

Fran Maier

Executive Director and President

Fran Maier is the Executive Director and President of TRUSTe, the leading brand in online privacy. Fran brings 15+ years of experience building consumer brands and enhancing consumer trust. She is known for her expertise in online privacy, online marketing best practices, and marketing to women. As a co-founder of Match.com she established credibility, safety and trust in online dating, making Match.com the favorite dating site for single women. In executive marketing roles at Women.com and Kmart's BlueLight.com subsidiary Fran has both established new start-up online brands and brought blue-chip offline brands onto the Internet.

Since Fran joined TRUSTe in 2001, the independent, non-profit has evolved to expand consumer choice from Web sites to downloadable software. TRUSTe's latest network reputation service is the Trusted Download Program, which promotes ethical behavior by adware and other software companies by publishing a "whitelist" of certified applications. It is the first adware standards program backed by industry leaders Yahoo! Search Marketing, CNET's Download.com, CA, AOL, and Verizon.

During that time TRUSTe has strengthened its monitoring and dispute resolution platforms while growing in influence and certifying more than 2,000 websites. Fran speaks widely on the issues of privacy, security, and trust, has appeared before the Federal Trade Commission and the US Department of Commerce, and has testified before the United States House of Representative's Subcommittee on Commerce, Trade, and Consumer Protection.

Fran holds a BA and MBA from Stanford University. She lives in Alameda, CA with her husband and two sons.

**SUMMARY OF TESTIMONY OF FRAN MAIER
EXECUTIVE DIRECTOR AND PRESIDENT OF TRUSTe
ON H.R. 964 (THE SPY ACT)
MARCH 15, 2007**

TRUSTe is an independent, nonprofit organization with the mission of advancing privacy and trust for a networked world. TRUSTe welcomes this opportunity to share our thoughts on H.R. 964, and to make the Committee aware of our efforts, together with our partners in the Trusted Download Program - AOL, CNET Networks, Computer Associates, Microsoft, Verizon, and Yahoo!, and with input from the Center for Democracy and Technology, to serve as the model for industry best practices in downloadable consumer software. The program that we have developed is an excellent example of what industry can accomplish to address consumer protection issues such as those posed by intrusive software downloaded without knowledge or consent of the consumer. It focuses on all consumer software, including advertising and tracking software that may be downloaded to consumers' computers, and certifies software applications around Program Requirements which set the industry standard for consumer downloadable software. On February 16, 2007, we announced the first group of certified software applications on the Trusted Download Program whitelist.

We are very supportive of a federal law to provide baseline protections for consumers from spyware, because such a law, coupled with private sector initiatives to encourage and maintain best practices for downloadable software, will provide tangible relief for Internet users who are currently plagued by problems associated with spyware and unwanted consumer advertising and tracking software. We applaud section 2 of the bill which outlaws certain egregious activities which should never be employed. We are pleased to note that both section 2 and section 3 of the bill, including the notice and consent and uninstallation requirements, are similar to the requirements contained in the Trusted Download Certification Beta Program Requirements, which are attached to this testimony.

The effectiveness of H.R. 964 would be strengthened by the inclusion of a safe harbor for industry self-regulatory compliance programs such as the Trusted Download Program. The law must provide a floor of protection, not a ceiling. Specifically, we recommend that the bill include a safe harbor provision modeled on the provision contained in the Children's Online Privacy Protection Act. As the Federal Trade Commission noted in its February 2007 report to Congress, the industry safe harbors approved under COPPA, including TRUSTe's COPPA Safe Harbor Seal Program, have been a success, benefiting consumers and businesses, as well as aiding the Commission in its enforcement efforts. We believe that H.R. 964 would be strengthened even further by including participation in self regulatory programs as a factor that a court must consider in determining penalties under section 4 of the bill.

**PREPARED STATEMENT OF FRAN MAIER
EXECUTIVE DIRECTOR AND PRESIDENT OF TRUSTe
before the
SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION
ENERGY AND COMMERCE COMMITTEE
U. S. HOUSE OF REPRESENTATIVES
on
H.R. 964 (THE SPY ACT) AND SELF-REGULATION FOR
BEST PRACTICES IN CONSUMER SOFTWARE**

MARCH 15, 2007

Chairman Rush, Ranking Member Stearns, and members of the Subcommittee, I am Fran Maier, Executive Director and President of TRUSTe. We are an independent, nonprofit organization with the mission of advancing privacy and trust for a networked world. Through long-term supportive relationships with our licensees, extensive interactions with consumers in our Watchdog Dispute Resolution program, and with the support and guidance of many established companies and industry experts, TRUSTe has earned a reputation as the leader in promoting privacy policy disclosures, informed user consent, and consumer education. I know that many of you are very familiar with our programs, and I am pleased that you have asked me to inform the Committee about private-sector initiatives in downloadable consumer software that have taken place since the Committee last considered the legislation that is now H.R. 964 (The Spy Act). I thank you for the opportunity to tell you about TRUSTe's Trusted Download Program, and to provide our insights on the bill.

H.R. 964 (The Spy Act)

TRUSTe applauds the Committee's work on the proposed legislation to date. We have long articulated a public policy for privacy protection that incorporates the strength of government oversight, the discipline of industry self-governance, and the innovation of privacy-enhancing technology. We are very supportive of a federal law to provide baseline protections for consumers from spyware because such a law, coupled with private sector initiatives to encourage and maintain best practices for downloadable software, will provide tangible relief for Internet users who are currently plagued by problems associated with spyware and unwanted consumer advertising and tracking software.

We applaud section 2 of the bill which outlaws certain egregious activities which should never be employed. We are pleased to note that section 3 of the bill, including the notice and consent and uninstallation requirements are similar to the requirements contained in the TRUSTe Trusted Download Certification Beta Program Requirements, which are attached to this testimony. This should not be a surprise since we used the past work of this Committee in H.R. 29 in the 108th Congress and H.R. 2929 in the 109th Congress as a starting point for the development of our program. From that starting point, we developed additional requirements which I will describe in more detail later in this testimony.

Based on our in-depth work in the consumer software field, we suggest that the effectiveness of H.R. 964 would be strengthened by the inclusion of a safe harbor for industry self-regulatory compliance programs. The primary challenge in legislating online consumer protection practices is ensuring that businesses view the law as a baseline of acceptable practices. The law must provide a floor of protection, not a ceiling.

Legislative safe harbors encourage a flexible self-regulatory regime that, if adhered to, will place a company in compliance with the regulation and create incentives for participation in programs that may exceed protections required by the law. Self-regulatory programs serve as an important first line of defense, responding quickly to consumer complaints, providing ongoing enforcement, and sending the industry a strong message about appropriate practices. They can also adapt to new technologies and business models to continue to protect consumers in light of the ever-changing landscape of on-line threats. Self-regulation elevates good industry actors by certifying them to best practices, and frees government to pick up where voluntary self-governing bodies leave off. Government can focus on bad actors that are not likely to adhere to self-regulation.

Given the global and dynamic nature of the Internet, and the data-gathering technologies that this legislation seeks to address, neither self-regulation nor government oversight can succeed alone. No government agency has the resources to effectively police the Internet without the active support of strong, effective self-governing bodies. Drawing on self-regulation and government oversight together through the framework of a safe harbor, an extremely effective means of both protecting consumers and enhancing e-commerce can be established.

