

---

COMMENTS TO THE FTC REGARDING PROPOSED "CAN SPAM" LEGISLATION

---

Re: the proposed "CAN SPAM" act, proposed by Mr. Burns in 1<sup>st</sup> session of 108th congress

The full text is not included here, but cited as found at the following location on the Internet, on 05/15/2003:

[http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108\\_cong\\_bills&docid=f:s877is.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s877is.txt.pdf)

Page 2, item 5, line 18 of the FINDINGS states: The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail or for both.

I suggest that these costs are present whether the message is actually 'received' by the intended person or not. For instance, the message may have been filtered, at which point a spammer may argue that it was not actually received, and so no offense occurred. Perhaps the word 'receipt' on line 18 should be changed to 'receipt or processing' to widen the scope slightly.

It is not true in all cases that the recipient cannot refuse such mail. The costs may still exist, even for individuals who can refuse, by having a third party block messages for instance. To accurately reflect the findings then, you might state that the recipients 'often cannot refuse', since this is a key aspect of unsolicited commercial email, that we wish to change.

Page 3, item 9, line 17 of the FINDINGS states: An increasing number of senders of unsolicited commercial electronic mail purposefully disguise the source of such mail so as to prevent recipients from responding to such mail quickly and easily.

While this is one reason for disguising the source, another reason worth noting is that the sender wants to hide his operations from others. He may realize that most of his messages are unwanted, and that his actions would be stopped if conducted openly. Often his actions conflict with the policies of his network provider, and the policies of the recipient's provider. Because of this recipients would likely report his actions, and result in network disconnection. I would suggest adding a phrase that indicates that this disguise is also done to prevent detection or identification by maintainers of the network.

Page 4, item 11, line 1 of the Findings states: In legislating against certain abuses on the Internet, Congress should be very careful to avoid infringing in any way upon constitutionally protected rights, including the rights of assembly, free speech, and privacy.

I agree with this wholeheartedly, as I think would congress, ISPs, end users, advertisers, and everyone affected by this legislation. I think it is a key element of the document, stating that the purpose is to preserve the viability of email as a form of communication, not to stifle it. In the area of 'free speech' however, it may be worth noting that commercial speech does not have exactly the same rights as private free speech. This may prevent spammers from simply stating that their commercial activities are protected in the same manner as a private conversation, or public announcement. Also, I would wish to have it understood that the ability should be preserved in email to send a non-commercial message without disclosing the identity of the sender, so long at that ability is not abused. This ability would exist, in much the same manner as paper mail could be sent from a post office without a return address or signature. Such communications is important and appropriate for many reasons such as making an anonymous report to the police, sending anonymous 'letter to the editor' to a newspaper, mailing advice or comments to a friend or co-worker etc. These are only a small percent of written communications, but I believe it is important to maintain this option for privacy in communications and not to create legal or technical blocks to this aspect of free speech.

Page 4, item 3, line 14 of the Policy states: Recipients of unsolicited commercial electronic mail have a right to decline to receive additional unsolicited commercial electronic mail from the same source.

When this sentence makes reference to the ‘same source’, are you intentionally leaving the definition of the word ‘same’ to be applied on a case by case basis? Some people might interpret that to mean the same company, others may define that as the same email address, or same internet domain, or same person. A spammer may operate under several different titles and present himself as many different sources. Email may also be sent on behalf of many different third parties, and justify each of them as a different ‘source’. Further, if someone is prevented from sending further email, because the recipient has asked not to get any more messages, then what is to prevent the spammer from giving the address information to another entity, who becomes a new ‘source’ of spam email? I leave it up to you to decide of the definition of ‘same source’ needs clarification – or if it should intentionally be left open to interpretation as applies to each case. This issue is also related to the text on page 15, line 7, item A.

Page 6, item 8, line 21 of the Definitions states: The term “header information” means the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address.

