Technological Responses to the Problem of Spam:
Preserving Free Speech and an Open Internet Values

Paula J. Bruening
Staff Counsel
Center for Democracy and Technology

Nearly from its inception the Internet has been recognized as a medium with unique potential to transform public discourse. Its abundant capacity, its global reach, and its "no gatekeeper" infrastructure promise to provide individual speakers a platform to publish, to conduct research and to communicate to a wider audience than ever before possible, without the barriers normally encountered in traditional broadcast and print media.

The use of basic email services by individuals for communications and commerce is perhaps the most vivid example of average consumers adopting an application to tap into this unique potential. Email places into the hand of users around the world, of all levels of technological expertise, from all walks of life, a tool that makes it possible for them to reach a nearly limitless number of listeners. Email also takes advantage of the "no gatekeeper" model of the Internet by enabling speakers with limited resources to reach a global and diverse audience directly.

But these efficiencies of the Internet and of e-mail also are at the root of the spam problem. The effortlessness with which one sender can transmit a commercial message to hundreds, thousands or even millions of recipients presents an irresistible temptation to purveyors of spam, resulting in a problem that plagues ISPs, business and individuals.

While the CAN SPAM Act, signed into law in 2003, places specific requirements on senders of commercial email and imposes criminal sanctions for abusive and predatory spam practices, the law's ultimate effectiveness remains to be determined. The pressing nature of the spam problem, however, prompts the development of alternative, technological solutions to the problem of spam that would function independently of, or in tandem with, the requirements of the CAN SPAM Act.

But responding to the problem of spam, whether through law or technology, is not a simple undertaking. Not only does this very complicated issue touch upon First Amendment and privacy concerns, it also involves regulating a decentralized and global technical infrastructure. As work toward these solutions to the spam problem proceeds, it is critical that concepts fundamental to the vision of the Internet – decentralization, "no gatekeeper" infrastructure, and abundant access - be respected and fostered.

Among the responses under consideration is the establishment of trusted email (or trusted sender) systems, under which a legitimate sender of bulk commercial email obtains from some entity a pre-approval, such that the sender is assured its email is recognizable and passes through the filters of ISPs participating in the system. One principle behind trusted email is that ISPs will be able to focus their anti-spam efforts more efficiently on illegitimate senders who could not meet the standards of a trusted email program, and that consumers will be able to better differentiate between mail from legitimate commercial senders and spammers, while also improving their faith in opt-out mechanisms offered by such trusted e-mailers.

In certain respects, ISPs already act as gatekeepers, making decisions about the delivery of email on a case-by-case basis, applying various technological means of judging email. These decisions

about blocking occur without transparency. Legitimate senders of bulk email must determine by trial and error what will get through, or work out private arrangements with ISPs to ensure that their email is recognized as legitimate. A key consideration for developers of new technologies to stem the flow of spam is whether they facilitate and systematize the ISPs' gatekeeper role in ways that improve transparency, accountability and the openness of the Internet for legitimate users or in ways that increase the control of a few trusted email authorities.

Further, while the proposed trusted email systems are focused on commercial rather than political speech, a significant concern is that the line between commercial speech and other kinds of speech (e.g., the political campaign that sells tee-shirts and coffee mugs) is often not easily drawn. Moreover, a systematized gatekeeper system may well have unanticipated effects on noncommercial speech, especially as it remains unclear whether trusted email will, in fact, be implemented in a way that makes ISPs more effective in screening untrusted mail, and thereby more likely to let untrusted political mail through.

Questions also arise about how ISPs will treat non-approved bulk email. Proponents of trusted email explain that non-approved email would be treated the same way it is now – it would be examined by origination, for "bulkiness" and according to other factors. But what would stop email service providers from rejecting all bulk email that does not use the trusted systems? It is assumed that ISPs are not interested in and not intending to block bulk political email. Presumably, ISPs will be able to distinguish bulk untrusted political email from bulk untrusted commercial mail and let the former through. Concerns persist that there is no requirement that they do so and therefore nothing to prevent ISPs from requiring trust seals from all senders, commercial and non-commercial.

Trusted sender systems also raise questions about the need for oversight mechanisms that would introduce complex Internet governance challenges. Some developers of trusted email systems predict that implementation will require the establishment of a trusted email oversight board to assure credibility of the system(s) and the balanced representation of industry, advocates and consumers in decision-making about the administration of trusted email systems. Because of the global nature of email, any governance mechanism for trusted email would need to account for and accommodate the sensibilities and requirements of diverse cultures, each of which have their own ideas about what constitutes appropriate online communication, how rules for oversight should be formulated, and how enforcement should be carried out. Governance of a trusted email system would likely encounter challenges and complications comparable to those faced by ICANN.

Trusted email systems represent only one approach to stemming the flow of spam. These systems provide, however, an important example of the issues that new technologies and non-legislative approaches to controlling unwanted email may raise. As these and other anti-spam efforts are developed, it will be necessary to closely examine their effects on free expression online and the original vision of an abundant, open Internet in order to mitigate any negative consequences.