We suggest that such a safe harbor provision be modeled on the provision contained in the Children's Online Privacy Protection Act (COPPA), 15 USC Chapter 9, sec. 1304. COPPA includes a provision enabling industry groups or others to submit for Federal Trade Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. It requires the Commission to act on a request for "safe harbor" treatment, within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment. Section 312.10 of the Children's Online Privacy Protection Rule sets out the criteria

for approval of guidelines and the materials that must be submitted as part of a safe harbor application. As the Federal Trade Commission noted in its February 2007 report to Congress on COPPA implementation, the industry safe harbors approved under COPPA, including TRUSTe's COPPA Safe Harbor Seal Program, have been a success, benefiting consumers and businesses, as well as aiding the Commission in its enforcement efforts.¹

In addition, we suggest that incentives for participation in industry self-regulatory programs be created by including such participation as a factor that the court shall consider in determining penalties under section 4 of the bill.

The Trusted Download Program Beta

The Trusted Download Program ("the Program"), which we developed with our partners - AOL, CNET Networks, Computer Associates, Microsoft, Verizon, and Yahoo!, and with input from the Center for Democracy and Technology, is the result of more than eighteen months spent in understanding the consumer software marketplace and developing rigorous yet workable certification criteria for consumer downloadable applications. The Program focuses on all consumer software, including advertising and tracking software that may be downloaded to consumers' computers.² The Program certifies software applications around Program Requirements which set the industry standard for consumer downloadable software.³ We are proud to have announced the first group of certified software applications on the Trusted Download Program whitelist on February 16, 2007.⁴ Further we are continuing to consult with

¹ Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress* (February 2007) at 22-24.

² The Program does not cover software that is downloaded exclusively to handheld devices, such as cell phones.

³ The Program Requirements are available as Schedule A to the Trusted Download Beta Certification Agreement (http://truste.org/pdf/Trusted_Download_Beta_Certification_Agreement.pdf).

⁴ The White List is available at http://www.truste.org/pvr.php?page=td_licensees.

industry experts, Program participants, advocacy groups and others, to refine our certification processes, standards, testing protocols and business model.

We developed the Trusted Download Program to address a serious problem: the downloading and installation of consumer software without notice or consent. Consumers are understandably frustrated when they discover unexpected software on their computers. In some instances the software application provides real value; in many instances, however, the software may be considered “spyware.” A lack of standards and definitions has made it difficult for consumers and businesses alike to distinguish between consumer software programs that utilize intrusive practices that are harmful to consumers, on the one hand, and legitimate software programs that advertise or use information for consumer benefit, on the other. As a result, the promise of easy-to-use and valuable consumer downloadable software has been severely hindered by a lack of trust.

Having recognized the problem and the need for industry action to identify a solution, TRUSTe, together with our partners, worked to build a marketplace for legitimate consumer software by achieving the following objectives:

- To significantly improve the consumer experience with downloadable applications
- To establish the first industry-wide standards for developers of downloadable applications
- To identify and elevate trustworthy applications for distributors and marketers
- To protect the valued brands of online advertisers by enabling them to know which applications are trustworthy and which are not
- Through partners, and potentially through a seal, consumers will also be able to recognize and reward trusted downloads

The Trusted Download Program meets these objectives with a combination of strict standards, thorough review by TRUSTe and by independent, third-party software testing laboratory, ongoing monitoring and enforcement by TRUSTe, and powerful market incentives.

Now I'd like to take a few moments to describe key provisions of the Program Requirements. As I mentioned earlier, many are consistent with H.R. 964; several go beyond the bill's requirements. I would like to make clear that we are not suggesting that the Committee adopt our more restrictive policies, but rather respectfully suggest that it is appropriate for Congress to create incentives for participation in self-regulatory programs that go beyond legal baseline requirements.

The Program Requirements are tiered, to take into account the many variations in software applications; the greater the potential for intrusiveness and harm to consumers, the stricter the standard for certification.

Notice

The Program imposes a layered approach that includes both a "primary notice" when an application is offered, and an easily accessible "reference notice" such as an End User License Agreement (EULA) or a privacy statement. The primary notice, which must present the underlying reason the software company will profit from the download of the application in clear terms, must be provided before consumers can install software. Further, such notice must explain material functionalities that impact the consumer experience, and the notice must be unavoidable. The reference notice supplements the primary notice with additional detailed information, but is not in itself sufficient for providing notice or obtaining consent. In addition,

all advertisements delivered in Trusted Download-certified advertising software must be labeled to identify the software that delivers them.

Consent

All software applications must offer consumers an opportunity to consent to the software download, after receiving the primary notice and prior to installation. This notice must be in plain language and prominently displayed. Consent for downloading advertising and tracking software, in particular, must be obtained through an affirmative act by the consumer (the consent option cannot be the default), and the option not to download software must be of equal prominence. When software is downloaded in a bundle format, where multiple applications are presented after a single download action, each application must present itself separately to the consumer and obtain separate consent.

Easy Removal

Instructions for uninstalling software must be easy to find and understand. Uninstall mechanisms must be available in places where consumers are accustomed to finding them, for example, in the operating system's Add/Remove Programs function. Uninstallation must effectively remove the application from the consumer's computer and the application must not reinstall itself without obtaining new consent. Uninstallation cannot be contingent upon a consumer's providing personally identifiable information, unless that information is required for account verification.

Pseudonymous Information

In addition to requirements governing the collection and use of “personally identifiable information,” the Program covers the collection and use of “pseudonymous” information, such as IP addresses, machine IDs, or Web page views, that correspond to a profile or account but is not sufficient, either alone or in combination with easily accessible public information, to identify or contact the individual to whom this information pertains. The inclusion of pseudonymous information within the scope of addressable tracking behavior preserves the program’s standards for prior notice and consent for an emerging set of ad serving and tracking applications that track user behavior on the internet and use this information to establish deep profiles or deliver potentially unwanted advertising, all without the collection of personally identifiable information.

Affiliate Controls

One flaw in the current advertising software business model has been the inability (or unwillingness) of the software companies to control the distribution of their software through third parties, where there is often a breakdown in consent to install and easy uninstallation of the software. The Program directly addresses this market failure, and builds on the baseline protections that would be established by H.R. 964, by requiring companies that develop and publish advertising software or tracking software to demonstrate control over their affiliate and distribution networks in order to be certified. Applicants in these markets must provide TRUSTe with complete transparency into their distribution practices, including the financial model, contracted intermediaries, and the end affiliates and bundling partners responsible for promoting their software to consumers. The Federal Trade Commission’s recent settlement with Zango,

Inc., imposes a similar requirement, as well as other operational steps that are substantially similar to the Trusted Download Program Requirements.⁵

Prohibited Activities

A software application submitted to the Trusted Download program will not be certified if it, *or any other application owned by the company submitting it*, exhibits behavior that is listed in the Program Requirements as a Prohibited Activity. The list of Prohibited Activities substantially parallels activities prohibited under H.R. 964, and will likely expand in reaction to future developments in the marketplace.

Provisional Certification

The Program requires provisional certification for companies that have engaged in Prohibited Activities in the recent past and for advertising and tracking applications that did not obtain their existing users with proper notice and consent. In order to be fully certified, these companies will be subject to additional oversight, including enhanced monitoring, and a requirement to go back to all consumers who downloaded an uncertified version of their software and obtain their consent for the certified version.