While the statement above is correct, it is not quite complete. Header information may also include other descriptive, tracking, status, or auxiliary information associated with the message. Some of this data is for the recipient, while other data is simply used by the computers to process messages. The scope for ‘header information’ should extend to all information associated with the message, whether generally displayed to the user or not. This could prevent abuse of the email system when spammers falsely manipulate information associated with the message, just because it was not accurately defined as ‘header’ data in the legal sense. For instance, in the future, such information may also include mail authentication, keys or digital signatures which would accompany the message.

Page 7, item A, lines 4 of the Definition states: The term “implied consent”, when used with respect to a commercial electronic mail message, means that (A) within the 3-year period ending upon receipt of such message, there has been a business transaction between the sender and the recipient (including a transaction involving the provision, free of charge, of information, goods, or services requested by the recipient)

This is a very open/broad statement. For instance, if a person visits the website of a company, without even typing any information- it could be said that they have requested the information content of that web-site free of charge. If a person walks into your restaurant and asks to see the menu, you have just provided them with free information about your company. These actions should **not** imply that visiting a web site or viewing a menu now grants the business owner rights to send you email. I think that perhaps this section should be reworked, to state the basis to establish a business relationship, or express interest. For instance, your bank, newspaper, school, church, landlord, utility, and ISP obviously have an established relationship. Perhaps even the cell phone company you disconnected last year, or even your local gas station would qualify. Some distinction should probably be made between a casual and substantive transaction. Even without such a business transaction, what if the user specifically makes his email address available to someone who then sends commercial email. They could write an email address a slip of paper, or hotel register, or customer interest card. If person could reasonably expect that email would result in that exchange of information- then the mail that follows is not spam, so long as it follows the other basic guidelines (denoting sender, allowing cancel, etc.). On the other hand there is a fine line in ‘reasonable expectations’. What if you drop a business card in the drawing for a free meal, or your cell phone broadcasts an email address to businesses as you walk by, or there is an email address advertised on your vehicle? How is permission implied or an expectation set? I believe that this section of the bill requires some clarification. Also, a company should not require customers to divulge an email address as a term of service, if business could be reasonably conducted without it. This should be at the customer’s discretion.

Page 7, item B, line 10 of the Definitions states: The recipient was, at the time of such transaction or thereafter in the first electronic mail message received from the sender after the effective date of this Act, provided a clear and conspicuous notice of an opportunity not to receive unsolicited commercial electronic mail messages from the sender and has not exercised such opportunity.

This section is important, in that it establishes that the recipient should be able to stop further communications in the first email – yet I don't see where it is clear that all further (2<sup>nd</sup>, 3<sup>rd</sup>, and 200<sup>th</sup> email) messages should also maintain the recipient's ability to stop email in the same manner.

Page 8, item 13, line 16 of Definitions states: The term "protected computer" has the meaning given that term in section 1030(e)(2) of title 18, United States Code.

Reading through section 1030, it states: the term "protected computer" means a computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

It would appear that this definition of "protected computer" is mostly focused on United States federal computers, and banks/financial institutions. Perhaps 40 years ago, these were the important computer systems to protect, but in the current world I think that we need a **much** more comprehensive definition. The only aspect of that definition that even might apply to most computers on the Internet today, would be that they 'may' be used for interstate or foreign communications, by virtue of the fact that email can be sent and received anywhere in the world. This is something of a stretch, and clearly not the intent. Still, the definition in section 1030 may exist for a reason, and need to distinguish between computers in the private sector, and the extremely secure machines used in banking and government. That definition may also be referenced in many other places within federal statutes, so I would not suggest running over to change/correct the definition without further study.

I would suggest making a definition of the term "Proprietary Computer", to mean a computer system maintained by a business or private individual, which should be used in accordance with the wishes, needs, and guidelines desired by that person or business. A definition of this sort is much closer to the description of a computer that I think you would intend for the "CAN SPAM" act. You can debate the exact wording, but it should be designed to "protect" more effectively than what's in section 1030.

