Policy Analysis
No. 408 July 26, 2001

Why Canning "Spam" Is a Bad Idea

by Clyde Wayne Crews Jr.

Executive Summary

Everyone hates getting "spam." But does every unsolicited commercial e-mail deserve that derogatory label? Unsolicited e-mail can be annoying, but addressing the issue legislatively will create more hassles than does spam itself. It's not apparent that businesses selling legitimate products have any less right to use e-mail than anyone else, and laws targeting only the most egregious spam won't work, because perpetrators will simply relocate offshore. Spam legislation will create legal and regulatory hassles for mainstream companies, even as they increasingly embrace "opt-in," permission-based e-mail, which gives consumers the ability not to be contacted unless they want to be.

The basic instructions to Internet users worried about spam will always apply: Avoid posting your e-mail address, set up a "junk" e-mail account, and never respond to spam. Join services that take you off mailing lists. Increasingly, e-mail filtering can change the default, for those who want it, from today's "everything reaches your mailbox unless you say no" to "nothing comes in unless you say yes." Even the development of "postage" that shifts costs back to the spammer seems plausible.

We do not know what will ultimately count as "unsolicited" or "commercial" e-mail. Questions may include the status of political e-mailings or informational newsletters that link to for-profit Web sites or contain embedded ads. Even pop-up ads on the Web might become suspect in the aftermath of spam legislation.

At bottom, spam legislation kicks open the door to further regulation of business communications. That is risky, because marketing is essential to the growth of tomorrow's online services and technologies.

Financial remedies would create incentives for enforcers to go on "spam hunts," looking for evil embedded in every e-mail. That threat would keep many legitimate businesses out of Internet marketing altogether. Legislation, and the flurry of litigation that would result, should not be allowed to interfere with the complex relationships between businesses, consumers, and more than 5,000 Internet service providers.

Finally, legislative bans on false e-mail return addresses and bans on software that can hide identifying information would have significant implications for anonymous speech—a cornerstone of our Republic. Strange as it may sound, spam and the use of "spamware" are means by which individuals can maintain a cloak of anonymity.

The regulation of spam would make it all too easy to impede solicited mail, unsolicited mail that is nonetheless welcome, legitimate commerce, emerging Internet innovations, and even free speech.

Clyde Wayne Crews Jr. is director of technology studies at the Cato Institute.

Unsolicited commercial mail can be extremely irritating, rude, or obscene, but it is more an annoyance than an assault except in rather specific instances.

Introduction

In the escalating debate over the torrent of unsolicited bulk commercial e-mail, otherwise known as "spam," it is important to remember that not every unsolicited message is evil. Despite the indignation of a highly mobilized and engaged anti-spam contingent, the ideal amount of unsolicited commercial e-mail is not equal to "none" for everyone. Sometimes, commercial e-mail is welcome or otherwise considered "friendly," even if unsolicited.

Unsolicited commercial mail can be extremely irritating, rude, or obscene, but it is more an annoyance than an assault except in rather specific instances, such as when the sender is peddling fraudulent or phony goods or is impersonating someone else in the message's header information. Or the sender may be breaking a contract with an Internet service provider (ISP) that limits bulk mailing.

Laws presumably designed to halt the spam scourge would do more harm than good, however, especially on an Internet that, contrary to expectations, has fostered few profitable marketing and business models. That is not to say that spam is the road to success; it isn't. But invasive regulation of e-mail communications will have unintended (although not unforeseeable) consequences for online commerce, regardless of the impact on spam. Now is no time for tinkering. A recent report predicts that 80 percent of San Francisco's remaining Internet companies will fail in the coming months.[1] Banner ad click-throughs are down, as is the money spent on such marketing. Although unsolicited e-mail may be an annoyance to many of us, it is part of a larger picture in which companies and entrepreneurs are groping for ways to keep the Internet's services and options growing while making a profit. Spam legislation would be a significant new form of communications regulation, and the effects would not be easy to contain.

It is not a given that businesses selling legitimate products have any less right to use e-mail than anyone else. The Internet as it exists today is a public, open system, and no one can legitimately claim a right to exclude others according to his particular preferences. As in the offline world, the government's role should be limited to that of protecting citizens against force and fraud.

Solutions to e-mail intrusions are already available to individuals and ISPs, and more are on the way. Furthermore, we are seeing signs that the spam problem, although terrible, is not getting worse. Government should not use the novelty of the technology to justify intervention. Conditions are changing every day. Congress doesn't have all the answers to the spam problem, and government interference now could impede the emergence of superior solutions.

Besides, if the idea is to target the most annoying kinds of spam (LOSE WEIGHT FAST! MAKE MONEY AT HOME! XXX!), legislation will be difficult or impossible to enforce. The offenders can easily relocate offshore, out of the reach of U.S. legislation. The effect of a spam law will simply be to force mainstream companies to jump through yet more hoops. Legitimate companies will end up being targeted, and, of those, small business will suffer the most. As discussed herein, reputable companies are implementing user-friendly marketing policies, such as "opt-in" and "opt-out," of their own accord. In particular, the phenomenon of opt-in, permission-based e-mail, in which consumers expressly agree to receive e-mail from specific companies before they receive any, is on the rise. Such e-mail can look a lot like spam but is actually "friendly fire" (and boasts enviable click-through rates!).[2]

Not all unsolicited commercial e-mail is created equal. Nor are all ISPs, which, in one major proposal, would be given legislative immunity for good-faith efforts to block and sue the senders of what is believed to be spam, even in the absence of customer consent, and in spite of what might otherwise have been negotiated privately. That scenario would be a litigious nightmare, resulting in considerable confusion. Government should enforce private contracts regarding the delivery of such bulk mail, but it should not dictate the rules or facilitate one party's ability to set the terms unilaterally. It is ironic, to say the least, that the very Congress that "spams" us with more than 4,000 regula-

tions each year proposes to protect us from sales pitches by such draconian methods.

Spam is just one form of marketing and is arguably less invasive than door-to-door selling or telemarketing. There are clearly different levels of "guilt" with respect to spamming practices. It is best to allow people to decide for themselves whether or not to entertain sales pitches, particularly given the range of problems legislation would create. And to the extent that unsolicited marketing is responsible for the growth of the Internet and future communications options, the hindrance of commerce could hamper access for many people, resulting in a government-created digital divide.

