TRUSTe Comments
Federal Trade Commission Spam Summit 2007

Best Practices in Email and Downloadable Software: Setting High Standards, Elevating Good Actors, Protecting Consumers

TRUSTe is pleased to provide the following comments on best practices in email and downloadable software, in connection with the Federal Trade Commission's ("Commission") 2007 conference entitled "Spam Summit: The Next Generation of Threats and Solutions." 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 industry best practices, including privacy policy disclosures, informed user consent, and consumer education.

As the leading certification authority for legitimate senders of commercial email and for providers of legitimate downloadable software, TRUSTe applauds the Commission's ongoing efforts to combat the torrent of spam and harmful, intrusive software that plagues consumers and hinders the efforts of legitimate businesses to build trusting relationships with them. Spam in its current and anticipated forms presents a picture that is certainly troubling, but there is another side of this story. Industry has invested in extensive efforts to address problems associated with spam and unwanted software generally, since the Email Authentication Summit hosted by the Commission and the U.S. Department of Department of Commerce in 2004. Our comments are intended to inform the Commission about industry's work to identify and implement best practices in this area.

Self-regulatory Programs that Work: Building Best Practices

Effective self-regulatory programs don't just happen. Based upon our experience as a leader in building best practices for the online marketplace, we have come to understand that a successful self-regulatory program must include the following key elements:

- In-depth analysis of the relevant market and the problem(s) the program seeks to address;
- Substantive involvement of all relevant stakeholders - businesses, consumer groups, technology experts and others – in identifying program objectives and standards;
- Strict standards that are grounded in actual business practices, together with a compliance and enforcement structure that gives those standards "teeth;"
- Ongoing reevaluation of the standards and compliance structure; and
- Powerful market incentives for participation, such as whitelists, which publicly identify and elevate good actors in the eyes of their key audiences of business partners and consumers, and reward best practices while avoiding false positive issues for companies.

In the pages that follow, we discuss the development of TRUSTe's Email Privacy Seal Program and the Trusted Download Program, as case studies of self-regulatory programs built around these elements. Each program is positioned to provide solutions to a seemingly intractable problem, in manner that rewards good actors and materially benefits consumers.

TRUSTe's Email Privacy Seal Program

When the Commission held its 2003 Spam Forum, spam was still in what could be called its "first phase." Projections based on historic data at the time predicted continued, rapid growth in spam. ISPs were pushing against the tide, with few public successes. A new breed of commercial anti-spam players was also emerging, with a focus on message heuristics and sender reputation. The CAN-SPAM Act1 became effective in January 2004, and the Commission and state attorneys general engaged in intensive enforcement efforts; and over the ensuing years, an interesting thing happened: spam's status as "internet threat of the moment" diminished. Through a combination of successes – commercial solutions impacting volume, ISPs more effectively policing incoming mail, the commitment to best practices by many corporate marketers, the introduction of authentication protocols, and continued law enforcement - many people argued, with good reason, that spam was on the decline. Of course, spam was still a massive drain on resources and a miserable nuisance and danger to consumers, but progress was being made.

In the last 12 months, we've seen a startling reversal of much of the progress that had been made since 2003, as spam enters a new phase. The relative decline of spam as a primary concern was due, in part, to the rise of other, even more invasive threats such as phishing, identity theft, spyware, and other malware – but spam has frequently playing the role of delivery vehicle for these new threats. The rise of image spam, which can cleverly evade virtually all existing commercial anti-spam solutions, the resurgence of botnets, and the proliferation of pump-and-dump stock schemes as the spammer's preferred financial vehicle, have led to an alarming resurgence in the volume of spam. This fact, together with the difficulties in CAN-SPAM compliance that seemingly affect a large portion of commercial

1 The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM"), 15 U.S.C. 7701-7713

entities, indicates that spam, in its old and new forms, is here to stay. Best practices in commercial email have never been more relevant.