Segregated Advertising Inventory

Advertising software providers whose applications have been certified must maintain segregated advertising inventory, so they can serve advertisements only to consumers whose consent has been obtained in accordance with the Program Requirements.

⁵ The Settlement is available on the Commission's Web site at <http://www.ftc.gov/os/caselist/0523130/0523130agree061103.pdf>

Monitoring

Certified applications will be monitored by TRUSTe, as well as an independent testing laboratory, for ongoing compliance. The monitoring process includes reviews of primary notice, matching of files to ensure the application has not changed, sampling the affiliate network to verify the integrity of the consumer consent path, and numerous other policy and technology reviews. Pro-active monitoring events are triggered at several points throughout the year for every application in the program. A company risks termination from the Program if TRUSTe verifies a violation of the Program Requirements for any one of its certified software applications.

Enforcement

If monitoring uncovers suspected non-compliance, the software in question, and in certain circumstances all of a company's certified applications, will be subjected to an investigation by TRUSTe. TRUSTe will also open an investigation based on credible evidence of any non-compliance provided by consumers, competitors, or other independent observers. Depending upon the severity of the violation, a company may be suspended from the Program (with a notation to that effect in its listing on the whitelist), or its software application may be removed from the Trusted Download whitelist altogether, or a company may be terminated from the Program and the fact of its termination made public. For the most severe violations, referral to the FTC is also an option.

I'd like to return for a moment to the market incentives inherent in the Trusted Download Program that we believe are its greatest strength and its greatest benefit for consumers and for businesses. As I mentioned earlier, the initial whitelist of Trusted Download certified software

applications is now on our Web site. We expect that consumer portals, advertisers, distributors and other businesses will use the whitelist to decide which software applications to use for advertising or to provide services to consumers. We are already seeing the market react. CNET's Download.com, a leading consumer download portal, is recognizing whitelisted companies on its download assessment page, where consumers decide whether or not to proceed with installation. AOL and others are beginning to extend distribution deals to applications on our whitelist. The Program Requirements, which are also publicly available on our Web site, give guidance to developers of downloadable software on how to build reputable applications that address the requirements of the market regarding notice, consent, and removal. The Requirements increase incentives for software designers to develop trusted applications by giving their potential business partners and advertisers transparency into their practices. Not only must application providers ensure that all new installations are performed with robust notice and consent, but when offering advertising they must additionally separate their user-base into two categories; 1) those obtained with certifiable notice and consent practices, and 2) those obtained prior to the implementation of certifiable notice and consent practices. Providing advertisers with the option to choose audiences will drive up the price of the certified portion, thereby providing the market incentive for application providers to obtain certification and to maximize the portion of their database obtained with best practices. Consumers will reap the benefits of certified downloadable applications, in the form of prominent, understandable disclosures, more explicit mechanisms for controlling software on their computers, easier and effective means of uninstalling that software, and more respectful use of their personal information.

The Trusted Download Program is an excellent example of what industry can accomplish to address consumer protection issues such as those posed by intrusive software downloaded without knowledge or consent of the consumer. With the right mix of leadership, expertise in relevant markets, stakeholder involvement, creativity and a commitment to do the right thing, self-regulatory programs can do credit to industry, complement regulatory initiatives, and benefit consumers and businesses alike. We are proud of the collegial effort that led to the Trusted Download Program, and we're excited to watch as the Program takes off and certified consumer software begins to proliferate.

Conclusion

TRUSTe welcomes this opportunity to share our thoughts on H.R. 964, and to make the Committee aware of our efforts, together with our partners in the Trusted Download Program, to serve as the model for industry best practices in downloadable consumer software. We look forward to working with the Committee, as you continue your own efforts to protect consumers and encourage innovation in the twenty-first century electronic marketplace.

About TRUSTe

TRUSTe was founded in 1997 to act as an independent, unbiased trust entity, and we have earned our reputation as the leading builder of trusting relationships between companies and consumers. The TRUSTe privacy program – based on a branded online seal, the TRUSTe "trustmark" – bridges the gap between users' concerns over privacy and Web sites' needs for self-regulated information disclosure standards. In May 2001, the Federal Trade Commission approved TRUSTe's Children's Privacy Seal Program as a safe harbor under the Children's Online Privacy Protection Act. We are proud to have received that designation. Hundreds of

thousands of young children who are active online are protected by our program, which currently includes some of the most popular Web sites, including www.disney.go.com, and www.kids.msn.com. TRUSTe is also certified as a safe harbor program under the Safe Harbor Framework administered by the U.S. Department of Commerce for U.S. companies wishing to receive personal data from countries in the European Union (“EU”). Our EU Safe Harbor Seal Program gives companies assurance that they are in compliance with the Framework and, therefore, with national data protection laws in all EU member states.

In addition to these efforts, TRUSTe is deeply involved in fostering best practices for email. Our permission-based Email Privacy Seal Program, which allows companies who agree to our strict standards to post a TRUSTe “We Don’t Spam” seal on online and offline forms where they collect email addresses, sets the industry standard for best practices consumer email. Finally, we are a California company, and we closely follow developments in California law, to keep our licensees informed about compliance issues. We also work closely with the California Office of Privacy Protection in its ongoing efforts to provide guidance to businesses and consumers on privacy and security issues.

**TRUSTe TRUSTED DOWNLOAD CERTIFICATION PROGRAM –
BETA PROGRAM REQUIREMENTS**

1. DEFINITIONS

(a) Action – means any allegation, investigation, demand, suit, legal proceeding, inquiry, or other legal action, whether formal or informal, initiated by any state or federal governmental authority.

(b) Ad Targeting – The term “Ad Targeting” means the use of Pseudonymous Information to determine User characteristics or preferences for use in ad delivery.

(c) Affiliate – means a person who, for financial consideration, offers the Program Participant’s Certified Software to Users in connection with an Affiliate Distribution Program.

(d) Affiliate, High Control – means an Affiliate that, for financial consideration, under a cost per acquisition (pay per install) model with Participant’s codes on their site, drives web traffic to Participant’s website in order to offer Participant’s Software Unit to Users. This distribution method allows the Participant to retain control of the download and installation process for its Certified Software.

(e) Affiliate, Medium Control – means an Affiliate that (1) offers Participant’s Software Unit to Users for financial consideration, and (2) in which the Participant controls the download and install process for its Software Unit; typically via some means of centralized software distribution from web servers owned or controlled by the Participant. This distribution method allows the Program Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is downloaded as part of the software bundle distributed by the Affiliate.

(f) Affiliate Distribution Program – means a process whereby (1) a Participant provides financial consideration to one or more Affiliates in exchange for the Affiliate(s)’ agreement to offer Certified Software to Users. Typically but not always, as part of the process, at least some Affiliates have the Participant’s authorization to hire or subcontract with others to distribute the Participant’s Covered Advertising Software or Covered Tracking Software to Users.

(g) 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 does not have an independent right to use the relevant User data on its own behalf or in any way other than to perform its obligations on behalf of the principal. Agents include Service Providers meeting these restrictions.

(h) Anonymous Information– The term “Anonymous Information” means information that does not fall within the definition of either Personally Identifiable Information or Pseudonymous Information . “Anonymous information” includes but is not limited to aggregate information.

