

Spam

A White Paper on Unsolicited Commercial E-mail

Robert Doss
National Consumers Alliance
Pensacola, Florida
© 2003 All Rights Reserved

Prologue

CONTENTS

Prologue...1
Disinformation and the Spam Problem...1
Recognizing Spam and Spammers...2
Locating Spammers...6
A High-Tech Protection Racket...7
Filtering Much More Than Spam...7
Protection Through Innuendo...8
Filtering Spam or Filtering Competition?...9
Spam at the Bar of Justice...10
Consumers Taking Control...11

Few issues have agitated American consumers in recent years like commercial e-mail has. Commercial e-mail has been prominent as a focus of media, social, and legislative attention while initiatives claiming to battle commercial e-mail, particularly *unsolicited* commercial e-mail, have been plentiful. Even so, few people really understand the problem, and efforts to defeat it have been consistently fruitless.

Unsolicited commercial e-mail has been a difficult issue to handle, unnecessarily complicated by those who have had an interest in defining and describing it to us and telling us what to do about it. What they've told us hasn't worked; so now, it's time for us to sink our own teeth into the problem and take care of it ourselves.

Disinformation and the Spam Problem

Defeating *any* problem relies largely on a thorough understanding of that problem. Therein rests the challenge in dealing with commercial e-mail, specifically *unsolicited* commercial e-mail or "spam." The chief reason we have proven utterly ineffective in handling spam is that we have bought in to a mischaracterization of the nature and scope of the problem. Not knowing what the problem is, how it is manifested, what its strengths and weaknesses are, and what its intrinsic characteristics are have brought tactical failure at every turn.

The word "spam" has not only become part of the popular vernacular, it has also been popularly misapplied to encompass legitimate e-mail advertising. We know how frequently and persistently we hear the term "spam" applied to virtually all unwanted e-mail and the pejorative "spammer" applied to all commercial e-mailers. The word spam is now even applied to *any* unwanted or obtrusive marketing material.

While labeling these plagues as spam makes villainizing them more convenient, it is not helpful in handling them effectively and constitutionally. There are a number of lawful activities that we might consider unwanted or obtrusive, like television commercials, but they are protected commercial speech. This hyperactive mischaracterization of the spam problem has muddled our understanding of what unsolicited commercial e-mail really is and created a highly lucrative counter-market for those who profit from fighting this evolving "spam" problem. This mischaracterization has made efforts to defeat genuine spam *counterproductive* and has rendered our interaction with legitimate commercial e-mailers *unproductive*.

While consumers have struggled to get the best of the spam problem, this rampant effort to mischaracterize the problem has resulted in the broadcast of false information to them, thus disguising the truth about commercial e-mail and frustrating meaningful progress in seeing it resolved. Lacking a clear picture about what spam is, who sends it, and how best to deal with it, consumers remain frustrated in their attempts to overcome it. This disinformation has been employed strategically by some to play on the public's insecurities and has been seeded with a grain of truth here and



there to strike a chord with consumers. In the hands of an unwitting public, the disinformation has evolved as a powerful and long-lived perception of reality.

Thus, our failure – or our inability – to handle the spam problem effectively has generated a crisis of confidence that threatens the reliability and cost-effectiveness of the Internet as a legitimate and productive vehicle for interstate commerce. Recognizing which e-mail is spam and which e-mail is not spam and dealing with each accordingly is essential if we are to see Internet commerce achieve its productive potential. Without a doubt, the mischaracterization of the spam problem is hurting eCommerce.

A certain amount of what we often regard as "spam" might be unwanted, but it's not spam. Unwanted commercial e-mail is a problem, but it's not the same problem that spam is.

Recognizing Spam and Spammers

At the outset, we must rebuke the suggestion that bulk e-mail, commercial e-mail, and e-mail we just don't want is necessarily spam. By definition, spam has three features: (1) It is unsolicited, (2) It is commercial, and (3) It is e-mail. Otherwise, it's not spam.

Where we have trouble in distinguishing spam from other commercial e-mail resides in accurately defining its "unsolicited" quality. This is confusing to us because we sometimes equate bad Internet etiquette to illegal behavior. We think that we have to specifically and directly ask for commercial e-mail to be sent to us for it to be legally considered "solicited" and that everything else is spam. We get tied up over opt-in, opt-out, and permission-based parameters when most state laws have no such stipulations.