How Big Is the Spam Problem?

It is easy to see why spam is widely used by the unscrupulous. It's as easy to send a million e-mails as it is to send one, and the spammer gets to pass the costs on to ISPs and users, or so it is alleged. Some organizations, like the Coalition against Unsolicited Commercial E-mail, have noted that spam accounts for about 10 percent of all e-mail traffic and has remained at about that level, even as the Internet has grown.[3] America Online has estimated that spam accounts for up to a third of its traffic.[4] Meanwhile, a recent and frequently cited study by the European Commission indicates that, although expensive, "it is safe to say the spam phenomenon is now in decline" and that spam had its "heyday" between 1995 and 1998.[5]

Although spam clearly remains a problem, a political fix would invite mischief. The debate is steeped in loaded language: take the word "spam" itself, or the depiction of gathering e-mail addresses as "harvesting." Some critics seem to detest unsolicited Internet commerce as a worldview, believe that marketers should never contact individuals until explicit permission has been given, and declare portentously that the "failure to control spam is the greatest economic tragedy of the Internet age."[6] Similar concerns were expressed when financial institutions opposed a variant of spam legislation in a March 20 letter to the House Energy and Commerce Committee. Spam critics fear that the marketing of preapproved credit cards will begin to take place online.[7] Other observers might see this evolution as a good thing. A commercialized Internet is critical to expanding online services. Needless intereference with Internet marketing would mean the loss of many services we get today.

Many ISPs like the idea of legislation to control spam, because large amounts of spam can hang up smaller networks that simply can't absorb the traffic. The control of spam lessens the burden of handling large amounts of traffic for larger networks too, even those not necessarily hostile to unsolicited mail. As Barbara Dooley, president of the Commercial Internet Exchange Association, has noted: "No one wants to stop legitimate marketing. We object to marketers shifting costs to the networks."[8]

The shifting of costs from spammers to ISPs is often noted, but it's important to recognize that those costs are not entirely unanticipated: ISPs do not typically go into the business unaware of the presence of spam. Between 1999 and 2000, for example, the estimated number of ISPs grew to more than 7,000, a 36 percent increase, despite the entrenchment of spam in the marketplace.[9] In fact, one reason that the cost of spam is difficult to ascertain is that ISPs think of dealing with spam as simply a cost of doing business.[10] Spam legislation might help some ISPs avoid undertaking certain costs of upgrading facilities and networks that they voluntarily plugged into the Internet. But that could damage the Internet as a whole if the amount of legitimate, multimedia traffic growth that emerges over the next few years dwarfs spam. Spam will grow but might become increasingly smaller as a proportion of total Internet traffic.

Some Internet users will, of course, be affected by spam more than others, regardless of aggregate levels. The real issue in dealing with spam is finding a way to shift the costs back to the spammer. The question is whether the best way to accomplish that is through the government or the marketplace.

The real issue in dealing with spam is finding a way to shift the costs back to the spammer. The question is whether the best way to accomplish that is through the government or the marketplace.

Legislative Proposals

There are three key pieces of legislation being considered so far in the 107th Congress. The Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 718) was introduced by Rep. Heather A. Wilson (R-N.Mex.). The House Energy and Commerce Committee markup of the bill (1) requires that senders give valid identifying information, (2) requires identifiers indicating that the message is unsolicited and offering the opportunity to opt out of future transmissions, (3) allows ISPs to set policies against bulk mail, and (4) allows recipients and ISPs to sue spammers. A bill of the same title sponsored by Rep. Wilson passed the House 427 to 1 in the 106th Congress but was never voted on in the Senate. Legislators are rethinking their rapid embrace of that legislation. Rep. Zoe Lofgren (D-Calif.), who had supported the legislation in 2000, said at a House Judiciary Committee hearing, "I question whether this is an appropriate area for legislation at all . . . people know how to deal with it now."[11]

The Wilson bill was narrowed in the House Judiciary Committee to criminalize bulk e-mail that contains falsified subject headers or originating e-mail addresses and to require that sexually oriented spam be identified as such. The competing versions will be reconciled by the House Rules Committee before floor action.[12]

Sen. Conrad Burns (R-Mont.) has introduced a related Senate bill, the bombastically named CAN SPAM Act of 2001 (S. 630), which omits the private right of action to sue spammers.

Rep. Bob Goodlatte's (R-Va.) Anti-Spamming Act of 2001 (H.R. 1017) would outlaw both unsolicited e-mail that falsifies header or routing information and the sale or distribution of "spamware" programs that aid such concealment. Rep. Rush Holt's (D-N.J.) Wireless Telephone Spam Protection Act (H.R. 113) would address the issue of wireless spam, which promises to be a hot button in the near future.

The bills just mentioned will be altered in upcoming negotiations, but many of their basic elements are likely to be part of future iterations of spam legislation.

Private Means of Coping with Spam

It is worth reviewing some of the means of coping with spam that are available today or on the horizon, because they help illustrate why legislation is not needed and underscore some of the problems, outlined in the next section, that legislation can create by changing communications rules in an adapting marketplace.

Individuals' Tools to Attack Spam

People like to have their cake and eat it, too. Many want an open Internet (which, after all, was the promise and attraction of the Internet)—as long as it's not too open. We treasure the freedom to contact anyone we choose but may not enjoy extending that freedom to others. But requiring e-mail users to give permission to senders would be a fundamental change in the rules. For better or for worse, the Internet has been, from the outset, an open network. Of course, everyone has the right to delete mail without opening it.

Many want an open Internet (which, after all, was the promise and attraction of the Internet)—as long as it's not too open. We treasure the freedom to contact anyone we choose but may not enjoy extending that freedom to others.

That said, people want the spam problem solved. At the individual user level, the basic instructions for avoiding spam still apply: Read the fine print before filling out online forms, don't post an e-mail address on Usenet newsgroup postings or in chat rooms (even "munging" the address with an insert like NOSPAM won't protect an e-mail for long),[13] and try to avoid posting an e-mail address on a personal Web site. If necessary, set up a separate "junk" e-mail account to use in online interactions. Finally, don't respond to spam, even to ask to be removed, since this is often just a trick to ensure that an e-mail address is live. Instead, report and send the spam to a service like SpamCop or your ISP, which will, in turn, report it to the spammer's ISP. Since most ISPs have "no spam" stipulations as part of their terms of service, this may help.[14]

Users can take additional action to preempt unwanted mail. For example, the Direct Marketing Association runs a list that Web surfers can visit and register to have their names removed from e-mailing lists. DMA member companies must abide by those pref-

erences. According to the site, "All DMA members who wish to send unsolicited commercial e-mail must purge their e-mail lists of the individuals who have registered their e-mail address with e-MPS [Mail Preference Service]."[15] The service can even block business-to-business e-mail, a growing concern lurking in the background of the spam wars. Of course, most spam comes from companies that are not members of DMA.