(i) Applicant – means a company that has submitted Software for Certification to the Program.

(j) 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 12) will be eligible for Certification of any of its software.

(k) Certified Ad Inventory – means the segregated ad inventory that may be displayed only to Users of Covered Advertising Software installed after its Provisional Certification Date or Legacy Users of Covered Advertising Software that was installed prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 11.

(l) Certified Covered Advertising Software – means a Participant's Covered Advertising Software that has been tested and awarded Certification, and is currently certified under this Program.

(m) Certified Software – means a Participant's Software Unit that has been tested and awarded Certification, including Provisional Certification, and is currently certified under this Program. Certified Software includes, but is not limited to, Certified Covered Advertising Software and Certified Covered Tracking Software.

(n) Certified Covered Tracking Software – means a Program Participant's Covered Tracking Software that has been tested and awarded Certification, and is currently certified under this Program.

(o) 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.

(p) Compliance Monitoring – means TRUSTe's monitoring of ongoing compliance with these Program Requirements.

(q) Covered Advertising Software – means software that displays advertisements such that the display of any advertisement is not directly triggered by the User's interaction with the Certified Software, unless such ads are displayed within the context of the application and the use of any other application is not disrupted. TRUSTe may consider other related formats or methods of delivery as part of the scope of the Program. The User's option to disable display of advertising does not exempt software from this definition. Covered Advertising Software is often bundled with other software, such as screensavers, games, weather applications, and other popular User software. Covered Advertising Software may include Covered Tracking Software where the Covered Advertising Software also meets the definition of Covered Tracking Software.

(r) Covered Tracking Software- means any software that collects a User's web browsing or other information entered into a separate application, where a purpose is to transfer such information to a destination off the User's computer that is not controlled by the User. Covered Tracking Software does not include software where the collection and transfer purposes are network integrity or functionality, application integrity, or information security. (Covered Tracking Software may include Covered Advertising Software where the Covered Tracking Software also meets the definition of Covered Advertising Software.)

(s) 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 affirmative consent.

(t) Distribution Bundle, High Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously

to Users by a Distribution Partner, in which the Participant controls the download and install process for its Software, typically by means of centralized software distribution from web servers owned or controlled by the Program Participant. This distribution method allows the Participant to ensure that the correct version of its Software Unit, with all the required disclosures, is consistently downloaded as part of the Distribution Bundle.

(u) Distribution Bundle, Medium Control - means two or more software programs, including Participant's Software Unit and other software, which are offered contemporaneously to Users by a Distribution Partner, in which the Participant does not directly control the download and install process for its Software Unit.

(v) Distribution Partner - means a person that, for financial consideration, distributes Software to Users on behalf of the Program Participant. Typically, but not always, the Distribution Partner includes their own software and/or software from third parties as part of a Distribution Bundle offered to Users.

(w) Effective Date - means the date this Agreement is signed by both parties, or, in the case of a Renewal, the day after the previous license expires, if the requirements for Renewal are satisfied.

(x) EULA - means an End User License Agreement.

(y) Informed Third Party(ies) - means those entities that Participant has designated in writing to TRUSTe to receive Certification status updates, including: failure to obtain Certification, Certification of the Software, placement on the Whitelist, placement on Probation or Suspension status, removal from the Whitelist, and/or termination from the Program.

(z) Just in Time Notice - means notice of a functionality that is added after a User has already consented to install Software but just prior to the execution of that functionality. When this happens, a User is provided with Primary Notice of the new functionality and 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 Covered Advertising Software. (**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.)

(aa) Legacy User - means all Users who have installed a Participant's Covered Advertising Software or Covered Tracking Software before the Provisional Certification Date of such Covered Advertising Software or Covered Tracking Software.

(bb) Market Research - The term "Market Research" means the use of Pseudonymous Information to understand how Users are using their computers and the Internet.

(cc) Material Change(s) - means an adverse change in a user's rights or protections, that would be of importance or consequence to the User, which may include:

- (i) Changes to privacy practices, meaning changes relating to:
 - (1) Practices regarding notice, disclosure, and use of Personally Identifiable Information and/or Third Party Personally Identifiable Information,
 - (2) Practices regarding user choice and consent to how Personally Identifiable Information and/or Third Party Personally Identifiable Information is used and shared, or

- (3) Measures for data security, integrity, or access.
- (ii) Modifications to Certified Software that are relevant to these Program Requirements, including but not limited to:
 - (1) Changes to one or more functionalities that are required to be disclosed per Sections 3, 5, 6, 7, 10 and 11 of these Program Requirements, and/or;
 - (2) Changes to the way any required functionalities are disclosed, including but not limited to changes to wording, font, size and/or order of the disclosures, and/or;
 - (3) Changes to the Software's method or means of storing data remotely.
- (iii) Material update or revision to Certified Software functionality including but not limited to: Substantive additions, reconfigurations and/or changes to Software functionality;
- (iv) Material Changes do not include any changes which solely affect the performance or integrity of the Software Unit, such as increases in speed, reliability, or information security.

(dd) Non-Certified Ad Inventory – means the segregated ad inventory that is displayed to Legacy Users of Covered Advertising Software that have not received the notice and/or given the consent required under Section 11.

(ee) Notice(s) – means the Primary Notice and the Reference Notice, together and individually.

(ff) Online Preference Marketing (or OPM) – means a process whereby data are typically collected over time and across web pages to determine or predict User characteristics or preferences for use in ad delivery on the web. The OPM process can use Pseudonymous Information or a combination of Personally Identifiable Information and Pseudonymous Information. OPM does not refer to the use of data by Participants for Ad Delivery or Reporting.

(gg) 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.

(hh) Primary Notice – means information actually presented to each user in a manner that is clear, prominent and unavoidable and designed to catch the User's attention during the installation process, prior to completion of the Software Unit(s) installation. The Primary Notice must be fully visible to a User without additional action on the part of the User, 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 Users in a way that they will see and understand so that they can make an informed decision about the proposed software value proposition.

(ii) Program – means the TRUSTe Trusted Downloadable Certification Program.

(jj) Participant – means a company that has software that is currently certified or provisionally certified in the Program. A participant must have control over all aspects relevant to Certification of the Certified Software.

(kk) Program Requirements – means the requirements for participation in the Program as specified in this Schedule A, as may be amended from time to time.

(ll) Provisional Certification – means an interim level of Certification of a Participant’s Software Unit, 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 11(c).

(mm) Provisional Certification Date – means the date on which a Participant’s Software Unit receives Provisional Certification pursuant to Section 11.

(nn) Provisionally Certified Software – means Software Unit that has received Provisional Certification.

(oo) Pseudonymous Information – The term “Pseudonymous Information” means information that may correspond to a person, account or profile but is not sufficient, either on its own, or through combination with other easily accessible public information, to identify, contact, or locate the person to whom such information pertains. (Beta Note: Examples include but are not limited to a User’s IP address, machine ID, and the web pages a User views.)

(pp) 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).

(qq) Registered Program Advertiser – means a company that has registered with TRUSTe pursuant to Section 14.

(rr) Service Provider(s) – means a third party that performs or assists in the performance of a function or activity involving the use or disclosure of Personally Identifiable Information or Third Party Personally Identifiable Information.

