any or all of them.

6. Access to preference management tools shall be Clear and Conspicuous as outlined in these Program Requirements.

7. Respect
    a. Participants shall honor and maintain the Individual's selected preference in a persistent manner until such time that the Individual changes that preference.

        i. If the Participant recognizes multiple Devices are associated with a single household, the Individual's preference shall apply to the Device from which the preference was exercised.

        ii. If the Participant recognizes multiple Devices are associated with a single Individual, the Individual's preference shall apply to all associated Devices.

    b. If a privacy preference is received, Participants shall no longer use historical data and not collect any new data for an Individual within 48 hours of being made aware of the Individual's privacy preference.

    c. All Participants shall do the following to ensure the Individual's preference is both communicated to, and persistently honored by, the Participant:

        i. Participants who are technically capable (such as **SSPs, Ad Exchanges, Ad Mediators**) will check or collect, and communicate these preferences to the other partners in the ad chain to ensure they can be persistently honored across all ad platforms (e.g. DSPs).

        ii. SSPs, Ad Mediators, **DMPs**, and other Participants that do not otherwise collect Individual data shall:

            1. Read the Individual's privacy preference either stored in the browser, Device, or by an approved provider of privacy management solutions;

            2. Ensure every **Ad Transaction** has an associated privacy preference (if one exists) easily accessible by all entities within the ad ecosystem; and

            3. Communicate preferences to other entities within the ad chain (e.g., DSPs), in order to ensure that they can be persistently honored across all ad platforms (e.g., DSPs).

4. **Ad Networks, Ad Servers**, *and* DSPs shall honor preferences received.

d. A preference indicated through any industry recognized standardized choice platform (e.g. DAA, DAAC, EDAA, or NAI) or browser preference management tool should be recognized as the Individual's express preference and honored per these Program Requirements.

C. Privacy Practices

1. Collection and Use Limitation

a. Participants shall only collect data where such data is limited to data reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement and/or in-ad notice.

b. Participants shall only use or allow the use of collected data for the following purposes:

i. OBA;

ii. Operations and systems management including:

1. intellectual property protection;

2. compliance, public purpose, and consumer safety;

3. authentication, verification, fraud prevention, and security;

4. billing or product or service fulfillment; or

5. **Ad Reporting** or **Ad Delivery**;

iii. Market research or product development including the analysis of the characteristics of a group of consumers or market, and product performance to improve existing or develop new products using de-identified data that has been de-identified in such a way that an Individual cannot be re-identified; and

iv. In accordance with the Participant's Privacy Statement and/or in-ad notice unless the Individual has been provided notice and has given Express Consent.

c. Collected data shall not be used to or be made available to Third Parties for the following purposes:

i. Credit eligibility;

ii. Employment eligibility;

iii. Insurance eligibility, underwriting, and pricing;

iv. Health treatment eligibility;

v. Providing targeted marketing to children under age 13; and

vi. Targeting or marketing to children under age 18 if such advertising contains content not reasonably appropriate for this age group.

d. An identifier issued for the specific purpose of communicating, honoring, reading, or otherwise managing privacy preferences shall not be used for any other purpose.

e. Participants shall not collect, use, or make available to Third Parties, except for Service Providers, data containing Contact Information or Sensitive Information unless the Individual has been provided notice and given Express Consent.

f. On web sites or apps directed towards children under age 13 as allowed by the Children's Online Privacy protection Rule, 16 C.F.R. Part 312, et seq Participant may:

i. Maintain or analyze the functioning of the website or online service;

ii. Perform network communications;

iii. Serve contextual advertising on the website or online service or cap the frequency of advertising;

iv. Protect the security or integrity of the user, website, or online service; or

v. Ensure legal or regulatory compliance.