Half the states in the Union have no restrictions on unsolicited commercial e-mail at all and most of those that do have restrictions, have established that e-mail is "solicited" if there is a preexisting business or personal relationship between the initiator of the commercial e-mail and the recipient.

Regardless of what we might all agree is good Internet etiquette, laws in many states require only that a recipient has to have done business of some kind with the mailer or with an affiliate of the mailer in order to constitute a preexisting relationship. While a consumer might not believe he has a preexisting business relationship with a company, in fact, he might have. Thus, a certain amount of what we often regard as "spam" might be unwanted, but it's not spam. Unwanted commercial e-mail is a problem, but it's not the same problem that spam is.

We would do well to recognize that, generally speaking, there are currently three types of commercial e-mail: (1) Solicited commercial e-mail that we want, (2) Solicited commercial e-mail that we don't want, and (3) Unsolicited commercial e-mail. Until the definition of what is considered "solicited" or a "preexisting business or personal relationship" is consistently, clearly, and constitutionally established, we will continue to receive legally-protected e-mail we don't want. Reclassifying what is currently solicited e-mail that we don't want as "spam," however, will not solve our problem. It might make us feel better, but it won't fix anything.



E-mail users who want to avoid showing "signs of life" should not open spam e-mail messages and they should disable "preview" options in their e-mail programs that essentially open e-mail messages automatically.

Spammers don't care how we define "solicited" or "a preexisting business relationship." While we squabble over etiquette, they will continue to crash the party, employing an assortment of nefarious methods by which they get our e-mail addresses. They can create lists of tens of thousands of addresses, sorted according to a variety of profiles in a matter of a few hours, depending on the speed of their Internet connection.

Quite often, they use "spambots," to scour the Internet for e-mail addresses so they can harvest them. Spambots search web pages, often according to a search criteria and scrape e-mail addresses from them. Spambots also search newsgroup postings, Internet bulletin boards, and chatrooms for e-mail addresses in much the same way. The software collects the data from Internet content and returns information to the harvester in the form of a table of e-mail addresses.

Spammers also use name or word generators that literally run through the alphabet and create thousands of name possibilities to attach to the prefix of your e-mail address (in front of the @aol.com or @yahoo.com portion of your e-mail address, for instance). They create a list of potential e-mail addresses and blast out e-mail messages with half a dozen addresses on each one, looking for a nibble. When they see that you've opened the e-mail, you're added to an "improved" list.

Keeping you from being nabbed by a name generator is part of the reason ISP's recommend using a mix of letters and numbers in personal e-mail addresses. Anyone who has tried to apply for an e-mail address and found that the name was already taken shouldn't be surprised that these generators can be so productive in creating e-mail addresses that work.

There is a bit of "conventional wisdom" that suggests that e-mail users can essentially subscribe to a list by clicking on an "unsubscribe" link in an e-mail message. E-mail users are told that they shouldn't click on unsubscribe links because doing so verifies to the spammer that the e-mail account is alive, active, and well. Rigging unsubscribe links in this manner is a bit old-fashioned these days to the extent that most "bad" unsubscribe links don't collect information, they just don't work.

The real legwork in the confirmation of active e-mail addresses is being performed by "tracking pixels," often little bits of code in the form of tiny transparent images that collect information such as your IP address, the date and time you accessed your e-mail, your e-mail scrolling and clicking actions, your recent browsing history, your browser version, and any number of other bits of information. Using tracking pixels is faster, more informative, more convenient, more responsive, and more conducive to the compilation of marketing data than a spying unsubscribe link. E-mail users who want to avoid showing "signs of life" should not open spam and they should disable "preview" options in their e-mail programs that essentially open e-mail messages automatically, thereby triggering pixel action. They also shouldn't use spam filtering and reporting software that essentially does the same thing.

It is not altogether astonishing that we look at the Internet direct marketing picture and deduce that spam must be working or we wouldn't keep seeing it. If spam is such a terrible thing, why is it working? If it's not working, why do we keep seeing it?

Recognizing what spam is and how we get it lends a lot to our ability to recognize who spammers are. Again, it's important to remember that a spammer is *not* everyone who sends recipients commercial e-mail they don't want. Consumers might not like all of the e-mail that they get and they might consider sending unwanted commercial e-mail to be poor behavior, but that's not necessarily a reflection on the legal character of the sender. It's essential that we separate the spammer from the legitimate e-mail advertiser and deal with them independently.

