BEFORE THE
FEDERAL TRADE COMMISSION
WASHINGTON, DC

In the Matter of	)	
	)	Project No. R411008
CAN SPAM Act Rulemaking,	)	
	)	
	)	

Comments of the Center for Democracy and Technology

The Center for Democracy and Technology (CDT) submits the following comments in response to the Federal Trade Commission's (FTC) Advanced Notice of Proposed Rulemaking and Request for Public Comment on the CAN SPAM Act Rulemaking.

CDT is an independent, non-profit public interest organization advocating democratic values and constitutional liberties in the digital age. As an outgrowth of its efforts to assure an open Internet that fosters free expression and its work to protect the privacy of users online, CDT has been actively engaged in the debate about how best to minimize the incidence of spam. In early 2002, CDT published the results of its independent research into the kinds of online behavior that result in users receiving spam in its report *Why Am I Getting All of This Spam.* In the summer of 2003, CDT convened a meeting of key stakeholders in the spam debate to consider what legislative provisions might best stem the flow of spam into users e-mailboxes. Later that year CDT focused specifically on technological solutions to the spam problem. On the basis of its participation in the spam debate, CDT submits the following comments in response the FTC's Advance Notice of Proposed Rulemaking and Request for Public Comment.

The Request for Comment asks for input on a wide range of issues related to the implementation of the CAN SPAM Act. CDT's comments respond to the FTC's specific request for input for its report setting forth a plan and timetable for establishing a nationwide marketing "Do Not E-mail" Registry, required by the provisions of the CAN SPAM Act.

1. *Rather than devote scarce resources to the burdensome task of implementing and administering a nationwide "Do Not E-mail" Registry, the Commission should focus its efforts on enforcement of the provisions of the CAN SPAM Act.*

   The CAN SPAM Act contains important provisions specifically designed to aid in the tracking and prosecution of spammers. In drafting the legislation, considerable effort was invested in "anti-spoofing" language in the law – a

prohibition against e-mailers including "header information that is materially false or misleading." The requirement was designed to make it possible for consumers to send to a functioning return email address a message opting out of additional unwanted email. It was also included to make it possible for authorities to locate and prosecute e-mailers that did not respect the opt-out. Spammers would no longer be able to hide behind false or misleading header information. This "anti-spoofing" provision was considered by many to be key to the CAN SPAM Act's success at reducing the amount of spam.

Focusing attention on a "Do Not E-mail" list would divert resources from this enforcement. Rather than prosecute spammers, the FTC would be implementing and administering an initiative whose potential for success is unclear, while fundamental requirements of the CAN SPAM Act likely go unenforced. Moreover, enforcement of the "anti-spoofing" provision is key not only to enabling consumers to opt-out – it is critical to law enforcement's ability to locate rogue spammers who may violate a proposed "Do Not E-mail" Registry.

Acting now to put a "Do Not E-mail" Registry in place is premature at best. CDT recommends that the FTC focus its attention on enforcing the key elements of the CAN SPAM Act.

2. *The success of the Do Not Call list does not necessarily map to a similar "Do Not E-mail" list. If the FTC chooses to implement a "Do Not E-mail" list, it must seek ways of doing so that are specifically suited to the realities of e-mail technologies.*

   The FTC's successful "Do Not Call" Registry enables consumers to register telephone numbers at which they do not wish to receive telemarketing calls. Registration is free and available online and at a toll free number. The "Do Not Call" Registry initiative makes it possible to file complaints about unwanted calls made in violation of the list, and to delete a registration when the consumer chooses to do so. Telemarketing firms pay to obtain the list, and are required to match their call lists against the FTC registry lists to "scrub" their lists of any number on the FTC registry.