2. Access

a. Participants shall provide Individuals with reasonable access to data collected about them, and other information associated with that data collection, that is retained for the purposes of OBA or other marketing purposes.

b. If Participant collects Contact Information or Sensitive Information directly from the Individual, about that Individual, the Participant must implement a reasonable and appropriate mechanism to allow the Individual to:

i. Correct or update inaccurate Contact Information or Sensitive Information; and

ii. Request deletion of Contact Information or Sensitive Information, or that collected information no longer be used.

c. If Participant collects any PII from an Individual under the age of 18, then Participant must implement a reasonable and appropriate mechanism to allow the Individual to have such PII deleted or permanently de-identified.

d. Such mechanism shall be:

i. Clear, conspicuous, and easy to use; and

ii. Confirm to the Individual inaccuracies have corrected.

e. Participant's Privacy Statement shall state how access is provided.

f. Participant is not required to permit an Individual access to Contact Information or Sensitive Information to the extent that:

i. Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others;

ii. The burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However, Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or

iii. The requested Contact Information or Sensitive Information is derived from public records or is **Publicly Available Information** and is not combined with non-public record or non-publicly available information.

iv. Other laws or regulations prevent the provision of such access.

g. If the Participant denies access to PII, Participant must provide the Individual with an explanation of why access was denied and contact information for further inquiries regarding the denial of access.

3. Material Changes

a. Participants will provide notice and obtain Express Consent prior to implementing any Material Changes to their data collection and use policies, if those policies will be applied to data collected prior to the change.

b. Participant must notify TRUSTe prior to implementing the Material Change:

i. For any Material Change in its data collection, use, or disclosure practices; and

ii. For content and delivery method of notice to Individuals, such as email, "in product" messaging, etc.

iii. Upon notification of a Material Change, TRUSTe will review the change to verify Participant's compliance with these Program Requirements.

D. Data Management

1. Participants shall implement appropriate controls and processes to manage and protect data within the Participant's control.

2. Such controls and processes shall be appropriate to the level of sensitivity of the data collected and stored.

3. Technology Controls

a. Participant shall use a unique Domain Name for all technologies (like cookies, device recognition technology, and scripts) to separate any individual technology used for OBA from one that is not used for OBA purposes (e.g. analytics).

b. For cookie-based preference management systems, the Participant shall use the same cookie name for all of its opt-out mechanisms. For example, the opt-out cookie set for the DAA opt-out mechanism has the same name as the cookie set for the NAI opt-out mechanism.

c. Technologies or other mechanisms used to manage opt-out preferences need to have a persistency of five years to adequately honor users' preferences.

4. Data Security
   a. Participant must implement procedures to protect data within its control from unauthorized access, use, alteration, disclosure, or distribution

   b. Participant shall adequately maintain and audit internal data technology systems within Participant's control such as:

      i. Regularly monitor and repair systems including servers and desktops for known vulnerabilities;

      ii. Limit access and use of data to personnel with a legitimate business need;

      iii. Implement protection against phishing, spam, viruses, data loss, and malware; and

      iv. Use reasonable encryption methods for the storage of Sensitive Information.

   c. Participant shall utilize encryption methods such as Secure Socket Layer for the transmission of Sensitive Information.

   d. Access to Sensitive Information retained by Participant must be at least restricted by username and password.

   e. Privacy Statement shall state that security measures are in place to protect data.

5. Data Quality
   a. Participant shall take commercially reasonable steps when collecting, creating, maintaining, using, disclosing or distributing data to assure that the information is sufficiently accurate, complete, relevant, and timely for the purposes for which such information is to be used.

   b. If any information collected by the Participant about an Individual is disputed by that Individual and is found to be inaccurate, incomplete, or cannot be verified, Participant shall promptly delete or modify that item of information.

6. Retention
    a. Participants shall retain data collected for Online Behavioral Advertising:

        i. For as long as commercially useful to carry out its business purpose or until an Individual expresses an opt-out preference, but no longer than 24 months in an identifiable form; or as required by law.

        ii. Data that has been de-identified so the data cannot be used to re-identify the Individual can be retained as long as commercially useful to carry out its business purpose.

    b. Participants shall state how long they retain data in their Privacy Statement.

7. First Parties
    a. Where the Participant has a direct relationship with its First Party partners, the Participants shall have processes in place to require its First Party partners to:

        i. Include disclosures in the First Party's Privacy Statement listing the types of third parties that collect data through the First Party's application or Web site including Third Parties that collect data about an Individual's online activities across multiple unaffiliated applications or web sites, and how that data is used; and

        ii. Provide Clear and Conspicuous access to preference management tools where Individuals can exercise their preference, including withdrawing consent, on whether their data is collected and used for the purposes of behavioral targeting.

8. Third Party Data Sources
    a. All data sources that the Participant uses must contain appropriate terms of use showing that all data received was obtained under legitimate means and limitations regarding the collection, use, and onward transfer of the data are satisfied.

