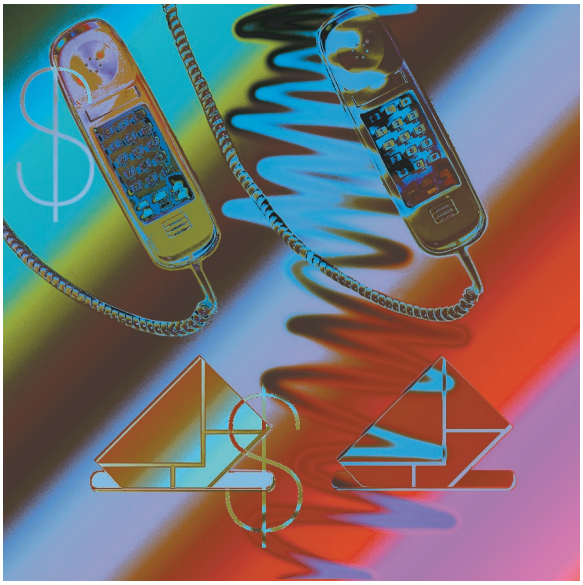
Technical forum



Selling interrupt rights: A way to control unwanted e-mail and telephone calls

Among the great irritations of modern life are unwanted e-mail (often referred to as "spam"[1]) and unwanted telephone calls. In this article I present an approach to controlling these intrusions.

The key idea is simple: My attention is a valuable commodity. If you (the sender) want to interrupt me by putting a message in my e-mailbox or by making my telephone ring, you must pay me for the privilege of doing so. More precisely, you must make a *binding offer* to pay me. If I am happy to hear from you, I will decline the payment; otherwise, I will collect it. This payment compensates me for suffering an unwanted interruption and—more importantly—it has cost you something to bother me. Since interrupting me is no longer free, advertisers and fund-raisers will no longer choose to send me repetitive, poorly targeted, low-yield messages.

Each recipient can set his or her own price. For example, I might set the potential cost of sending an e-mail message to me at $1.00. If you want my phone to ring, the potential cost would be $5.00, or perhaps more if you call at dinnertime or early in the morning. Of course, my friends and business associates would never actually pay these fees. I would only collect the fee from callers who have annoyed me. But once I have been interrupted, it's my decision whether to collect the fee, not the sender's.

People in the public eye may have to set their price much higher to avoid constant interruptions. People who are not bothered much by these messages might charge only a few cents—just enough to discourage the truly indiscriminate mass marketers.

Here's the catch: Such a system will only be accepted if we can make it relatively painless and hassle-free, both for the owners of phones and e-mail accounts and for their nonspamming friends and associates. In the rest of this article, I suggest some ways in which we might accomplish that.

There have been a number of proposals to combat spam through the use of a delivery fee, to be optionally collected by the message recipient. The idea of an "e-stamp" fee for e-mail is generally attributed to Esther Dyson (see Reference 2, for example). Brad Templeton's proposal is a version of e-stamps.[3]

But the details are critically important if the scheme is to be widely adopted by the general public. The version presented here is convenient for users, requires no new laws, no new e-payment or e-signature schemes, and it works equally well for telephone calls and e-mail.[4]

The problem in more detail

The flood of nuisance calls and telemarketing calls is a serious and fast-growing problem for anyone who owns a telephone. The problem is especially serious if telemarketers obtain your cell-phone number: a constantly ringing cell phone is especially annoying, but many of us are reluctant to turn the phone off lest we miss an important call. Unwanted faxes are also an annoyance because they waste paper and ink, costing the recipient money.

E-mail spam is a serious problem for those of us who depend on e-mail (and soon that will include almost everyone). Although the cost and inconvenience of each interruption may be small, the cumulative effect of all these intrusions can be substantial.

The problem becomes worse every year as more and more advertisers, entrepreneurs, and fund-raisers decide that your privacy and tranquility are less important than their desire to make some money. The problem is that it costs them next to nothing to bother you. If only a tiny fraction of recipients respond positively to whatever they are offering, they achieve their goal. That is true even if they anger all the other recipients, who have no effective way to strike back.

