



ELECTRONIC PRIVACY INFORMATION CENTER

---

Testimony and Statement for the Record of

Marc Rotenberg  
Electronic Privacy Information Center, Executive Director  
Georgetown University Law Center, Adjunct Professor

Hearing on  
Spam  
(Unsolicited Commercial E-Mail)

Before the

Committee on Commerce, Science and Transportation,  
United States Senate

May 21, 2003  
253 Russell Senate Office Building

## Summary of Recommendations

- Continue to support strong enforcement action by the FTC
- Promote international cooperation, particularly with consumer protection agencies
- Recognize that many of the current spammers are likely subject to prosecution under current unfair and deceptive trade practices laws
- Enact a federal baseline that establishes an opt-in standard, gives consumers legal rights to go after spammers, and does not preempt state law
- Anticipate that similar problems may arise with cellular phone advertising in the near future

## Statement

Mr. Chairman, members of the Committee. Thank you for the opportunity to testify today about the problem of Unsolicited Commercial E-mail, or “spam.” My name is Marc Rotenberg. I am the Executive Director of the Electronic Privacy Information Center. EPIC is a non-profit, non-partisan research organization. We work in close association with a wide range of consumer and civil liberties organizations, both in the United States and around the world.

There are few issues of greater concern today to users of the Internet than spam. Spam is also one of the most complex policy issues for the Internet. Even though there is broad agreement about the urgency of the problem, there are still questions about the appropriate role of law and technology, the relationship between the federal government and states, and even the question of how best to tackle a consumer problem that clearly has a significant international dimension.

## Scope of the Spam Problem

As Chairman Muris noted at the recent FTC public workshop, the spam problem is increasing rapidly. In 2001 the FTC began to routinely collect spam. During that year, the FTC received an average of 10,000 messages per day. In 2002, that figure went up to 47,000 a day. The number has gone to 130,000 e-mails a day this year. As a measure of how fast a new e-mail address can attract spam, Chairman Muris reported that the FTC had seeded an e-mail address in a chat room. That e-mail address began receiving spam in eight minutes.

It has been estimated that 40% of e-mail in the United States is spam, creating an annual cost of over \$10 billion. These costs are incurred through lost productivity and the additional equipment, software and labor needed to deal with the problem.

On spam, the interests of Internet users and the Internet industry are generally aligned. Only the Direct Marketing Association has expressed opposition to sensible opt-in legislation. However, as the recent FTC Workshop made clear, this position is simply not viable in the online world. Permission-based marketing, which relies on the

affirmative consent of consumers, has always been a good business practice. Now it may be critical to stem the flood of undesired e-mail.

### Factors Contributing to Spam

Several factors contribute to the spam problem. First, it is inexpensive and relatively simple to send spam to a very large number of Internet users. Unlike traditional junk mail, the marginal cost for each additional electronic message is essentially zero. Therefore, spammers are as likely to send to a million users as they are to a thousand.

Second, the origin of spam is often difficult to determine. Spammers will frequently send messages from domains they do not own and in ways that conceal the source of the message. The spammers also show little regard for any effective list management. There is no meaningful effort to obtain consent or allow users to opt-out of undesired marketing.

Third, spam raises difficult jurisdictional problems. Spammers may send messages from one state to another and even from one country to another. While there is general agreement across jurisdictions about the need to reduce spam, there are questions about how best to coordinate enforcement measures.

Fourth, there are definitional problems associated with spam. Commercial marketers who engage in bulk e-mail advertising may be reluctant to concede that their messages are spam even though the vast majority of recipients find the messages burdensome and undesirable. Some Internet users may consider bulk political mail as “spam,” though for both practical reasons and the First Amendment, it is appropriate to distinguish between commercial and non-commercial bulk mail.

Fifth, technical solutions are imperfect. While ISPs have had some success identifying the source of spam, spammers rotate domains and even change the key terms in a message to avoid detection. Similarly, typical users find it difficult to adapt filters and other techniques to accurately remove spam. There is always the risk that a filter will delete messages that the user needs to receive. Other techniques, such as challenge and response, may be too cumbersome for most users.

Sixth, the long-time reluctance of the private sector to acknowledge the need for a legislative solution to the spam problem coupled with the Direct Marketing Association’s active opposition to Internet privacy has certainly contributed to the problem. While the industry’s desire to avoid regulation is understandable, here the failure to establish strong measures to limit spam are contributing to a tragedy of the commons that threatens to undermine the commercial potential of the Internet.