9. Service Providers
    a. The Participant must take commercially reasonable steps to ensure that its Service Providers with whom it shares data either:

        i. Abide by the Participant's privacy policies as reflected in the Participant's privacy statement; or

        ii. Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's privacy statement; and

iii. Abide by the rights and obligations attached to the data by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the data.

10. User Complaints and Feedback
    a. Participant shall provide users with reasonable, appropriate, simple and effective means to submit complaints, express concerns, or provide feedback regarding Participant's privacy practices at no cost to the user.

    b. Participant shall also cooperate with TRUSTe's efforts to investigate and resolve non-frivolous privacy complaints, questions and concerns raised either by users through TRUSTe's dispute resolution process or TRUSTe.

E. Accountability

1. Participants shall have processes in place to comply with these Program Requirements.

2. Participants shall state in their Privacy Statement that they comply with these Program Requirements, and other self-regulatory frameworks as applicable.

3. Cooperation with TRUSTe
    a. Provide, at no charge to TRUSTe or its representatives, full access to Online properties (i.e., including password access to premium or members only areas) for the purpose of conducting initial, on-going monitoring, or re-certification reviews, or resolving non-frivolous privacy complaints to ensure that the Participant's Privacy Statement(s) is consistent with actual practices, and comply with these Program Requirements.

    b. Provide TRUSTe information regarding how data is collected including information on the technologies used to obtain that data, how that data is used, and the choices provided to Individuals regarding the collection and use of that data.

4. Certification Renewal
    a. Participant shall undergo at least an annual certification renewal review of their data practices to verify compliance with these Program Requirements
    b. The certification renewal review includes, but is not limited to, the following assessments for either new practices or Material Changes to the Participant's existing practices around:
        i. Data collection, use, and sharing;
        ii. Consumer controls;
        iii. Data management (e.g. policies and processes around data access, retention, and storage); and
        iv. Privacy Statement.

5. Compliance Monitoring
    a. Participants shall undergo periodic monitoring checks throughout the certification period to verify ongoing compliance with these Program Requirements.

6. Termination for Material Breach
    a. In the event TRUSTe reasonably believes the Participant has materially breached these Program Requirements, TRUSTe may terminate the Participant's participation in this program upon twenty (20) business days' prior written notice ("Notice of Termination") unless the breach is corrected within the same twenty (20) business day period ("Cure Period").

        i. Material breaches of these Program Requirements include but are not limited to:

            1. The Participant's continual, intentional, and material failure to adhere to these Program Requirements;

            2. The Participant's material failure to permit or cooperate with a TRUSTe investigation or review of the Participant's Online properties practices pursuant to these Program Requirements;

            3. The Participant's continual, intentional, and material failure to comply with any Suspension Obligations;

            4. The Participant's material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe; or

            5. Any deceptive or unfair trade practices by the Participant.

7. Suspension Status
    a. In the event TRUSTe reasonably believes that Participant has materially violated these Program Requirements, Participant may be placed on "Suspension".

    b. Notice will be provided with a description of the violation and any remedial actions that TRUSTe will require the Participant to take during the Suspension Period ("Suspension Obligations").

    c. The Participant will be considered to be on Suspension immediately upon receiving notice from TRUSTe. Suspension shall last until such time as the Participant has corrected the material breach or Program Requirements violation to TRUSTe's satisfaction, but not for a period of greater than six (6) months ("Suspension Period") unless mutually agreed by the Parties.

    d. Suspension Obligations may include, but are not limited to:

        i. Compliance with additional Program Requirements;

        ii. Cooperation with heightened compliance monitoring by TRUSTe;

iii. Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe's additional compliance monitoring; and

iv. The Participant shall comply with all Suspension Obligations.

v. During the Suspension Period, the Participant's status may be indicated via a TRUSTe Validation webpage or TRUSTe may require the Participant to cease using the TRUSTe trustmarks.

vi. At the end of the Suspension Period, TRUSTe will, in its discretion, either:

1. Determine that the Participant has complied with Participant's Suspension Obligations, thereby satisfying TRUSTe's concerns;

2. Extend the Suspension Period by mutual agreement with the Participant; or

3. Determine that Participant has failed to comply with Participant's Suspension Obligations and immediately terminate the Participant for cause.

