



TRUSTED DOWNLOAD PROGRAM CRITERIA BETA 11/16/05

TRUSTe TRUSTED DOWNLOAD CERTIFICATION PROGRAM - BETA

I. PURPOSE AND PRINCIPLES

The Purpose of the Program

Concerned businesses have lacked a comprehensive set of standards, incentives and enforcement mechanisms to enable them to protect their customers from exposure to malicious software. TRUSTe, in cooperation and partnership with the Program Sponsors, have created the Trusted Download Certification Program in order to address unwanted and deceptive software by (i) establishing acceptable practices for the development and distribution of downloadable software, (ii) monitoring ongoing compliance with such standards by software applications over time, and (iii) publicly certifying compliance with such standards.

The Program is a Business Certification Program, Not a Consumer Facing Seal.

While TRUSTe intends that consumers will derive important indirect benefits from the Program, the Program is primarily designed to provide businesses with best practice standards and certification for software. The Program establishes a whitelist intended to be used by companies as a tool for evaluating potential business relationships. TRUSTe encourages companies to utilize these standards in a way that is tailored to address their unique business objectives.

For example, TRUSTe understands that some potentially unwanted software applications may reach users' computers, and that anti-spyware software will continue to provide a means of detecting and removing software that fails to meet the standards of the anti-spyware industry or the interests of anti-spyware consumers. TRUSTe hopes that anti-spyware companies will consider the whitelisting of a company as a useful input into their research efforts, but recognizes that anti-spyware companies may have different valid methods of evaluating programs and may consider additional relevant factors important to their users.

The Program Focuses on Behavior, Not Technology.

TRUSTe believes that technology itself is neither good nor bad, but that technology can be used in ways that benefit consumers or in ways that harm consumers. The Program therefore focuses not on regulating technology, but rather on regulating behavior (that is, the uses or misuses of technology). The Program bans altogether some behaviors that are rarely, if ever, used in legitimate software. Other behaviors that may have legitimate commercial application, such as collecting information for use in certain types of online marketing, are subject to standards of notice, consent and consumer control (as well as subject to a third-party evaluation and enforcement regime) so that consumers may take advantage of them knowingly in a value-for-value exchange.

The Program is Built on the Principles of Transparency and Control.

The Program Requirements reflect commitment to two fundamental principles: (1) full transparency, both in the installation process and during the operation of software, and (2) consumer control over their ongoing use of software. In its broadest sense, transparency means

that software is distributed to consumers and operates in ways that consumers understand. Control reflects a commitment to giving consumers easy and obvious means of controlling the software on their computer hard drives. For example, it means that software should be as easy to remove as it is to install.

The Program Acknowledges the Importance of Enforcement

Recognizing that clear requirements are only part of the solution, TRUSTe has developed a set of enforcement mechanisms to support the Program, including: third-party evaluation and software testing, ongoing monitoring, and establishing verifiable accountabilities between Program Participants and their Distribution Partners and Affiliates. Such enforcement mechanisms are essential to ensuring that the goals of the Program are achieved.

If certain Program Applicants have previously exhibited practices that would have fallen below the current Program Requirements, additional remediation may be required, as outlined in Section XI.

The Scope of the Program

The types of issues addressed by the Program are most prominent in consumer software applications, and this Program is not intended to cover business to business downloads such as enterprise-wide intranet and back office applications.

The Program outlines certain requirements for all Certified Software and specifies additional requirements for all Certified Adware and Certified Trackware. This approach ensures that these Program Requirements address practices which historically have created a significant proportion of consumer confusion and anxiety. However, all software, even software which does not meet the Program definitions for Adware and Trackware, will be tested for monitoring, relays, and behaviors which have historically been associated with spyware.

The Program, as launched, only applies to applications which are downloaded within the United States.

(Beta Note: TRUSTe recognizes that the Program will launch in beta mode, and anticipate that these Program Criteria will change over time as learnings are accumulated. TRUSTe recognizes that such changes may require substantial alterations to the business processes of Program Participants, Program Partners and others that plan to utilize these Program Requirements. With this in mind, TRUSTe intends to seek input from a qualified advisory committee and provide reasonable notice prior to making significant changes.)

About TRUSTe

TRUSTe® is an independent, nonprofit organization that promotes and enables trust based on privacy, transparency and the establishment of best practice standards for organizations conducting business on the internet. We certify and monitor web site privacy and email policies, monitor practices, and resolve thousands of consumer privacy problems every year.

II. DEFINITIONS

Adware – The term “Adware” means software that displays Covered Advertisements. TRUSTe may consider other related formats or methods of delivery as part of the scope of the program. Adware is often Bundled with other software, such as screensavers, games, weather applications, and other popular consumer software. (Adware may include Trackware where the Adware also meets the definition of Trackware.)

Affiliate – The term “Affiliate” means a person who, for consideration, distributes the Program Participant’s Adware or Trackware to consumers in connection with an Affiliate Distribution Program.

Affiliate Distribution Program – The term “Affiliate Distribution Program” means a process whereby (1) a Program Participant pays consideration to one or more Affiliates in exchange for their agreement to offer Adware or Trackware to consumers; and (2) as part of the program, at least some Affiliates have the Program Participant’s authorization to hire or subcontract with others to distribute the Program Participant’s Adware or Trackware to consumers.

