

Testimony of

**Clyde Wayne Crews Jr.
Director of Technology Policy
Cato Institute**

**Before the Subcommittee on Regulatory Reform and Oversight of the Committee on Small
Business of the United States House of Representatives**

“Spam and its Effects on Small Business”

2360 Rayburn House Office Building

October 30, 2003

The increasingly apparent downside of an Internet on which you can contact whomever you want, is that anyone can contact you.

Unsolicited commercial email, or “spam,” is unquestionably a huge problem. Bulk spammers pay no postage. Ultimately, the resolution is to shift costs back to the sender. The question is whether that should happen legislatively, or via technology, pricing, industry consortia, or some combination.

Ironically, a recent Reuters story indicated that filtering in some ways is becoming too powerful, as even friends are required to jump hurdles to get into their acquaintances’ white-listed, moat-surrounded mailboxes. It seems the “openness” that was central to the “Internet experience,” as the marketers like to say, is now a bug. It seems no longer the case that everybody necessarily needs or wants to be connected to everybody else, or shares conforming views of what acceptable online etiquette entails.

However, the real issue isn’t merely that legislation likely won’t rid us of spam (given the Net’s global pool of scofflaws); rather, legislation like “ADV” mandates or “do-not-spam” lists don’t address the fundamental factors at the root of the spam problem: (1) lack of authentication of senders, and (2) the ability of spammers to shift the costs of sending bulk email to recipients.

As for those legal attacks on spam being debated, some are appropriate and necessary. Such misdeeds as peddling fraudulent merchandise, or forging the name of a person or organization as the sender of a spam should be punished, as should phony “unsubscribe” promises, as should breaking an agreement made with an Internet service provider that prohibits bulk mailing. The law also should go after those that invade computers, such as by launching programs that hijack and send out spam from third party computers. Abusive forms of spam like “dictionary attacks” and spoofing seem related to hacking more than to commerce. Such behavior is already illegal of course.

To a great extent, unfortunately, legislative commands will be ignored by the most egregious spammers, and alternative solutions are going to become more urgent.

Maybe that’s a blessing in disguise, because even spam itself is not a single dilemma and may require different responses anyway: for example, solving the problem of kids seeing porn in the inbox is a different than solving the problem of ISPs overwhelmed with Viagra ads.

Market solutions, unlike legislative decrees, better lend themselves to cross-problem application, beyond spam. For example, just as the emerging email problem was anticipated years ago, one might similarly predict problems emerging as costs imposed on Internet service providers by free file-sharing services like Kazaa escalate. Spam (getting stuff) and piracy (taking stuff) alike are partly fostered by a pair of broader features: the lack of tiered pricing for network use, and the ability to hide one’s identity or origin online. The Internet’s “all you can

eat” buffet may need to end for email and file-sharing alike, a different proposition from passing a law.

The Internet wasn’t originally designed to be the mass commercial and consumer medium that it is today. If one were to design a commercial network today from the bottom up, it would probably incorporate authentication of the senders of email. Indeed, changing Internet plumbing in midstream to allow verification of sender origin wouldn’t aid just the spam problem but also cybersecurity and hacking concerns that industry needs to address perhaps more urgently even than spam.

Legislation shouldn’t stand in for or delay the day of reckoning for what should be (perhaps must be) a technical or organizational or market-driven fix. But one thing is clear: If the industry doesn’t solve spam, the law will step in, in ways some legislative proponents may come to regret.

Proposed legislation, for example, would impose subject-line labeling requirements for commercial email (commercial messages would have to say “ADV”); mandate an “unsubscribe” mechanism; ban the use of “harvesting” software; set up stiff non-compliance fines or even bounties; and establish an expensive (and likely hackable) Do-Not-Spam list at the Federal Trade Commission.

But if legislation sends the worst spammers offshore, all we’ll have accomplished is legal and regulatory hassles for small businesses trying to make a go of legitimate e-commerce, and mainstream companies that already follow “best practices” like honoring “unsubscribe” requests.

Besides, commercial e-mail, even if unsolicited, may be welcome if the sender is selling legitimate wares in a non-abusive manner. Most of us can agree on the outrageousness of the porn that hits our family in-boxes. But, on the other hand, thousands of people bought “The World’s Smallest Radio-Controlled Car” at Christmastime, or the Most-Wanted card deck during the Iraqi war. .

Proposed legislative penalties can easily keep many small businesses out of Internet marketing altogether, for fear of a misstep. Is that really our goal? (It takes effort to unsubscribe addressees, and inadvertent mistakes will happen.)

We should guard against unintended consequences, especially given the difficulty of enforcing legislation against the actual culprits. How might the definition of “spam” expand? Is it just “bulk unsolicited commercial” mail, or is it “anything you didn’t ask for?” Many say the latter.

What will be the consequences of legislation for noncommercial e-mailers like nonprofit groups that send in bulk? Many things aren’t commercial but are still unwanted: press releases, resume blasts, and charitable solicitations. I’ve even seen the term “scholarly spam” for material like that sent by organizations like my own.

Notably, politicians exempt themselves from anti-spam legislation, remaining free to send campaign material. But if we need “ADV” for commercial advertisements, then what about “REL” for religious “spam” like a piece I received warning of the coming apocalypse?