III. Definitions

A. "Ad Company Ad Company" is an entity that helps optimize or serve an ad, and includes the following types of entities. Note: a single entity may fall under multiple types.

1. "Ad Exchanges" are technology platforms that facilitate automated, auction-based pricing and buying of online advertising inventory in real-time. Ad Exchanges represent a sales channel to **App Developers**, **Web site Publishers**, and Ad Networks, and a source of online advertising inventory for advertisers and agencies.

2. "Ad Mediator" is an ad-tracking platform that is integrated with multiple Ad Networks at an API level, facilitating Ad Networks' management and ad optimization.

3. "Ad Network" is an entity that connects advertisers with App Developers and Web site Publishers that host online advertisements.

4. "Ad Server" is a computer system that stores, maintains and serves (uploads) advertising banners for one or more websites. Ad servers program, track, and report several statistics about website visitors which are used by advertisers to custom tailor ads and offers to suit different categories of visitors.

5. "Data Management Provider" ("DMP") is an entity that organizes and interprets unique demographic and interest-based information that allow App Developers, Web site Publishers, and advertisers to discover and target relevant audiences at scale.

6. "Demand Side Platform" ("DSP") is a system that allows advertisers to manage their bids across multiple Ad Exchanges in order to minimize expenses while maximizing results.

7. "Real-time Bidding (RTB) Exchange" allows for the buying digital inventory from multiple App Developers and Web site Publishers on an impression-by-impression basis, typically involving an auction pricing mechanism.

8. "Supply Side Platform" ("SSP") is a system that allows App Developers and Web site Publishers to automate the management of their inventory across multiple Ad Exchanges or Ad Networks for purposes of efficiency.

B. "Ad Delivery" means the delivery of online advertisements or advertising-related services using Ad Reporting data. Ad Delivery does not include the collection and use of Ad Reporting data when such data is used to deliver advertisements to a computer or device based on the preferences or interests inferred from information collected over time and across non-Affiliate sites, because this type of collection and use is covered by the definition of Online Behavioral Advertising.

C. "Ad Reporting" means the logging of page views on a Web site(s) or the collection or use of other information about a browser, operating system, domain name, date and time of the viewing of the Web page or advertisement, and related information for purposes including but not limited to:

   1. Statistical reporting in connection with the activity on a Web site(s);

   2. Web analytics and analysis; and

   3. Logging the number and type of advertisements served on a particular Web site(s).

D. "Ad Transaction" is the recorded exchange, movement or conveyance of ad related data, including money, between at least two parties.

E. "Affiliate" means an entity that controls, is controlled by, or is under common **Control** with, another entity.

F. "App Developer" is the entity that owns, Controls, and operates the mobile application with which the Individual interacts.

G. "Clear and Conspicuous" means a notice that is reasonably easy to find, and easily understandable in terms of content and style to the average reader.

H. "Control" of an entity means that one entity (1) is under significant common ownership or operational control of the other entity, or (2) has the power to exercise a controlling influence over the management or policies of the other entity. In addition, for an entity to be under the Control of another entity and thus be treated as a First Party under these Guidelines, the entity must adhere to the Online Behavioral Advertising policies that are not materially inconsistent with the other entity's policies.

I. "Cross-App Data" is data collected from a particular device regarding applications use over time and across non-**Affiliated** applications.

J. "Deterministic" is an algorithm, model, procedure, process, etc., whose resulting behavior is entirely determined by its initial state and inputs, and is not random or stochastic.

K. "Device" is a thing made or adapted for a particular purpose, typically a piece of electronic equipment that allows the user to process, receive, and send data.

L. "Device Recognition Technology" is either **Deterministic** or **Probabilistic** statistical identification approach based on the collection of information about the attributes of a discrete device and browser combination used to identify and recognize the same device at a later point in time.

M. "Express Consent" means the affirmative consent to a practice by the Individual after being provided notice, but prior to implementing the practice.

N. "First Party" means the entity that is the owner of the Web site or app or has Control over the Web site or app with which the Individual interacts and its Affiliates.

O. "Icon" is an icon in or around an Online Behavioral Advertisement that that contains a link to the notice and preference management tool enabling Individuals to exercise choice.