Beyond such preemptive moves, the filtering of e-mail is a common tactic for avoiding spam. E-mail filters can do a number of things: They can block spam by sending e-mail to a "bulk folder" if the e-mail is not specifically addressed to the recipient only but instead contains numerous hidden addressees. Filters can block on the basis of the sender's e-mail address (sometimes called "blacklisting") or on the basis of words in the subject line or body. The Hotmail e-mail system, for example, makes spam easy to deal with, even though the system is itself quite susceptible to spam. At the user's option, bulk mail goes into a special folder and is held there for two weeks and then automatically deleted. During that time, the user can open the folder and scan for legitimate mail that shouldn't have been routed there. Rather than opening and reading any of the spam, a user need only note legitimate messages and click the "This is not bulk mail" button. Messages from those senders will never be sent to the bulk bin again.

Increasingly, consumers can configure e-mail to accept only certain addresses ("white-listing"). If consumers so choose, the default can increasingly evolve from today's "everything comes in unless you say no" to "nothing comes in unless you say yes." SpamCop, for example, offers white lists or safe list filters, which can be integrated with existing e-mail accounts.[16]

E-mail tools for kids, such as that provided by E-mail Connection, can be set up so that a child can correspond with only parent-approved recipients, such as playmates and family members.[17] (Of course, problems of children's unattended use of the Internet go well beyond e-mail. But there are solutions for that, too. Some parents have opted to join private networks, such as eKids Internet and JuniorNet, in which only members of the network itself, not "outsiders" on the public Internet, participate. At the same time, many of the features of the public Internet are duplicated through partnerships, giving children the best of both worlds.)

Two potential ways of blocking spam, besides standard filtering, are the use of passwords and postage. Whereas filtering will zap some innocent e-mail and will "leak" spam into the regular mailbox, password and postage systems hold the promise of avoiding those problems. Such tools are truly novel, removing even the need for opt-out requirements, because spam simply won't reach one's inbox except on the user's terms. For example, one programmer offered, for several years, a program for Unix users in which the sender gets an automatic response containing a password when he sends an e-mail, unless he is listed in the recipient's "privileges database." The sender must then respond with the password embedded in the message. The initial autoresponse states: "Spam foiling in effect. My e-mail filter autoresponder will return a required e-mail password to users not yet in the privileges database."[18] Since spam is automatized with software that will never answer such a query, this process blocks spam.

On a more user-friendly basis, a company called MailCircuit offers spam-free e-mail services on what it calls its "Handshake System." The company ensures: "If you don't want it, you do not have to receive it," noting, "Our Mail Verification Program stops unwanted mail period."[19] By this unique method, when e-mail comes to a recipient, the sender receives an automatic message asking for a unique response. If the sender replies, he is added to the "friends" list, and future messages go through. Again, since spam is automatized, this process will stop it. If the spammer's e-mail is fake, he will not get the autoresponse, and the spam will not be seen.

As noted in the next section, techniques are emerging by which ISPs can charge "postage" to legitimate e-mailers. We might eventually see, in addition, mechanisms by which individuals are paid postage for receiving unsolicited mail

E-mail tools for kids, such as that provided by E-mail Connection, can be set up so that a child can correspond with only parent-approved recipients, such as playmates and family members.

(which might mirror the notice from sellers that is often seen on eBay: "I accept PayPal."). In some cases the recipient would collect the money. In others he might choose to waive the fee, particularly if the system were to expand beyond commercial e-mail to encompass all "unknown" e-mail.[20] These systems might entail massive reengineering of aspects of the e-mail communications infrastructure, however, and they would also diminish some of the open character that drew people to the Net in the first place.[21] But such tradeoffs are probably inevitable. What an innovation it would be for individuals, rather than the U.S. Postal Service, to collect postage! As they are starting to do with commercial mailers, ISPs may ultimately facilitate the payment of postage to individuals if the ISPs can share some of the spoils.

Blacklisting can lead to problems, such as the inadvertent blockage of non-spammers, but it is a perfectly legitimate exercise of property rights.

ISP Tools to Attack Spam

In addition to the filters used by consumers, various filtering options are available to ISPs, such as those that root out e-mail with terms like "XXX" or "Earn Money Fast!" ISPs are also able to block bulk mail that originates from dial-up accounts, which many spammers use to hide their header information.[22]

ISPs also block known spammers listed in directories such as the Mail Abuse Prevention System's Realtime Blackhole List.[23] Blacklisting can lead to problems, such as the inadvertent blockage of nonspammers, but it is a perfectly legitimate exercise of property rights. Some bulk mailers regard blacklisting as vigilante behavior, and disputes often arise. Granted, ISPs may be going overboard in some instances, for example, when blacklisting any Web site that sends spam or that offers software that could be used for spamming. But at least blacklisters are subject to market pressures and discipline. In one recent instance, New Zealand's largest ISP (Xtra), an accused spammer, sought to have itself removed from the Open Relay Behavioural Modification System blacklist. However, as the operator of the list says:

> What [Xtra] doesn't seem to understand is that the Internet is a cooperative of privately owned networks. . . . No one has the right to send e-mail anywhere. It is a privilege that is granted by the owners of those networks.[24]

E-mail marketers should be held to the terms of the contracts they make with ISPs. Those who are unfairly blocked can get around the blacklists by contacting the major ISPs directly to request reinstatement.