Agent – The term “Agent” means a third party contracted with to perform a business process, provide a service, or deliver a product on behalf of the principal who retained the agent. An agent doesn’t have an independent right to use the relevant consumer data on its own behalf or in any way other than to strictly perform its obligations on behalf of the principal. Agents include service providers meeting these restrictions.

Applicant – The term “Applicant” means a company that has submitted software for certification to the Program. An Applicant must have control over all aspects relevant to certification of the software it submits for such certification.

Bundle – The term “Bundle” means a package of software programs offered to Users.

Certification – The term “Certification” means the determination by TRUSTe that software submitted to the Program is compliant with the Program requirements. While Certification applies to software (*i.e.*, the Program does not offer Certification to companies), no company that violates any company-level Program Requirement (such as performing the Prohibited Activities in Section XII) will be eligible for Certification of their software.

Certified Ad Inventory – The term “Certified Ad Inventory” means the segregated ad inventory that may be displayed only to Users of Adware installed after its Provisional Certification Date (and thus compliant with the Program Requirements) or Legacy Users of Adware that was installed prior to the Provisional Certification Date but have received the notice and/or given the consent required under Section XI.A.3.

Certified Adware – The term “Certified Adware” means a Program Participant’s Adware that has been tested and awarded certification, and is currently certified under this Program.

Certified Software – The term “Certified Software” means a Program Participant’s software application that has been tested and awarded certification, and is currently certified under this Program. Certified Software includes, but is not limited to, Certified Adware and Certified Trackware.

Certified Trackware – The term “Certified Trackware” means a Program Participant’s Trackware that has been tested and awarded certification, and is currently certified under this Program.

Children's Website – The term “Children's Website” means (as defined in Section 312.2 of the Children's Online Privacy Protection Rule, 16 C.F.R. Part 312) a website that, based upon its subject matter, visual or audio content, age of models and other language or characteristics, is targeted or directed to children under the age of thirteen.

Covered Advertisement – The term “Covered Advertisement” means an advertisement displayed to consumers that is either (i) activated by a software program that is not obviously active at the time the advertisement is displayed or (ii) that is not clearly associated with the software program that activated it (such as by labeling, design integration or temporal or geographic proximity). For purposes of this definition, the presence of an icon in the system tray is not, by itself, sufficient to demonstrate that the software program is obviously active. Covered Advertisements do not include Advertisements that are displayed with the authority of web site on which those Advertisements appear. **(Beta Note:** It is anticipated that TRUSTe may determine that other types of advertisements are potentially unexpected and unwanted by users, and reserves the right to include those types of advertisements under this definition.)

Default Option – The term “Default Option” means an option that is pre-selected, so that a User can accept the option without taking any additional affirmative action indicating consent. For purposes of this definition, allowing Users to accept an option by selecting the “Enter” key on their computer keyboards is not an affirmative action indicating consent.

Distribution Partner – The term “Distribution Partner” means a person that, for consideration, offers Adware or Trackware to consumers on behalf the Program Participant.

EULA – The term “EULA” means an End User License Agreement.

Just in Time Notice – The term “Just in Time Notice” means that a User is provided with Primary Notice of a particular functionality and is given the opportunity to provide consent just prior to execution of that functionality. Waiting until just prior to execution of certain functionalities can provide the User with better context to make certain consent decisions. While the Program permits the use of Just in Time Notice for some Certified Software, the Program does not permit its use for Certified Adware. **(Beta Note:** Just in Time Notice may not be used where such use would negatively impact the original value proposition of the Certified Software, as determined by TRUSTe.)

Legacy User – The term “Legacy User” means all Users of a single computer that have installed a Program Participant's Adware or Trackware before the Provisional Certification Date of such Adware or Trackware.

Monitoring – The term “Monitoring” means the collection by software of information about a User, a User's computer and/or web usage and the transfer of that information from the User's computer to a computer controlled by someone other than the owner of the User's computer. **(Beta Note:** This definition is intended to cover the use of information on a non-aggregate basis.)

Non-Certified Ad Inventory – The term “Non-Certified Ad Inventory” shall mean the segregated ad inventory that is displayed to Legacy Users of Adware that have not received the notice and/or given the consent required under Section XI.A.3.

Non-Personal Information – The term “Non-Personal 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 identify, contact using PII, or locate the person to whom such information pertains.

Online Preference Marketing – The term “Online Preference Marketing” (OPM) means a process whereby data is typically collected over time and across web pages to determine or predict consumer characteristics or preferences for use in ad delivery on the web. The OPM process can use Non-Personal Information or a combination of Personally Identifiable Information and Non-Personal Information. OPM does not refer to the use of data by Program Participants for Ad Delivery or Reporting.

Personally Identifiable Information – The term “Personally Identifiable Information” (or “PII”) means any information (i) that identifies or is used to identify, contact, or locate the person to whom such information pertains or (ii) from which identification or contact information of an individual person is derived. Personally Identifiable Information includes, but is not limited to: name, address, phone number, fax number, email address, financial profiles, medical profile, social security number, and credit card information. Additionally, to the extent unique information (which by itself is not Personally Identifiable Information) such as, but not necessarily limited to, a personal profile, unique identifier, biometric information, and/or IP address is associated with Personally Identifiable Information, then such unique information also will be considered Personally Identifiable Information. Notwithstanding the above, Personally Identifiable Information does not include information that is collected anonymously (*i.e.*, without identification of the individual user) or demographic information not connected to an identified individual. Personally Identifiable Information includes Third-Party Personally Identifiable Information.

