Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

March 31, 2004

Mr. Donald S. Clark, Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW Room 159-H
Washington, DC 20580

RE: CAN-SPAM Act Rulemaking, Project No. R411008 – Comments on Do Not Email Registry

Dear Mr. Clark:

On behalf of the members of the Software & Information Industry Association (SIIA), we are pleased to offer our comments in response to the request for information by the Federal Trade Commission (FTC) on the practical, technical, security, privacy, enforceability and other concerns, including the relative costs and benefits, which exist regarding the establishment of a Do Not Email Registry.

As the principal trade association of the software code and information content industry, the more than 600 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world as well as many smaller and newer companies.

Background Information

SIIA and its member companies bring a unique perspective to the FTC's request as leading innovators of software and digital content over the Internet and through the leadership role we have played in promoting effective privacy protections for many years. We were one of the earliest industry leaders to recognize the importance of adopting effective privacy policies and privacy enhancing technological tools. Since these early steps, SIIA has, through technical assistance and privacy seminars, worked with hundreds of companies to develop, write, and implement effective, consumer-friendly privacy policies.

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

In the U.S., we actively engage with the FTC on implementation of its Section 5 policies in this area, and in the execution of the legal frameworks of the Children's On-Line Privacy Protection Act (COPPA), Gramm-Leach-Bliley Act (G-L-B Act), and the Health Information Portability and Accountability Act (HIPAA). At the international level, SIIA is working to encourage company participation in the "safe harbor agreement" negotiated between the Department of Commerce and the European Union. SIIA has regularly advised the Organization for Economic Cooperation and Development (OECD) on privacy enhancing technologies.

In addition, SIIA has actively worked with the FTC in implementing its "culture of security" framework, and made effective presentations before the FTC on related issues of software licensing and combating cross-border fraud.

Unique among many industry associations, SIIA supported the FTC's establishment of its "Do Not Call Registry" last year, and lobbied heavily in support of the legislation passed by Congress to get the Registry up and running,[1] and we continue to monitor its impact on our members.

Moreover, we are deeply engaged in the implementation of the CAN-SPAM Act as a major step toward combating unwanted, fraudulent and invasive unsolicited commercial email (UCE), which directly affects our members' own marketing, network and security systems.

Comparisons to the "Do Not Call Registry" are Inappropriate

At the outset, SIIA would like to address the inevitable comparisons to the "Do Not Call Registry." Beyond some minimal organizational experiences, the implementation-to-date of the "Do Not Call Registry" offers little basis for evaluating the complexities of a Registry established to combat UCE. There are a number of reasons for this.

First, and foremost, the "Do Not Call Registry" was established as an integral part of the amended Telemarketing Sales Rule (TSR) and after nearly a decade of experience of implementing of the Telemarketing Sales Act (TSA) by the FTC. This experience included voluntary do not call lists maintained by businesses and advocated by industry trade groups. Despite the best intentions of those that advocate a Do Not Email Registry, this proposal does not fit neatly into the legal requirements, prohibitions, and enforcement tools of the CAN-SPAM Act and cannot rely on any real world experience with using a such a tool for UCE.

---

[1] See **SIIA Letter to House Energy and Commerce Cmte. Chairman Billy Tauzin in Support of a National "Do Not Call" Registry**, January 17, 2003, found at: http://www.siia.net/govt/SIIA_TauzinTSR16Jan2003.pdf. SIIA has not been a party to any of the litigation seeking to enjoin or oppose the Registry.

The amended TSR was crafted to focus on the demonstrated experiences of using telemarketing tools to call *consumers*. Unlike the requirements of the CAN SPAM Act, the amended TSR includes a very broad business-to-business exemption. Moreover, the required (and discretionary) rulemakings by the FTC are in their very preliminary stages and thus there is little, if any basis, for determining whether a Do Not Email Registry could be a cost-effective tool to implement the requirements of the Act and its related regulations. Further complicating the implementation of a UCE list is the fact that the amended TSR required negotiation with only one other agency -- the Federal Communication Commission (FCC) – while the CAN-SPAM Act provides enforcement action by at least 10 other federal independent and executive branch agencies, as well as state attorneys general, which would all have to agree on the requirements and implementation of the Do Not Email Registry.[2]

Second, the numeric-based telephone system bears little if any technical and operational relevance to the Internet domain name address system. The "Do Not Call Registry," and the application of the list by telemarketers to their own systems, was predicated on a standardized numeric telephone exchange system that has been in use in the United States and Canada for well over 50 years. By comparison, the assignment of specific email addresses does not resemble in any way such standardization. This directly relates to the workable design and implementation of any do not email list, since the lack of consistency in emails means that tools developed for the "Do Not Call Registry" would not be directly applicable to emails.

