

BEFORE THE  
FEDERAL TRADE COMMISSION  
WASHINGTON, D.C.

In the Matter of )  
 ) Project No. P044411  
Notice of Proposed Rulemaking )  
Proposed Mark for Sexually Oriented Spam )

Comments of the Center for Democracy and Technology

The Center for Democracy and Technology (CDT) is an independent, non-profit public interest organization advocating democratic values and constitutional liberties in the digital age. CDT has been actively involved in policy and consumer education efforts to reduce the amount of spam. CDT has conducted research on the origins of spam and what kinds of online behavior make computer users more likely to receive spam. We have convened consultations of experts, industry representatives, and consumer advocates to consider proposed technology and policy solutions, their effectiveness, their viability for industry, and their potential impact on speech online. On the basis of the insights gathered through these ongoing efforts, CDT respectfully submits the following comments.

CDT is keenly aware of the tremendous problem spam poses to ISPs, businesses and individual users and endorses a three-part approach to addressing the spam problem: enforcement of appropriate, effective law; technological solutions; and consumer education about online behaviors that encourage spam and the user tools available to take control of it.

CDT supports the efforts of industry, with the encouragement and support of the FTC and NIST, to develop email authentication systems. Such systems may prove to be powerful tools for controlling the flow of spam. At the same time, CDT believes that it is important to avoid the adoption of one or a very small number of authentication or validation systems that become mandatory to use in order to send email over the Internet. Some of CDT's concerns are raised by, for example, Questions 4 (about the handling of unauthenticated messages) and 22 (about anonymous political speech), but are also raised more broadly by the focus of the FTC/NIST Summit on domain-level email authentication systems. CDT's specific concerns are:

- There are currently a multiplicity of technical and industry efforts to devise ways to reduce spam, and neither industry nor government should at this point focus only on one or two such efforts to the exclusion of others. For example, beyond systems that attempt to authenticate the domain of the sender, there are efforts and

proposals to permit e-mail to be validated using seals-of-approval or systems that require the sending user agent to execute a computationally demanding calculation. These technical and industry efforts should continue to be developed, and should be encouraged by both industry and government.

- Although it is unrealistic for receiving mail servers to be able to recognize dozens of different e-mail authentication or validation schemes, CDT is hopeful that the industry will ultimately support a variety of different approaches to e-mail authentication/validation, so that e-mail senders are able to use the system that best suits their individual needs (in terms of cost, ease of use, speed, reliability, etc.). More generally, it is important that e-mail senders continue to have a variety of simple and low (or no) cost options for sending and receiving e-mail, and e-mail authentication/validation systems should not preclude such options.
- It is also important that unauthenticated, un-validated e-mail continue to be a viable possibility. Thus, as raised by Question 4, receiving e-mail servers should not reject unauthenticated, un-validated e-mail as a matter of course, and such mail should not be delayed unduly. Although unauthenticated/un-validated e-mail can certainly be examined by origination, for bulkiness, and according to other factors in use today (to identify and weed out unsolicited commercial spam), such e-mail should still be able to be sent and received (albeit likely at a somewhat lower speed of processing). This requirement is necessary both to address the unavoidable (and likely lengthy) period of transition to e-mail validation systems, and to accommodate anonymous e-mail as discussed below.
- CDT believes that email is an Internet application that fosters free expression and that allows users to engage in political speech with a nearly limitless number of listeners. It strongly agrees with the assumption that underlies Question 22, that anonymous political speech (including speech conveyed in bulk email) is an important right that should be protected, and should be a viable possibility using Internet email. The right to, and value of, anonymous speech is not, however, limited to anonymous political speech, but can include a variety of types of non-commercial communications (such as, for example, the transmittal of information or questions concerning medical or other sensitive personal topics). Thus, it is important that anonymous non-commercial speech be permitted and viable in a future Internet that has (we hope) effectively controlled the commercial spam problem.

CDT appreciates this opportunity to comment, and looks forward to continuing to work with the FTC and NIST on this issue.

Respectfully submitted,

Paula J. Bruening  
John B. Morris, Jr.  
Center for Democracy and Technology  
1634 I Street, NW  
11<sup>th</sup> Floor  
Washington, DC 20006  
(202) 637-9800