TRUSTe recognized early on that the best defense against spam's negative impact on reputable email marketers was a good offense: identifying best practices for email, embodying those practices in program standards, and permitting businesses that agreed to abide by those standards to post a public, consumer-facing seal attesting to their commitment to best practices. After lengthy consultations with industry (including our founding partners ReturnPath and DoubleClick) and consumer advocates, it became clear that, in order to rebuild the consumer trust that spam had eroded, a self-regulatory program built around best practices would have to require affirmative consent for email marketing. In 2005, TRUSTe launched the Email Privacy Seal ("EPS") Program, which sets the industry standard for email based upon consumer consent.

The EPS Program Requirements are strict and objective, and include all of the baseline requirements of the CAN-SPAM Act for legitimate commercial email. EPS Licensees must provide a conspicuous, functioning unsubscribe mechanism in every commercial or promotional email. An unsubscribe request must become effective within 10 days of receipt and must be honored indefinitely, unless a consumer wishes to opt in to additional email marketing. The EPS Program Requirements do not stop there, however. Unlike CAN-SPAM, they require clear and conspicuous notice of how email addresses will be used and whether they will be shared with third parties. Notice must be provided both in a Web site privacy statement and on Web pages where email addresses are collected. Consumers' affirmative consent must be obtained for receiving all commercial or promotional email, including e-newsletters and surveys, and for sharing email addresses and other Personally Identifiable Information ("PII") with third parties. EPS Licensees must also meet detailed accountability standards for their email infrastructure and relationships with third parties. Bounces and other replies must be reliably processed and bounce rates must be very low; outbound email servers

must have valid DNS entries; companies must register with abuse.net, and provide valid information to the Whois Database. If they acquire email addresses from third parties, EPS companies must demonstrate due diligence in ensuring that clear and conspicuous notice was provided, and affirmative consent obtained, for the sharing of those email addresses.2

Companies seeking EPS certification go through a rigorous TRUSTe review of their email practices and must agree to the strict EPS standards. Once certified, companies are required to post the EPS "We Don't Spam" seal on web sites where they collect email addresses. The seal links to a validation page on TRUSTe's web site that summarizes the EPS standards and gives assurance that a company is a verified TRUSTe licensee. EPS licensees are subject to ongoing monitoring of their practices by TRUSTe, including seeding of their proprietary lists, automated spam trap notifications, and automated monitoring of collection page disclosures. Licensees must agree to fully cooperate in TRUSTe's Watchdog Dispute Resolution Process for resolving consumers' complaints about the use of their email addresses. EPS licensees may be terminated by TRUSTe for violations of the Program Requirements, and the termination made public on TRUSTe's Web site. TRUSTe may take further action, including referral of a terminated EPS licensee to the Commission, where circumstances warrant.

TRUSTe's Email Privacy Seal Program provides a powerful incentive for participation: it elevates reputable email marketers by making it easy for consumers to identify them. Consumers benefit by having clear notice of a company's email practices at the time they matter most – when a consumer is considering providing her email address to a web site. The EPS seal provides reassurance that a third-party has authority to oversee a web site's email practices and that consumers have recourse to a fair, independent means of resolving privacy

2 The EPS Program Requirements are available on the TRUSTe Web site at http://truste.org/pdf/EPS_Program_Amendment_1.0.pdf . A summary of the Program Requirements is also available, at http://www.truste.org/requirements.php#req4.

and spam-related complaints. The marketplace benefits from improved email practices and from more and better disclosures about those practices.