Third, the "Do Not Call Registry" – and in fact, the amended TSR as a whole – is targeted to a specific, limited set of actors. The FTC carefully considered this question in calculating the fees to be charged for the "Do Not Call Registry" and estimated that 3,000 telemarketers or sellers may pay for access to the information in the national registry.[3] In fact, the range of possible "users" of the "Do Not Call Registry," according to the FTC, ranged from fewer than 100 to fewer than 3,000. As will be discussed further below, the number of possible users of a list of email addresses that do not wish to receive UCE is beyond the scope of any reasonable calculation by the FTC. Moreover, the burdens will fall disproportionately on legitimate businesses and the worst actors of all will escape the burdens of the list.

---

[2] See Section 7(b) of the CAN SPAM Act.

[3] See Federal Trade Commission, **Telemarketing Sales Rule User Fees,** Notice of proposed rulemaking; Request for public comment, May 29, 2002, found at:
http://www.ftc.gov/bcp/rulemaking/tsr/tsrrulemaking/tsrfrn020529.pdf

Relative Costs Outweigh the Benefits

Based on our review of all the relevant information available, including the limited comparisons offered by the "Do Not Call Registry," the scope of the "spam problem", the requirements of the CAN-SPAM Act, and the variety of practical issues surrounding use of email addresses as unique identifiers, SIIA believes that the costs of implementing a Do Not Email Registry could well exceed (probably more than double) the costs of the "Do Not Call Registry" while providing little (if any) actual reductions in UCE (over and above the enforcement provisions already found in the CAN-SPAM Act). More seriously, the scheme is very likely to cause confusion among consumers and businesses while draining scarce resources from enforcement of the current law.

SIIA would like to emphasize to the FTC that the effective and timely enforcement of the CAN-SPAM Act, in combination with the use of effective technological measures and operational practices, will do the most to reduce the amount of fraudulent, unwanted and invasive UCE. We appreciate that the FTC has been given these new responsibilities without additional resources to devote to the problem. It is, therefore, essential that the FTC not be distracted from this central mission of implementing the CAN-SPAM Act. Unfortunately, implementation of a Do Not Email Registry would be precisely the distraction that the FTC should not be burdened with while conquering this problem. According to some early estimates, the CAN-SPAM Act is showing reduced levels of UCE and consumer complaints to their Internet Service Providers.[4]

The FTC posed a number of specific questions in its request for comment. The following responds to several of these:

Security. As noted above, we believe that the costs of a Do Not Email Registry will far exceed the costs of the "Do Not Call Registry." In other words, it will simply not be enough to replicate the design of the existing Registry to develop the UCE list. One area, in particular, that will require more operational and technical work is the area of security. Unlike the phone numbers found in the "Do Not Call Registry," the email addresses found in any UCE list will be a treasure trove for malicious and unscrupulous spammers. Professional hackers will know that the emails will be largely accurate since those who sign up will be motivated to provide a "real" address to a sanctioned Do Not Email Registry. The level of technical security, therefore, must be extremely high.

Even if the technical issues could be addressed satisfactorily, the operational issues remain just as problematic. Any registry will have to permit downloading of the entire file of registered emails to a *large* number of potential senders – a number that is certainly several orders of magnitude higher than the narrowly targeted number that use the "Do Not Call Registry." While the "Do Not Call Registry" presented a low level of risk of misuse

[4] AOL Says It Sees Sharp Decline in 'Spam' E-Mail, March 21, 2004, found at: http://www.reuters.com/newsArticle.jhtml;?storyID=4608651.

of the numbers found in the list, the same cannot be said of any Do Not Email Registry. In fact, to avoid any possibility of misuse, the FTC will have to adopt authentication, verification and compliance procedures that it does not currently employ and which will likely require a level demanded of large financial institutions or even defense and national security agencies of the federal government.