Nearby, section 1030 also states: the term "computer" means an electronic, magnetic, optical, electro-chemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

The world of computers has developed a variety of devices between the traditional mainframe or desktop computer and a small calculator. For the purposes of is bill, the above definition would still apply – but I think that the focus is really on any device which can be used to send or receive and store an electronic message using an email address. This is commonly digital and textual in nature, but in the future may include other non textual content.

Page 9, item 14 line 4 of the Definitions states: If an electronic mail address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial electronic mail message sent or delivered to that address before it was reassigned.

This clause seems correct, yet it also seems to ask for some clarification of policy. The sender of the message will not know of a change, at the time the mail address is assigned to a new person. Provision should be made that due diligence should be made to maintain accuracy of the senders address lists, that the new person assigned that address should have the immediate right and ability to communicate the change, and prevent further email from being sent from the same source. Further, if the sender could not know that the address has been reassigned, then email sent on the basis of earlier permission should not constitute spam. This is not meant to open a loophole, but to prevent unnecessary fines and lawsuits.

Page 12, item 1, line 6 of the Requirements states: It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message that contains, or is accompanied by, header information that is materially or intentionally false or materially or intentionally misleading. For purposes of this paragraph, header information that is technically accurate but includes an originating electronic mail address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading.

I would like to see this requirement extend one step further, to include deceptive information used to obtain the domain name, which constitutes part of the email address itself. In many instances, spammers will register a domain name, using false or misleading identities, and incorrect addresses to avoid complaints or prosecution that would result from their activities. Domains are also mentioned on page six item four. The policy statements of some domain registrars indicate that information should be accurate, but they are often reluctant to disable fraudulent entries. If you include a policy requiring accurate information for domain registration in this bill, then it would help. The registrars could then make reasonable attempts to correct inaccuracies, and then alter/disable/cancel domains without expecting lawsuits as a result.

Page 15, item A, line 3 of Section 5 states: It is unlawful for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of an unsolicited commercial electronic mail message that falls within the scope of the request.

I can understand that in some large organizations, it may take a while to process a request to stop sending email – yet the bill should not specify an open loophole of ten days, in which spammers may send as much mail as they want. I believe that almost all computer systems can respond to a stop request **much** sooner than this. The law should be written to specify that the sender should make reasonable efforts to stop sending messages to the same address immediately, and suggest that further messages could be stopped within a single business day after the request is received.

Also, there is a possible problem in the ending qualifier stating “within the scope of the request.” The sender may be conducting 100 advertising campaigns, on behalf of several different entities, which contain the same email address. Each message sent may have the provision to cancel further mail messages from the ‘same source’, saying “cancel further messages”. The sender that may not consider this request to include a scope for the other 99 messages. The law should specify that when asking not to receive further email, the recipient may specify the scope of that request. The request to stop might include only that topic be discontinued for three months (as in a newsletter). The scope of request might specify all email relating to a sub-group of messages (as in, stop sending promotional ads, but I still want my electronic bill). The scope might be all inclusive, to say “I never want to hear from you or any of your associates again!” The sender should not be allowed to limit the scope of the cancel request –

and if the cancel request does not specify a specific scope, then it should default to the largest scope under which the sender has any influence. This would include removing the recipient from all mailing lists, and communicating that request to any other parties who had access to that data in the past, so they can do the same.

Some businesses use privacy agreements that specify that information may be shared with other parties or “business parties”. When this is the case, those parties should be listed by name. If any other segments of the business or business partners have access to this information, then both companies must track the distribution of that data, and use of that information must include the obligation to maintain contact, and remove data from the list when requested. In this way, if you give your email to the local McDonalds franchise, and the information is obtained by McDonalds headquarters in Chicago, then if a person receives an email, and requests that no more email be sent, then ALL associated email will stop.