(ss) Software Disclosures – means the statements made in the Self-Assessment in regard to the software.

(tt) Software Unit – means the Software described in Exhibit 1 that is to be tested and reviewed for Certification by TRUSTe.

(uu) 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.

(vv) TRUSTe Marks – means collectively the registered certification marks and trademarks of TRUSTe.

(ww) User – means an authorized user or owner of a computer on which a Software Unit is downloaded.

(xx) Whitelist – means the list maintained by TRUSTe of all Certified and Provisionally Certified software, and the associated Participants that are currently in the Program.

2. Program Management

(a) Certification. The process of certifying Software for compliance with the Program Requirements shall be as provided for below:

(i) Certification shall apply to an individual Software Unit. Participant shall provide TRUSTe with a description, unique identifier and an archival format for each Software Unit it wishes to certify. Participant shall provide TRUSTe with all documentation, whether in written, electronic, or other appropriate format, reasonably requested by TRUSTe in connection with the Certification process. Such documentation shall include a completed Self-Assessment Form, Attestation Form, and other information about the Software as may be reasonably requested by TRUSTe.

(ii) Once Participant has submitted its application, no Material Change is permitted, without written notice to TRUSTe. Any Material Change may trigger restarting the Certification process at TRUSTe's discretion.

(iii) TRUSTe shall review the Self-Assessment and test the Software Unit for compliance with the Program Requirements. The Software Unit version must remain stable until testing is completed. A Certification decision, and corresponding report or reports summarizing TRUSTe's findings, will be provided to the Participant. If TRUSTe does not certify the Software, Participant shall be permitted 30 days time to remedy the failure and resubmit the Software for Certification, whereupon TRUSTe shall provide a second review and test process, and a second report and Certification decision.

(b) Material Changes. Any Material Change to the Certified Software may trigger the need for recertification of the Software, which may require additional fees as provided for herein. TRUSTe will respond to all requests made by Participants to implement Material Changes within five (5) business days of receipt of notice of the requested Material Change.

(c) Participant Obligations. During the Term hereof, and solely with respect to the Software Units for which it seeks certification, the Participant shall:

(i) Make no Material Change to any features, functions, characteristics, architecture, or coding of the Software, in a manner affecting its compliance with the Program, without 1) notifying TRUSTe in writing or electronically of Participant's intent to do so, and 2) obtaining TRUSTe's written decision as to whether such change triggers a recertification requirement;

(ii) Immediately notify TRUSTe in writing of any Material Change in the Software Unit or in the circumstances or facts that initially served as a basis for Certification, or which are otherwise related to Program compliance;

(iii) Immediately provide notice in writing to TRUSTe of any change in the name of a Software Unit or change in the Participant's name;

(iv) Except to the extent prohibited by law, provide notice to TRUSTe of any private lawsuit or Action against it or the Certified Software by any person, law enforcement, or other governmental entity in any country, related to Participant's activities connected to the Program or to the Program Requirements. Such notice shall be provided within five (5) business days of learning of such private lawsuit or Action;

(v) Cooperate with TRUSTe during TRUSTe's Compliance Monitoring and audit activities; and

(vi) Continually provide updated complaint contact information to TRUSTe.

(d) TRUSTe Obligations. TRUSTe shall within a reasonably prompt period of time:

(i) Test the submitted Software and evaluate the Software and Software Disclosures against the Program Requirements;

(ii) Provide a pass/fail decision, as well as a report, regarding the Software and Software Disclosures, to the Participant;

(iii) Retest and provide a second report, as well as a second pass/fail decision, if necessary; and

(iv) Provide ongoing Compliance Monitoring for Software in the Program, to the extent provided for in these Program Requirements.

(e) Whitelist. TRUSTe may, but is not required to, maintain a list of all current Software and/or Participants that are members of the Program ("Whitelist"). Participant hereby consents to the use of its name and the name of the Certified Software on any Whitelist compiled by TRUSTe during the Term. TRUSTe may also respond to any inquiry regarding whether Participant and/or the Software Unit is a member of the Program.

(f) Dispute Resolution. Participants that are also members of the Truste Web Seal Program must participate in TRUSTe's Watchdog process, as described on the TRUSTe website, to resolve non-frivolous, as defined by TRUSTe, privacy concerns or complaints related to Certified Software raised by Users. If Participant does not respond directly to consumer concerns or complaints in a satisfactory and timely fashion, TRUSTe will act as the liaison between the Participant and the consumer to resolve the issue, including recommending any necessary corrective action. (**Beta Note:** It is anticipated that the Program shall include a dispute resolution program for all Participants, not just those that are Licensees of the TRUSTe Web Seal Program. TRUSTe shall operate a User-facing website that accepts inquiries and complaints from Users. TRUSTe or its designee shall refer all inquiries and complaints from Users to the relevant Participant for the Participant's response within a reasonable time to be specified by TRUSTe or its designee. Inquiries and complaints will also, in appropriate circumstances, trigger additional Compliance Monitoring of the Participant's software.)

(g) Updates to Informed Third Parties. TRUSTe will provide ongoing Certification status updates as necessary to Informed Third Parties, if any.

(h) English Only. All Software for which Participant is seeking Certification hereunder must have all User-facing statements written entirely in the English language. Downloading of the Software must be the same no matter the geographic location of the User.

3. Notice. The Program Requirements adopt a layered-notice approach: Program Participants must disclose, or reasonably ensure disclosure in accordance with Section 3, the most important information as outlined below about their Certified Software (including, in the case of Certified Covered Advertising Software or Certified Covered Tracking Software, the proposed value proposition), clearly and prominently, outside of the Reference Notice, prior to installation, along with a link to the Reference Notice.

(a) The Primary Notice. The Primary Notice (which is required when any functionality described in Section 3(a) is present) must appear clearly, prominently and unavoidably, before Users can install the Certified Software. Primary notice may be presented

using Just in Time Notice, except in the case of Certified Covered Advertising Software. This Primary Notice must include the following information:

- (i) For all Certified Software:
 - (1) Whether installing the software, alone or as part of a bundle, may:
 - A. Redirect the User's Internet searches;
 - B. Add a toolbar to the User's web browser or modify other functionality of the browser or desktop as determined by TRUSTe;
 - C. Change the User's home page, default search provider or error page handling or otherwise modify browser settings as determined by TRUSTe;
 - D. Change the User's default provider, web proxy or other changes to Internet settings as determined by TRUSTe;
or
 - E. Cause known material adverse effects on system performance for typical Users as determined by TRUSTe.
 - (2) A prominent link to all applicable Reference Notices.
- (ii) In addition, for all Certified Covered Advertising Software:
 - (1) The name of the Program Participant.
 - (2) The essence of the proposed exchange, including (as applicable):
 - A. The name or brand of the Certified Covered Advertising Software, and if the Certified Covered Advertising Software is bundled with other software (and if such other software has a separate name or brand), the name or brand of the other software;
 - B. Whether the Certified Covered Advertising Software will perform collection and transfer of information to a computer not under the User's control for the purpose of Ad Targeting and/or Market Research.
 - C. 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 Covered Advertising Software is integrated, while they are online generally, or at other specified times; and
 - D. If applicable, that the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons.
 - (3) A prominent link to all applicable Reference Notices.

