Exhibit A

TRUSTe Program Requirements

I. Structure

TRUSTed Websites requires compliance with the following program requirements. Upon satisfactory certification TRUSTe provides companies with a TRUSTe Privacy Seal as evidence of compliance - certified companies must display this seal on their website privacy policy page and may elect to place the seal on additional webpages as well.

II. Definitions

The following definitions shall apply herein:

A. "Behavioral Targeting" is the collection and use of information on an Individual's Online activity over a period of time for the purpose of developing and using predictive models to determine potential future behavior or interests.

B. "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.

C. "Expressed Consent" means the affirmative consent (opt-in) to a practice by the Individual, after being provided notice, but prior to implementing the practice.

D. "Foreign Language Privacy Statement" is the Participant's Privacy Statement translated into a language other than English.

E. "Geo-location Data" is information obtained through an Individual's use of a Mobile Device and is used to identify or describe the Individual's actual physical location at a given point in time.

F. "Individual" means the discrete person to whom the collected information pertains.

G. "Inferred Consent" means consent which is implied by an Individual, regarding the collection, use, disclosure, distribution of PII after notice and opportunity to withdraw consent (opt-out) is given by Participant, but not taken by the Individual.

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

1. Practices regarding notice, collection, use, and disclosure of PII and/or Third Party Personally Identifiable Information;
2. Practices regarding user choice and consent to how PII and/or Third Party Personally Identifiable Information is used and shared; or
3. Measures for information security, integrity, access, or individual redress.

I. "Mobile Device" is a portable electronic geo-location enabled device which allows the user to process, receive, and send data without being limited to a specific geographical location.

J. "Online" is the state where an Individual is connected by computer or Mobile Device to one or more other computers, Mobile Devices, or networks, as through a commercial electronic information service or the internet.

K. "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.

L. "Personally Identifiable Information [PII]" means any information or combination of information that can be used to identify, contact, or locate a discrete Individual.

M. "Primary Purpose" means use of PII that is reasonably expected by the Individual (i) at the point of collection; and (ii) including compatible uses in features and services to the Individual that do not materially change expectations of user control and third party sharing. Such use may be at least those uses described in the Participant's terms of service governing the Participant's products or services which give rise to the Individual's interaction with the Participant.

N. "Privacy Statement" shall mean the statements of Participant's information collection and usage practices, as such practices are updated from time to time. Participant's Privacy Statement includes, but is not limited to:

1. A single, comprehensive statement of all the Participant's information practices ("Comprehensive Privacy

Statement");

2. A summary notice highlighting the Participant's information practices ("Short Notice"); or
3. Disclosure of specific information practices posted at the point of information collection ("Just in Time Notice").

O. "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.

P. Recipient" means the Individual who receives an Email Message.

Q. "Retargeting" is a form of behavioral advertising by which online advertising is delivered to an Individual based upon the Individual's previous online actions.

R. "Search Engine" is a publicly facing service that collects and organizes content from across the internet for the primary purpose of responding to a search request. Such service may not retain information beyond caching or other service enhancing techniques, or use the information to create a persistent profile of the Individual for purposes other than enhancing search techniques.

S. "Secondary Purpose" is the use of PII in a way that is not reasonably expected by the Individual relative to the transactions or ongoing services provided to the Individual by Participant or the Participant's Service Provider. Such purpose may or may not be described by Participant's terms of service governing Participant's products or services which give rise to the Individual's interaction with the Participant

T. "Service Provider" is anyone other than the Participant or the Individual that performs, or assists in the performance of, a function or activity which may involve the use or disclosure of PII or Third Party PII. Such use must only be on behalf of 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.

U. "Social Network" is an online service that offers the following features:
1. A platform that enables the interaction between two or more Individuals for the purpose of creating social or business relationships, and sharing of information;
2. Functionality that enables Individuals to create a profile that includes information of their own choosing such as photos, and links to personal pages of other connected Individuals (e.g. friends, business contacts);
3. Mechanisms to communicate with other Individuals such as instant messenger, email, or posting to a profile or newsfeed; and
4. Search functionality that enables Individuals to search for other Individuals that is based upon that Individual's preferences.