Page 16, item A, line 25 of Section 5 states: ...the electronic mail address of the recipient was obtained, using an automated means, from an Internet website or proprietary online service operated by another person

The intent of this phrase is to prevent use of “harvested addresses” to send spam. This is very important, but the wording of this phrase is not clear about what constitutes “automated”. Much of what is done with computers can be considered automated. The entire field of computers was once referred to by the acronym A.D.P. for Automated Data Processing. Having a web site that allows users to type in their email address, and request to be added to your distribution list could be considered ‘automated’ from the computer owner’s point of view – yet consent was clearly granted in this case. If the authorized email was sent by a third part, then that party would fall under the description outlined above.

I think that the focus here is to prevent the collection of email addresses or other information from someone else’s computer without their clear knowledge or consent. On the other hand, to some extent, even collecting email addresses from a computer system you own and operate does not always convey permission to send email. For instance, if I run an NNTP newsgroup server, or an online message board, or come other type of service such as ICQ, then harvesting email addresses from my own computers does not mean that I can send them inappropriate email messages. Permission is the key. Perhaps this phrase could be reworded to be more concise, and allow for more possibilities.

Page 27, item (i), line 1 of Enforcement / Damages states: (paraphrased) A provider of Inter-net access service may bring a civil action to recover damages in an amount equal to the actual monetary loss incurred by the provider of Internet access service as a result of such violation, or \$10 per message.

When this section refers to the “result of such violation”, does this imply all activities associated with the spamming campaign? For instance, the sending of email is often just a part of an overall effort. This activity may start with address harvesting activities, or a “dictionary attack” where the spammer polls an email server, asking for millions of possible email addresses, trying to find the valid email addresses. As a result of this activity, the ISP may pay much higher network bandwidth charges, they may have to use more computers, CPU time, disk storage, networking equipment, resources and manpower to deal with the onslaught of traffic. Because of this, the costs to the ISP may extend beyond the impact of the actual email messages sent. The recoverable damages should reflect this.

Page 1, Section 1, line 5 of Title: As a side note, be sure that people do not get hung up on appropriateness of the name of the bill. The title in Section 1 includes the term pornography, but the bill itself deals very little with the actual **content** of the message, and whether it is appropriate, or pornographic. The bill actually deals with proper procedures for sending any commercial email, and permissions. Indeed, finding a definition for pornography may be as difficult as reaching a consensus on the definition for

spam. (which was not possible with the group of experts at the FTC Spam Forum two weeks ago).  
I realize that you want to keep the “Can SPAM” name, but don’t let it cause distraction.

-----  
Miscellaneous Spam Thoughts  
-----

Spam is not just a computer and email issue. Spam is a SOCIAL problem, with a technology context. Companies always want to advertise, whether Large or small.

People in general want to express themselves, but that doesn't mean that we consider it acceptable that thousands of people drive through residential neighborhoods with loudspeakers bothering the residents day and night. I am entirely for 1<sup>st</sup> amendment rights of free speech, whether I agree with their message or not- but nobody could dispute the nuisance aspect of hundreds of people with loudspeakers in my yard, who make it difficult to talk with my mother on the phone.

People shouldn't have to hide their email address from the world, just so the spammers won't flood their mailbox with junk. I enjoy a lively discussion about technical topics or social issues, and may want people to be able to reach me, to converse in these areas. My work also involves email communications, and I would be happy if hundreds of people could find me for professional reasons. Yet, in all of these areas, having a high visibility email address simply invites spammers to bury you with thousands of annoying messages, you would rather not receive.

I may also want to express certain things in a completely anonymous fashion – with the freedom to state my opinion publicly, without bias and without people being concerned about the author.

We have had paper spam (junk mail ads) in our mailboxes for most of the century. Most people get more junk mail than personal mail. Many of the issues here are exactly the same as spam email. You have address collection, customer lists being sold, and people being targeted for things that they may not want. In addition, there is no reliable opt-out mechanism, so once your address information is 'out there', it is nearly impossible to stop the junk mail, and hardly worth your time. There are three main differences between this and Email spam. First, the economic ... Second Fair trade practices... Third Accountability (tenuous, could have NO return addr) What if you got 500 junk mails daily at home. It would take you two hours each evening, to sort through the paper spam, just to make sure you hadn't overlooked a letter from your cousin, or the electric bill you needed to pay. Soon you would be so frustrated, that you would quit opening ANY mail, and throw it all in the trash. Meanwhile, your poor mailman is breaking his back every day to deliver those letters that you don't even want to see.