- (iii) In addition, for all Certified Covered Tracking Software:
 - (1) The name of the Program Participant.
 - (2) The essence of the proposed exchange, including (as applicable):
 - A. The name or brand of the Certified Covered Tracking Software, and if the Certified Covered Tracking Software 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.);
 - B. When the collection and transfer of information to a computer not under the User's control for the purposes of Ad Targeting and/or Market Research will occur. As applicable, disclose that the collection and transfer of information to a computer not under the User's control will occur only while Users are using the Certified Covered Tracking Software, while they are online generally, or at other specified times; and
 - (3) A prominent link to all applicable Reference Notices.

(b) **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:

- (i) For All Certified Software:
 - (1) All of the information contained in the Primary Notice. It is not necessary to have EULA's and/or Privacy Statements tailored to each means of distribution; and
 - (2) Instructions on how to uninstall the software, as provided for in Section 7.
- (ii) In addition, for all Certified Covered Advertising Software:
 - (1) A description of the types and frequency of the advertisements displayed by the software;
 - (2) Information (such as a link) on how to access the Program Participant's website and customer support mechanism;
 - (3) If the software will display ads with pornographic advertisements or advertisements for online gambling, alcohol, tobacco, firearms or other weapons, an explanation of how Users can manage their computers to make sure that children are not served with advertisements from Certified Covered Advertising Software installed by adults; and
 - (4) If the software will display ads with pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, disclosure that software should be installed only by Users age eighteen (18) and over.
- (iii) In addition, for all Certified Covered Tracking Software:

- (1) Information (such as a link) on how to access the Participant's website and to the Participant's customer support mechanism; and

4. Consent to Install. Participants must provide Users with a means to give their consent to install the Participant's Certified Software prior to the completion of any such installation. The consent mechanism must meet the following standards:

(a) For all Certified Software:

(i) Users must be given a means to indicate their consent to install the Certified Software after receiving all applicable Primary Notices;

(ii) The language used to describe Users' options to consent to install Certified Software must be plain and direct;

(iii) Installation of software shall not proceed if a User declines consent to install the Certified Software or closes the dialog box containing the consent option; and

(iv) 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, unless Users have indicated it is acceptable to ask them later.

(b) In addition, for all Certified Covered Advertising Software and Certified Covered Tracking Software:

(i) 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; and

(ii) The option to decline consent to install Certified Covered Advertising Software or Certified Covered Tracking Software must be of equal prominence to the option to consent to the installation of Certified Covered Advertising Software or Certified Covered Tracking Software.

5. Notice and Choice Requirements for Uses of PII and Pseudonymous Information.

(a) **Primary Notice**. If PII or Pseudonymous Information is collected and transferred to a computer not under the User's control through the Certified Software, the following information must be provided in a Primary Notice:

(i) For all Certified Software: Either (i) a link to the Reference Notice, or (ii) instructions on where the user can find the Reference Notice, alerting Users to the information about choices available to them regarding their data.

(ii) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software: A description of the PII collected or transferred to a computer not under the User's control through the Software Unit, the uses of PII obtained through the Certified Software by Participant, and the types of companies to which Participant will transfer PII.

(Beta Note:With TRUSTe's prior approval, certain information required to be included in the Primary Notice may be moved to a "learn more about this" link, as long as all required disclosures are complete, clear, prominent and unavoidable, in TRUSTe's sole judgment and discretion.)

(b) **The Reference Notice**. If PII or Pseudonymous Information is collected through the Certified Software, the Reference Notice must be available by prominent link from the Primary Notice. The Reference Notice must include at least the following elements:

- (i) For All Certified Software:
 - (1) Whether the software collects PII, and if so, the following additional disclosures:
 - A. What PII is being collected;
 - B. The identity (including name, address and e-mail address)of the entity collecting such information;
 - C. How such information will be used;
 - D. A description of the types of entities with whom the information is shared, if at all;
 - E. The purposes for which data is disclosed to third parties;
 - F. How and when the User may exercise choice, as required in Section 5(c), below;
 - G. Whether Users' PII will be supplemented with information from other sources;
 - H. The User's access rights to correct material inaccuracies in Personally Identifiable Information, such as account or contact information; and
 - I. A general statement describing data security practices (Beta Note: Program Participant must implement reasonable procedures to protect Personally Identifiable Information and/or Third Party Personally Identifiable Information within its control from unauthorized use, alteration, disclosure, distribution, or access. Program Participant shall utilize appropriate, commercially reasonable means, such as encryption, to protect any sensitive information, such as social security numbers, financial account and transaction information, and health information that it collects.)
 - (2) In addition, for all Certified Covered Advertising Software or Certified Covered Tracking Software:
 - A. Whether the Certified Software collects Pseudonymous Information, and if so, the following additional disclosures:
 - I. The types of Pseudonymous Information collected by the Certified Software;
 - II. The Participant's use of Pseudonymous Information;
 - III. Whether the Participant shares Pseudonymous Information with Third Parties and if so, whether the Program Participant places any restrictions on its further use or dissemination; and

IV. Additionally, the Reference Notice must contain information, such as a link, on how to access the Participant's website and the Participant's customer support mechanism.

(c) **Choice Requirements.**

(i) For All Certified Software:

(1) The User to whom PII pertains must be offered an opt-out choice if PII collected through the software may be used in the following ways:

- A. 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 Users;
- B. Disclosure or distribution to third parties, other than Agents; or
- C. Merger of Pseudonymous Information with previously collected PII on a going forward basis (*i.e.*, after the user provides PII) for use in Online Preference Marketing, where such use had not been previously disclosed to and accepted by the User.
- D. 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.

(2) The User to whom PII pertains must be provided with notice and provide his or her affirmative consent prior to the merger of PII with Pseudonymous Information previously collected through the software for use in Online Preference Marketing.

(3) 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.]

6. **Special Requirements for Certified Covered Advertising Software.** Consumers should be able to understand why they receive ads from a Participant. The mechanism displaying Ads in Certified Covered Advertising Software must be branded so that Users understand the name of the Certified Covered Advertising Software, the name of any software that has bundled with the

Certified Covered Advertising Software, and the name of the Participant providing the Certified Covered Advertising Software.

(a) **Reaffirmation.** Shortly after the User consents to the installation, Certified Covered Advertising Software must display an informational notice that (i) demonstrates a representative example of the Certified Covered Advertising Software's advertisements, (ii) provides the User with more information on how the Covered Advertising Software functions, and (iii) provides information on how to uninstall the software, which may be provided via a prominently labeled link. **(Beta Note:** When a Covered Advertising Software provider has more than one format, a representative example must be sufficient to enable a reasonable User to make an informed decision.)

(b) **Branding.** Advertisements displayed by Certified Covered Advertising Software must be branded with, or within close proximity to, the name of the Participant and the brand of the Certified Covered Advertising Software (if distinct from the name of the Participant).

(c) **Co-Branding. The mechanism displaying the** advertisement 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 advertisements including clear instructions for removal of the Certified Covered Advertising Software. The link itself must be clearly labeled to communicate to Users that (i) the 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 6(c) will be amended, in a time period that is reasonable given the technical challenges, to require that Certified Covered Advertising Software make the list of programs referred to in this sub-section displayable within the advertisement itself and not merely as a link.)