V. "Third Party(ies)" is an entity(ies) other than the Participant or the Individual which is not directly affiliated with the Participant; and, if affiliated with the Participant, where such affiliation is not reasonably known to the Individual.

W. "Third Party Personally Identifiable Information [Third Party PII]" means PII that is collected by Participant from an entity other than the Individual

III. Minimum Program Requirements

A. All Participants wanting to be certified that their Online information collection and use practices comply with TRUSTe's Privacy Program Requirements must comply with the following requirements:

B. Participant Accountability
1. Participant shall have processes in place to comply with these Program Requirements
2. Cooperation with TRUSTe
   a. Provide, at no charge to TRUSTe or its representatives, full access to the Online properties (i.e., including password access to premium or members only areas) for the purpose of conducting reviews to ensure that Participant's Privacy Statement(s) is consistent with actual practices.
   b. Provide, upon TRUSTe's reasonable request, information regarding how PII gathered from and/or tracked through Participant's Online properties is used.

3. Annual Recertification
   a. Participant shall undergo re-certification to verify ongoing compliance with these Program Requirements annually.

4. 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").
   b. Material breaches of these Program Requirements include but are not limited to:
      1. Participant's continual, intentional, and material failure to adhere to these Program Requirements;
      2. Participant's material failure to permit or cooperate with a TRUSTe investigation or review of Participant's Online properties or practices pursuant to the Program Requirements;
      3. Participant's continual, intentional, and material failure to comply with any Suspension Obligations;
      4. Participant's material failure to cooperate with TRUSTe regarding an audit, complaint or the compliance monitoring activities of TRUSTe; or
      5. Any deceptive trade practices by the Participant

5. Suspension Status
   a. In the event TRUSTe reasonably believes that Participant has materially violated these Program Requirements, Participant may be placed on suspension.
      1. Notice will be provided with a mutually agreed upon description of the violation and any remedial actions that TRUSTe will require Participant to take during the Suspension Period ("Suspension Obligations").
      2. 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.
      3. Suspension Obligations may include, but are not limited to:
         a. Compliance with additional Program Requirements;
         b. Cooperation with heightened compliance monitoring by TRUSTe; and
         c. Payment to TRUSTe of mutually agreed additional amounts as compensation for TRUSTe's additional compliance monitoring.
         d. Participant shall comply with all Suspension Obligations.
      4. During the Suspension Period, Participant's status may be indicated via a TRUSTe Validation webpage or TRUSTe may require Participant to cease using the TRUSTe trustmarks.
      5. At the end of the Suspension Period, TRUSTe will, in its discretion, either:
         a. Determine that Participant has complied with Participant's Suspension Obligations, thereby satisfying TRUSTe's concerns;
         b. Extend the Suspension Period by mutual agreement with the Participant; or
         c. Determine that Participant has failed to comply with Participant's Suspension Obligations and immediately terminate Participant for cause.

C. Privacy Practices
The following requirements apply if the Participant collects PII:

1. Collection Limitation
   a. Participant shall only collect PII where such collection is:
      1. Limited to information reasonably useful for the purpose for which it was collected and in accordance with the Participant's Privacy Statement in effect at the time of collection; or
      2. With notice to and consent of the Individual

2. Use of PII

a. Participant shall use PII in the provision of those services advertised or provided for, and in accordance with their posted Privacy Statement in effect at the time of collection, or with notice and consent as described in these Program Requirements.

b. Information collected by the Participant or the Participant's Service Provider may be used to tailor the Individual's experience on the Participant's Online property.

