US ISPA
US Internet Service Provider Association

1330 Connecticut Avenue, N.W. ♦ Washington, D.C. 20036 ♦ 202.862.3816 (v) ♦ 202.261.0604 (f)

March 31, 2004

Office of the Secretary
Federal Trade Commission
600 Pennsylvania Ave. NW, Room 20580
Room 159-H
Washington, DC 20580

Re: Can-SPAM Act Rulemaking, Project No. R411008

Dear Secretary:

The U.S. Internet Service Provider Association ("US ISPA") submits these comments to assist the Commission with preparing its report to Congress setting forth a plan and timetable for establishing a nationwide Do Not E-mail Registry. US ISPA is a trade association made up of major service providers. Its members include America Online, Inc., BellSouth, EarthLink, MCI, Microsoft, SAVVIS, SBC, Verizon. US ISPA and its members have focused on both the legal and policy issues of unsolicited commercial e-mail as the rising tide of spam directly impacts the service provider industry.

Spam is one of the biggest problems facing service providers and their customers today. It is for this reason that service providers supported passage of the CAN-SPAM Act. Our members are deeply committed to stopping unlawful and unwanted spam from reaching their customers' in-boxes. They employ sophisticated filters to block spam; educate their customers on the means by which they can avoid spam; and work with law enforcement to combat unlawful spamming practices. Service providers are battling spam on many fronts because they realize that building trust in their service is critical to their own business success and because they know that without these efforts, e-mail will no longer be seen as a reliable and efficient communications tool.

Our members certainly support the *goal* of a Do Not E-mail registry: empowering consumers to control their in-boxes. But we have serious concerns that such a registry when implemented could actually compromise our customers' privacy and worsen the spam problem. Service providers, which, along with consumers, shoulder the majority of the expense and burden of handling spam, are eager to embrace workable solutions to the spam problem. Unfortunately, a Do Not E-mail registry could cause more harm than good.

US ISPA appreciates the opportunity to provide comments to the Commission on the viability of a Do Not E-mail registry. Our comments make three points. *First*, spam is not the same as telemarketing and the factors that have enabled the Do Not Call registry to work simply are absent or quite different in the e-mail context. *Second*, several of our members and other technology vendors are in the process of developing solutions to spam based on identifying the origin or identity of e-mail senders. These authentication solutions, which, in combination with industry best practices, will enable consumers to exercise control over the e-mails that flow into their in-boxes, provide a better alternative to any form of a Do Not E-mail registry. *Third*, authenticating e-mail senders is technically complicated and industry should take the lead in testing and implementing these proposals in the marketplace.

Based on these points, US ISPA recommends that the principal element of any plan for a Do Not E-mail registry should be to allow industry to develop a workable and comprehensive authentication solution prior to the establishment of an actual registry.

I. Spam Is Different From Telemarketing.

The Do Not Call registry is an effective mechanism to stop unwanted telephone solicitations. However, there are inherent differences between telemarketing and spam that would make a Do Not E-mail registry impractical and counterproductive in reducing spam.

A Do Not E-mail registry would be a prime target for security attacks. Spammers are in a constant search for valid e-mail addresses, employing sophisticated harvesting and other tactics to obtain them. A list of valid e-mail addresses on the Do Not E-mail registry would be a prime target of security attacks and the costs associated with protecting the list from such attacks could be significant. This is in sharp contrast to telephone numbers, most of which are already published and readily available.

Absent difficult and expensive processes and procedures to protect against the release of names to unlawful spammers, the Do Not E-mail list would jeopardize consumer privacy and give spammers the means to spam. If the Do Not E-mail list is distributed to senders of commercial e-mail, it is impossible to prevent unlawful spammers—both domestic and foreign—from obtaining copies and using them to send spam. This is true notwithstanding civil or criminal prohibitions on misuse of the lists, which unlawful spammers have to date ignored. If even one bad actor obtains the list, it will be widely available on the Internet and, contrary to the goals of the registry, every listed e-mail address will be bombarded with spam.