Increasingly there will be ways for ISPs to shift some of the cost and inconvenience of spam back to the spammer. One option is for ISPs to develop ways to charge for commercial e-mail. A company called ChooseYourMail "charges advertisers a delivery fee that is shared with the ISP. This enables the ISP to defray rising mail server costs and help keep monthly access fees low for their subscribers."[25] Such payment systems help place the burden where it belongs and are an early step toward "postage" for commercial e-mail on the Internet. This development meshes nicely with the concept of "permission marketing," which is changing the commercial mailing industry norms. In this paradigm, consumers opt in to receiving e-mail, as opposed to merchants sending it unsolicited.[26]

"Postage" need not be paid in cash if the intent is to shift costs back to the sender of unsolicited mail. It could instead be "paid" by the sender in consumed CPU (central processing unit) cycles.[27] In this scenario, the message would not go through until the sender's computer was forced by the recipient's to perform a mathematical exercise, which would weed out the automated spamming programs.

Other people envision a future in which ISPs would no longer be "naive," as they are today, and in which anyone sending e-mail would need a unique identifier, a "license" of sorts.[28] Such unique identifiers would constitute a market version of the "identifier" that legislation such as H.R. 718 would attempt to impose. ISPs and technology providers may need to "collude" to implement such postage and identifier systems on a wide scale, so they must be allowed to experiment.

Privately owned networks, such as eKids, will not experience significant problems with spam. Commercial e-mail policies would be spelled

out to members by contract. Such networks could disallow unsolicited mail altogether. Some of those that permit it may require spammers to pay fees to account for the strain they place on the network. Or, conversely, network owners could require that member ISPs maintain a capacity for a minimum volume of mail.

"Peer Pressure" on the Bulk Mail Industry

As already noted, permission-based e-mail is growing. This new industry is devoted to spelling out the differences between "permission e-mail" and spamming and touting the advantages of the former.[29] The embrace of this voluntary opt-in approach to marketing by online merchants is a new source of peer pressure on the commercial mailing industry. Practitioners hope to make e-mail less intrusive and more respectable—in other words, more welcome. What the market needs most now is time to adjust to these new realities, not legislation that might thwart them. Opt-in, permission mailing seems to be the future of mainstream Internet marketing because consumer response rates exceed those for unsolicited mail:

> Permission e-mail has been identified as the next generation of Internet marketing. Enjoying significant click-through rates over banner ads and other forms of online marketing, it has experienced phenomenal industry growth and has led Jupiter Communications to predict that commercial e-mail marketing will become a $7.3 billion business by 2005. Forrester Research reports e-mail use accounts for more than 35 percent of all time spent on the Internet and estimates that 50 percent of consumers will be communicating via e-mail by 2001. Clearly, permission e-mail has emerged as one of the most powerful Internet marketing mediums ever. [30]

Third-party stamps of approval will arise as bulk mailers seek to legitimize themselves. As Removeyou.com's Thomas Brock told the *Wall Street Journal*: "We are not here to kill the spam industry. We are here to save it. We are simply forcing the bulk-mail industry to do the right thing."[31] His group maintains a list of people who don't want to be spammed. When individuals forward spam to Removeyou, the company contacts the spammer and invites it to join. If the spammer joins, its lists will be purged of the addresses of those individuals who do not wish to receive unsolicited e-mail. This can help the e-mailer maintain a better image.

Problems with Government Regulation of Spam

Given the developments discussed above, it is apparent that in a number of ways the market is moving toward solutions to a problem that is arguably stabilizing. The fact that spam can be annoying isn't a sufficient reason for passing laws against it. The prospects for privately taming bulk e-mail are good, and legislation intended to target spam could hinder other methods of online commerce and impede private solutions. A legislative cure would be worse than the disease: It would create immense uncertainly and bring to bear needless, expensive enforcement and litigation costs. Moreover, most small businesses are not yet on the Internet. As they come aboard, they will not have an easy time getting over legislative hurdles to unsolicited commercial mail or competing effectively against established companies for whom e-mail marketing may not be crucial.

Loopholes in legislation, which could easily emerge from the give and take that will characterize a spam bill debate, could have unintended consequences. What if a loophole explicitly permits certain kinds of bulk mail that emerging market institutions would have chosen to shut out? For example, recent federal medical privacy standards granted to pharmacies the right to share consumer information with third parties, although consumers might have preferred to negotiate otherwise.

Another spam battleground will likely emerge in the area of wireless devices such as cell phones and hand-held computers. Ironically, it is the government's mandate that cell phones

The prospects for privately taming bulk e-mail are good, and legislation intended to target spam could hinder other methods of online commerce and impede private solutions.

Ironically, it is the government's mandate that cell phones incorporate 911 location capability that has swung the door open to spam in this particular arena.

incorporate 911 location capability that has swung the door open to spam in this particular arena. The mandate is costly, and the best way for manufacturers to pay for it is to allow marketers access to customers. Some consumers worry about the possibility of being tracked by wireless devices and getting electronic notification of discounts at stores they pass on the street and worry about the electronic profile that would emerge.[32] Nonetheless, the industry's trade associations, sensitive to public reaction and its impact on profits, are, of their own accord, devising opt-in standards that would ensure that no customer gets pitched without having granted permission.[33] Thus, it is noteworthy that even when government "subsidizes" unsolicited mail, peer pressure kicks in to control it.

Most legitimate vendors are increasingly offering opt-in or at least opt-out options for customers, and consumer protections are becoming quite sophisticated, yet easy to use. Although the uncertainties and regulatory hurdles that will come from legislation will hobble legitimate businesses, the laws will be unenforceable as far as the most offensive material goes, as these operations can easily relocate overseas. In fact, much spam already originates from Pacific Rim nations.[34]

What Will Count as Spam?

Spamming used to refer to the practice, by an individual, of posting the same message to numerous newsgroups.[35] Might the definition of illegal unsolicited e-mail change over time? Will it be sensibly defined in the first place? It is conceivable that, in the wide universe that is the Internet, spam could come to mean not just "unsolicited commercial" e-mail but other unsolicited communications as well.

It is uncertain what will ultimately count as unsolicited commercial e-mail. If a reputable company sends mail unasked but provides a return address and removes your name when requested, that would presumably be legal under proposed legislation. Businesses would get one bite at the apple, so to speak. But that could easily change as spam legislation is further debated and modified. Some consumer groups are calling for a "federally mandated 'opt-in' policy on commercial e-mail."[36] Such pressure will not go away, and today's legislative prospects are the camel's nose under the tent. Opt-in laws would outlaw all contacts except for those specifically agreed to in advance—a clear constitutional problem and a death sentence for electronic commerce (particularly for small firms).