Primary Notice – The term “Primary Notice” means information presented in a manner that is clear, prominent and unavoidable and designed to catch the consumer’s attention. The Primary Notice must be fully visible to a consumer without additional action on the part of the consumer, such as having to scroll down the page to reach the beginning of the required disclosures. The purpose of the Primary Notice is to ensure that important information is disclosed to consumers in a way that they will see and understand so that they can make an informed decision about the proposed software value proposition.

Program – The term “Program” means the TRUSTe Trusted Downloadable Certification Program.

Program Participant – The term “Program Participant” means a company that has software that is currently certified or provisionally certified in the Program. A Program Participant must have control over all aspects relevant to certification of the Certified Software.

Program Requirements – The term “Program Requirements” means the requirements for participation in the Program as specified in this document.

Program Sponsors – The term “Program Sponsors” mean the entities that participated in the development of this Program with TRUSTe. A list of the Program Sponsors may be found in Section XVI.

Provisional Certification – The term “Provisional Certification” means an interim level of certification of a Program Participant’s software, during which time the Program Participant will be subject to all requirements that apply to its Certified Software as well as certain additional requirements, including, as relevant, those specified in Section XI.C.

Provisional Certification Date – The term “Provisional Certification Date” means the date on which a Program Participant’s software receives Provisional Certification pursuant to Section XI.

Reference Notice – The term “Reference Notice” means information that is easy to locate (*e.g.*, via an easily accessible scroll box or a prominent and clearly labeled link) and easy to read and comprehend. Examples of Reference Notices include Privacy Statements and End User License Agreements (EULAs).

Registered Program Advertiser – The term “Registered Program Advertiser” means a company that has registered with TRUSTe pursuant to Section XV.

Third-Party Personally Identifiable Information – The term “Third-Party Personally Identifiable Information” (or “Third-Party PII”) means Personally Identifiable Information that is collected by a Program Participant from a User other than the User to whom it pertains or whom it identifies. For the purposes of this definition, the collection of Internet search terms entered by a User is not considered PII.

Trackware - The term “Trackware” means any software that performs Monitoring other than (i) software which has been affirmatively activated by a user (*e.g.*, by clicking onto a program icon or activating software via the Start/Programs Menu) or (ii) software that collects information to facilitate the operation of a program that a user has knowingly used, executed or enabled. (Trackware may include Adware where the Trackware also meets the definition of Adware.)

User – The term “User” means a user of a computer.

III. NOTICE

The Program Requirements adopt a layered-notice approach: Program Participants must disclose, or reasonably ensure disclosure in accordance with Section IX, the most important information as outlined below about their Certified Software (including, in the case of Certified Adware or Certified Trackware, the proposed value proposition), clearly and prominently, outside of the Reference Notice, prior to installation, along with a link to the Reference Notice.

- A. **First Layer – The Primary Notice.** The Primary Notice (which is required when any information described in this Section III.A is required) must appear clearly, prominently and unavoidably, either (i) before consumers can install the Certified Software or (ii) other than in the case of Certified Adware, using Just in Time Notice. This Primary Notice must include the following information:

1. For all Certified Software:

- a. Whether installing the software, alone or as part of a Bundle, will:
 - i. Redirect the consumer's Internet searches;
 - ii. Add a toolbar to the consumer's web browser or modify other functionality of the browser or desktop as determined by TRUSTe;
 - iii. Change the consumer's home page, default search provider or error page handling or otherwise modify browser settings as determined by TRUSTe;
 - iv. Change the consumer's default provider, web proxy or other changes to Internet settings as determined by TRUSTe; or
 - v. Cause material adverse effects on system performance for typical Users as determined by TRUSTe.

2. In addition, for all Certified Adware:

- a. The name of the Program Participant.
- b. The essence of the proposed exchange, including (as applicable):
 - i. The name or brand of the Certified Adware, and if the Certified Adware is Bundled with other software (and if such other software has a separate name or brand), the name or brand of the other software.
 - ii. Whether the Certified Adware will perform Monitoring.
 - iii. That ads will be displayed and a brief indication of the types of ads displayed and when ads will be displayed.

As applicable, disclose that the ads will appear only while Users are using software in which the Certified Adware is integrated, while they are online generally, or at other specified times.

- iv. If applicable, that the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons.
- c. Link to all applicable Reference Notices.

3. In addition, for all Certified Trackware:

- a. The name of the Program Participant.
- b. The essence of the proposed exchange, including (as applicable):
 - i. The name or brand of the Certified Trackware, and if the Certified Trackware is integrated into or bundled with other software (and if such other software has a separate name or brand, the name or brand of such other software.)
 - ii. When the Monitoring will occur. As applicable, disclose that the Monitoring will occur only while Users are using the Certified Trackware, while they are online generally, or at other specified times.
 - iii. Link to all applicable Reference Notices.