There is often a strong emotional component in our reaction to spam. Many of us are infuriated by these constant, uncontrollable intrusions. We feel helpless in the face of this flood, and we are angry with those strangers who violate long-established norms of courtesy to satisfy their own greed. The anger grows if the sender is unapologetic, rude, aggressive, or pretends to offer an "opt out" or "do not call again" procedure that doesn't actually work. Many of these unwanted messages are offensive to certain recipients: ads for sex and gambling sites, illegal chain letters, scams, or offers for semi-legal drugs. For many of us, the anger caused by these intrusions is a greater distraction than the intrusions themselves.

Spam is a privacy issue. When we complain about the erosion of personal privacy, we may be concerned about dangerous stalkers or of having our Web-browsing habits made public. But a more immediate concern for most of us is the fear that our personal information will fall into the hands of unscrupulous marketers, who will then torment us with unwanted calls and messages. How did you react the last time a store clerk asked for your phone number or an on-line merchant asked for your e-mail address? You may have handed over the information, but you probably did so reluctantly.

So spam is a serious problem. If phone and e-mail customers could pay a small monthly fee to have this problem magically disappear, many would gladly do so.

Bad solutions

Before discussing the proposed solution, we first examine the shortcomings of current proposals.

Legislation. One much-debated solution to the problem of spam is legislation: objectionable forms of electronic advertising and telemarketing would be banned. Unfortunately, it is very hard to define precisely which messages and behaviors should be illegal. One person's objectionable spam is another person's welcome source of information. Charities and political organizations are among the worst offenders, but legislators are reluctant to interfere with their fund-raising efforts.

If a law banning spam is not written very carefully and very narrowly, it could easily intrude upon our First Amendment right to free speech. And, of course, well-funded lobbyists for the spam industry are working tirelessly to ensure that any legislation is full of loopholes. Even if wise laws could be enacted in this area, enforcement would be very difficult. As long as the Internet allows the free flow of messages across national borders, spammers can simply move their operations to a country that lacks anti-spamming laws.

Many states have recently enacted laws requiring telemarketers to respect a unified statewide "do not call" list. A federal law of this kind is under consideration. But even then problems remain: it is hard to define exactly who qualifies as a telemarketer under this law, loopholes abound, and it is difficult to enforce these laws when messages may cross state and national borders.

Spam filters. A number of software "spam filters" have been developed. These programs try to recognize unwanted e-mail messages and place them in

a special "probable spam" folder, rather than the normal in-box folder. Most spam-filter programs classify messages based only on the form and content of the message headers, which adhere to a standardized and easily parsed format. For example, messages whose headers show they are from known spammers or from Internet sites associated with known spammers may be rejected. This method does not always work because spammers can change their apparent net addresses faster than the list of known offenders can be updated. Also, there can be legal liability for the software vendor if innocent (or even not-so-innocent) sites are denied access because they have been classified as spammers.

Some systems have attempted to reject spam messages based on the content of the "Subject" line or the message body, looking for phrases such as "make money fast." Unfortunately, these content-based methods are not very reliable. Users must either risk missing some messages that they really want to see or they must periodically look at the contents of the "probable spam" folder in order to find any legitimate messages erroneously filtered out. The need to review rejected messages defeats the whole purpose of the spam filter, which is to get these messages out of your life once and for all. So, while many recipients employ software filters to *reduce* the amount of spam they receive, few would claim that filtering systems come close to solving the problem.

At present, there is no effective technology for filtering phone calls. In general, this would require speech-understanding technology that is far beyond the current state of the art. Some telephone systems do allow users to block calls from specific callers (usually for a fee), but again it is easy for telemarketers to circumvent this mechanism.

Some devices currently on the market send a fake "line disconnected" tone (known as an "SIT" or "special identification tone") back to the caller. Human callers simply ignore this signal, but the auto-dialing machines used by large-scale telemarketers may be fooled into removing the supposedly inactive phone number from their calling list. Unfortunately, such schemes are self-defeating. If this technique becomes popular, telemarketers will simply reprogram their auto-dial machines to ignore these signals.