Levels of abuse vary. Some spammers send only a handful of mailings at a time, say a hundred or so targeted e-mails, and work diligently to remove from their list those who want no further contact. Others exhibit contempt for those who don't want their messages.[37] Legislation would inappropriately lump those groups together.

As it stands, H.R. 718 defines a "commercial electronic mail message" as one that "primarily advertises or promotes the commercial availability of a product or service for profit or invites the recipient to view content on an Internet Web site that is operated for commercial purpose." That is quite a loose definition. What will count as "primarily," for example? Many newsletters that are not wholly commercial include links to Web sites that are run for profit. Is that spam or not? Even electronic newsletters from media services, which sometimes contain advertisements and links between stories, could conceivably face problems. It is unfair to treat ads differently just because they happen to be part of a news service, and someone will inevitably point that fact out. The media business is for-profit, after all.

Even organizations that are primarily informational in nature, perhaps even labors of love (say a gardening Web site) that allow sponsors to insert brief advertisements in e-mail newsletters, could face trouble from spam legislation. And, given the penalties in the proposed legislation, there are clearly incentives to go on spam hunts, looking for evil embedded in every e-mail.

In such an environment, regulation could lead to better-disguised spam, more annoying than today's blatant version. Spam legislation that attempts to split hairs between what is commercial and what is not could lead to our receiving dubious "public service announcements" that happen to include an offer for a product somewhere down the line.

Another unanswered question regarding the definition of spam is the status of political e-mailings. Some Internet users may already get more junk mail from their representatives than they do from spammers. Rep. Bob Goodlatte (R-Va.) mentioned "chain letters" in testimony offered to the Senate.[38] Would those be subject to legislation? Gartner Group Inc. has referred to potentially nuisance e-mail in the workplace as "occupational spam," the removal of which would create "a 30 percent savings in the time that is usually lost in handling unproductive e-mail."[39] Are forwarded jokes or hoaxes part of tomorrow's spam problem, too? What about e-mailed press releases ("For Immediate Release") blasted from public relations firms? The broadening of what is classified as spam is not that remote a possibility.

Unintended Impacts on the Right to Anonymity and Free Speech

Mandatory opt-in rules for e-mail have serious implications for free speech. Spam is, at bottom, merely advertising. Such business speech is simply speech that proposes a transaction. While anti-spammers believe customers should ask before being solicited, there is a viewpoint among some bulk mailers that the Internet is a public resource, created in part with taxpayer funds, and that e-mail addresses, like street addresses, are a matter of public record.[40] To the extent that is true, there is a problem in saying that we shall enjoy the freedom to contact or visit companies anytime we like, but they can't contact us. Even the opt-out requirement in legislation like H.R. 718 can be problematic: does it preclude all future contact from a company by e-mail or just contact about a particular subject or offering? It is fine for consumers to effect complete blackouts from companies if they like. But implementing this with federal legislation is overly heavy-handed, arguably even a violation of free speech, and better left to emerging contractual relationships.

In addition, such limitations would set a troubling precedent. Could advertising restrictions spread elsewhere, for example, to the increasingly common Web pop-up ads? Some people might argue that those are even more intrusive than unsolicited e-mail.

Rep. Goodlatte's H.R. 1017 would ban the use of false e-mail return addresses in commercial e-mail, as well as the software used to hide header information. The proposed requirement that valid header information be shown has significant implications for free speech because of its impact on legitimate anonymous speech by senders. As strange as it may sound, spam and the use of spamware happen to be means by which individuals can maintain a cloak of anonymity. Anonymous speech is a cornerstone of our Republic. Thomas Paine's *Common Sense* was signed "An Englishman." The *Federalist Papers* were signed "Publius."[41] Given that the Internet can serve as the "anonymous pamphlet" of today, individuals must retain the right to safeguard their anonymity even in (or perhaps especially in) a mass-communications tool like e-mail.[42] Another twist on the theme of anonymity is Spam Mimic, a Web site that disguises a normal message by making it look like spam so that e-mail "sniffers" might be more likely to ignore it.[43]

Individuals must not lose the right to send anonymous bulk mail, and hiding one's identity in spamware is the practical means of doing so. Very simple, thumbnail-sized code may be enough to forge the "from" line of an e-mail.[44] Yet H.R. 1017 could make such simple but critical bulk-messaging software illegal.

As we sit on the cusp of a revolution in peer-to-peer networking, the Internet is the most significant, largely unregulated, open forum we have. The benefits of leaving it alone, despite problems with some of the "communicators" that populate cyberspace, vastly outweigh the potential costs.

In a way, the spam debate helps illustrate that the underlying Internet debate is not really about privacy, even though that gets a lot of media attention these days. The real question is whether the government will allow individuals to remain anonymous when they actually have the technological means to do so.

Spam legislation would take away with one hand what the government proposes to give with the other in the high-profile privacy

As strange as it may sound, spam and the use of spamware happen to be means by which individuals can maintain a cloak of anonymity.

debate now taking place. Anti-spam legislation would artificially damage the ability of individuals to safeguard their own privacy and would help set the stage for unnecessary privacy regulations. That is the kind of unintended consequence that can result when the government believes regulation is the solution to every problem.

Federal Immunity for ISPs Will Distort Emerging Internet Markets

Some versions of legislation would explicitly permit both blocking of commercial e-mail and fines by ISPs. ISP policies on blocking spam are certainly appropriate. Putting such policies into federal law would, however, amount to an unwarranted federalization of contracts.

ISPs already have the right to block spam, but some proposed legislation would give them financial incentives to do so. Since many legitimate communications can easily be confused with spam, legislation could induce ISPs to block them more readily. Today's ISP-initiated efforts to block spam are "regulated" by the market, which provides some restraint. Monetary legal remedies, however, along with legal immunity for ISPs, would generate unnecessary confusion, frivolous lawsuits, and interference with legitimate marketing in a marketplace that is already developing spam remedies on its own.