As one might infer, if spam is unsolicited commercial e-mail, then a spammer is one who *sends* unsolicited commercial e-mail. Laws in some states also include those who *cause* unsolicited commercial e-mail to be sent. Sometimes, this is assumed to include the merchants who buy spam lists and merchants whose offers are advertised by e-mailers, even when the merchants have no control over those lists.

Since money is the fuel that powers spam, knowing how spammers get paid helps separate them from legitimate e-mailers because it says a lot about how they are motivated and how spam is "caused."

Spammers are not paid to sell products; they're paid to send e-mail messages to millions of e-mail addresses, generally on a cost per thousand (CPM) basis. Not everyone who is paid on a CPM basis is a spammer, but as a rule, only the most selective CPM list owners are *not* spammers. Spammers will not hang their pay on the performance of their list, regardless of the quality of the advertisement and the offer.

A dwindling number of advertisers are paid on a CPA, or cost per action (or cost per sale) basis. CPA publishers are paid a bounty for each sale made on advertising to their lists. It's a "pay for performance" method.

CPA advertisers tend to understand that spam is a relatively ineffective way to advertise, so they pay for performance to lend bottom-line accountability to the quality of the list. The quality that CPA advertisers are looking for when they pay on a performance basis suggests that they're not knowingly, or even willingly, paying for advertisement to be sent to those who don't want it. They recognize that it is a terrible waste of money and resources to send e-mail to those who don't want it because unwanted e-mail doesn't typically sell products. If it doesn't sell, it doesn't earn them commissions. Payment on a CPA basis accompanies an expectation and incentive for performance that spammers cannot satisfy – they don't even try.

It is thus reasonable for a CPA advertiser to make the point that he doesn't *cause* spam to be sent because he is not paying for thousands of e-mail messages to be sent; he's paying for an outcome that does not typically favor blasting a mailing to a spammer's database.

It is not altogether astonishing that we look at the Internet direct marketing picture and deduce that spam *must* be working or we wouldn't keep seeing it. Certainly, we assume, marketers wouldn't continue to broadcast this stuff if it didn't sell products. Therein is the paradox. If spam is such a terrible thing, why is it working? If it's not working, why do we keep seeing it?

It's true that spam is working, but it's not working the way many think it is. While we would naturally assume that the marketing is being "consumed" by the buying public, it is actually being consumed by some Internet retailers who use it to gain marketing distribution.

Most of those who assemble and peddle spam lists don't exist for the sake of selling products. They exist for the sake of generating e-mail and getting paid for it, regardless of the results.

Contrary to what many think, spam is not in consumers' e-mail inboxes because they're buying all of the products e-mail campaigns are hawking. Spam is in their inboxes because the price is right for advertisers and marketing resources are in such abundance there's a sense that advertisers can't miss with it.

In reality, e-mail advertisers "miss" rather persistently. With sales revenue reports indicating that Internet retail companies continue to operate at a loss, it is clear that Internet e-mail marketers are not experiencing sales volumes at the rate that their mailings would suggest, but spam distribution is still there because spammers are doing a good job of selling it.

Spammers don't sell consumers products, they sell advertisers distribution volume. A spammer's job is to "sell to the seller." In doing so, they promote distribution so fiercely that they can get an advertiser to doubt his own campaign test data, his product, and his advertising material when results indicate a bad run. Quite often, spammers throw the advertiser a bone after a bad campaign run by offering to generate a complimentary run on a campaign to help make up for shortfalls in performance. These gestures generally do little good, but they often get the advertiser to come back for more at a later date. Unfortunately, this results in a good number of legitimate advertisers being drawn into using spam lists unwittingly. Some advertisers are victims of outright fraud to the tune of thousands of dollars, duped by spammers into believing they're purchasing or using legitimate lists.

Where consumers help make spam work is in buying "the home run" – the one offer an Internet marketer needs to make it through the year. Consumers don't need to buy any of the mortgage plans, find-your-youth supplements, diet miracles, better sex life, lower interest rates, septic tank tips, bread recipes, or other scientific and economic breakthroughs. They need simply to buy a couple of decks of Iraqi Most Wanted playing cards to renew a retailer's faith in a spammer's list. The success of one or two campaigns is often all it takes to make it a productive year for spammers and delay the evolutionary phasing out of unsolicited commercial e-mail.