Unlisted phone numbers and secret e-mail addresses. As a last resort, many users opt for an unlisted phone number or attempt to keep their primary e-mail address secret—available only to a small circle of friends and associates (the user's in-group). This approach has two disadvantages.

First, if the secret number or address is compromised, changing it to a new one is a major inconvenience. Not only must a new account be created, but all members of the recipient's in-group must be notified. Anyone omitted is suddenly unable to communicate with the recipient.

Second, having an unlisted number or a secret e-mail address is inconvenient for both the recipient and the sender. For anyone not in your in-group, it is as if you don't have a phone or an e-mail account. These people have no easy way to get in touch with you, even if they are quite sure that their call would be welcome. Many times a day you must decide whether to give the secret number to people that you deal with: the clerk at the store, or the mechanic fixing your car. If you give out the number too often, it will sooner or later be compromised, and you will face all the hassles listed above; if you don't give it out, your life can become very inconvenient.

Some people get around this by having one unlisted phone line that rings, plus a listed number that only takes voice messages. Similarly, they may have a public e-mail account that is known to everyone, and a private one that is known only to the in-group. But even this solution can be awkward, and it requires periodic review of the messages stored on the public account, which is probably full of spam. At best, it is a partial solution.

A better solution

Let's begin with two observations.

First, only the recipient can decide if a message was, in fact, unwelcome, and this can only be done *after* the interruption has occurred and the message has been received.

Second, though recipients may feel powerless to deal with spam, *the recipient owns and controls the devices that ultimately execute the interruption*: the telephone that rings or the computer that stuffs a new message into the recipient's in-box. Computers and most modern phone sets have the ability to execute a fairly complex policy on the recipient's behalf, deciding in each case whether to allow the interruption.

So the problem is to come up with an easily executed policy that does what the recipient really wants. It

must allow the recipient's friends and associates to contact him or her with little or no additional inconvenience, it must allow unexpected contacts from friends or welcome strangers, and it must block or discourage all spam—that is, all messages that will ultimately turn out to be unwelcome. How can we accomplish that?

The proposed solution has three parts:

1. Each phone or e-mail account has an *accept list* that is maintained by the owner and that consists of the owner's friends and associates. Messages from people on this list are delivered without further ado.
2. The owner of a phone or e-mail account can create *interrupt tokens* and provide them to people and companies that might have some legitimate need to contact the owner in the future. An interrupt token is a numeric code that can be attached to a message, allowing it to be delivered.
3. Uninvited callers or mail senders must make a binding offer to pay an *interrupt fee* to the recipient. The fee is, in effect, held in escrow. If the call is completed and if the recipient chooses to collect the fee, the money is transferred to the recipient's bank account; if not, the fee is returned to the sender, or perhaps is never collected in the first place. There are a number of ways in which this payment system might be implemented. The primary goal is to minimize the inconvenience to the owner and to welcome callers.

We can now examine each part of this scheme in more detail. To avoid confusion, we focus first on the version of this system for telephone calls. Later we consider the analogous version for e-mail. We assume that the telephone set has a computer in it with some nonvolatile storage and a decent user interface. Of course, the telephone set and the computer don't necessarily have to be in the same box, as long as they can communicate somehow.

The accept list. For each telephone number, the owner creates an accept list. This is just a list of telephone numbers from which calls will be accepted unconditionally. The originating telephone number can usually be determined via "Caller Identification," a service available to most telephone users in the U.S. and in many other countries.

The list can have "wild cards" in it. For example, I might choose to accept all calls from 412-268-XXXX, which is the exchange for the Carnegie Mellon campus. If that policy later becomes a problem, I can simply remove or narrow this entry.

For callers on the accept list, the telephone system behaves just as it always has. That is, the anti-spam machinery imposes no new burden on these callers. The only new burden on the owner of the phone is the need to maintain the accept list. The user interface should make it easy to add, review, and delete names and numbers. It should also be easy to download an accept list from the owner's electronic datebook or computer, and it should be easy to transfer an accept list from one phone to another.

Uninvited callers or mail senders must make a binding offer to pay an interrupt fee to the recipient.

Interrupt tokens. If you want to call me but you are not on my accept list, or if you are not calling from your usual phone, you must provide a valid interrupt token. Otherwise, my phone will not ring and you will hear a recorded message explaining what to do.