Legislation should not interfere in the complex relationships between ISPs, marketers, and users. The ability of ISPs to block e-mail with impunity, even in good faith, as specified in the legislation, casts doubt on the promise that prearranged or permission-based e-mail would get delivered. Indeed, an amendment to the version of H.R. 718 marked up in the House Energy and Commerce Committee gives a sweeping opt-out right to ISPs, allegedly similar to the one given consumers.[45]

Just as ISPs might engage in good-faith blocking, companies sometimes send e-mail by mistake or with no ill intent. Yet the good-faith clause would allow an ISP to block out and sue companies, or even smaller competing ISPs, that may have been wrongly accused of being a source of spam.[46] Recent testimony in the Senate on spam legislation noted how customers can be "cut off" without their knowledge:

> We are concerned about reports that ISPs, in their eagerness to help their subscribers avoid receiving unwanted UCEs [unsolicited commercial e-mails], may block e-mail that subscribers not only want, but have specifically contracted to receive as part of an electronic business relationship. . . . [The bill] does nothing to prevent this from happening, and does not even require ISPs to give notice to consumers that they intend to block, or that they have blocked, the transmission of e-mail either in general or from particular senders.[47]

Spam has been around for a long time, predating many ISPs that nonetheless chose to hook up to the Net. Not all ISPs are created equal, and some are even "spam-friendly." For example, in one case, a bulk e-mailer called MonsterHut won a temporary injunction requiring an ISP to continue transmitting bulk mail over its network on the basis of a contract specifying that MonsterHut had the right to do so.[48] Interestingly, while the population of ISPs has grown despite the existence of spam, some people believe it is the ISPs whose days are numbered, arguing that the market is going to gravitate toward fewer large providers as the broadband Internet grows and eventually overtakes dial-up services.[49] If that occurs, the remaining ISPs could wield greater contractual control over the bulk e-mail moving through their systems, further rendering legislation unnecessary.

Legislation that would endow ISPs with significant new power would disrupt permission-based e-mail alternatives, just as they are gaining a foothold. Legislation, as Jerry Ceresale of DMA put it, "doesn't account for prior relationships."[50] It will become increasing common for people to transfer commercial agreements to the online world, yet spam legislation would needlessly put such arrangements at risk.

Spam legislation would take away with one hand what the government proposes to give with the other in the high-profile privacy debate now taking place.

Will ISPs know, care, or bother to keep track of the fact that a consumer has signed up, whether offline or online, to receive information from, for example, Sears, Gap, or Tower Records? Will an ISP block mailings from the Scotts Company reminding registered customers when to put down fertilizer and grass seed? Breaking the shrink-wrap and lid on new software can indicate acceptance of the software's usage agreement, and installation of the software can automatically send "home" over the Internet the user's consent to receive future e-mailings and updates. Will ISPs interfere with those communications? As friendly commercial e-mail traffic grows, new regulations could create problems. Those transmissions may increasingly contain critical or time-sensitive information, such as financial data. Similarly, items like notices to members from trade associations or clubs could be blocked in error. In addition to the lawsuits that would be filed by ISPs against alleged spammers, we could see an overwhelming amount of litigation resulting from interference with private communications. Mark Lackritz, president of the Securities Industry Association, characterized H.R. 718 as a "trial lawyer's relief act."[51]

According to the sponsors of H.R. 718, a "pre-existing" relationship would allow a company to continue contacting the customer by e-mail in spite of the legislation. In addition to the risk that such e-mail would inadvertently be blocked, that provision could lead to a scramble by companies to collect personal data that they might otherwise not have bothered about.[52] There's nothing wrong with accumulating such information, but creating artificial pressure to sign up customers in advance of sweeping anti-spam rules (H.R. 718 would take effect 90 days after enactment) seems counter to the spirit allegedly motivating this legislative push.

When ISPs reduce traffic unilaterally, consumers may be free of spam, but they may also miss out on desired communications. Legislation would relieve ISPs of critical market incentives to create superior solutions, such as "postage" systems, whereby ISPs and their consumers get paid for each piece of unsolicited commercial mail they accept. This is not to say that the consumer is entitled to such payment but that such an outcome might be a sensible resolution of the spam problem. A regulatory "solution" could foreclose what could be a unique opportunity.

A Spam Identification Requirement Creates Problems

Another problem is establishing what qualifies as "clear and conspicuous" identification of spam in a message header, as some proposals would require. Usually, spam is obvious to the recipient at first sight. But legislation would require an explicit identifier in the heading of the e-mail, such as the word "SPAM."

The intent of that requirement seems to be to aid spam filters, but that might not be the result. Filtering technologies may be moving in directions that would be impeded by mandatory identifier information. Those requirements may also conflict with other types of private identifiers for solicited or unsolicited commercial e-mail. Mandatory identifiers could also interfere with "preview screen technology used by many consumers to rapidly screen messages and their content."[53] Besides, such tagging might require companies to obtain legal counsel on what counts as "clear and conspicuous," leading small or reluctant businesses to avoid e-mail altogether.

Identifiers would hurt small businesses in particular by unfairly stigmatizing unsolicited mail. For example, identifiers would likely fail to distinguish between "XXX" and, say, "home gym equipment" or "flower seeds," an important distinction in the minds of many consumers. Identifiers could also cause confusion in cases in which messages are only partly commercial.

Spam Legislation Can Hinder Emerging Messaging Technologies

The desktop is today's dominant means of accessing the Internet, but it is entirely conceivable that, over time, it will decline significantly in importance relative to mobile and other devices (hand-helds, cell phones, the Carrier/GE Internet-connected thermostats, automobiles, and so on).

Another problem is establishing what qualifies as "clear and conspicuous" identification of spam in a message header. . . . The intent of that requirement seems to be to aid spam filters, but that might not be the result.

At bottom, what's being proposed with spam legislation is the further regulation of communications. E-mail just happens to be the format of the day that lends itself to marketing.

Those are struggling industries and services, and new marketing strategies will be needed if they are to proliferate. Legislation impeding commercial e-mail could stall them. Strategy.com, for example, is facing severe hard times after parent MicroStrategy disclosed in 2000 that it had overstated sales and earnings. Strategy.com also faces a skeptical venture capital environment.[54] But the company had been one of the most prominent outfits with a business plan centered on offering targeted services to consumers over remote devices. Artificial restrictions on commercial e-mail are the last thing companies in these struggling service areas need.

Legislative precedent could also hinder emerging services such as Instant Messaging (the compact nature of IM may not lend itself to opt-out messages or identifiers), advertising on the eventual wireless Web, peer-to-peer interactions, and even services like the Internet faxing tools offered by J2 Global Communications (formerly Fax4Free.com) or eFax.