3. Choice
   a. Participant shall offer the Individual control over their collected Personally Identifiable Information as follows:
      1. Participant must provide the Individual an opportunity to withdraw consent to having PII used by the Participant for a Secondary Purpose.
      2. Participant must provide the Individual a Just in Time Notice and the opportunity to withdraw consent to having PII disclosed or distributed to Third Parties, other than Service Providers, at the time PII is collected;
      3. Participant shall honor and maintain the Individual's choice selection in a persistent manner until such time the Individual changes that choice selection; and
      4. Participant shall provide a means by which the Individual may change their choice selection.
   b. Consent is not necessary where the use, disclosure or distribution of PII is required by law, court order, or other valid legal process.
   c. Express Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual.
   d. Privacy Statement shall state when the Individual can exercise control over the use and sharing of their PII and how to exercise that control
   e. Such mechanism shall be easy to use and offered at no cost to the Individual

4. Collection and Use of Third Party PII
   a. Participant shall use Third Party PII collected solely to facilitate the one-time completion of the transaction that is the Primary Purpose for which the information was collected by the Participant except as allowed in Section III.C.4.d regarding Search Services.
   b. Participant must obtain Express Consent from the Individual to whom such Third Party PII pertains before such Third Party PII may be used, disclosed, or distributed by the Participant for any purpose other than the Primary Purpose for which such information was collected by the Participant, except as allowed in Section III.C.4.d regarding Search Services.
      1. Participant may use Third Party PII to send a one-time email message to the Individual to solicit their Express Consent.
   c. Regarding Third Party PII the Privacy Statement shall state:
      1. The types of the entity(ies) collecting Third Party PII;
      2. What kind of Third Party PII is collected, either through active or passive means;
      3. How collected Third Party PII is used and/or disclosed;
      4. What types of additional Third Parties if any, including Service Providers, collected Third Party PII is shared with.
   d. Search Services

1. A Search Engine may provide search results containing Third Party PII, without the notice and choice requirements noted above, providing:
   a. The results were obtained from public or published sources on the Internet;
   b. The information is not used to create a persistent profile of the Individual outside the scope of enhancing Search Engine techniques;
   c. Participant shall have a mechanism for the Individual to request removal from displayed search results if the display of such results will:
      i. Cause physical harm to the Individual; or
      ii. Interfere with the safeguarding of important countervailing public interests, including national security, defense, or public security.
   d. Privacy statement shall state how Individual can request removal from displayed search results.
2. A Participant that compiles information about Individuals, who are neither customers of or registered users of, that Participant's services; and then sells access to that information to Third Parties may provide search results containing Third Party PII without the notice and choice requirements noted above, providing:
   a. Information obtained about the Individual is from public or published sources which have no prohibition around onward transfer or use associated with the information;
   b. The Participant shall provide the Individual a mechanism to stop having their information displayed in search results:
      i. Such mechanism shall be easily accessible to the Individual; and
      ii. Privacy Statement shall state how the Individual can stop having their information displayed in search results.
   c. This does not include situations where Participant disclosed Third Party PII back to an entity that has rights to such information.

5. Access
   a. Participant must implement reasonable and appropriate mechanisms to allow the Individual to correct or update inaccurate PII.
   b. Participant must implement reasonable mechanisms to allow the Individual to request deletion of PII or that collected PII no longer be used.
   c. Such mechanism should be consistent with how the Individual normally interacts or communicates with the Participant
   d. Such mechanism or process shall be clear, conspicuous, and easy to use
   e. Such mechanism or process shall confirm to the Individual inaccuracies have been corrected; and
   f. Participant's privacy statement shall state how access is provided.
   g. Participant is not required to permit Individual access to Personally Identifiable Information to the extent that:
      1. Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others;
      2. 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
      3. The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information.
   h. If 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.

6. Promotional and Newsletter Email Communications
   a. All newsletters and promotional email messages that Participant sends to the Individual must include Participant's postal address and a functional unsubscribe mechanism.
   b. The location and instructions concerning the unsubscribe mechanism must be Clear and

Conspicuous, and the mechanism itself must be functional for no fewer than thirty (30) days following the sending of the newsletter or promotional email message.

c. Participant must honor the Individual's request to unsubscribe from a newsletter or promotional email message beginning on the tenth (10) business day after the Participant receives the unsubscribe request, unless the Individual subsequently requests to receive newsletters or promotional email messages from Participant.

d. An unsubscribe mechanism is not required for administrative or customer service-related email messages (e.g. account management or provisioning of requested services, warranty or recall information, safety or security announcements).