An interrupt token is just a randomly generated sequence of perhaps ten digits—a sort of password—that is associated with my specific phone number. Each potential caller is given a distinct interrupt token. My phone set contains software for managing these tokens—a *token management system* or TMS. When I want to give someone a token for my phone, I just ask the TMS to generate a new one and to remember that this new token is now valid. For each outstanding token, the TMS remembers whether it is *single-use* or *multiple-use*, an expiration date, and optionally a record telling who the token was given to. Some tokens may only be valid for calling at certain times in the day—only during business hours, for example.

When a call comes in, the phone set silently answers. A recorded message asks the user to key in a valid interrupt token. If a token is received and if it is on my list of valid tokens, the phone then rings; if not, the caller receives a further recorded message telling how to proceed. (I will say more about that below.) If the incoming token is single-use, it is deleted

from the list of valid tokens once the recipient has answered.

Of course, the caller's telephone may be smart enough to remember tokens as well as phone numbers and to deliver the appropriate token automatically whenever one is needed. This saves time, and it could become a popular option for smart phones, which must store a lot of numbers in any case. But low-tech callers using standard touch-tone phones can also use this system. They simply write down the token in their address book, along with the owner's phone number, and key in the token upon request.

Multiple-use tokens can be given to friends and associates who call you frequently, but who do not always call from the same phone. Such tokens can also be given to companies with whom you frequently do business. If an unscrupulous company should sell this token to a telemarketer or begin using it in an obnoxious way, you simply de-activate that token. This does not affect your other friends and associates, who all have distinct tokens. When you ask someone to call you back, you give them a single-use token as well as your phone number.

Sometimes you may need to create a new token while you are away from your home phone. Perhaps you are in a store placing an order, and you want to give the clerk a single-use token so that the store can call you when the item comes in. There are several ways in which this can be handled. The low-tech solution is to pre-generate a few spare tokens and to carry them around on a piece of paper. When you hand one out, you just cross it off the list and perhaps make a note of the person you gave it to. A more convenient solution is to use a cell phone to generate a new token on the spot. Your cell phone can then call your home phone to update its TMS database.

Interrupt fees. If you want to call me but have not obtained an interrupt token in advance, you must make a binding offer to pay whatever interrupt fee I may demand. If you don't do this, my phone won't ring. Once we are connected it is my choice, as the recipient of the call, whether to collect this fee or not. If you are a telemarketer, I probably will collect the fee. If you're a long-lost high-school friend, I probably won't collect. If you are calling on behalf of the local public television station or my alma mater, I might not collect the first time you call, but that would change if you become a frequent pest.

The most convenient way to implement this system requires the cooperation of the telephone companies. They already have the machinery in place to collect fees from callers. This is used for long distance, 900 numbers, and for services such as directory assistance. The fees appear on the caller's phone bill. If the caller refuses to pay, it is treated like any other unpaid bill. The caller's phone service may be terminated and his or her credit rating may be affected.

The caller would hear something like this:

> [Distinctive machine-recognizable tone that encodes the amount of the required interrupt fee.]
>
> *Please enter a ten-digit interrupt token now. If you do not have a valid token, the call cannot be completed unless you authorize a $x payment, which will appear on your phone bill. The called party may choose to accept or decline this payment. Press star-star now to authorize this charge. For more information, call 1-800-555-1234 or visit Web page www.whatever.com.*

(The phone number and Web site above are maintained by the recipient's phone company or by a consortium of phone companies.)

The caller does not have to listen to this whole message. If the caller's smart phone is prepared to send a token, it can do so as soon as it hears the distinctive tone. Or the caller can begin entering the token manually or can authorize the charge as soon as he or she hears the start of the message. A caller who is not familiar with this system would listen to the whole message and perhaps would consult the Web site or the 800 number for a more detailed explanation.

The recipient's phone will indicate (with a visual display or a distinctive ring) whether the call was completed via the accept list, a token, or whether a fee was offered. In the latter case, the default is to decline the fee, but the recipient can press a button during or after the call to collect the fee. The caller may try to persuade the recipient not to collect the fee, but it is ultimately the recipient's decision.