If a salesman walks up to the door of my home, he is not trespassing unless I have "no trespass/solicit" signs in my yard. I can tell him to go away, yet, just as with spam, that doesn't keep the next salesman from calling. This is another form of opt-out. Even with the "No Solicit" signs in my yard, if 300 salesmen come to my door, to interrupt my work, it would disrupt my schedule even more if I tried to fine or prosecute every salesman. After slamming the door in the face of 120 salesmen, what would a person do? First, you get angry at the interruptions and the frustration, then most people would just quit responding. You disconnect the doorbell, and switch you phone to an unlisted number. A week later, when your long lost cousin from Denver stops by to visit, he knocks at the door but gets no answer then leaves, even though you would have liked to see him. Your cousin would have called ahead to let you know, but your phone number was changed, and unlisted, and you never saw the letter he sent last month, since it was lost in the avalanche of junk mail and credit card ads.

Eventually, you may decide to hire some of those 10¢ per hour salesmen to sort through your mail, instead of bothering you all day.

Givens:

- Any policy you put in place, will be ignored by most of the spammers without effective enforcement.
- Any policy you put in place, only extends to the borders of your government.
- The borders of your government don't stop the flow of mail (electronic or paper).
- It is difficult to set an exact legal or computer definition of spam.
- Failure to solve this problem, threatens to collapse all forms of electronic textual communications.

The internet was designed to be decentralized. In many ways this is a GOOD thing. It avoids single points of failure, and keeps any ONE company from having control or ownership, just as no ONE company has complete control over the market and economy. It's also occasionally a bad thing, since it's difficult to get a consensus of how to run things, or fix problems. There are a handful of 'standards' groups, who set up the protocols and guidelines that computers use, but this generally covers technical features, and was not meant to set law or policy.

Spam is what Internet advertisers know  
Give them some alternate methods, providing benefits, but controls  
Make it easy for Users to have control of their own information  
Most people I have talked to agree that this is the correct solution, ultimately.  
Right now, we're too busy sorting tons of unwanted mail, and can't implement good solutions.

Mosquitoes and malaria have been a problem in the United States. Nobody owns the mosquitoes, or is responsible for their behavior, yet they pose a public health and nuisance risk. Since private industry has no ability or responsibility to take action, when this gets to be a problem, the government steps in, and takes measures to control the situation. It is never completely solved, but reduced to acceptable levels, and no longer poses a major risk. At home most people still have screens on their windows but can enjoy an evening in the back yard. If they really don't like bugs, then they buy citronella candles or bug zappers. Occasionally we still have a problem with fruit flies from Asia, fire ants from Mexico, and bees from South America, but so far we have been able to recognize the threat and take some action.

I think we can at least manage this level of control over the internet, and probably do much better in the long term. Yes, the spammers are smarter than mosquitoes, but they are bigger and leave more of a paper trail.

Ref: <http://www.remove.org/company/mail.html>

"The amount of paper junk mail sent each year in the USA is staggering -- some 4 million tons, nearly half of which is never opened. Even if you recycle there are still enormous environmental costs in terms of ink, energy to produce deliver and recycle the paper, recycling inefficiencies and loss of virgin forest to create the high quality glossy paper much junk mail uses"

Junk mail is not only a waste of time for you but also a large problem for landfills. Federal Law Title 39, Part IV, Chapter 30, Section 3001 states that any person who mails matter for sweepstakes, promotions, and or other solicitation offers. must prevent the mailing of such matter to any person who requests for it not to be mailed to them anymore. Marketers can be liable up to \$10,000 per piece of mail that they send once they are notified that you do not want to receive junk mail.