The Trusted Download Beta Program

In addition to building best practices for email, TRUSTe has been a leading proponent of addressing the issues posed by the downloading and installation of consumer software without notice or consent. As noted earlier, a fairly recent development is the delivery of such software through spam. 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 - AOL, CNET Networks, Computer Associates, Microsoft, Verizon, and Yahoo!, and with input from the Center for Democracy and Technology - worked for more than eighteen months to understand the consumer software marketplace and to develop rigorous yet workable certification criteria for consumer downloadable applications. Our goal was to build a marketplace for legitimate consumer software by accomplishing the following objectives:

- Significantly improve the consumer experience with downloadable applications by requiring clear and conspicuous notice and affirmative consent before software is loaded
- Establish the first industry-wide standards for developers of downloadable applications
- 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, enable consumers to recognize and reward trusted downloads
- Identify and elevate trustworthy applications for distributors and anti-spyware vendors

The Trusted Download Beta Program is the result of these efforts. It meets our objectives with a combination of strict standards, thorough review by TRUSTe and by an independent, third-party software testing laboratory, ongoing monitoring and enforcement by TRUSTe, and powerful market incentives. The Program focuses on all consumer software, including advertising and tracking software, that may be downloaded to consumers' computers.3 The Program certifies software applications around Program Requirements which set the industry standard for notice, consent, and ease of uninstall.4 We are proud to have announced the first group of certified software applications on the Trusted Download Program Whitelist on February 16, 2007.5 We launched the Program in beta to allow us to continue consultations with industry experts, Program participants, advocacy groups and others, to refine our certification processes, standards, and testing protocols.

The Trusted Download 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. Key Program standards include:

Notice: The Program imposes a layered approach that includes both an unavoidable "primary notice" provided when an application is offered and before consumers can install it, and an easily accessible supplementary "reference notice" such as an End User License Agreement (EULA) or a privacy statement. The underlying reason the software company will profit from the download of the application, and the material functionalities that impact the consumer experience must be disclosed in the "primary notice." In addition, all advertisements delivered in Trusted Download-certified advertising software must be labeled to identify the software that delivers them.

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

4 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**).

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

Consent: All software applications must offer consumers a prominently displayed opportunity to consent to the software download, after receiving the primary notice and prior to installation. 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 corresponds 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 in the Program's scope extends the Program's standards for prior notice and consent to 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 some 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 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.6

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 in proposed legislation currently being considered by the Congress, and includes activities such as surreptitious key-stroke logging, high-jacking consumers' browsers, changing computer settings and other intrusive and damaging behaviors that occur without consumers' knowledge or consent. The list will likely expand in reaction to future developments in the marketplace.

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

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.

Monitoring: Certified applications will be monitored by TRUSTe, as well as by 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 other 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. Severe violations may be referred to the Commission.

The market incentives inherent in the Trusted Download Program are perhaps its greatest strength and its greatest benefit for consumers and for businesses. As noted above, the Program employs a Whitelist of Trusted Download certified software applications, and the initial list is now on our web site.[7] Consumer portals, distributors and other businesses have already begun to 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 favorably. 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

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

proceed with installation. AOL and others have indicated that they will consider whether a company's software is on the Program's Whitelist before extending distribution deals.

The Trusted Download 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 providing 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 also 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, with 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.

Conclusion

TRUSTe's Email Privacy Seal Program and the Trusted Download Program are examples of how much self-regulation can accomplish if it is purposeful, relevant, technologically sophisticated, and driven by industry-enhancing and consumer-protective goals. Each Program is aimed at reputable businesses that want to demonstrate their commitment to best practices and consumer privacy. Outright fraudsters do not join self-regulatory programs, however. For this reason, each Program is intended as a complement to

government enforcement efforts. We look forward to continuing our work with the Commission as it redoubles its efforts to address the twin scourges of spam and malicious downloadable software.

Frances Maier
Executive Director and President
TRUSTe

About TRUSTe

TRUSTe helps consumers and businesses identify trustworthy online organizations through its Web Privacy Seal, Children's Privacy Seal, EU Safe Harbor Seal, Email Privacy Seal and Trusted Download Programs. An independent, nonprofit organization celebrating its 10th anniversary in 2007, TRUSTe certifies more than 2,000 Web sites, including the major internet portals and leading brands such as Microsoft, IBM, Oracle, Nestle, Intuit and eBay. TRUSTe resolves thousands of individual privacy disputes every year. A complete description of all of our programs may be found on our Web site at www.truste.org.

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 also serves 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.

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.