A system like this can be implemented without the cooperation of the phone company, but it is somewhat less convenient for callers. It would no longer be an option to simply add the fee to the caller's

phone bill. Instead, the caller would hear something like this:

> [Distinctive machine-recognizable tone that encodes the amount of the required interrupt fee.]
>
> *Please enter a ten-digit interrupt token now. If you do not have a valid token, one can be purchased by phone at 1-800-555-1234. The cost is $x. The called party may choose to collect this payment or refund it to you. Press star-star to call to this number now. Alternatively, you can purchase the token on line at www.whatever.com.*

When you call this number (a *token agent*) or visit the Web site, you will be asked for the number of the phone you wish to call and you will be asked for a credit-card number, a prepaid account that can be debited, or some other form of guaranteed payment. If some secure Internet micro-payment scheme becomes well established, it could be used here. Once payment has been assured, the token agent then hands the user a ten-digit *conditional interrupt token* that can be used to complete a single call to the number in question.

If the call is completed and the recipient chooses to collect the fee, the recipient's phone set signals the token agent that the fee for that specific token should be collected and transferred to the recipient's bank account. If no such notification is received within, say, 24 hours, the token expires and the charge is refunded to the caller (or is not billed in the first place).

The e-mail version. The procedure for filtering e-mail is analogous. It uses the same three-part mechanism: an accept list, a system of interrupt tokens, and an interrupt fee that must be offered by uninvited senders.

When a message arrives at my machine or mail-server, it is examined. If the sender is on my accept list, the message is passed through to my in-box. If the message header or body contains a *Token:* field with a valid ten-digit interrupt token, it is likewise passed through to the in-box. If the message contains no valid token, the sender receives a machine-generated reply:

> *E-mail messages cannot be delivered to the account ⟨foo@xyz.com⟩ unless the message contains a valid ten-digit interrupt token. If you do not have a valid token for this account, you can purchase one for $x. The recipient may choose to collect this payment or refund it to you. See the Web site "www.whatever.com" for details.*
>
> *Once you have obtained a valid token, please re-send your message with a field like this in the message header or on a separate line near the start of the message body:*
>
> *Token: xxxxxxxxxx*

This is a bit inconvenient for the sender, especially if the sender has not kept a copy of the original message. However, that problem would only exist the first time a particular sender tries to contact you. After that, the sender would know that a token is required.

The inconvenience of rejected messages would occur less frequently if we create a protocol that allows potential senders to determine whether a given e-mail address requires a token *before* the message is actually sent. Smart e-mail software would routinely check this before sending a message to a given recipient. This service could be a simple Internet directory or it could be something like the "finger" protocol. At present, users are reluctant to reveal their e-mail addresses via such mechanisms for fear that more spammers will find them, but in this case the spammers would also learn that it is futile (or expensive) to send unwanted mail to this particular address.

The Web site mentioned in the response is a token agent whose function is to issue conditional interrupt tokens, just as in the telephone case. In the case of e-mail, we can safely assume that all senders will know how to access a Web site, so we don't need an 800 number. If the recipient of a message chooses to collect the fee, the recipient simply clicks the appropriate button in his or her mail reader. The agent is then notified (via a coded e-mail message) that the fee should be collected. If the recipient does not explicitly collect the fee within a certain period, the fee is refunded to the sender or is not billed in the first place.

Here is how the proposed solution would work for mailing lists. When I join a mailing list, I provide a multiple-use token that allows the (slightly updated) mailing-list software to forward messages to me without a problem. I must provide this token because few mailing-list owners will want to risk offering a payment to everyone on the list. Because a lot of spam

comes in via these lists, the mailing-list owner will require that anyone posting to the list must make a binding offer to pay a significant fee. If someone posts a legitimate message to the list, this fee will not be collected, but spammers will be required to pay. This procedure does not require that messages be approved by a moderator *before* they are sent to the group—a labor-intensive task. Instead, messages are forwarded to the list automatically, and the list owner collects the offered fee whenever he or she is alerted to an inappropriate message appearing on the list.