   The fairly straightforward approach of the "Do Not Call" list does not map directly to a similar registry of consumers who wish to avoid unwanted e-mail. While consumer satisfaction with the "Do Not Call" list makes the concept of a "Do Not E-mail" list an attractive one, the technical realities of e-mail communications do not lend themselves to a "Do Not E-mail" list approach. Should the FTC decide to go forward with a "Do Not E-mail" list, it will be important that it take into account the complexities of e-mail technologies and the problem of spam.

a. *There is no working model for the proposed "Do No E-mail" Registry.* The nationwide "Do Not Call" registry, administered by the FTC, had as its precursors similarly designed state and industry sponsored lists of consumers who did not wish to receive telemarketing calls. These state and industry registries provided the means to test such an approach to eliminating unwanted telemarketing calls. What was proven was that while the approach imposed an undue burden on consumers (who were required to register with multiple state registries and an industry registry to obtain relief from unwanted calls) the administrative structure of such a registry could work. Consumers who placed their names on the state and industry lists did not, within the limits of the list's reach, receive unwanted calls. The proposed list has no similar "proof of concept" model, and it is critical that the FTC seek approaches specifically designed to accommodate the realities of e-mail communications, which differ markedly from those of phone communications.

   Consumer satisfaction with the effectiveness of the "Do Not Call" Registry raises high expectations for the proposed "Do Not E-mail" Registry. If the new e-mail registry is not properly designed and administered in a manner specific to *e-mail* rather than telephone technology, those high consumer expectations are not likely to be met.

b. *If not designed properly, a "Do Not E-mail" Registry could be easily and inexpensively gamed.* The proposed "Do Not E-mail" Registry would necessarily be a US based system and subject to enforcement under US law. E-mail technology is designed in such a way that would allow outlaw spammers to game the system at little or no cost. Without incurring any additional cost, e-mail originally generated inside the US could be routed through servers located offshore, and thus present the appearance of falling outside US jurisdiction. While technically telemarketing calls governed by the "Do Not Call" Registry could be similarly routed outside the US, the cost of doing so would be prohibitive to a telemarketing company.

c. *Maintenance of a "Do Not E-mail" list presents challenges that the "Do Not Call" Registry does not.* Unlike telephone numbers, e-mail addresses are easily and readily changed, and consumers often use multiple e-mail addresses. Consumers will need to be constantly vigilant to keep the proposed "Do Not E-mail" Registry current, or they will unwittingly find themselves unexpectedly receiving spam.

3. *Should the Commission determine to proceed with the proposed "Do Not E-mail" Registry, security of the system will be key to its success, and to public trust in the system.*

A master list of e-mail addresses generated by consumers themselves will, of necessity, create an attractive, valuable resource to rogue spammers looking for new, "live" online prospects. Were a "Do Not E-mail" list implemented, among the FTC's top priorities must be the security of the list.

Creation of the proposed "Do Not E-mail" Registry will require that consumers release to the government information for which there is no other comprehensive registry – their e-mail address. While it may be possible to remove one's information from the phone lists, generally consumers expect that their telephone number will be available to the public when they sign up for service.

E-mail addresses are not publicly available, and the consumer places the privacy of that information a significant risk in releasing it to government for a "Do Not E-mail" list. Further, leaking e-mail information may well have dire consequences beyond those suffered by the unauthorized release of telephone lists. The fluidity of e-mail address information and the highly automated character of e-mail technology nearly assures subsequent and repeated sharing of e-mail information that will result in even higher volumes of spamming than otherwise would be expected.

To take advantage of the proposed "Do Not E-mail" Registry, consumers will be required to make known to the government information that it might otherwise consider private. A security breach would aggravate the very problem the list was designed to address. For the system to succeed, and to maintain the public's trust, the FTC will have to take strong technical and policy measures to assure that the information contained in a proposed "Do Not E-mail" Registry is secure.

CDT is grateful for the opportunity to file these comments and to participate in this important dialog. We look forward to working with the FTC as it continues its efforts toward stemming the flow of spam.

Respectfully submitted,

Paula J. Bruening
Ari Schwartz
Center for Democracy and Technology
1634 I Street, NW
Washington, DC 20006