7. Public Disclosure of PII
   a. A Participant may allow a user to post PII in an online forum, chat room, blog or other public forum, where the PII being displayed was placed there by a user who is also the Individual.
      1. If appropriate and commercially reasonable, provide a process or mechanism to allow the Individual to request timely removal of any publicly displayed PII where it has been legally and rightfully shared; and
      2. State in the Privacy Statement how the Individual can request removal of publicly displayed PII.
   b. The Privacy Statement shall state information posted by Individuals in online forums, chat rooms, blogs, or other public forum may be displayed publicly.
   c. The Privacy Statement shall accurately describe the extent to which an Individual's displayed PII is publicly available.
   d. If Participant provides a publicly accessible online directory or similar service, the Participant shall:
      1. Provide the Individual a reasonable and appropriate mechanism to request removal of their PII from the directory;
      2. Ensure the mechanism is consistent with how the Individual normally interacts or communicates with the Participant
      3. State in the Privacy Statement how the Individual can request removal; and
      4. Such mechanism to request removal of a listing where access to the online directory or similar service is limited to other registered Individuals may be contingent on the Individual no longer using that service.

8. Material Changes
   a. Participant must notify Individuals of any Material Changes to its PII collection, use, or disclosure practices prior to making the change.
   b. Participant must obtain prior approval from TRUSTe
      1. For any Material Change in its PII collection, use, or disclosure practices; and
      2. For method and notice to Individuals, such as email, "in product" messaging, etc.

D. Privacy Statement
   1. Participant shall maintain and abide by an accurate up-to-date Privacy Statement approved by TRUSTe in its sole discretion that states Participant's information practices and is in conformance with these Program Requirements including, but not limited to:
      a. What information is collected, either through active or passive means, type of entity(ies), excluding Service Providers, collecting the information, and how the collected information is used;
      b. What types of Third Parties if any, including Service Providers, collected information is shared with;
      c. Whether PII is appended with information obtained from third party sources;
      d. How and when the Individual can exercise choice as required in these Program Requirements;
      e. How the Individual can request access to their information as required in these Program Requirements;
      f. What types of security measures are in place to protect collected information as required in these Program Requirements;
      g. What tracking technologies are used by the Participant or Third Parties including Service Providers and the purpose for using those technologies;

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

i. How the Individual will be notified of any Material Changes in the Participant's privacy practices;

j. That collected information 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;

k. Effective date of Privacy Statement;

l. If required, statement of participation in the TRUSTe program and define participation scope; and

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

2. At a minimum, Participant shall link to a Comprehensive Privacy Statement that discloses the Participant's information practices.

3. Access to the Privacy Statement shall be Clear and Conspicuous.

4. As commercially reasonable, Privacy statement must be available when the Individual engages with the Participant, such as through an application, Web site homepage or landing page.

5. Privacy statement must be available at the point where the Individual provides PII, or through a common footer.

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

7. Short Notice
   a. If Participant chooses, they may provide a Short Notice highlighting their information practices including but not limited to:
      1. Summarize what information is collected by the Participant and how the Participant collects that information, either through active or passive means;
      2. Summarize how Participant uses collected information;
      3. Whether Participant shares PII with third parties, excluding Service Providers;
      4. How the Individual can exercise choice and request access pursuant to these Program Requirements; and
      5. How to contact the Participant including company name, email address or link to online form, and postal address.

   b. Access to the Short Notice shall be Clear and Conspicuous.

   c. Short Notice shall link to Comprehensive Privacy Statement.
      1. Access to the Comprehensive Privacy Statement shall be Clear and Conspicuous.

   d. Any Short Notice shall be consistent with Comprehensive Privacy Statement.