Conclusions

The advantage of the scheme proposed here for the people who adopt it is clear: for them, the problem of e-mail spam and unwanted telemarketing calls would be almost completely eliminated. Those unwanted messages that get through because someone actually paid the required fee would be viewed as a windfall rather than a nuisance. Users of this scheme would no longer feel compelled to conceal their phone numbers or e-mail addresses.

The cost to each user would be relatively small. Users would have to buy at least one new "smart" telephone set and/or upgrade their e-mail software. They might have to pay a small fee—perhaps a dollar or two per month—to their token agent (possibly their phone company or Internet service provider). The actual income to most users from collecting interrupt fees would probably be negligible—the fees serve mainly as a deterrent.

The primary disadvantage of the proposed scheme is some inconvenience for callers, and perhaps some momentary anxiety for welcome but unexpected callers, who would have to offer a payment and hope that the recipient doesn't collect it. But once people become used to this system, the anxiety should be minimal.

This scheme requires no new legislation. Politicians and legal scholars may argue endlessly about freedom of speech versus privacy, but certainly each of us has the right to ignore or block phone calls or incoming e-mail messages, and to do this systematically if we choose to. Similarly, this scheme requires no new e-payment mechanism beyond the ones we already use for paying our phone bills and for shopping on line.

To implement and popularize this scheme will require four actions:

- Produce the enhanced mail software and the smart telephone sets (simple software extensions of existing smart phones). This is a money-making opportunity for someone. Note that if the system is implemented by a phone company or an Internet service provider, the necessary functionality could be provided "upstream" as part of the service rather than in the end-user's equipment.
- Establish a token agent, accessible both by phone and through the Internet. As mentioned before, this agent may just be an existing phone company or ISP. This too is a money-making opportunity. The token agent would keep a percentage of each fee actually collected, and would probably also charge the account owner a monthly fee for this service. Many people would gladly pay a dollar or two per month for this service, and the number of potential customers is enormous.
- Through advertising, newspaper columns, and other media, explain the new system to the general public so that people won't be surprised the first time they encounter it. Some people may not adopt the system immediately and may resent being asked to offer a payment in order to call or e-mail a friend. But if the system is explained properly, everyone will understand that this is part of a plan to stamp out the universally hated telemarketing calls and spam.
- The parties involved in implementing this scheme (phone companies, ISPs, token agents, and makers of mail software and token-aware phones) should work together to develop standards. This will minimize confusion and facilitate widespread adoption of this scheme.

This scheme is more convenient for everyone if telephone companies and ISPs take an active part in implementing it, and if they all agree on a common set of conventions. Message traffic will be reduced if the message filtering is done "upstream" by the service provider rather than by the end-user's telephone or mail software. However, if these service providers are slow to adopt the scheme, it can be adopted incrementally, one user at a time. As long as at least one token agent is in business, and at least one company is producing phone sets and e-mail software that implement these policies, individual users can adopt the scheme whenever they choose. There is no need to wait until the system is adopted by everyone else, and no need for a huge up-front investment to reorganize the worldwide communication system.

Acknowledgments

I would like to thank Michael Young, Stuart Feldman, Steve R. White, Toby Everett, Arthur Ciccolo, and several anonymous referees for input and constructive criticism that helped shape this contribution. However, the views expressed here are the author's, and do not necessarily reflect the views of these colleagues or of IBM.

Cited references and note

1. SPAM® is a registered trademark of Hormel Food Corporation, referring to a family of ham-like products. The use of the word "spam" to refer to unwanted e-mail is of obscure origin, but may have something to do with a comedy sketch by the Monty Python group depicting a restaurant in which every dish contains spam.
2. M. W. Lynch, "Unlovely Spam," *Reason Online* (October 1997), http://reason.com/9710/col.lynch.shtml.
3. B. Templeton, "E-Stamps," http://www.templetons.com/brad/spume/estamps.html.
4. Some ongoing discussion of these issues may be found at a Web site maintained by the author; see http://www.cs.cmu.edu/~sef/spam-discussion.htm. The author can be reached at fahlmans@us.ibm.com or at sef@cs.cmu.edu.

Scott E. Fahlman
IBM Research Division
Hawthorne, New York