Federal law [Title 39, Part IV, Chapter 30, Section 3001](#) paragraph (L) regarding paper mail, states: [paraphrased]

Any person who uses the mail for promotional material shall adopt reasonable practices and procedures to prevent the mailing of such matter to any person who submits to the mailer of such matter a request that such matter should not be mailed. Any mailer shall maintain or cause to be maintained a record of all requests made under paragraph The records shall be maintained in a form to permit the suppression of mail to an applicable name at the applicable address for a 5-year period.

What about the ‘untouchables’ ... such as an offshore spammer, who conceals his network address, and sends messages through 1000 unsuspecting proxy machines, so he is nearly impossible to trace.

Paper mail, false representation [Title 39, Part IV, Chapter 30, Section 3005](#) <http://www4.law.cornell.edu/uscode/39/3005.html>  
Pandering [Title 39, Part IV, Chapter 30, Section 3008](#) <http://www4.law.cornell.edu/uscode/39/3008.html>

However, this is based a few important elements: First, the US postal system can limit abuses at the point of origin. If a post office sees a truck load of mail, which appears improper, they can stop it before it is distributed across the country.

Postal regulations also rely on the fact that a mailing address is linked to a physical piece of property, owned by a person or other legal entity. Obtaining ownership or usage rights to that property takes time (often weeks), and generally leaves a paper trail. This makes it more possible to track down abusers of the system, and makes it impractical for offenders to simply move from location to location daily.

With computers and electronic communications you can set up shop and move faster, and at less cost.

What about maintaining the possibility of anonymous written communications. There is certainly a need for this sort of communications within society, whether in paper or electronic form. Messages to legal authorities, regulatory agencies, or an employer may contain important information, but require the sender to remain unknown. In almost every instance, these will be low volume messages however. An ISP may maintain the ability for its customers to send these sorts of messages, but limit them to one per hour, or some reasonable amount. In this way the ability is preserved, but abuse limited.

## EARTHLINK ANNOUNCES LEGAL ACTION AGAINST NEW YORK SPAM RING

### ISP Seeks Court Order to Stop "Buffalo Spammer"; Federal Hearing Set for Today

ATLANTA, May 7, 2003 -- EarthLink (Nasdaq: ELNK), one of the nation's leading Internet service providers, today announced its legal action to shut down a Buffalo, New York spam ring accused of sending more than 825 million illegal emails since March 2002. A hearing is scheduled for this morning in U.S. District Court in Atlanta.

EarthLink alleges that Howard Carmack, aka the "Buffalo Spammer," and his accomplices used stolen credit cards, identity theft, banking fraud and other illegal activities to fraudulently purchase Internet accounts and send out unsolicited, commercial emails.

"Spam is the bane of the Internet. By taking legal measures to shut down a spammer like Carmack, EarthLink can help preserve the Internet experience for all consumers, not just EarthLink subscribers," said Pete Wellborn, EarthLink's outside legal counsel who led the investigation. "With the Buffalo spammer, EarthLink is continuing its tradition of using state and federal laws to stop spammers."

EarthLink has a long history of fighting spam. Its multifaceted approach includes legal action, innovative technical solutions such as the EarthLink spaminator, legislative support and consumer education. In addition, EarthLink is planning to launch new tools to fight spam, including its spamBlocker product.

The Carmack case is the latest example of EarthLink using state and federal laws to take legal action against spammers who illegally abuse the Internet. In 1997, EarthLink obtained an injunction against Sanford Wallace, the most prolific spammer of his time, followed by a \$2 million judgment against Wallace's company, Cyber Promotions, in 1998. Last year, in what is believed to be the one of the largest victories against a spammer, EarthLink received a \$25 million judgment against K.C. Smith, shutting down an operation that had generated more than 1 billion unwanted emails on the Internet.