8. Just in Time Notice
   a. If Participant chooses to provide Just in Time Notice, the Just in Time Notice shall be consistent with Comprehensive Privacy Statement.

9. Foreign Language Privacy Statement.
   a. If Participant seeks TRUSTe certification of a Privacy Statement in a language other than English, TRUSTe shall use commercially reasonable efforts 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.

E. Data Governance
   1. Participant shall implement controls and processes to manage and protect PII within its control including the ones listed in this Section III.E.
      a. Such controls and processes shall be
         1. Appropriate to the size of the Participant's business; and

2. Appropriate to the level of sensitivity of the data collected and stored

2. Data Security
   a. Participant must implement commercially reasonable procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution.
   b. Participant shall maintain and audit internal information technology systems within Participant's control such as:
      1. Regularly monitor and repair systems including servers and desktops for known vulnerabilities;
      2. Limit access and use of PII, or Third Party PII, to personnel with a legitimate business need where inappropriate access, use, or disclosure of such PII, or Third Party PII, could cause financial, physical, or reputational harm to the Individual;
      3. Implement protection against phishing, spam, viruses, data loss, and malware; and
      4. Use reasonable encryption methods for transmission of information across wireless networks, and storage of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual
   c. Participant shall utilize encryption such as Secure Socket Layer for the transmission of information if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.
   d. Access to PII or Third Party PII retained by Participant must be at least restricted by username and password if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual.
   e. Privacy Statement shall state that security measures are in place to protect collected PII and/or Third Party PII.

3. Data Quality
   a. Participant shall take commercially reasonable steps when collecting, creating, maintaining, using, disclosing or distributing PII 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, as appropriate, based on the results of the investigation.

4. Data Retention
   a. If a Participant receives and retains PII or Third Party PII, the Participant must limit its retention to no longer than commercially useful to carry out its business purpose, or legally required; and must disclose in their Privacy Statement how long they will retain that information.
   b. Regardless of the time period of retention, so long as a Participant has PII or Third Party PII in its possession or control, the requirements included herein shall apply to such information.

5. Service Providers
   a. Participant must take commercially reasonable steps to ensure that it's Service Providers with whom it shares PII either:
      1. Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or
      2. Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and
      3. Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII.

6. 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.
   b. Participant shall also cooperate with TRUSTe's efforts to investigate and resolve non-frivolous privacy complaints, questions and concerns raised either by:
      1. Users through TRUSTe's dispute resolution process; or
      2. TRUSTe.

7. Data Breach

a. Participant must notify an Individual of a data breach within 45-days of a known breach as required by law or if the unauthorized disclosure of PII can cause financial, physical, or reputational harm to the Individual unless otherwise required by law.

b. Unless otherwise required by law, notice to the Individual must disclose the following:
   1. That a breach occurred;
   2. What type of information was breached;
   3. When the breach happened;
   4. What steps Individuals can take to protect themselves;
   5. What the actions the Participant is taking regarding the breach (e.g. investigation); and
   6. What steps the Participant is taking to ensure the event does not happen again.

c. Participant must notify TRUSTe when it believes a data breach occurred. Participant must provide TRUSTe a copy of the notice to be sent or sent to affected Individual(s).

F. Behavioral Targeting

1. Participants engaging in Behavioral Targeting or Retargeting shall disclose the following regarding Participant's Behavioral Targeting and/or Retargeting Practices in its Privacy Statement:
   a. If information, collected either through active or passive means, is used by either the Participant or Third Party(ies) for the purpose of Behavioral Targeting or Retargeting;
   b. If PII collected by the Participant is linked to information collected through Web usage activity from sources, e.g. Web sites other than Participant's, for the purpose of Behavioral Targeting or Retargeting;
   c. Whether PII or Third Party PII is collected by, or shared with, additional Third Parties for the purposes of Behavioral Targeting or Retargeting; and
   d. How and when the Individual can exercise choice as required in this Section III.F.