This point is worth repeating: Most of those who assemble and peddle spam lists don't exist for the sake of selling products. They exist for the sake of generating e-mail and getting paid for it, regardless of the results. Only the most diligent among them care about the effectiveness of their lists as long as they have at least passable marketability to advertisers. The rub is that while spammers do not typically care whether consumers want to receive their e-mail, the overwhelming majority of other commercial e-mail advertisers do.

Spammers are an unusual breed in business. So far, they have been able to survive low Internet sales, direct targeting by authorities, and the angst

of e-mail users. If they were engaged in practically any other business, they would have been gone long ago.

Locating Spammers

The most corrupt, dangerous, and troublesome e-mail marketers and spammers are those that operate on the fly or abroad or use offshore Internet relays while giving all of the appearances of being legitimate domestic enterprises.

As easy as it can be to find genuine spam (or have it find you), it is stunningly difficult to spot and locate spammers. We don't generally find them in the yellow pages under "spam" and they don't normally tell the secrets of their success at the local Rotary Club. They don't typically belong to the Chamber of Commerce or the Better Business Bureau, and they don't often do business the way other companies do it.

Spammers might operate under half a dozen different names at once through different ISP's and list a number of different mailing addresses and telephone numbers. Consumers calling the telephone numbers often find they're out of service. Spammers often change company names like some people change socks. More often than not, spammers operate out of any place where they can connect their mail servers to an Internet Service Provider (ISP) through a high speed connection.

Spammers try to find ISP's that won't seriously confront them over spam complaints or at least hope to earn enough money for the ISP's that they'll look the other way. Spammers who are not so fortunate rotate through Internet Protocol (IP) addresses and ISP's to keep their complaint volumes beneath the radar. Finding the right ISP and maintaining low visibility helps them sustain practically uninterrupted operations.

While spammers establish all the appearances of typical business operations, they conceal the fact that there is often no physical business address, no tangible customer service apparatus, no contact telephone number, no infrastructure, and no meaningful company culture. Legitimate Internet businesses must maintain a meaningful infrastructure to manage resources and business support operations, but spammers can often get by without it. Some of the more prosperous spammers run elaborate operations in simple office settings but are nonetheless quite difficult to identify and locate.

Spammers sometimes call themselves "list managers" - it sounds better than "spammer" - but they buy lists or have "subsidiaries" whose lists they "manage" or "broker." "Managing" and "brokering" lists keeps spammers from appearing to assemble the lists and keeps spammers at arms length from the law. Bearing in mind the inherent intricacy of the spam industry, we should recognize, however, that not all spammers list false addresses and telephone numbers and not all list managers and brokers are really spammers.

By the same token, we should not make the mistake of assuming that commercial e-mailers for whom we can readily find street addresses and telephone numbers and accuse of spamming or violating of a nuance of an ISP's terms of service are the ones that are causing the most problems. They are not. The most corrupt, dangerous, and troublesome e-mail marketers and spammers are those that operate on the fly or abroad or use offshore Internet relays while giving all of the appearances of being



legitimate domestic enterprises. Oftentimes, their spam messages aren't merely junk mail – they're platforms from which scams are perpetrated.

Let us hesitate to congratulate ourselves too much when we write band-aid legislation or nab a legitimate commercial e-mail marketer in the next city we think is a spammer while the real spammers are snickering in the shadows or abroad as their computers rattle off another several million e-mail messages. Likewise, we must resist the temptation to follow the piper who, at once, tunes us in to the problem yet appears stunningly inept at handling it.

To a great extent, many of these "first responders" have helped create the calamity they have placed themselves on the scene to repair. In many ways, they're running a high-tech protection racket – arsonists peddling fire hoses.

A High-Tech Protection Racket

Equipped with an understanding of what spam is and how it subsists, we *must* be incredulous about why so many have been so ineffective and inarticulate in finding an effective solution. This is a time for making insightful distinctions and asking tough questions about *all* aspects of the spam industry, particularly those that operate in plain sight and appear to be allied with consumers.

The truth about the spam industry is, in fact, just as elusive and as significant a problem as the spam issue itself is. The question is "why?" The answer is agonizingly simple.