7. **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:

(i) 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 Windows operating system);

(ii) Uninstallation of Certified Software must remove the Certified Software from the User's computer. Uninstallation of Certified Software may be conditioned on the uninstallation of other software on a User's computer (for example, uninstallation of Certified Covered Advertising Software may be conditioned on the uninstallation of other software that is bundled with the Certified Covered Advertising Software), 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.);

(iii) Once a User 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, in particular, pursuant to new consent;

(iv) Uninstall instructions for all Certified Software must also be available from the Participant's web page either directly or through a link. **(Beta Note:** TRUSTe

anticipates a future requirement that Certified Software provide a link to the TRUSTe web page where uninstall instructions are posted); and

(v) 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, and only used, to authenticate and/or identify the User.

(b) In addition, for all Certified Covered Advertising Software:

(i) Uninstallation instructions for Certified Covered Advertising Software must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:

- (1) By a link from the advertisements themselves, or from the browser window or frame where such content is provided, or from a conspicuous and recognizable icon;
- (2) In the Reference Notice;
- (3) By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and
- (4) On the Program Participant's website.

(ii) Customer support information for Users' uninstall questions must be available by link from the software mechanism displaying the advertisements.

(c) In addition, for all Certified Covered Tracking Software:

(i) Uninstallation instructions for Certified Covered Tracking Software must be available in multiple places that are easy for Users to find. At a minimum, uninstall instructions must be available:

- (1) In the Reference Notice;
- (2) By link from a listing in the Start/Programs menu (or functionally similar menu in other non-Windows software platforms); and
- (3) On the Participant's website.

8. Software or Notice Updates.

(a) A Participant cannot retroactively apply Material Changes to the Certified Software or to the Privacy Statement or EULA of Certified Software unless it gives Users Primary Notice of the change and an opportunity to uninstall the Certified Software prior to applying the change. Changes to installed Certified Software that would transform it into Covered Advertising Software or Covered Tracking Software must be treated as a new installation under these Program requirements.

9. Third-Party Distribution / Affiliate Practices.

For all Covered Advertising Software or Covered Tracking Software; and certain Certified Software of Participants, as determined by TRUSTe, who distribute Software Units via Distribution Partners; Affiliates, High Control; or Affiliates, Medium Control;

(a) If Participants use Distribution Partners or Affiliates, they must:

(i) Have contractual provisions in place with such Distribution Partners and Affiliates prohibiting them from causing Participant's Certified Software to not comply with these Program Requirements. 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 subcontractors bind the subcontractors to comply with these Program Requirements;

(ii) Disclose to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, the names of Distribution Partners and Affiliates as well as locations (e.g. URLs of affiliates within an Affiliate Distribution Program) where such Distribution Partners and Affiliates provide or drive traffic to Certified Software to consumers so that such third-party distribution and affiliate practices may be reviewed, tested, and monitored for compliance with these Program Requirements;

(iii) Disclose to TRUSTe and, if applicable, 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 Certified Software to Users so that such modifications may be monitored for compliance with these Program Requirements;

(iv) Demonstrate to TRUSTe and, if applicable, TRUSTe's authorized evaluator, subject to an appropriate confidentiality agreement, that Participant has an effective process for evaluating Distribution Partners and Affiliates within an Affiliate Distribution Program;

(v) Evaluate on an ongoing basis Distribution Partners and Affiliates, and report any known material non-compliance with these Program Requirements involving Certified Software. Failure to report any such substantive non-compliance in a timely manner shall be grounds for a suspension or termination of a Participant from the Program and de-certification of all or any of such Program Participant's Certified Software; and

(vi) If the Program Participant learns that a Distribution Partner or Affiliate has engaged in practices that materially violate these Program Requirements, the Program Participant must follow the Program's specified re-opt-in procedures (as specified in Section 11 of these Program Requirements) to re-opt in at least one User of each computer that may have received the Certified Software by those means.

10. Special Protections for Children. Participants with Certified Covered Advertising Software or Certified Covered Tracking Software must take the following steps:

(a) Prevent the distribution of their Certified Covered Advertising Software or Certified Covered Tracking Software on Children's Websites, including by prohibiting their Distribution Partners and Affiliates from such distribution;

(b) Engage in commercially reasonable oversight to determine where advertisements promoting the installation of their Certified Covered Advertising Software or Certified Covered Tracking Software appear;

(c) If their Certified Covered Advertising Software delivers pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, disclose in the Reference Notice that their Certified Covered Advertising Software or Certified Covered Tracking Software should be installed only by Users age 18 and over;

(d) If their Certified Covered Advertising Software delivers pornographic advertisements or advertisements for alcohol, tobacco, firearms or other weapons, Program

Participants must ensure that such ads are branded so that they may be recognized by child protection software filters by either;

(i) including the phrase “for adults 18 years” in text somewhere on the face of the Covered Advertisement, or

(ii) including the phrase “for adults 18 years” in the meta keyword tag for the page containing the Covered Advertisement, or

(iii) including the phrase “for adults 18 years” within the “alt”, “name” or “id” attribute of the image tags within the Covered Advertisement; and

(e) Follow the branding steps in Section 6 to make sure that each time Users of Certified Covered Advertising Software see an advertisement, they have a means of understanding why they received the advertisement and easy-to-find information on how to stop getting advertisements from the Certified Covered Advertising Software.

11. Provisional Certification. In certain cases additional transparency may be useful to companies considering partnerships with Participants. In particular, companies may desire transparency into both (i) the recent, though terminated, prior practices of a potential partner that are prohibited under Section 12 of these Program Requirements; or (ii) the efforts of a Participant to provide Legacy Users of a Participant’s Certified Covered Advertising Software or Certified Covered Tracking Software with the level of notice now required under this Program. In order to provide such additional transparency, Program Applicants that would otherwise be entitled to Certification of their Software shall have their Software be eligible only for Provisional Certification in the following circumstances:

(a) Legacy Users of Covered Advertising Software or Covered Tracking Software. Compliance with the Program Requirements for new installations of Covered Advertising Software or Covered Tracking Software is just one step in receiving Certification for such Covered Advertising Software or Covered Tracking Software. The next step is making sure that all Users who previously received such Covered Advertising Software or Covered Tracking Software from the 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 Covered Advertising Software or Covered Tracking Software.

(i) Step One: Applicant Status. Potential 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 Covered Advertising Software or Covered Tracking Software.

(ii) Step Two: Provisional Certification for New Installs and Client Software Upgrades. Once an Applicant has submitted its Covered Advertising Software or Covered Tracking Software to the Program, the Applicant and its software has been determined by TRUSTe to meet the Program Requirements, and the Applicant has warranted that on an ongoing basis all new installations of such Covered Advertising Software or Covered Tracking Software installations will meet the Program Requirements, the submitted Covered Advertising Software or Covered Tracking Software shall receive Provisional Certification (“Provisional Certification Date”). Participants with Provisionally Certified Software that is Covered Advertising Software or Covered Tracking Software shall be required to do the following:

(1) Within six (6) months of the Provisional Certification Date, the Program Participant must initiate updating/upgrading the Covered Advertising Software or Covered Tracking Software

programs of their Legacy Users, where possible, recognizing that some distribution contracts may not allow for Program Participants software to be modified to become a compliant Covered Advertising Software or Covered Tracking Software program. (**Beta Note:** TRUSTe recognizes that some existing contracts may prohibit the required changes; nevertheless, TRUSTe will not fully certify software that has not been updated/upgraded in accordance with this provision.)