At bottom, what's being proposed with spam legislation is the further regulation of communications. E-mail just happens to be the format of the day that lends itself to marketing. As noted, even the adoption of pop-up ads on the Web would be suspect under spam legislation. After all, no one explicitly asks for those ads. Interestingly, spam legislation limiting e-mail marketing could unintentionally promote pop-up marketing in the short term, leading to yet another backlash.

Spam Legislation Is a Pathway for Ill-Considered Privacy Legislation

Some Internet users claim that spam violates privacy. Spammers use data robots to "harvest" e-mail addresses from newsgroups and Web sites; however, they do not typically know anything about the individuals they bombard with e-mail. But if legislation imposes mandatory opt-in or opt-out policies, or both, with respect to marketing, that will pave the way for broader privacy legislation that could have several negative effects.

Tools to secure Internet privacy are improving all the time, with new browser technologies that police Web sites according to user preferences being just one of many options available to consumers. Consumers share no single level of privacy, and no government rule is capable of acknowledging that fact.

Levels of privacy protection are competitive features, as they should be. Markets are essential to providing the mix of features people desire. The proper role for government is to enforce privacy contracts when they are violated by the companies that offer them, not to dictate such contracts in legislation.

Privacy legislation, particularly the opt-in variety that is so admired, also violates free speech. Even if corporate free speech is the initial target, media speech could easily end up in the crosshairs. Privacy is a key value and people want it protected. Ultimately, the question is, who provides the best discipline, markets or politicians?

Spam legislation amounts to a stealth privacy bill, in the sense that it seeks to impose the rudiments of ill-considered privacy legislation in the presumably narrow arena of unsolicited e-mail. But this opens the door to sweeping anti-commercial policies and a range of unintended consequences. One can easily anticipate the alleged "reasonableness" that a future legislator might invoke in applying the anti-solicitation principles of spam legislation to the Internet at large: "My new legislation simply applies the reasonable consumer protection principles embodied in 'opt out' language from spam legislation to Web sites and pop-up ads."

Unreasonable Statutory Penalties Create Mischief

The fines stipulated in proposed legislation exceed the actual harm done by typical spam. Remedies of $500 per incident (up to a $50,000 maximum), as appeared in the version of the Wilson bill marked up by the Commerce Committee, would be off-putting to many small businesses thinking of trying to conduct e-mail marketing. The risk of being sued wrongly is obvious. Surely, it's not that much of a burden to delete unwanted e-mail or take other steps to not receive it in the first place. The level of federally specified remedies creates

significant potential for mischief. If people are going to get $500 for every unwanted e-mail, spam hunting could be much more lucrative than a job.

E-mail has always operated on the principle that everyone need not grant explicit permission to be contacted, which is arguably the essence of the Internet revolution. If that premise were to be reversed and penalties added, that would represent a fundamental change, offering plenty of opportunity for mischief. For example, e-mail could come from a familiar seller, but a user could claim he didn't remember consenting and could sue. Often, consumers sign up with merchants who indicate they may pass on the information, although the consumer doesn't explicitly give permission.

Ironically, the end result of spam legislation could be the creation of hordes of lawyers specializing in offering to help individuals lay claim to the $500 remedies they are "entitled" to. One must wonder, would those solicitations qualify as spam?

Conclusion

The Federal Trade Commission already has power to "prosecute fraudulent or misleading commercial e-mails."[55] States, likewise, have powers to prosecute fraud. Some e-mail pitches are clearly fraudulent, and some spam accounts are even set up with fake or stolen credit cards.[56] Those should be targeted. Otherwise, it's better to let existing and emerging market tools address the spam problem than to risk the harmful impacts of legislation on legitimate commercial e-mail, emerging Internet communications methods, and free speech. ISPs should, and do, have a right to block unsolicited commercial e-mail. Such private efforts by ISPs to block spam do not constitute state action—the networks are private property, after all. But federally promoted incentives to block spam with impunity, and to sue the alleged offender when private contracts may have evolved otherwise, will create unnecessary chaos.

The government can't stop spam. In the final analysis, the market will have to do the heavy lifting. Regulation is likely to simply harm legitimate commerce. In trying to legislate against unsolicited mail, it is all too easy to hamper the flow of solicited mail, too. Congress should resist the temptation to pass clumsy and intrusive laws in response to constituents' every petty annoyance.

The government can't stop spam.

Notes

1. Noted in Elisabeth Goodridge, "Bleak Future Predicted for San Francisco Internet Firms," *Information Week.com*, March 29, 2001, http://www.informationweek.com/story/IWK20010329S0002.

2. The term "friendly fire" was used by columnist Leslie Walker in "Buried under a Mountain of Spam," *Washington Post*, May 3, 2001, p. E8.

3. John Mozena, cofounder and vice president, Coalition against Unsolicited Commercial E-Mail, as cited in Jim Hu, "Yahoo Adds Spam Filter to E-mail, but Will It Work?" *CNET News.com*, December 1, 1999, http://news.cnet.com/news/ 0-1005-200-1476013.html.

4. Cited in Maureen Sirhal, "Experts Struggle to Gauge Impact of 'Spam,'" *National Journal's Technology Daily*, May 7, 2001, p. 4, http://nationaljournal.com/about/technologydaily/.

5. Quoted in ibid.

6. Jason Catlett, president and CEO, Junkbusters Corp., Testimony and Statement for the Record on Unsolicited Commercial E-mail before the Communications Subcommittee of the Senate Committee on Commerce, Science, and Transportation, April 26, 2001, p. 2.

7. Jennifer DiSabatino, "Privacy Advocates Say Amended Spam Bill Lacks Teeth," *Computerworld*, April 17, 2001, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59815,00.html.

8. Quoted in Michael Schroeder and Glenn R. Simpson, "Lobbying Effort Fails to Block 'Spam' E-mail Bill," *Wall Street Journal*, March 29, 2001, p. A4.

9. Cahners In-Stat Group, "National ISPs Stand to Gain Most in Growing U.S. Market," September 25, 2000, http://www.instat.com/pr/2000/is0004sp_pr.htm.

10. Noted in Sirhal, "Experts Struggle," p. 4.

11. Maureen Sirhal, "Lawmakers Question Need for Regulation of Spam," *National Journal's Technology Daily*, May 10, 2001, http://nationaljournal.com/pubs/techdaily/pmedition/tp010510.htm.

12. Adriel Bettelheim, "House Judiciary Committee Narrows Scope of Bill Aimed at Regulating 'Spam,'" *CQ Weekly*, May 26, 2001, p. 1262.

