

## **Public Comment – National “Do-Not-Email” Registry Project No. R411008**

TRUSTe is please to have the opportunity to provide comments on the National “Do-Not-Email” Registry required by the Controlling the Assault of Non-Solicited Pronography and Marketing Act of 2003 (CAN-SPAM Act)

### **About TRUSTe**

TRUSTe is an independent, nonprofit organization dedicated to enabling individuals and organizations to establish trusting relationships based on respect for personal identity and information in the evolving networked world. Founded in 1997, TRUSTe runs an award-winning global privacy certification and seal program. Its seal programs are considered Safe Harbors for the Children's Online Privacy Protection Act (COPPA) and the EU Safe Harbor Framework. Today, TRUSTe maintains the largest privacy seal program with more than 1,300 Web sites certified throughout the world including AOL, Microsoft, IBM, Nationwide and The New York Times. TRUSTe's mission extends standards, certification and oversight into legitimate email for IronPort's Bonded Sender Program and wireless with the Wireless Privacy Principles and Implementation Guidelines. For more information on TRUSTe please visit [www.truste.org](http://www.truste.org).

### **Practical Limitations of the Registry**

The goal of the Registry is to decrease the amount of spam in the inbox and give the consumer control of her inbox. The Registry may not be the most efficient, effective and viable means of attaining this goal. The Do-Not-Call list has been effective in decreasing the number of solicitation phone calls, but that doesn't mean that a Do-Not-Email Registry will be. The technology is different from telemarketing, so you need better controls on who has the list and how it is used.

The Registry has a number of limitations and costs that must be weighed against the possible benefits before it could be successful.

- **It will not affect the amount of spam that is already illegal.** From one perspective, the world of spam can be divided into two distinct sections: a) spam that is already illegal, usually sent by unscrupulous individuals that have run afoul of a range of laws, and b) spam that is Can-Spam compliant, often sent from legitimate companies that are effectively bound by the law.

The Registry will not reduce the amount of spam in the first category.

- **It may increase the amount of spam consumers receive, if not set up properly.** Technical hurdles to setting up the list include ensuring spammers cannot game the system so that they gain access to legitimate email addresses and ensuring the security of the system from hackers.
- **Consumers may feel misled.** What can consumers expect to happen once they have signed up for the Do Not Email Registry? Consumers can certainly expect to receive email from friends and family, but additionally, consumers should also expect to receive unsolicited commercial email from:
  - Transactional and relationship messages from businesses they are doing business with
  - Information from businesses and organizations they have opted-in to receive
  - individuals or businesses that are already acting outside of the law.

Key to succeeding will be a clear understanding by the consumer, otherwise the consumer will instantly lose trust in the Registry.

- **It will only affect the 'good actors.'** The burden of compliance, which is sure to require significant investments of time and/or money, will fall on companies that are acting within the law – an unintended 'penalty' for CAN-SPAM compliance.
- **Moves the opt-out requirement of CAN SPAM to an opt-in standard unless the rules are changed.** As drafted today, CAN SPAM makes no distinction between companies with or without a prior business relationship, but rather a distinction between the types of email being sent. Thus, if a company wishes to market to its existing customer base, it would need to either filter its list through the Do-Not-Email Registry or obtain opt-in consent for marketing purposes.

### **Recommendations**

The sentiment of Chairman Muris that consumer's should not sign up to the list because all the spammers will use it to spam you, is a key component of addressing the issue. In order for this registry to work it must maintain the privacy of consumers' email addresses, be viable for legitimate businesses, and be enforceable by the Commission.

Rather than creating an all encompassing Do-Not-Email Registry that has many hurdles to overcome, the Commission could develop a mixture of solutions that depend upon enforcement by the Commission, use of technology by industry, and development of self regulatory programs.

#### *Decrease Illegal Spam*

Before a Do-Not-Email Registry can be effective, the illegal spam needs to be addressed through enforcement at the Commission and technology, such as authentication and reputational services at the industry level.

As noted in the FTC's study on *False Claims in Spam* issued in 2003, over 80% of spam that the FTC receives is either deceptive because of false subject lines, headers, and from lines or is selling illegitimate products. From a consumer standpoint, if the illegal spam is still in her inbox, but the legitimate commercial email is blocked, the problem has not been solved. Resources should continue to be directed at enforcement before testing and building a Do-Not-Email Registry.

#### *Trust Unsubscribe*

While working to decrease the impact of illegal spam, projects must be put in place to put TRUST back into the unsubscribe. This is the second step toward decreasing spam in the inbox and increasing consumer control. This should be done at the industry level through self regulation and at the Commission level through enforcement. The goal should be that 6 months - 12 months from today, the Chairman should be instructing consumers to unsubscribe from unwanted email rather than just deleting it. This will take consumer education, since all have been telling consumers NOT to unsubscribe.

These two steps will go far in decreasing the amount of spam in the inbox and giving consumers better control of the mail they receive.

If after first two steps have been successful and yet there is still a need for a Do-Not-Email Registry, the Commission should review existing self regulatory programs for industry guidelines and best practices to handle the policy issues around the Registry. Existing rules for emailing would need to be modified so that an opt-in standard is not required for marketing to an organization's existing customers. It should also review existing self regulatory Do-Not-Email Registries to identify working models.

The costs of building a system that imposes extensive new requirements on legitimate businesses outweigh the minimal benefit to consumer in the way of decreasing spam.