2. Participant shall provide instructions or link to a mechanism that enables the Individual to withdraw consent for the use of their information for the purposes of behavioral advertising.
   a. At a minimum, such instructions or link shall be made available in the Participant's Privacy Statement.

3. Participant engaging in Behavioral Targeting or Retargeting shall offer choice to the Individual as follows:
   a. An Individual must be provided an opportunity to withdraw consent to having PII linked to information collected through web usage activity for the purpose of Behavioral Targeting or Retargeting;
   b. An Individual must be provided an opportunity to withdraw consent to having PII shared with Third Parties, other than Service Providers, for the purpose of Behavioral Targeting or Retargeting at the time such PII is collected; and
   c. Express Consent must be obtained prior to sharing PII with Third Parties, other than Service Providers, for the purposes of Behavioral Targeting or Retargeting, if the unauthorized use or disclosure of that information could cause financial, or physical harm to an Individual.

G. Social Networks

1. Participants that enable users to network with other users of a community need to comply with the following:
   a. Express Consent with confirmation is required for an Individual to establish a profile.
   b. Provide a reasonable and appropriate mechanism to allow the Individual to manage their privacy settings.
      1. Mechanism should be consistent with how the Individual normally interacts or communicates with the Participant
      2. Mechanism shall be clear, conspicuous, and easy to use
      3. Mechanism shall confirm to Individual that privacy settings have been set; and
      4. Privacy Statement shall state how the Individual can update their privacy settings.
   c. Provide a reasonable and appropriate mechanism to allow the Individual request deletion or deactivation of a profile.
      1. Mechanism should be consistent with how the Individual normally interacts or

communicates with the Participant

2. Mechanism shall be clear, conspicuous, and easy to use
3. Mechanism shall confirm to Individual profile has been deleted or deactivated; and
4. Privacy Statement shall state how the Individual can request deletion or deactivation of their profile

d. Provide a reasonable and appropriate mechanism to allow the Individual to request removal of an unauthorized profile.
   1. Mechanism should be consistent with how the Individual normally interacts or communicates with the Participant
   2. Mechanism shall be clear, conspicuous, and easy to use
   3. Mechanism shall confirm to Individual the unauthorized profile has been removed; and
   4. Privacy Statement shall state how the Individual can request removal of an unauthorized profile.

e. Individuals between the ages 13-17 must provide Express Consent to the collection, use, disclosure of either:
   1. PII pertaining to that Individual; or
   2. Third Party PII pertaining to an Individual between the ages of 13-17.

f. If Participant enables users to import Third Party PII from another source to their profile, the Participant must do the following:
   1. Treat all collected information as if it is Third Party PII as outlined in Section III.C.4.
      a. Collected information cannot be used to create a publishable profile unless the Participant obtains the Express Consent of the Individual.
   2. Provide Clear and Conspicuous notice to the user as to why they are providing a password or other access to their email account; and

IV. US-EU and US-Swiss Safe Harbor Requirements

A. Participants want to self-certify with the Department of Commerce (DOC) for compliance with the U.S.-E.U. Safe Harbor or Swiss Safe Harbor Frameworks and list TRUSTe as its third party dispute resolution mechanism must comply with the Minimum Program Requirements and the following:
   1. Participant must provide an Individual with access to PII within thirty (30) calendar days of request.
      a. If Participant does not provide an Individual the requested access within thirty (30) calendar days of the Individual's request, Participant must provide the Individual with a timeline establishing when the requested access will be provided.
      b. Privacy Statement shall disclose the timeline establishing when the Individual can expect a response to their request for access.
   2. Privacy Statement shall include the following statement: "[Participant] complies with the [E.U.][Swiss] Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use and retention of personal information from [the European Union][Switzerland]."
      a. The statement must include the following link to the Department of Commerce's Web site: http://export.gov/safeharbor

V. Additional Email Requirements

A. Participants wanting to be certified for practices around the sending of commercial and promotional email must comply with the Minimum Program Requirements and the following:
   1. Participants must ensure that the following disclosures are accessible from the point of email address collection except where email address is used only to authenticate an Individual for purposes of accessing that Individual's account information:
      a. The nature of commercial or promotional email messages to be sent and the types of entities that will be providing content;
      b. Whether Participant sells, rents or otherwise shares Recipients' email address with Third Parties other than Service Providers; and
      c. If receiving commercial or promotional email messages is a requirement to receive a service, a disclosure of such requirement.