B. **Second Layer – The Reference Notice.** The Reference Notice must be available by prominent link from the Primary Notice, when the Primary Notice is required. In addition the Reference Notice must include at least the following elements:

1. For All Certified Software:

- a. All of the information contained in the Primary Notice. It is not necessary to have EULA's and/or Privacy Policies tailored to each means of distribution.
- b. Instructions on how to uninstall the software.

2. In addition, for all Certified Adware:

- a. A description of the types and frequency of the advertisements displayed by the software.
- b. Information (such as a link) on how to access the Program Participant's website and to the Program Participant's customer support mechanism.

- c. If the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons, an explanation of how to manage the operating system to make sure that children are not served with advertisements from Certified Adware installed by adults.
 - d. Disclosure that software should be installed only by Users age 18 and over.
 3. In addition, for all Certified Trackware:
 - a. Information (such as a link) on how to access the Program Participant's website and to the Program Participant's customer support mechanism.
 - b. Disclosure that software should be installed only by Users age 18 and over.

IV. CONSENT TO INSTALL

Program Participants must provide consumers with a means to give their consent to install the Program Participant's Certified Software prior to the initiation of any such installation. The consent mechanism must meet the following standards:

- A. For all Certified Software:
 1. Users must be given a means to indicate their consent to install the software after receiving any applicable Primary Notice.
 2. The language used to describe Users' options to consent to install software must be plain and direct.
 3. Installation of software shall not proceed if a User declines consent to install the software or closes the dialog box containing the consent option.
 4. Users may only be asked once in any installation process to reconsider their decision not to install software or to close the dialog box with the consent option.
- B. In addition, for all Certified Adware and Certified Trackware:
 1. Users must be given a means to indicate their consent to install the software after receiving any applicable Primary Notice, and the option to consent may not be the Default Option.
 2. If an option to decline consent to install Certified Adware or Certified Trackware is given, it must be of equal prominence to the option to consent to the installation of Certified Adware or Certified Trackware.

3. In a browser window, if no option to decline consent to install Certified Adware or Certified Trackware is given, the User must be provided with a clearly marked option to close the browser window containing the consent option. Closing the browser window must result in the same action as if a User were to decline consent.

V. NOTICE & CHOICE REQUIREMENTS FOR PII AND NON-PERSONAL INFORMATION

- A. **Primary Notice.** If PII or Non-Personal Information is Monitored through the software, the following information must be provided in an Primary Notice:
 1. For all Certified Software:
 - a. Either (i) a link to the Reference Notice, or (ii) instructions on where the user can find the Reference Notice must be provided, alerting User to the availability of information and choices available to them regarding their data.
 2. In addition, for all Certified Adware or Certified Trackware:
 - a. The uses of PII by the Program Participant and the types of companies to whom the Program Participant will transfer PII.
- B. **Second Layer – The Reference Notice.** If PII or Non-Personal Information is collected through the software, the Reference Notice must be available by prominent link from the Primary Notice. The Reference Notice must include at least the following elements:
 1. For All Certified Software:
 - a. Whether the software collects PII, and if so, the following additional disclosures:
 - i. What PII is being collected
 - ii. The identity of the entity collecting such information
 - iii. How such information will be used
 - iv. With whom the information is shared, if at all
 - v. The scope of use or disclosure considered related to the primary purpose for which the data was collected.
 - vi. How and when the User may exercise choice, as required in section V.C., below.

- vii. Whether User's PII will be supplemented with information from other sources.
 - viii. A general statement describing data security practices as well as User access rights.
2. In addition, for all Certified Adware or Certified Trackware:
- a. Whether the software collects Non-Personal Information, and if so, the following additional disclosures:
 - i. The types of Non-Personal Information collected by the software.
 - ii. The Program Participant's use of Non-Personal Information.
 - iii. Whether the Program Participant shares Non-Personal Information with Third Parties and if so, whether the Program Participant places any restrictions on its further use or dissemination.
 - b. Additionally, the Reference Notice must contain information, such as a link, on how to access the Program Participant's website and the Program Participant's customer support mechanism.

C. Choice Requirements.

1. For All Certified Software:
- a. The User to whom PII pertains must be offered opt-out choice before PII collected through the software may be used in the following ways:
 - i. Use not related to the primary purpose for which the User provided it. The scope of use deemed related to the primary purpose shall be defined in the Reference Notice and shall be reasonable to consumers.
 - ii. Disclosure or distribution to third parties, other than Agents.
 - iii. Merger of PII with Non-Personal Information collected on a going forward basis (*i.e.*, after the user provides PII) for use in Online Preference Marketing.

(Beta Note: Certified Software Providers may require the collection or use of PII as part of the value proposition of the software, and may decline to provide the software if User opts out from such use.)

- b. The User to whom PII pertains must be provided with notice and provide their affirmative consent prior to the merger of PII with Non-Personal Information previously collected through the software for use in Online Preference Marketing.
- c. Before Third-Party PII collected through the software may be used or disclosed for any purpose other than the primary purpose for which such information was collected, the person to whom such information pertains must provide affirmative consent. [Notwithstanding such restriction, such information (i) may be disclosed pursuant to legal process (e.g., subpoenas, warrants) or (ii) may be used to send a one-time e-mail message to the person to whom the information pertains in order to solicit such opt-in consent.] [**Beta Note:** One example of the behavior this provision is intended to prohibit is the use of Third-Party PII collected through the software (e.g., via an address book) to send unsolicited bulk communications to third parties.]