13. See http://www.antionline.com/features/jargon/spamblock.html.

14. Noted in J. D. Biersdorfer, "To Protest Unwanted E-Mail, Spam Cop Goes to the Source," *New York Times*, June 24, 1999, http:// www. nytimes.com/library/tech/99/06/circuits/articles/24spam.html.

15. The DMA's list is available at http://www.e-mps.org/en/.

16. See, for example, David P. Hamilton, "You've Got Mail (You Don't Want)," *Wall Street Journal*, April 23, 2001, p. R 21.

17. Information is available at http://www.e-mail-connection.com/EMKFINAL.html.

18. See http://www.uwasa.fi/~ts/info/spamfoil.html.

19. For an explanation of the process, see http://www.mailcircuit.com/handshake.htm.

20. See, for example, Declan McCullagh, "Consuming Spam Mail," *Contributors' Forum*, Library of Economics and Liberty, February 12, 2001, http://www.econlib.org/library/columns/McCullagh spam. html.

21. Paul Hoffman and Dave Crocker, "Unsolicited Bulk E-Mail: Mechanisms for Control," *Internet Mail Consortium Report: UBE-SOL*, May 4, 1998, http://www.imc.org/ube-sol.html.

22. Hamilton.

23. See http://www.mail-abuse.org.

24. Quoted in Michael Foreman, "Xtra May Use Court to Get Off Blacklist," *New Zealand Herald Online*, May 1, 2001, http://www.nzherald.co.nz/storyprint.cfm?storyID=184372.

25. ChooseYourMail, http://www.mailcircuit.com/cym.htm.

26. See, for example, Linda A. Goldstein, "Permission E-Mail Marketing vs. Spamming," *Digitrends.net*, November 24, 2000, http://www.digitrends.net/marketing/13640_12335.html.

27. McCullagh, "Consuming Spam Mail."

28. Michelle Finley, "Other Ways to Fry Spam," *Wired News*, April 24, 2000, http://www.wired.com/news/print/0,1294,35776,00.html.

29. See, for example, Walker, p. E8; and Goldstein.

30. YesMail.com, "About Permission e-mail," http://www.yesmail.com/learn/.

31. Quoted in Hamilton.

32. For an overview of this issue, see Heather Fleming Phillips, "Wireless Industry Treads Carefully on Privacy," February 7, 2001, http://www.siliconvalley.com.

33. See, for example, Simon Romero, "Locating Devices Gain in Popularity but Raise Privacy Concerns," *New York Times*, March 4, 2001, http://www.nytimes.com/2001/03/04/technology/04LOCA.html.

34. Noted in McCullagh, "Consuming Spam Mail."

35. Noted in James W. Butler III and Andrew Flake, "The Effective Control of Unsolicited Commercial E-mail," Internet Policy White Paper, U.S. Internet Industry Association, September 1988, p. 1, http://usiia.policy.net/pubs/.

36. Maureen Sirhal, "Anti-Spam Bills Debated at Hearing, in Letters," *National Journal's Technology Daily*, April 26, 2001, http://nationaljournal.com/pubs/techdaily/pmedition/tp010426.htm.

37. Geoff Duncan, "Those Bulk E-Mail Blues," *TidBITS*, September 30, 1996, http://db.tidbits.com/getbits.acgi?tbart=00863.

38. Bob Goodlatte, Testimony on Spamming before the Communications Subcommittee of the Senate Committee on Commerce, Science, and Transportation, April 26, 2001, http:// www.senate.gov/~commerce/hearings/0426buc.PDF.

39. "Please, Don't Share," Sidebar in DiSabatino, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO59815,00.html.

40. Duncan, http://db.tidbits.com/getbits.acgi?tbart=00863.

41. See Jonathan D. Wallace, "Nameless in Cyberspace: Anonymity on the Internet," Cato Institute Briefing Paper no. 54, December 8, 1999, p. 2, http://www.cato.org/pubs/briefs/bp54.pdf.

42. Ibid.

43. The Spam Mimic Web site is http://www.spammimic.com.

44. See, for example, Declan McCullagh, "Use a Spam, Go to Prison," *Wired News*, March 24, 2001, http://www.wired.com/news/print/0,1294,42599,00.html.

45. Noted in Adam S. Marlin, "Anti-Spam Bill Approved by Panel over Industry Objections," *CQ Daily Monitor*, March 29, 2001, p. 6.

46. See, for example, U.S. Internet Industry Association, Letter to Rep. Heather Wilson, February 17, 2001. Copy in author's files. The USIIA can be contacted at http://www.usiia.org/contact. html.

47. Jeremiah S. Buckley, general counsel, Electronic Financial Services Council, Testimony before the Communications Subcommittee of the Senate Committee on Commerce, Science, and Transportation April 26, 2001, p. 3, http://www.senate.gov/~commerce/hearings/0426buc.PDF.

48. Stefanie Olsen, "Giving Spam the Network Boot," April 19, 2001, http://news.cnet.com/news/0-1005-200-5668645.html.

49. Nico Detourn, "The High-Speed Decline of the ISP," *Motley Fool*, December 13, 2000, http://www.fool.com/Server/FoolPrint.asp?File=/news/2000/twx001213.htm.

50. Quoted in Declan McCullagh and Ryan Sager, "Cooking up a Revised Spam Bill," *Wired News*, March 27, 2001, http://www.wired.com/news/print /0,1294,42630,00.html.

51. Quoted in Sirhal, "Lawmakers Question Need," p. 6.

52. Butler and Flake, p. 8.

53. Ibid.

54. See Cynthia L. Webb and Dina ElBoghdady, "MicroStrategy Unit to Slash Staff: Strategy.com Will Reduce Its Workforce by Two-Thirds," *Washington Post*, May 5, 2001, p. E1.

55. Noted in Sirhal, "Anti-Spam Bills Debated."

56. Hamilton.

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before congress. Contact the Cato Institute for reprint permission. Additional copies of Policy Analysis are $6.00 each ($3.00 each for five or more). To order, or for a complete listing of available studies, write the Cato Institute, 1000 Massachusetts Ave., N.W., Washington, D.C. 20001, call toll free 1-800-767-1241 (noon - 9 p.m. eastern time), fax (202) 842-3490, or visit our website at www.cato.org.