### Difficulty Consumers Face with Spam

While ISPs clearly face a significant cost that can be measured in bandwidth, staff hours, hardware, and even litigation fees, consumers face the ongoing annoyance that

spam simply makes the Internet less friendly and e-mail less useful. For the consumer facing a mailbox full of spam, even good software programs do not solve the problem of the time and cost of downloading e-mail before it can be analyzed and assessed. These burdens fall particularly on consumers in rural regions, consumers who are traveling outside the country, and others who are likely to pay high fees while connected to the Internet.

The most widely used spam filters, while they can be effective, invariably under block and over block incoming mail. As a result, users continue to receive undesired e-mail and are losing important e-mails that may include business proposals or simply notes from friends. Some spam filters group incoming messages as likely being spam, but the consumer must still sort through the messages.

In addition, many of the techniques proposed by some are simply impractical or nonsensical. For example, a challenge response method to determine whether e-mail is coming from an actual person would probably discourage even desired communication. Similarly, routinely changing mail addresses is an impractical solution as is trying to prevent one's mail address from being posted on a web site where it can be harvested by one of the programs is not a workable approach as anyone who has a publicly accessible staff directory knows.

A better approach for the consumer is one that empowers individuals to go after the spammers who misuse their personal e-mail address for unsolicited commercial e-mail and impose costs and burdens.

### Technical Measures

It is clear that industry groups and technical groups are eager to find a solution to the spam problem. Many innovative approaches are currently being pursued even as some of the routine flaws that are exploited by spammers are fixed.

Congress should continue to encourage technical solutions, but the possibility of technical solutions should not be a reason to avoid legislation. ISPs clearly favor better legal tools as well as better technologies to go after spammers when they can be identified. Moreover, without legal sanctions there is no practical basis to put an end to egregious spamming.

There is one caution on the technology front that should be brought to the attention of the Committee. Several technological solutions, not surprisingly, focus on determining the actual identity of spammers, and would make identification through digital certificates and other means a requirement for sending e-mail to multiple recipients. While this approach may be appropriate for commercial speech, it would not be appropriate for political or religious speech. The Supreme Court has made clear in a series of cases that the right to speak anonymously is a central element of the First Amendment. Any attempt by the government to require identification for bulk e-mail that would include political speech would raise significant Constitutional concerns.

## Legislative Proposals

S. 877, the CAN SPAM Act, sponsored by Senator Burns and Senator Wyden, contains many important elements for a good anti-spam measure. All unsolicited marketing e-mail would be required to have a valid return e-mail address so recipients could ask to be removed from mass e-mail lists. Once notified, marketers would be prohibited from sending any further messages to a consumer who has asked them to stop.

The bill would enable Internet Service Providers (ISPs) to bring action to keep unlawful spam from their networks. The legislation contains enforcement provisions allowing the Federal Trade Commission to impose civil fines on those who violate the law. State Attorneys General would be given the ability to sue on behalf of citizens who have been targeted by unscrupulous marketers.

This a good starting point, but we urge the Committee to go further, particularly to protect consumer interests. As the Burns-Wyden measure currently stands, it is simply not a sufficient solution. It gives the FTC a great deal of authority and the ISPs many opportunities to bring complaints. However, for the state attorneys who are already on the front lines and for the users who are also saddled with the costs and burden of spam there is not enough in the bill currently to reform egregious online practices or assure that spammers will be pursued.

Three critical changes are necessary to strengthen the Burns-Wyden measure. First, the Committee should endorse a full opt-in regime for unsolicited commercial e-mail except in those cases where a prior business relationship exists. Opt-in is the logical basis for Internet mailings. In fact, most Internet lists today are based on opt-in. These lists typically also provide users with the opportunity to update their contact information and remove themselves from the list if they choose. There are many opportunities for companies to obtain consent and to build online marketing techniques, in parallel with the traditional Internet lists, which would be welcome by consumers. Where there is a genuine preexisting relationship, then it would be appropriate to communicate by e-mail. Simply visiting a web site is not sufficient. There should be some actual exchange for consideration before a “preexisting business relationship is established.”

Second, the bill should incorporate a private right of action that allows individuals to bring action in small claims court, similar to the approach established by the Telephone Consumer Protection Act (TCPA) for junk faxes and telemarketing. The opportunity to pursue a modest judgment in small claims court has provided a useful incentive in the effort to stem junk faxes and would be helpful for spam. In fact, many of the state measures take an approach similar to the TCPA in recognition that those who are the target of spam should have the legal right to seek redress against those who are responsible for the spam. Also, as the TCPA has shown, a national do not e-mail list may help with enforcement, though technical experts have expressed some concerns about the possible misuse of a national Do Not Spam list.

Third, the bill should not preempt state law. While it is clear that some revisions have been made to the CAN SPAM Act to take account of the important efforts of states to combat spam, the bill still unduly restricts state legislatures that have been on the front lines of the problem. Even with the FTC's important enforcement efforts, there is a real risk that a "one size fits all" approach will not be effective and will undermine the basic structure of federalism in the United States that allows the states to pursue different approaches to common problems.