P. "Individual" means the discrete person to whom the collected data pertains.

Q. "Material Change" means degradation in the rights or obligations regarding the collection, use, or disclosure of data for an Individual. This usually includes any changes to Participant's:

1. Practices regarding notice, collection, use, and disclosure of data;

2. Practices regarding user choice and consent to how Personally Identifiable Information is used and shared; or

3. Measures for information security, integrity, access, or Individual redress.

R. "Online Behavioral Advertising (OBA)" means the collection of data from a particular computer or device regarding Cross-App data or Web viewing behaviors over time and across non-Affiliate apps or Web sites for the purpose of using such data to predict Individual preferences or interests to deliver advertising to that computer or device based on the preferences or interests inferred from such Web viewing behaviors. Online Behavioral Advertising does not include the activities of First Parties, Ad Delivery or Ad Reporting, or contextual advertising (i.e., advertising based on the content of the app or Web page being visited, a Individual's current visit to an app or Web page, or a search query).

S. "Participant" means the entity that has entered into an agreement with TRUSTe to participate in the TRUSTe program(s) and agreed to comply with the program requirements included therein.

T. "Personal Directory Data" is data created by the Individual, and stored on and accessed through a particular device. Examples of Personal Directory Data include calendar, address book, phone/text log, and photo/video data.

U. "Personally Identifiable Information (PII)" is any information or combination of data about an identified or identifiable Individual that can be used to identify, contact, or locate that Individual. PII includes the following subcategories:

1. "Contact Information" is information that can be used on its own to directly reach an Individual. Examples of Contact Information include first and last name plus mailing or home address, email address, telephone or mobile phone numbers.

2. "Persistent Device Identifiers" are distinctive device characteristics, or numbers or alphanumeric characters that are associated with and used to recognize a specific app, browser cookie, or device. Examples of Persistent Device Identifiers include IDFA, Android ID, IMEI, and MAC address.

3. "Precise Geo-location Data" is data that describes the precise real-time location of an Individual or a device, and is derived using technologies such as GPS level longitude and latitude, or WiFi triangulation.

4. "Sensitive Information" is information where unauthorized use or disclosure of that information would be likely to cause financial, physical, or reputational harm to an Individual. Examples of Sensitive Information include:

    i. Financial Information such as credit card or bank account number;

    ii. Government-issued identifiers such as SSN, driver's license number

    iii. Insurance plan numbers

    iv. Racial or ethnic origin of the Individual;

    v. Political opinions of the Individual;

    vi. Religious or similar beliefs of the Individual;

    vii. Individual's trade union membership;

    viii. Precise information regarding the Individual's past, present, or future physical or mental health condition and treatments including genetic, genomic, and family medical history;

    ix. Individual's sexual life or orientation;

    x. The commission or alleged commission of any offense by the Individual; or

    xi. Any proceedings for any committed or allegedly committed offense by the Individual and the disposal or such proceedings or the sentence of any court in such proceedings.

5. PII does not include Pseudonymous Information.

V. "Privacy Statement" means the conspicuous statement of the Participant's data collection and use practices, as such practices are updated time to time.

W. "Probabilistic" is the situation or model where there are multiple possible outcomes, each having varying degrees of certainty or uncertainty of its occurrence.

X. "Pseudonymous Information" means information that may correspond to a person, account, or profile but is not sufficient, either on its own, or through combination with other easily accessible public information, to contact or locate the Individual to whom such

information pertains. Examples include IP address, machine ID other than Persistent Device Identifiers, and the web pages a user views.

Y. "Publicly Available Information [PAI]" means any information reasonably believed to be lawfully made available to the general public from:

1. Federal, state or local government records;
2. Widely available source(s) having no additional prohibition around onward transfer or use; or
3. Disclosures to the general public that are required to be made by federal, state or local law.

Z. "Service Provider" is an entity(ies) other than the Participant or the Individual that performs, or assists in the performance of a function or activity that may involve the use or disclosure of data. Such use must only be on behalf of the Participant or Individual and only for the purpose of performing or assisting in that specific function or activity as agreed to by the Participant and Individual.

AA. "Third Parties" are entities other than the Participant or the Individual that are not directly affiliated with the Participant, and if affiliated with the Participant, where such affiliation is not reasonably known to the Individual.

BB. "Web site Publisher" is the entity that owns, Controls, and operates the Web site (including Mobile Web sites) with which the Individual interacts.