- (2) Immediately undergo a higher degree of Compliance Monitoring of its Covered Advertising Software or Covered Tracking Software under the Program.
- (3) Immediately segregate the advertising inventory that is displayed to its Covered Advertising Software Users into two distinct sets: Certified Ad Inventory and Non-Certified Ad Inventory.
 - A. Certified Ad Inventory shall be inventory that is displayed to Users of Covered Advertising Software installed after the Provisional Certification Date (and thus compliant with these Program Requirements) or displayed to Legacy Users of Covered Advertising Software that was installed prior to the Provisional Certification Date who have received the notice and/or given the consent required under Section 11(a)(iii) below.
 - B. Non-Certified Ad Inventory shall be inventory that is displayed to Legacy Users of Covered Advertising Software that who not received the notice and/or given the consent required under Section 11(a)(iii) below.
- (4) Explicitly make available to advertisers the ability to purchase only Certified Ad Inventory described in Section 11(a)(ii)(3) above.
- (5) Ensure that no advertisements from Registered Program Advertisers (see Section 14 below) appear within Non-Certified Ad Inventory.

(iii) Step Three: Messaging to Legacy Users. Understanding that the Program represents a new, comprehensive standard, and that some Participants have modified their practices over time, the Program allows for a two-tiered notice and consent regime to Legacy Users.

- (1) Participants must complete the appropriate form of messaging, as applicable, within nine (9) months of the Provisional Certification Date to achieve full Certified status for their Provisionally Certified Covered Advertising Software or Covered Tracking Software.
 - A. Legacy Users Who Received Covered Advertising Software or Covered Tracking Software Under Substantially Compliant Disclosures. Legacy Users who received Covered Advertising Software or Covered

Tracking Software pursuant to disclosures substantially similar to those in Sections 3 and 5 and who consented to the installation must be given a notice describing the material facts about the operation of the software including uninstallation instructions.

B. Legacy Users Who Received Covered Advertising Software or Covered Tracking Software Under Disclosures Not Substantially Compliant with These Program Requirements - Legacy Users who received Covered Advertising Software or Covered Tracking Software pursuant to disclosures not substantially similar to those in Sections 3 and 5 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 Covered Advertising Software or Covered Tracking Software on their systems or to uninstall the Covered Advertising Software or Covered Tracking Software. 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.

(2) After the full program launch Covered Advertising Software and Covered Tracking Software can no longer serve ads to those Users who have not re-opted in per the Program Requirements.

(b) Other Activities that Trigger Provisional Certification. In TRUSTe's discretion, TRUSTe may designate a Participant's Certified Software as Provisionally Certified if other substantial risk factors calling into question the credibility of the Participant are present, after providing notice to the Participant and a reasonable opportunity to respond.

(c) Additional Requirements for Program Participants with Provisionally Certified Software.

(i) Notwithstanding any written consent obtained pursuant to Section 2(a) of the Agreement, Program Participants with Provisionally Certified Software may not mention their software's Certification in any manner without including the qualification "Provisional."

(ii) Participants with Provisionally Certified Software may be subject to additional Compliance Monitoring or reporting requirements as determined by TRUSTe.

(iii) Provisionally Certified Software will be so designated on a webpage maintained by TRUSTe.

(iv) Provisionally Certified Software will be so designated on any Whitelists maintained by TRUSTe.

(d) Evaluator Requirement - Participants and Program Applicants that meet the following criteria may be required to submit to an evaluation of their compliance with the Program, including Section 11(a)(iii), if applicable.

(i) Evaluation Criteria:

- (1) If Program Applicant asserts that one or more of its Legacy Users were acquired in compliance with Program Requirements as per Section 11(a)(iii)(1)(A), TRUSTe may require that they submit to an evaluation of the methods and procedures used in making that determination.
- (2) If Program Applicant or Participant currently distributes their Covered Advertising Software or Covered Tracking Software with one or more Medium Control Affiliates, TRUSTe may require that the Program Applicant or Participant submit to an evaluation of the business practices for each of the Program Applicant's or Participant's Affiliates and all Distribution Partners as they reasonably pertain to these Program Requirements.
- (3) If Program Applicant or Participant currently is, or within the past six months was, under investigation by Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an evaluation of all business practices that reasonably pertain to these Program Requirements.
- (4) If Program Applicant or Participant is, or becomes, within six month of application to the Program, the subject of a publicly filed proceeding and/or settlement by the Federal Trade Commission, State Attorneys General, or similar body, TRUSTe may require that Program Applicant or Participant submit to an evaluation of all of its business practices that reasonably pertain to these Program Requirements.

(ii) Evaluation Scope

- (1) The evaluations are to be performed by, in TRUSTe's discretion, either TRUSTe or a firm chosen by the Program Participant from a list of pre-selected evaluators deemed suitable by TRUSTe, and will occur during normal business hours and at a time mutually agreed to by the Participant and the evaluator.
- (2) The results of the evaluation shall be confidential, provided that the top-level results of all evaluations shall be provided to TRUSTe upon completion.
- (3) In all instances, TRUSTe reserves the right define the scope of the evaluation.

(iii) Eligibility for Full Certification. Participants with Provisionally Certified Software will be eligible for full Certification of their compliant Software Unit(s) upon the last to occur of the following:

- (1) Six (6) 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 11, if applicable.

(iv) Notwithstanding any distribution contract constraints, Participants with Legacy Users must re-opt in such Legacy Users within one (1) year.

12. Prohibited Activities. All Participants shall not, and shall take steps in accordance with Section 9 to ensure that their Distribution Partners or Affiliates do not, do any of the following: (**Beta Note:** It is anticipated that additional Prohibited Activities may be added to this list over time.)

(a) Take control of a User's computer by deceptively:

(i) using the computer to send unsolicited information or material from the computer to others;

(ii) 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;

(iii) using the computer as part of an activity performed by a group of computers that causes damage to another computer;

(iv) delivering advertisements that a User cannot close without turning off the computer or closing all other sessions of the Internet browser for the computer; or

(v) 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 User for the purposes of causing damage or harm to the computer or the 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 Software Unit that:

(i) is substantially similar to a web page or Software Unit established or provided by another person; and

(ii) misleads the User that such web page or Software Unit is provided by such other person.

(e) Induce the User to install the Software onto the computer, or prevent reasonable efforts to block the installation or execution of, or to disable the Software, by:

(i) 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;

(ii) misrepresenting that the Software will be uninstalled or disabled by a User's action, with actual or constructive knowledge that the Software will not be so uninstalled or disabled;

(iii) causing software that the User has properly removed or disabled to automatically reinstall or reactivate on the computer;

(iv) 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;

(v) using randomized or intentionally deceptive file names, directory folders, formats or registry entries for the purpose of avoiding detection and removal by a User;

(vi) 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;

(vii) requiring completion of a survey, or disclosure of PII, to uninstall software;

(viii) 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

(ix) 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 unrelated to the software itself, or that installing software is necessary to open, view or play a particular type of content online or offline (*e.g.*, can not 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 the 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 Software to be bundled with the Software unit currently engaging in any of the Prohibited Activities listed in this section.

13. Scope of Certification. Material Changes to the Certified Software may trigger a recertification requirement.

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