VI. SPECIAL REQUIREMENTS FOR CERTIFIED ADWARE

Consumers should be able to understand why they receive ads from a Program Participant. Ads displayed by Certified Adware must be branded so that Users understand the name of the Certified Adware, the name of any software that has Bundled with the Certified Adware, and the name of the Program Participant providing the Certified Adware.

- A. **Reaffirmation.** Shortly after the User consents to the installation, Certified Adware must display an informational notice that (i) demonstrates a representative example of the Certified Adware's Covered Advertisements, (ii) provides the User with more information on how the Adware functions, and (iii) provides information on how to uninstall the software. (**Beta Note:** When an Adware provider has more than one format, a representative example must be sufficient to enable a reasonable User to make an informed decision.)
- B. **Branding.** Covered Advertisements displayed by Certified Adware must be branded with the name of the Program Participant and the brand of the Certified Adware (if distinct from the name of the Program Participant).
- C. **Co-Branding.** Covered Advertisements must also contain, on their face, or via prominently labeled link, a list of the programs and, if applicable, a representative list of the content that cause the display of such Covered Advertisements including clear instructions for removal of the Certified Adware. The link itself must be clearly labeled to communicate to Users that (i) the Covered Advertisement was displayed because the User has certain software titles on his computer and, if applicable, access to certain web-based content; and (ii) that the link will take the User to a list of those programs. (**Beta Note:** It is anticipated that this Section VI.C will be amended, in a time period that is reasonable given the technical challenges, to require that Certified Adware make the list of programs referred to in this sub-section displayable within the Covered Advertisement itself and not merely as a link.)

VII. UNINSTALL

Certified Software must provide Users with an easy and intuitive means of uninstallation. In addition, the following uninstall requirements shall also apply.

- A. For all Certified Software:
 1. The name of the Certified Software must be listed in the customary place for user initiated uninstall within the software platform (*e.g.*, an Add/Remove Programs facility in the operating system);
 2. Uninstallation of Certified Software may be conditioned on the uninstallation of other software on a User's computer (for example, uninstallation of Certified Adware may be conditioned on the uninstallation of other software that has bundled with the Certified Adware), provided that the other software meets the uninstall requirements of this section; (**Beta Note:** TRUSTe recognizes that Certified Software may require the User to install other software (*e.g.*, Adobe Acrobat, Flash), and that the other software may legitimately remain on a User's computer after uninstallation of the Certified Software. TRUSTe, in its discretion, will determine whether or not the other software is left behind after uninstallation for a legitimate reason; for example, because the User has installed software program(s) that also require the use of the other software in order to function.)
 3. Once a consumer has uninstalled Certified Software, the Certified Software may not reinstall on a User's computer unless the reinstallation is performed pursuant to the Program Requirements; and
 4. Uninstall instructions for all Certified Software must also be available from a web page operated by TRUSTe.
 5. No PII shall be required in order to uninstall Certified Software unless the PII was previously collected in compliance with the Program, and it is reasonably necessary to authenticate and/or identify the User.
- B. In addition, for all Certified Adware:
 1. Uninstallation instructions for Certified Adware must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:
 - a. By a link from the Covered Advertisements themselves, or from the browser window or frame where such content is provided, or from a conspicuous and recognizable icon;
 - b. In the Reference Notice;

- c. By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and
 - d. On the Program Participant's website.
 - 2. More information, including customer support information for Users' uninstall questions, must be available by link from the Covered Advertisements displayed by the Certified Adware.
- C. In addition, for all Certified Trackware
 - 1. Uninstallation instructions for Certified Trackware must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:
 - a. In the Reference Notice;
 - b. By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and
 - c. On the Program Participant's website.

VIII. SOFTWARE OR POLICY UPDATES

A Program Participant cannot retroactively apply material changes to the Certified Software or to the Privacy Policy or EULA of Certified Software unless it gives Users Primary Notice of the change and an opportunity to uninstall the software prior to applying the change. Changes to installed Certified Software that would transform it into Adware or Trackware must treat such changes as a new installation under these Program requirements.

IX. THIRD-PARTY DISTRIBUTION / AFFILIATE PRACTICES

If Program Participants use Distribution Partners or Affiliates, they must:

- A. Have in place contractual provisions requiring that Distribution Partners and Affiliates abide by these standards. In the context of an Affiliate Distribution Program, the contract between the Program Participant and its Affiliate must further require that contracts between the Affiliate and its sub-contractors bind the sub-contractors to comply with these Program Requirements.
- B. Disclose to TRUSTe or TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the names of Distribution Partners and Affiliates as well as locations where such Distribution Partners and Affiliates provide Certified Software to consumers so that such third-party distribution may be reviewed, tested, and monitored for compliance with these Program Requirements.