We shouldn’t discount the creativity of lawyers looking to sue easy marks, given that the bad guys will often be out of reach. Rest assured lawyers will go after those who occasionally slip up when implementing “unsubscribe” requests, or after newsletters that contain embedded ads but that might have failed to put “ADV” in the subject line. Navigating the treacherous email commerce of tomorrow will be easier to handle for large firms relative to small firms. Is this fair?

The invective around spam is so heated that you don’t know whose line you’re going to cross. Some of us occasionally send an unrequested email to strangers with a link to our company affiliation in our email signature line. That’s a subtle solicitation, whether we admit it or not. Remember, “spam” is a made-up word, subject to interpretation.

Aggressive pop-up ads may become targets in the aftermath of spam legislation, too (they already are in Germany). They’re not e-mail, but they are unsolicited and commercial, and getting more insistent than ever, employing animation and sound. Some ads aren’t merely pop-up but take over the screen.

As for 1st Amendment concerns, legal bans on “pseudonymous” e-mail return addresses can affect untrammelled speech and anonymity for individuals, and will be ignored by spammers anyway. Well-meaning individuals can use “spamware” to create the contemporary version of the anonymous pamphlets that have played such an important role in our history.

That said, while I don’t want the government to outlaw anonymous emailing, the private sector may need to prohibit it on private networks if that’s what canning spam requires.

Another worrisome issue is the tendency of legislation to set up “rules” for advertising. Indeed, much of the Internet industry’s newfound support of email “spam” legislation seems defensive and aimed at protecting the right and ability to send legitimate commercial email. Those motives are understandable and appropriate.

But there can be a downside to seeing legislation as the avenue to legitimacy. Surely, post-legislation, marketers will feel that they have met federal requirements, like ADV and a street address, and therefore ISPs have no right to block their messages even if the ISP would prefer not to deal with them. (One commenter said the “CAN SPAM” bill meant that you “can spam.”) In that environment, would advertisers be able to sue whenever their mail gets filtered or blacklisted, even in the absence of a contract with the ISP? Blacklists are one of the key means of dealing with spam today. I want to permit and retain ruthless blocking by ISPs, not have that ability over-ridden by the fact that a business followed some legislative checklist. Contracts, not legislation, must rule here. ISPs must retain the right to end such unwanted relationships.

Either the industry or Congress can set terms, but hardly both.

There's some good news. If the desire is to stop spam in personal inboxes, one can do it already, without legislation. So-called "handshake" or "challenge-and-response" email accounts do not allow any email through from strangers unless they respond to a "challenge," such as supplying a generated password or answering a query. In over two years, I've never received a spam in one such account that I use: That doesn't mean I won't. But because the most offensive spam is sent by automatic bulk mailing programs that aren't capable of receiving a reply, spam no longer appears in the inbox. Whatever legislators do, however, white-lists or such challenge-style systems are essential for children's accounts.

There are significant transitional costs to changing the default expectation from today's "everything comes in unless you say 'no'" to "nothing comes in unless you say 'yes,'" but the spam problem is so bad that there may well emerge a culture of tolerance, an expectation that e-mail recipients from now on will ask you, "Who's there?" at least the first time you come knocking.

Meanwhile, service providers need to get busy on standards, such as for authentication of senders. Identifiers or "seals" for trusted commercial e-mail could be a critical means of helping tomorrow's ISPs block unwanted e-mail, but it could require major reworking of Internet protocols, and unprecedented industry coordination. A new consortium including America Online, Microsoft, and Yahoo to establish Trusted Sender standards like those long called for by TRUSTe would bolster this approach.

Such major overhaul of the Net architecture has been likened to widening all the nation's roads six inches. It is a monumental undertaking. But if it truly is the case that lack of authentication and pricing is at the root of the spam problem, legislation doesn't directly solve those issues. It may be that a system in which originators of messages remain anonymous is altogether inappropriate for a commercial information society of tomorrow. Maybe it needs to be impossible, not merely illegal, to send a commercial email if the network owner can't discern who you are via some form of origin certification or digital signature. If so, that's a job for the industry that can't be replicated by passing a law.

Already Commissioner Orson Swindle of the Federal Trade Commission has indicated he thinks the industry can do far more to address the problem on its own, such as by granting users more control over their inboxes. ISPs might also limit the number of outgoing messages per subscriber account, for example. MSN Hotmail recently did so, and Yahoo did it long ago. Yahoo also recently implemented a sort of reverse challenge-response. Users who suddenly started sending in bulk found themselves challenged by Yahoo.

Today's flat fees for sending email aren't a fact of nature or a natural right. Ultimately, email "postage" or protocols that allow users or ISPs to charge fractions of a cent for receiving unsolicited email would end bulk spam once and for all. Bonded sender programs are already being set up that might anticipate such a sea-change. But such innovations would be a long way off.

Given the understandable desire to stop outrageous unsolicited email, it is all too easy for Congress to undermine legitimate commerce, communications, and free speech, and delay

needed changes in industry structure, relationships, practices and technologies. Meanwhile spam could continue pouring in from overseas. We need locked inboxes, authentication, and perhaps “postage” to allow users to customize their inboxes to reflect their own conceptions of “spam.” Those solutions are even better if they are harmonious with other priorities like cybersecurity. The industry needs to get busy before Washington does.

Whether or not Washington passes an anti-spam law this session, the industry must still grapple with what are fundamentally technological and economic dilemmas rather than legislative ones. If industry doesn’t resolve sender authenticating issues and end cost shifting, Congress will act—but without solving either problem.

###