UCE will not be stopped. As noted above, the challenges of establishing a "Do Not Call Registry" are miniscule compared to a Do Not Email Registry. A central impracticality is that the UCE list will do nothing to stop the worst offenders. In our view, it will simply be unenforceable. As the FTC has recognized in a variety of forums, a primary impediment to consumer protection and law enforcement agencies has been the identification and location of a targeted spammer.[5] As Director Beales has indicated:

> "Spammers can easily hide their identity, falsify the electronic path of their email messages, or send their messages from anywhere in the world to anyone in the world. Tracking down a targeted spammer typically requires an unusually large commitment of staff time and resources, and rarely can it be known in advance whether the target's operation is large enough or injurious enough to consumers to justify the resource commitment."

Enforcement initiatives taken since the beginning of the year demonstrate this point. As widely reported in the media, the the nation's largest providers of email and Internet access services (America Online Inc., EarthLink Inc., Microsoft Corp. and Yahoo! Inc.) filed suit on March 10th in federal district courts in California, Georgia, Virginia and Washington state under the provisions of the CAN-SPAM Act that prohibit deceptive solicitations, use of open proxies to disguise their point of origin, falsified "from" e-mail addresses (spoofing), absence of a physical address in the e-mail , and absence of an electronic unsubscribe option.[6] The complaints had to rely on suing more than 90 "John Doe" defendants who were beyond the reach of existing means of identification.

By contrast, since the law went into effect January 1, 2004, legitimate businesses have amended their e-mail marketing procedures to comply with the CAN-SPAM Act. In doing so, these businesses are honoring consumers' and businesses' requests to be taken off e-mail distribution lists.

Thus, nothing about a Do Not Email Registry will address the problem of receiving e-mail from the targeted spammers. The Registry will only enhance the limitations placed on legitimate businesses.

---

[5] See, e.g., Testimony of J. Howard Beales, III, Director, Bureau of Consumer Protection, Federal Trade Commission, before the House Committee on Small Business, "Spam and its Effects on Small Business," October 30, 2003, found at: http://www.house.gov/smbiz/hearings/108th/2003/031030/beales.html.

[6] A copy of their joint press release announcing the filings can be found at: http://media.aoltimewarner.com/media/press_view.cfm?release_num=55253838.

Disproportionate impact on legitimate (and small) businesses. The burden of compliance with a Do Not Email Registry will be on the legitimate businesses that are working to comply with the provisions of the CAN SPAM Act. The worst actors will escape the penalties for not complying with the UCE list and will not pay anything to maintain it. In particular, small and medium sized businesses will bear a disproportionate burden, since they will have to invest in tools that allow them to download, compare and manage the entire UCE list. Unlike the telemarketing industry, where many of the call preparations are mechanized based on standardization, no such consistency exists with regard to email lists maintained by businesses which use a variety of formats, databases and internet-based tools to manage and send emails. Note that it will be impossible to segment the UCE list by specific region – as can be done by the "Do Not Call Registry" where five area codes can be downloaded for free. Compliance will depend on access to and manipulation of the entire Do Not Email Registry.

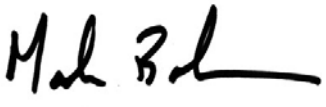
Conclusion

We appreciate that the FTC is required to write a report setting forth a plan and timetable to establishing a nationwide Do Not Email Registry. We note, however, that it is not mandatory that the plan be implemented. We urge the FTC to withhold implementation and indicate that a timetable is not practical.

We suggest that the FTC, in its report to Congress, outline a plan for determining the practical, technical, security, privacy, enforceability and other concerns that exist to establishment of a Do Not Email Registry. Unlike the Congressional review that preceded the legislation authorizing the "Do Not Call Registry," no such formal review of the issues was done for a Do Not Email Registry. As outlined above, SIIA believes that limited applicability of the lessons of the "Do Not Call Registry," and the overwhelming costs relative to any benefits of a Do Not Email Registry, point to a fundamental need for further delineation of the issues, especially since regulations required by the CAN-SPAM Act have not even been formalized.

If you have any further questions, or need additional information, please do not hesitate to contact us.

Sincerely,



Mark Bohannon
General Counsel &
Senior Vice President Public Policy