- C. Disclose to TRUSTe or TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the modifications that Distribution Partners or Affiliates are permitted to make to Certified Software as well as locations where Distribution Partners and Affiliates provide such modified software to consumers so that such modifications may be monitored for compliance with these Program Requirements.
- D. Engage in demonstrable random monitoring of Distribution Partners and Affiliates within an Affiliate Distribution Program and self report any non-compliance of these Program Requirements involving Certified Software. Failure to report knowledge of non-compliance in a timely manner shall be grounds for a suspension or termination of a Program Participant from the Program and de-certification of all or any of such Program Participant's Certified Software.
- E. If the Program Participant learns that a Distribution Partner or Affiliate has engaged in practices that violate the Program Requirements, the Program Participant must engage in the process specified in Section XI.A.3 to at least one User of each computer that may have received the software by those means.

X. SPECIAL PROTECTIONS FOR CHILDREN

Program Participants with Certified Adware or Certified Trackware must take the following steps:

- A. Prevent the distribution of their Certified Adware or Certified Trackware on Children's Websites, including by prohibiting their Distribution Partners and Affiliates from such distribution.
- B. Engage in commercially reasonable monitoring to determine where advertisements promoting the installation of their Certified Adware or Certified Trackware appear.
- C. Disclose in Reference Notice that their Certified Adware or Certified Trackware should be installed only by Users age 18 and over.
- D. If their Certified Adware delivers pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons, Program Participants must disclose the IP addresses of the server sending such ads to Net Nanny and other similar services, as prescribed by TRUSTe.
- E. Follow the branding steps in Section VI to make sure that each time Users of Certified Adware see a Covered Advertisement, they have an obvious means of understanding why they received the Covered Advertisement and easy-to-find information on how to stop getting Covered Advertisements from the Certified Adware.

XI. PROVISIONAL CERTIFICATION

In certain cases additional transparency may be useful to companies considering partnerships with software providers. In particular, companies may desire transparency into both (i) the recent, though terminated, prior practices of a potential partner that are prohibited under Section XII of this Program; or (ii) efforts of a Program Participant to provide Legacy Users of a Program Participant's Certified Adware or Certified Trackware with the level of notice now required under this Program.

Accordingly, in order to provide such additional transparency, Program Applicants that would otherwise be entitled to Certification for their software shall have their software be eligible only for Provisional Certification in the following circumstances:

- A. Legacy Users of Adware or Trackware. Compliance with the Program Requirements for new installations of Adware or Trackware is just one step in receiving Certification for such Adware or Trackware. The next step is making sure that all Users who previously received such Adware or Trackware from the Program Participant (the "Legacy Users") fully understand the deal they have made and continue to agree to it. To that end, the Program requires a three-step process to achieve full Certification for Adware or Trackware.
 1. Step One: Applicant Status. Potential Program Participants meet the first step, Applicant status, by submitting their software to the Program for review

and by obligating themselves to timely make all changes necessary to comply with the Program both prospectively and retroactively as applied to Legacy Users of their Adware or Trackware.

2. Step Two: Provisional Certification for New Installs and Client Software Upgrades. Once an Applicant has submitted its Adware or Trackware to the Program, the Applicant and its software has been determined by TRUSTe to meet the Program Requirements, and the Applicant has pledged that all new installations of such Adware or Trackware installations meet the Program Requirements, the submitted Adware or Trackware shall receive Provisional Certification (“Provisional Certification Date”). Program Participants with Provisionally Certified Adware or Provisionally Certified Trackware shall be required to do the following:
 - a. Within six months of the Provisional Certification Date, the Program Participant must initiate updating/upgrading the Adware or Trackware programs of their Legacy Users, where possible, recognizing that some distribution contracts may not allow for Program Participants software to be modified to a compliant Adware or Trackware program.
 - b. Immediately undergo a higher degree of monitoring of its Adware or Trackware under the Program.
 - c. Immediately segregate the advertising inventory that is displayed to its Adware Users into two distinct sets: Certified Ad Inventory and Non-Certified Ad Inventory.
 - i. Certified Ad Inventory shall be inventory that is displayed to Users of Adware installed after the Provisional Certification Date (and thus compliant with the Program Requirements) or displayed to Legacy Users of Adware that was installed prior to the Provisional Certification Date but have received the notice and/or given the consent required under Section XI.A.3 below.
 - ii. Non-Certified Ad Inventory shall be inventory that is displayed to Legacy Users of Adware that have not received the notice and/or given the consent required under Section XI.A.3 below.
 - d. Explicitly make available to advertisers the ability to purchase only Certified Ad Inventory described in Section XI.A.2.c above.
 - e. Ensure that no advertisements from Registered Program Advertisers (see Section XV below) appear within Non-Certified Ad Inventory.
3. Step Three: Messaging to Legacy Users. Understanding that the Program represents a new, comprehensive standard, and that some Program

Participants have modified their practices over time, the Program allows for a two-tiered notice and consent regime to Legacy Users.