2. Prior to sending commercial or promotional email messages the Recipient must be provided the opportunity to withdraw consent to having his/her email address added to a mailing list. Commercial or promotional email messages sent under this form of consent must include Clear and Conspicuous identification that the message is an advertisement or solicitation.
3. If Participant has not collected the Recipient's email address directly, the Participant must perform due diligence to ensure that Clear and Conspicuous notice was provided regarding the use and disclosure of the Recipient's email address, and that the Individual had the opportunity to withdraw consent.

B. Participant Accountability. Participant shall ensure that the mail infrastructure used to send email messages is well maintained and operated in a responsible manner:
1. Email address list maintenance systems must be employed to reliably receive and process bounces and other replies from receiving networks.
2. The Participant's IP address(es) for outgoing email must have valid reverse DNS entries. The IP address of the host name of the reverse DNS entry must match the IP address of the sending mail server.
3. Participant must create and maintain the standard role email accounts abuse@sender.domain and postmaster@sender.domain for all of its domains that send email in order to facilitate handling complaints and other issues.
4. Participant must comply with relevant internet standards such as the Network Working Group Request for Comment ("RFC") Nos. 2821 and 2822, which describe how Email Messages must be formatted in order to be processed properly by receiving networks.

C. Transparency. Participant shall ensure that email messages are truthful and accurately identify the source of the message.
1. The domain name or message headers must not be falsified or obscured in any way.
2. The subject line and content of every email message must not be false or misleading.

VI. Mobile Services

A. Participants wanting to be certified for collecting PII through an application on a Mobile Device or through a Web site optimized for a Mobile Device must comply with the Minimum Program Requirements and the following:

B. Mobile Short Notice
1. Participants will provide enhanced notice outside of the Privacy Statement by linking from a TRUSTe icon or text link to a TRUSTe-hosted Short Notice.
2. The following disclosures will appear within the TRUSTe-hosted Short Notice:
   a. Whether geo-location data is collected and how geo-location data is used;
   b. What types of information is collected and how it is used;
   c. Whether Participant shares PII with Third Parties, including Service Providers;
   d. How the Individual can exercise choice and request access pursuant to these Program Requirements;
   e. What tracking technologies are used by the Participant or Third Parties including Service Providers and the purpose for using those technologies;
   f. What security measures are in place to protect collected information as required in these Program Requirements; and
   g. How the Individual can contact the Participant, including company name, email address or a link to an online form, and physical address.

C. Geo-location Data
1. Participant must obtain Express Consent from the Individual the first time Geo-location Data is used by the Participant to provide services.
2. Participant may provide additional notifications through a Just in Time Notice or a persistent icon, to remind Individuals that their Geo-location Data is being used by the Participant to provide a service.
3. Participant must obtain Express Consent from the Individual prior to the sharing of Geo-location Data with Third Parties other than Service Providers.
4. Participant must obtain Express Consent from the Individual prior to any use of Geo-location Data for Secondary Purposes.

D. Privacy Statement shall state:

1. What information is collected from an Individual's Mobile Device;
2. Whether information is shared with another application installed on the Individual's Mobile Device;
3. How Geo-location Data is used;
4. If Geo-location Data is used to create a profile about the Individual;
5. How long Geo-location Data is retained;
6. What type of Third Parties, including Service Providers is Geo-location Data is shared with and for what purpose;
7. How the Individual can restrict the disclosure of Geo-location data to Third Parties; and
8. How the Individual can revoke consent to the Participant's collection and use of Geo-Location Data.
   a. Such mechanism shall be easy to use.