In the Carmack case, EarthLink has filed a motion for preliminary and permanent injunctive relief and a motion for a default judgment in federal court alleging that Carmack "assumed the identities of other Carmack family members and of innocent third-parties to disguise his own involvement in these illegal activities." According to EarthLink's motion, Carmack's spam included advertisements for computer virus scripts, "work at home" and get rich quick schemes, bulk email software and lists to be used by other spammers, and cable TV descramblers.

As in previous cases, EarthLink is asking for injunctive relief that will prevent Carmack from illegally spamming any Internet user, regardless of the user's ISP. At today's hearing, EarthLink will present evidence regarding its request for injunctive relief. EarthLink is also seeking \$16 million in damages.

EarthLink's Abuse Team identified a spike in spam from the Buffalo, New York, area in March 2002. The Abuse Team determined that the spam originated from a single spammer or spam ring, and in June, EarthLink filed a "John Doe" lawsuit against person or persons unknown. By October 2002, EarthLink had identified several individuals connected with the Buffalo spam ring. These individuals provided additional information that implicated Howard Carmack.

By November 2002, with witness testimony and additional investigation, "EarthLink had accumulated a mountain of evidence proving Carmack to be the mastermind of the Buffalo Spammer ring," according to EarthLink's motion. Carmack avoided EarthLink's process servers and private investigators for several months before being served with EarthLink's complaint in February 2003.

Mary Youngblood, EarthLink's Abuse Team manager who led the investigation within EarthLink to identify Carmack, noted, "EarthLink has a dedicated team of spam-fighting professionals, and we remain vigilant in our efforts to identify spammers and help bring them to justice."

Man Charged With Fraud in Spam Case – New York Times, May 15, 2003

**By SAUL HANSELL**

Eliot Spitzer, the New York attorney general announced that on Tuesday, May 13 2003 a man was arrested and charged in state court with forgery and fraud in connection with millions of unsolicited e-mail messages, commonly known as spam. The man, Howard Carmack, (36, from Buffalo NY) pleaded not guilty and was released on \$20,000 bail. Mr. Carmack was charged with four felony and two misdemeanor counts, the most serious of which carries a prison sentence of three and a half to seven years. Mr. Carmack previously was convicted of forging postal mail orders, a lawyer involved in the case said.

New York State does not have a law specifically against sending spam. Mr. Carmack was charged with forgery because he replaced his own e-mail return address with those of other people, according to the complaint filed by Mr. Spitzer's office. He was also charged under New York's law against identity theft, which took effect last year, based on accusations that he used stolen credit card numbers to sign up for 343 Internet accounts from EarthLink. The company estimates that Mr. Carmack in the last year sent about 825 million e-mail messages that offered software for use by spammers, lists of e-mail addresses and herbal sexual stimulants.

"Spam itself is not illegal," Mr. Spitzer said. "When it involves forged documentation and identity theft, it clearly is illegal." The previous week, Mr. Carmack was ordered to pay \$16.4 million to [EarthLink](#), the Internet provider he used to send the spam, after he did not respond to a civil suit the company had brought in federal court in Atlanta. While trying to deal with spam email EarthLink had spent the better part of a year trying to track down Mr. Carmack, who was simply referred to as the "Buffalo spammer" before his true identity was known. Last year it filed a suit against an unnamed defendant, referred to as John Doe, in order to gather evidence and identify the actual spammer. When he was arrested, Mr. Carmack did not have a lawyer. An Erie County public defender, Don Barry, was assigned to assist him. But the judge, Diane Devlin, determined that Mr. Carmack owned his own business and was not entitled to a court-appointed lawyer, Mr. Barry said in a telephone interview yesterday. A woman answering Mr. Carmack's telephone yesterday afternoon said he was not home and declined to provide further information. At the time of this article, his next court date was set for Monday May 19<sup>th</sup>

Note, this document is not in it's desired "finished form" but is submitted to meet the May 16<sup>th</sup> deadline. A revised copy will be submitted to superceded it.

Joseph Steinhauser.