The mischaracterization of spam has created its own profit-motivated industry. There exists a lucrative booty of software and services that profit from the misidentification of bulk or commercial e-mail as spam. There are dozens of spam filtering software titles on the market, but the growth and impact of spam hasn't slowed at all. Services designed to report spam to ISP's, services offering to certify or "white list" non-spammers, and free e-mail services offering spam-free options abound. While their "solutions" have been very profitable for them, they have proven grossly ineffective for consumers.

To a great extent, many of these "first responders" have helped create the calamity they have placed themselves on the scene to repair. In many ways, they're running a high-tech protection racket – arsonists peddling fire hoses. These opportunists have generated bogus information that plays on consumer fears; then, they have delayed and misplayed effective corrective action that has been costly to consumers while keeping the threat of spam alive and well. This has been vastly detrimental, inflicting great harm on eCommerce in general and legitimate advertisers, merchants, and consumers in particular. They are responsible for much of the damage spam has done to the Internet marketplace.

Filtering Much More Than Spam

The filters utilized by e-mail services and sold by software developers are also worth a closer look. Advertised as spam filtering software, it is helpful to look at their filtering algorithms to notice that the focus is centered not on unsolicited commercial e-mail's tell-tale indicators such as forged or false Internet header information, deceptive subject lines, or fabricated originator information, but instead on a broader scope with equal or greater

weight on commercial content such as images, colored text, unsubscribe links, and traceable header information indicating the e-mail was sent from a bulk commercial mailer. Thus, these filters are not specifically engineered to filter spam; they're designed to filter commercial content.

Merchants will not long survive if they cannot compete, and compete on some equal footing. When a climate exists in which all commercial e-mailers are presumed guilty of spamming, having been thus characterized by competitors, the options they have left are normally harmful to commerce.

Quite often, filters that screen for commercial content are also used to screen "spam" for reporting to ISP's, law enforcement, and watchdog services. Aside from bottling up the law enforcement mechanism and placing ISP's in the precarious position of potentially terminating profitable business relationships with companies that might be guilty of no wrongdoing, filtering is blockading a good amount of legitimate commercial content as well.

To frustrate filters and filter users, genuine spammers write subject lines and content to circumvent the filtering, and they endeavor to make filters a nuisance by flooding them with so much traffic that they are too sluggish to be practical. Without a doubt, flooding filters with traffic means MORE spam, not LESS.

With the constant tweaking of the filter algorithms to keep pace with spam, the filters are catching increasing amounts of routine e-mail that recipients want. Thus, filters that are advertised as becoming more and more intuitive as time goes by actually often become less and less intuitive because there is so much data to filter and therefore, more incidental filtering of personal and legitimate commercial e-mail.

Protection Through Innuendo

Some e-mail users utilize services like SpamCop to report spam "perpetrators" to ISP's. When e-mail users report spam to SpamCop, there is no investigation to determine whether the reported spam is really spam or not; it's up to the ISP's to decide on further action. Part of SpamCop's service includes an assurance to those who report spam that their service will not reveal to ISP's or "spammers" the e-mail addresses of those claiming to have received the "spam." They "protect" e-mail recipients' addresses under the pretense that a spammer might take revenge on the recipient if it's known who reported the spam.

However, since e-mailers have no idea who reported the e-mail as spam and since there is no meaningful effort to determine which complaints really relate to spam and which don't, legitimate commercial mailers have no way of showing evidence that a recipient opted in to a list. Furthermore, with this "protection," legitimate mailers have no opportunity to satisfy the recipient's desire not to receive additional e-mail. Obviously, lacking the e-mail addresses of those who are reporting the e-mail as spam, they can't do anything about the recipient receiving further e-mail. They can't stop sending what they don't know is unwanted. The result is that the recipient continues to receive the unwanted e-mail and the complaints keep rolling in. Really, who prospers from this process?

Filtering Spam or Filtering Competition?

When e-mail service providers filter competing commercial e-mail as though it's spam, then marry this "service" with services like SpamCop, we essentially have a free e-mail service provider screening competing commercial material and reporting it as though it is illegal or otherwise illicit.

When consumers sign up for free e-mail services and elect to have the e-mail service provider filter incoming "spam," they often don't realize that with many of these services, the process of filtering commercial e-mail results in blocking and sometimes reporting as spam, commercial e-mail EXCEPT FOR e-mail from sponsors and affiliates of the free e-mail service provider.