A Do Not E-mail registry would increase the use of dictionary attacks. Even if the lists were not shared with senders of commercial e-mail but rather senders were required to submit their list of e-mail addresses to the registry for scrubbing against the national Do Not E-mail list, spammers could still abuse the system by following a three-step process: (1) spammers would generate lists of e-mail addresses using random combinations of names, letters, and numbers (so-called "dictionary attacks"); (2) spammers would submit their list (which would contain made-up, fake addresses mixed with potentially valid ones) to the registry and the registry would remove only the valid, registered e-mail addresses from the spammer's list; (3) the "scrubbed" list would be returned to the spammer, who would then compare it against the original list and retrieve all of

the valid addresses on the Do Not E-mail list. This use of dictionary attacks would be much cheaper for spammers than their current methods, which require them to send millions of messages and wait to receive bounce backs from invalid e-mail addresses to determine which are valid. Unfortunately, dictionary attacks can be used in this way even if the Do Not E-mail list was encrypted.

The likelihood for abuse is high and enforcement would be difficult. In sharp contrast to the cost of making telephone calls in high volumes, spam is cheap to send. Indeed, the marginal cost of every additional message is effectively zero. Thus, the likelihood for abuse by spammers who get their hands on the list is high. But the frequent use of fraudulent transmission tactics—such as forging e-mail addresses and Internet domain names—would make it extremely difficult to identify those who have misused the list. The cross-border scope of the spam problem, again in contrast to telemarketing, would further hamper enforcement efforts.

Service providers already prohibit unsolicited bulk e-mail from being sent over their systems. It is unclear what types of e-mail communications would be prohibited from being sent to addresses on the Do Not E-mail registry. Today, most service providers already prohibit unsolicited bulk e-mail from being sent over their private networks. Thus, a Do Not E-mail registry that prohibits these types of e-mail communications from being sent to registered addresses would have very little benefit, if any. In addition, a one-size-fits all regulatory definition of spam may capture e-mail desired by recipients and may not work with filters that employ dynamic and sophisticated means to determine which messages to let through. Thus, contrary to the goals of empowering consumers, a Do Not E-mail registry could actually thwart the ability of service providers to respond flexibly to the demands of their customers and to offer their customers choice as to the messages they want and do not want to receive. Finally, those unlawful spammers who today ignore rules regarding use of service provider networks, as well as the CAN-SPAM law, will likely not comply with a Do Not E-mail registry.

A domain-wide registry would face similar problems. To deal with many of these issues, it has been suggested that the Do Not E-Mail registry should be comprised of entire ISP and corporate-level domains as opposed to individual e-mail addresses. Under this approach, a class of e-mail messages could not be sent to any address within a domain that is listed on the registry unless the e-mail address was on a separate list, presumably maintained by each service provider, of customers who had indicated a willingness to receive such mail. Such a scheme could prove costly for service providers to implement. Also, as noted above, the majority of service providers prohibit bulk unsolicited e-mail from being sent over their systems. Thus, an approach that allows customers to choose to receive these types of e-mail communications could contradict service providers' explicit Terms of Use Agreements. Conversely, while corporate-level domains face no legal barriers to opting-out of receiving an entire class of e-mail messages, it is not clear how service providers would make this decision on behalf of their subscribers. Would they ask the subscribers to vote? Would the majority rule apply? In addition, to the that extent service providers would have to share even a portion of their subscribers' e-mail addresses with the Commission or senders under a domain-wide registry, this approach could compromise the privacy of their subscribers. Finally, although this approach may solve the dictionary attack problem inherent in a registry based on individual e-mail addresses, the challenges posed by

fraudulent senders and the cross-border extent of the spam problem would still exist under a domain-wide registry, rendering enforcement a significant obstacle.