- a. Program Participants must complete the appropriate form of messaging, as applicable, within nine months of the Provisional Certification Date to achieve full Certified status for their applicable Adware or Trackware.
 - i. Legacy Users Who Received Adware or Trackware Under Substantially Compliant Disclosures — Legacy Users who received Adware or Trackware pursuant to disclosures substantially similar to those in Sections III and V and who consented to the installation must be given a notice describing the material facts about the operation of the software including uninstallation instructions.
 - ii. Legacy Users Who Received Adware or Trackware Under Disclosures Not Substantially Compliant with These Program Requirements — Legacy Users who received Adware or Trackware pursuant to disclosures not substantially similar to those in Sections III and V must be given a notice describing the material facts about the operation of the software and an opportunity to provide consent to continue to have the Adware or Trackware on their systems or to uninstall the Adware or Trackware. The option to provide consent may not be the Default Option. Users who decline consent or who close the dialog box shall be promptly provided with uninstall instructions. If the User subsequently fails to uninstall the software, any ads served to that User must be part of the Program Participant's Non-Certified Ad Inventory.

B. Prior Performance of Prohibited Practices and other Activities that Trigger Provisional Certification.

1. Program Participants that have been found by TRUSTe to have likely directly and recently engaged in practices prohibited under Section XII of this program will have all of their otherwise Certified Software be designated as Provisionally Certified (“Provisional Certification Date”).
2. In TRUSTe's discretion, TRUSTe may designate a Program Participant's Certified Software as Provisionally Certified if other substantial risk factors calling into question the credibility of the Program Participant are present, after providing notice to the Program Participant and a reasonable opportunity to respond.

C. Additional Requirements for Program Participants with Provisionally Certified Software.

1. Program Participants with Provisionally Certified Software may not mention their software's Certification in any manner without including the qualification "Provisional."
 2. Program Participants with Provisionally Certified Software may be subject to additional monitoring or reporting requirements as determined by TRUSTe.
 3. Provisionally Certified Software will be so designated on a webpage maintained by TRUSTe.
 4. Provisionally Certified Software will be so designated on any whitelists served by TRUSTe.
- D. Evaluation Requirement - Prior to receipt of Provisional Certification, Program Participants and Program Applicants that are eligible for Provisional Certification must submit to an independent evaluation of their compliance with the Program, including Section XI.A.3, if applicable. The evaluations are to be performed by a firm chosen by the Program Participant from a list of pre-selected evaluators deemed suitable by TRUSTe during normal business hours and at a time mutually agreed to by the Program Participant and the evaluator. The results of the evaluation shall be confidential, provided that the top-level results of all audits shall be provided to TRUSTe upon completion of the evaluation.
- E. Eligibility for Full Certification. Program Participants with Provisionally Certified Software will be eligible for full Certification of their compliant software upon the last to occur of the following:
1. Six months following the Provisional Certification Date;
 2. The provision of top-level evaluation results to TRUSTe that demonstrate compliance with the Program; and
 3. Satisfaction of the requirements described in Section XI.A.3, if applicable.

XII. PROHIBITED ACTIVITIES

(Beta Note: It is anticipated that additional Prohibited Activities may be added to this list over time.)

All Program Participants must pledge that they will not, and will take steps in accordance with Section IX to ensure that their Distribution Partners or Affiliates do not, do the following:

- A. Take control of a consumer's computer by deceptively:
1. using the computer to send unsolicited information or material from the computer to others;
 2. accessing, hijacking or otherwise using the computer's modem or Internet connection or service and thereby causing damage to the computer or causing the owner or authorized User, or a third party defrauded by such

- conduct, to incur charges or other costs for a service that is not authorized by the owner or User;
 - 3. using the computer as part of an activity performed by a group of computers that causes damage to another computer;
 - 4. delivering Covered Advertisements that a User cannot close without turning off the computer or closing all other sessions of the Internet browser for the computer; or
 - 5. using rootkits or other software that are typically used to hack into a computer and gain administrative-level access for unauthorized use of a computer.
- B. Modify security or other settings of the computer that protect information about the owner or authorized User for the purposes of causing damage or harm to the computer or the owner or User.
- C. Collect PII through the use of a keystroke logging function without authority of the owner of the computer.
- D. Induce the User to provide PII to another person by intentionally misrepresenting the identity of the person seeking the information. This includes inducing the disclosure of information by means of a web page or application that:
- 1. is substantially similar to a web page or application established or provided by another person; and
 - 2. misleads the User that such web page or application is provided by such other person.
- E. Induce the User to install software onto the computer or prevent reasonable efforts to block the installation or execution of or to disable software, by:
- 1. presenting the User with an option to decline installation but, when the option is selected by the User or when the User reasonably attempts to decline the installation, the installation nevertheless proceeds;
 - 2. misrepresenting that software will be uninstalled or disabled by an User's action, with knowledge that the software will not be so uninstalled or disabled;
 - 3. causing software that the User has properly removed or disabled to automatically reinstall or reactivate on the computer;
 - 4. changing or concealing the name, location or other designation information of the software for the purpose of preventing a User from locating the software to remove it;

5. using randomized or intentionally deceptive file names, directory folders, formats or registry entries for the purpose of avoiding detection and removal by a User;
 6. causing the installation of software in a particular computer directory or computer memory for the purpose of evading a User's attempt to remove the software;
 7. requiring completion of a survey to uninstall software;
 8. requiring, without the authority of the owner of the computer, that a User obtain a special code or download a third-party program to uninstall the software; or
 9. intentionally causing damage to or removing any vital component of the operating system when uninstallation is attempted.
- F. Misrepresent that installing software or providing log-in and password information is necessary for security or privacy reasons, or that installing software is necessary to open, view or play a particular type of content online or offline (*e.g.*, can't falsely state software is necessary for accessing web site).
- G. Induce the User to install, download or execute software by misrepresenting the identity or authority of the person or entity providing the software to the User. This includes, but is not limited to use of domains with misspelling of frequently visited web sites (*i.e.*, 404 squatting).
- H. Remove, disable, or render inoperative by deceptive means a security, anti-spyware or anti-virus technology installed on the computer without obtaining prior consent from the User.
- I. Install or execute software on the computer with the intent of causing a person to use the software in a way that violates any other provision of this section.
- J. Allow any of their Certified Applications to be Bundled with an application currently engaging in any of the Prohibited Activities listed in this section.