Thus, *competing* commercial e-mail is considered spam whereas *affiliated* commercial e-mail is not. Many consumers don't realize that when they subscribe to the free e-mail service, they agree to receive third-party offers or offers sent by the service provider on behalf of third-parties.

When e-mail service providers filter *competing* commercial e-mail as though it's spam, then marry this "service" with services like SpamCop, we essentially have a free e-mail service provider screening competing commercial material and reporting it as though it is illegal or otherwise illicit with an eye toward choking out the competing advertisement through an enforcement mechanism.

These efforts to deny competitors access to bandwidth and sometimes bind them in legal action are nothing less than part of a strategy to drum competitors out of business while portraying themselves as spam victims. Reporting competing e-mail as unsolicited commercial e-mail could be characterized as a hoarding of economic resources that harms the public and reduces normal interstate competition; as such, it is potentially a violation of the Sherman Antitrust Act.

Merchants will not long survive if they cannot compete, and compete on some equal footing. When a climate exists in which all commercial e-mailers are presumed guilty of spamming, having been thus characterized by competitors, the options they have left are normally harmful to commerce. That's why the federal government has approved fair trade statutes.

The average legitimate e-mail advertiser generally has three choices when accused of spamming: (1) They can either fold under the competition and their vulnerability to enforcement, (2) They can go underground and do what they already stand accused of while concealing their identity, or (3) They can gut it out and hope that the e-mail marketing industry clears up for them before their business fails. For many of those who don't make it legitimately, the problem is not with normal competition; the problem is in competing in an environment where their businesses have been mischaracterized so severely that they can't compete fairly.

Normally, the economics of e-mail marketing make stunningly low prices and great deals a possibility, but when the advertising market is cornered and consumer exposure to these offers is restricted, prices invariably increase and consumers lose again. Small "mom and pop" and bargain retailers for whom the Internet is a perfect match are an endangered species in this climate. This too, is bad for consumers.

Spam at the Bar of Justice

Powered by that essential grain of truth, the anti-spam movement has gained popular momentum; now, the outcry against "spam" has yielded highly reactionary legislation, designed to lay the strap of enforcement into the hind sides of the dreaded spammers with lawyers not far behind.

With little or no meaningful effort undertaken by law firms to establish the legitimacy of complaints before filing them, the courts are barraged with thousands of spam lawsuits, many lamely pursuing class action status.

Clarence Darrow said, "The law does not pretend to punish everything that is dishonest. That would seriously interfere with business." His words appear to ring particularly true in light of well-intended anti-spam legislation that, unfortunately, tends to be imprecise, ineffective, generally counterproductive, inconsistent, and potentially unconstitutional. Many of these statutes betray the same confusion that plagues consumers, casting industry giants as "victims" as they gain a competitive advantage from marginalizing competition.

With powerful Internet Service Providers at the side of legislators during the drafting of legislation, it should be no surprise that laws intended to protect ISPs' bandwidth and consumer rights do much more than *defend* ISPs and consumers. More significantly, they contribute to ISPs' *offensive* playmaking and improve ISPs' strategic position by opening to legal prosecution a good amount of legitimate commerce, essentially criminalizing – or at least persecuting – ISPs' competitors.

Law firms are getting great mileage out of these gaps in the precision of the law by aggressively pursuing legal action on behalf of "spam victims" and tying up what are otherwise low-overhead Internet operations in costly litigation. There is an "out" for Internet marketers, however; they can pay what many consider extortion money of thousands of dollars to forego extensive court action. At least one Internet marketer, however, has discovered that paying the ransom to halt one action resulted in the end of that action in time to be served with another by the same law firm.

Sometimes, the "victims" of spam are employees of the law firms that are looking for an opportunity to bring legal action. Some of these employees have opted in to large list distributor services, then have waited sufficient time for the services to make resale distribution with other marketers before returning to the original site to unsubscribe. With the fruit ripe for picking, they have sued the downstream marketers that legally bought and resold lists and established lawfully-constituted business relationships.

In some instances, law firms are using free e-mail services that offer free bulk e-mail filtering as "spam" bait. Thus, they are subscribing to free e-mail accounts that include receiving commercial e-mail as a part of the service as they await the inevitable "spam."

Unfortunately, with little or no meaningful effort undertaken by law firms to establish the legitimacy of complaints before filing them, the courts are barraged with thousands of spam lawsuits, many lamely pursuing class action status.