II. Alternatives Exist that Will Help Stop Spam From Reaching Consumers.

The fight against spam has posed a challenge in large part because most unlawful spam is untraceable. Today, when e-mail is transmitted over the Internet from one organization to another, no authentication of the sender of the e-mail or the computers delivering it on the sender's behalf occurs. In other words, no verification is performed to ensure that an e-mail that purports to be sent from "user@ftc.gov" does in fact originate from computers under the control of the FTC. It is therefore simple for virtually anyone with a computer connected to the Internet to send e-mail and appear to be someone else in doing so.

Needless to say, spammers routinely exploit this capability and forge or "spoof" e-mail addresses from which they send e-mail. These fraudulent practices have made it extremely difficult for spam filters—designed to allow service providers to manage their e-mail load and empower consumers—to work effectively. Unlawful e-mail that appears to originate from legitimate senders slips through filters. And e-mail from legitimate senders, whose reputation has been tarnished from spoofing, often gets blocked.

To address this problem, several of our members and other technology vendors are developing systems that will allow e-mail senders to authenticate their identity, and, later to show that they have agreed to meet industry standards of accepted, non-spamming behavior. These systems will not prevent unlawful spam from being sent. But they will make spoofed e-mail easier to identify and filter and thereby prevent it from reaching consumers' in-boxes.

US ISPA believes authentication solutions in combination with industry standards hold real promise for combating the spam problem. Today, the costs of detecting and remedying the forging of addresses by unlawful spammers is placed entirely on consumers and the receiving organization, from large service providers to small offices and home e-mail servers. Yet as authentication measures are implemented and deployed, it will become more difficult to make a lucrative living as a spammer. Shifting the economic balance in favor of consumers and receiving organizations, and away from unlawful spammers, is necessary if we are going to succeed in eradicating spam.

III. Industry Should Drive Authentication Solutions.

We understand that the Commission is considering registry models that may include an authentication component. We commend the Commission for recognizing the importance of authentication to resolving the spam problem. That said, developing and implementing an authentication solution is a technically difficult process that will require extensive industry collaboration. For this reason, we believe the private sector is in the best position to oversee this process.

There are many factors that need to be considered in developing and implementing an e-mail authentication solution. The ultimate technical solution must be scalable and support

organizations that have both hundreds or even thousands of e-mail servers as well as those that have just one. It must be cost effective for legitimate senders, recipients, and Internet infrastructure providers. And it must be openly published so that any organization wanting to comply with its provisions may do so.

Perhaps the most difficult challenge for an authentication solution is ensuring its robustness to spammer attacks. The solution must be designed so that it cannot profitably be circumvented by spammers here and abroad who either register as authenticated senders or take over the computers of such senders. To do this, the solution will need to quickly detect spammers and send updated information to the hundreds of millions of recipients who check for authentication. This will likely require real-time monitoring of per-sender volume across the Internet. It also will require resolution of difficult questions, including whether or not reports of spam are indeed spam, simply user error, or attacks by third parties on an unpopular sender. Performing these decisions rapidly and correctly, and without burdening legitimate senders, will require nuanced solutions that can be readily adjusted in the face of spammer attacks.

It is simply too early to determine which authentication proposal, or some combination of them, will provide the most meaningful and workable standard for the marketplace. But we do know that flexibility is going to be the key to success. The process of reaching a viable authentication solution will involve evaluating various design options; testing them in different scenarios and across dissimilar systems; identifying and resolving problems that arise; and implementing them with various stakeholders. It also will require working across borders to integrate foreign senders into the solution so that filters can be aggressively deployed. These are complex and time-consuming tasks that we believe industry rather than government has the expertise and available resources to handle.

IV. Conclusion

In light of the privacy, security, and enforcement concerns raised with a Do Not E-mail registry, and the benefits to consumers of industry-developed authentication solutions, US ISPA believes the first phase of any plan for a Do Not E-mail registry should be to encourage and facilitate the private industry innovation that will implement a meaningful and comprehensive authentication solution.

Sincerely,

Stewart A. Baker
U.S. Internet Service Provider Association