As Washington Attorney General Christine Gregoire stated on behalf of the Attorney Generals for 44 states, a weak federal statute that preempts stronger state laws will reduce the level of consumer protection and facilitate the continued growth of spam. This would clearly not be a desirable outcome.

### House Proposals

Several proposals are also under consideration in the House. Those bills that establish opt-in, provided for a private right of action, and leave the states free to pursue innovative approaches will respond to the spam problem most effectively. There is also an interesting provision in one of the House measures that would penalize automated harvesting techniques that are deployed for the purpose of sending unsolicited commercial e-mail. This provision may help with the spam problem.

### Additional Issues

Mr. Chairman, you asked us also to address related issues that may be of interest to the Committee. I'd like to note that the problems of Unsolicited Commercial E-mail are likely to arise in a new setting that will impact million of consumers in the United States and that is cell phone based advertising. Although we are still in the early stages, it is apparent from the experience of other countries that consumers are beginning to express concern about advertising on their phones. If it is permission-based, there should be few problems. But if marketers begin to send bulk text messages or video messages to cell phone users, there will certainly be negative effects on the growth of cell phone based services. Already, providers in the United States are proposing to send e-mail to cell phones.

There is also significant work on the spam problem underway in many countries outside of the United States, and in particular in the European Union. It is interesting to note that virtually all of these approaches rely on an opt-in and some private right of action. The approach taken in the European Union Communications Directive emphasizes permission-based marketing and the need to ensure that even after opt-in is established, consumers retain the right to opt-out of online marketing lists.

Similarly, an extensive report from the Australian government on the spam problem released just last month urges the adoption of legislation based on prior consent where there is no preexisting business relationship; requires commercial electronic messages to contain accurate details of the senders names and physical and electronic

addresses; and further recommends appropriate codes of conduct for marketers and effective means of enforcement.

Finally, a joint resolution issued in 2001 by the Trans Atlantic Consumer Dialogue, an alliance of more than sixty consumer organizations in the United States and Europe, recognized that the use of unsolicited commercial electronic communication is a growing burden for people who use e-mail. The TACD said, “governments need to work together to develop common approaches to address consumer concerns about unsolicited commercial e-mail.” The group acknowledged the important differences between commercial and non-commercial speech, and urged the adoption of a policy based on prior affirmative consent.

### Conclusion

Mr. Chairman, spam is a complex problem. There is no simple legislative solution. A multi-tiered approach that includes aggressive enforcement, better technology for identifying and filtering spam, and cooperation at the state and international level will all be necessary. In addition, baseline federal legislation that gives users the opportunity to go after spammers and ensures that marketing lists are built on explicit consent and not on deception is a critical part of the effort to stem the tide of undesired commercial e-mail. Given the rapid increase in the spam problem in just the last two years, I urge the Committee not to delay action on legislation.

### References

Prepared Statement of the Federal Trade Commission before the Subcommittee on Commerce, State, the Judiciary and Related Agencies of the Committee on Appropriations, United States House of Representatives, April 9, 2003 (Chairman Timothy J. Muris).

Coalition Against Unsolicited Commercial E-mail  
<http://www.cauce.org/>

Commission Nationale Informatique et Libertés, web site on spam.  
[http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam\\_sommaire.htm](http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm)

CNIL's Report on Spam  
[http://www.cnil.fr/thematic/docs/internet/boite\\_a\\_spam.pdf](http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf)

EPIC Spam Page  
[http://www.epic.org/privacy/junk\\_mail/spam/](http://www.epic.org/privacy/junk_mail/spam/)

FTC Spam Page  
<http://www.ftc.gov/spam/>

Federal Trade Commission, "False Claims in Spam" (April 2003)  
<http://www.ftc.gov/spam/>

CAN-SPAM Act, S. 877 (Senators Burns-Wyden)  
<http://www.spamlaws.com/federal/108s877.htm>

Internet Society, "All About the Internet: Spamming"  
<http://www.isoc.org/internet/issues/spamming/>

Junkbusters  
<http://www.junkbusters.com/>

National Office of the Information Economy, "Final Report of the NOIE Review of the Spam Problem and How It Can Be Countered" (April 2003)

David E. Sorkin, Spam Laws  
<http://www.spamlaws.org/>

Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("Directive on Privacy and Electronic Communications")  
<http://register.consilium.eu.int/pdf/en/02/st03/03636en2.pdf>

TransAtlantic Consumer Dialogue (TACD), "Resolution on Unsolicited Commercial E-mail" (2001)  
<http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=98>