Even as the spam issue evolves in legislatures and court rooms, some are actively campaigning for measures that will benefit them in the future as

well. Not surprisingly, as we founder toward new legislation, an exploitive disinformation campaign continues to cloud the issue, generate passion, and complicate our ability to see the problem clearly enough to resolve it decisively.

While meaningful enforcement is necessary, the fact remains that the most effective solutions arise from a well-informed public employing reasoned and patient strategies for dealing with the problem.

Once the final note is struck on the legal finagling to extract a pound of flesh from "spammers," we might learn that the disinformation campaign has also created a 1st Amendment Constitutional argument and Commerce Clause concerns of such complexity and reach that they could set back efforts to combat real spam by years.

By then, with ISP's and spammers having drummed legitimate mailers off of the competitive track, spam and price competition on the Internet will be at its worst for consumers with Internet competition skewed beyond repair.

Ultimately, there are limits on the extent to which state and federal legislatures can succeed in resolving our commercial e-mail problem because the nature of spam makes prosecution of the real culprits quite difficult. Because spammers' methods are fairly obscure and they are difficult to locate, the enforcement effort is and will likely remain fairly ineffective. If attempted with precision, the law enforcement campaign would be enormous and likely need to span international borders.

While meaningful legislation and enforcement are necessary, determined spammers, particularly those operating offshore, will always find a way around the law. The fact remains that the most effective solutions will arise from a well-informed public, employing reasoned and patient strategies for dealing with the problem. Although spam appears indomitable, it *can* be severely challenged on consumers' terms through spammers' purse strings and the mechanisms by which their viability and effectiveness are measured.

Consumers Taking Control

From the start, we consumers need to be diligent in knowing the difference between spam and other commercial e-mail. As we've discussed, there is a difference and we should not allow others to profit from convincing us otherwise. With that distinction made, our tactics can also achieve clarity.

As we've discussed, spammers are ripping off a good number of retailers by representing their lists to be something they're not. To bolster their assertions about list performance, they include measurement data to indicate things like "click-through rates" and "open rates." Again, when e-mail programs preview e-mail, they register data helpful to the spammer's pitch to retailers by populating "open rate" metrics. These data points enable spammers to tell retailers, "they're clicking on it, but they're just not buying it" which says that the spammers are sending e-mail to receptive lists of recipients that are willing to shop for the right offer. The illusion promotes additional media buying.

We should degrade the spam lists' appeal by not opening or previewing e-mail we think might be spam. We should recognize that the process of viewing the spam's header material to see where it came from is often

enough to show a "click" and get us more of the same. Frequently, reporting and filtering spam results in electronically "opening" the spam which, again, shows up as a "click." If we are going to use our right index finger on spam, we should use it to simply highlight the spam and hit the delete button. If we simply delete it, it will not take long before it is no longer financially feasible to send it, and spammers will move on.

With or without state or federal legislation governing unsolicited commercial e-mail, consumers must ultimately decide to render it obsolete by not previewing or otherwise opening mail they suspect is unsolicited.

E-mail marketers know intuitively that the only campaigns that are working with any consistency right now are the "home runs" and the campaigns from well-known and reputable retail mailers. Consumers should continue to slam the door on gimmicks and rip-offs from spammers by simply deleting them from their inboxes. We already know that spammers will not ever voluntarily run the home runs exclusively since it costs them as much to run a poorly-performing offer as it does to run a good one. However, consumers can show retailers that buying e-mail advertising for anything other than the home runs is a waste of money. This kind of selectivity will reduce the volume of spam.

As we've already discussed here, there are tremendous bargains available on the Internet. The cost savings are in fact very good. Consumers should not shy away from them; they simply should not shop with companies that appear to be doing things "the easy way."

Internet retail companies that take the easy way normally cut corners on services to the customer and lack a physical location, an in-house staff, and a business philosophy centered on customer service. Companies that take the easy way out can beat some of the competition on pricing, but as we've seen, consumers generally pay for it in the end. Spam is the leading "easy way out" mechanism.

With or without state or federal legislation governing unsolicited commercial e-mail, consumers must take control and show that they can make the essential distinctions with regard to the spam industry and prove that they are determined to help restore e-mail's credibility as a valuable resource for consumers and legitimate marketers. Consumers have the power and the authority to confront this issue head-on, so they must.