XIII. SCOPE OF CERTIFICATION

Material changes to the Application will trigger a recertification requirement.

XIV. DISPUTE RESOLUTION/ONGOING MONITORING/ WHITELIST/ TERMINATION

(Beta Note: It is anticipated that the Program shall include a dispute resolution program for Program Participants. TRUSTe shall operate a consumer-facing website that accepts inquiries and complaints from Users. TRUSTe or its designee shall refer all inquiries and complaints from Users to the relevant Program Participant for the Program Participant's response within a time to be specified by TRUSTe or its designee. Inquiries and complaints will also, in appropriate circumstances, trigger additional monitoring of the Program Participant's software.)

TRUSTe will maintain a whitelist of all Certified and Provisionally Certified software, and the associated Program Participants.

Where a Program Participant or its software fails to comply with one or more Program Requirements, TRUSTe shall have available to it various forms of recourse, including imposing probation, suspension, and/or termination of the application or Participant from the Program. While Certification in the Program is application-specific, probation, suspension and termination may, in TRUSTe's discretion, be either software-specific or company-wide.

TRUSTe may, in its discretion, based on credible, substantially-supported evidence of a breach of the Program Requirements, impose a status of probation or suspension on a Program Participant or its software. While probationary status will not result in removal from the whitelist, suspension will result in immediate removal.

Upon conclusive evidence of a breach, TRUSTe may, in its discretion, terminate either a Program Participant or its software. Termination will result in immediate removal from the whitelist and notification of any company that has registered with TRUSTe pursuant to Section XIV.

An application or Program Participant may be placed in any one or more of the three categories (probation/suspension/termination) in any order. That is to say, probation could occur either before suspension (*e.g.*, to allow additional investigation) or after suspension (*e.g.*, to allow for heightened monitoring). Also, no status is a prerequisite for another status. That is to say, a Participant could be terminated without undergoing either probation or suspension.

XV. ADVERTISER REGISTRY

[Beta Note: It is anticipated that the Program will include an advertiser registry that will permit companies to register with TRUSTe their commitment to avoid advertising to users of Adware that has not been certified under this Program (including Legacy Users of Program Participants' Adware that have not received the notice and/or given the consent required under Section XI.A.3)].

TRUSTe shall maintain a website for advertisers to enroll as Registered Program Advertisers.

XVI. INFORMATION ABOUT THE PROGRAM SPONSORS

About America Online, Inc.

America Online, Inc. is a wholly owned subsidiary of Time Warner Inc. Based in Dulles, Virginia, America Online is the world's leader in interactive services, Web brands, Internet technologies, and e-commerce services.

About CNET Networks, Inc.

CNET Networks, Inc. (NASDAQ: CNET) is a worldwide media company and creator of content environments for the interactive age. CNET Networks takes pride in being "a different kind of media company," creating richer, deeper interactive experiences by combining the wisdom and passion of users, marketers and its own expert editors. CNET Networks' leading brands -- such as CNET, GameSpot, MP3.com, Webshots, and ZDNet -- focus on the personal technology, entertainment, and business technology categories. The company has a strong presence in the US, Asia and Europe.

About Computer Associates International, Inc.

Computer Associates International, Inc. (NYSE:CA), one of the world's largest management software companies, delivers software and services across operations, security, storage, life cycle and service management to optimize the performance, reliability and efficiency of enterprise IT environments. Founded in 1976, CA is headquartered in Islandia, N.Y., and serves customers in more than 140 countries. For more information, please visit <http://ca.com>

About Verizon Communications, Inc.

Verizon Communications, Inc. (NYSE: VZ), a Dow 30 company, is a leader in delivering broadband and other communication innovations to wireline and wireless customers. Verizon operates America's most reliable wireless network, serving 49.3 million customers nationwide, and one of the nation's premier wireline networks, serving home, business and wholesale customers in 28 states. Based in New York, Verizon has a diverse workforce of nearly 215,000 and generates annual revenues of more than \$71 billion from four business segments: Domestic Telecom, Domestic Wireless, Information Services and International. For more information, visit www.verizon.com.

About Yahoo! Inc.

Yahoo! Inc. is the No. 1 Internet brand globally and the most trafficked Internet destination. Headquartered in Sunnyvale, Calif., Yahoo!'s mission is to provide online products and services essential to consumers' lives and offer a full range of marketing solutions to enable businesses to connect with Yahoo!'s hundreds of millions of users worldwide. For more information about Yahoo!, visit www.yahoo.com.