

An Overview of the Email Channels Technology Underlying ZoEmail

Robert J. Hall
AT&T Labs Research
180 Park Ave, Bldg 103
Florham Park, NJ 07932
`bob-2EChanSumm-@channels.research.att.com`

April, 2003

The views expressed in this paper are those of the author alone, based upon his experience in researching, implementing, and analyzing anti-spam technologies. They do not reflect those of AT&T Corp. nor those of ZoEmail LLC.

1 Key Ideas

A spammer can't send you email if he doesn't know your address.

The patented[3] Email Channels technology[1, 2], invented and originally developed by me during the latter half of the 1990s at AT&T Laboratories Research and currently being commercialized by ZoEmail LLC[4], allows a user effectively to have many variants of a common “base” address, with each variant to be used by a different set of correspondents. The variants, also known as *channels* or *channelized addresses*, are chosen so that knowing one will not reveal any of the others. Typically, a user would allocate a channel for private use by each close friend or colleague, ones for use by particular companies, services, or websites, and general public channels for use on business cards and personal web pages. By having many channels, if a correspondent sends spam and won't stop, one simply clicks “close channel” and that person's future messages are rejected by the mail servers *before* they are accepted and stored on the ISP's machine, *before* they are downloaded through a slow modem link, and most importantly *before* the user sees them. (There is also an option to “switch” the channel of a legitimate correspondent, in case that correspondent has accidentally leaked the channel address to a spammer.)

Channelized address formats. There are many ways to embed the channel identification into a standards-compliant email address. Current channelized systems (including my original system and ZoEmail LLC's first release) insert the *channel identifier*, a substantially unguessable character string uniquely designating the channel, between hyphens immediately to the left of the at-sign:

bob-2EChanSumm-@channels.research.att.com

rjhall-3SpamForum-@zoemail.com

...

(For those interested, the detailed structure of this format are discussed in reference[1].) In another embodiment of the idea, the user Bob of the server zoemail.com could have the addresses

tiger@Bob.zoemail.com (easy to remember/type/tell)
alice3556@Bob.zoemail.com (private for alice@foobar.com)
uixp7aggc@Bob.zoemail.com (random, for use with e-commerce site)

...

Here, the user identification has moved entirely to the right of the at-sign and the channel identifier is to the left. I believe this has conceptual as well as implementational advantages for high scale deployments which are, again, too detailed to discuss in this paper. Of course, many other channelized address formats can be imagined as well.

The channel identifier string itself can be generated in many ways. For example, it is clearly desirable for users to be able to choose some of the channel identifiers to be memorable and easily typed. However, it is also useful for the PCA to generate channel identifiers randomly (using strong pseudo-random number generation) for maximum resistance to guessing attacks.

The Personal Channel Assistant. Now, managing many different return addresses would be a headache if not for the Personal Channel Assistant (PCA), a software agent that takes care of the details of managing the individual channels. With the PCA, typical day-to-day usage looks and feels just like it does today, with extra controls used only when it is necessary to close a channel or allocate a channel for a non-routine purpose.

Each user's PCA communicates channel-open/close information with a "Channels Bouncer", an SMTP server with the capability of authenticating the messages' channel addresses as they arrive.

One embodiment of the PCA acts as an email proxy, which can be used with any off-the-shelf email user client, so end users need not change their email client software at all. Email Channels can be implemented within a web mail system as well, which avoids the need to distribute the PCA software to client machines, allows them to access their channels protected mail from anywhere in the Internet, and provides reliable backups of the user's PCA-enhanced address book database.

Compatibility with Existing Email. Since channelized addresses are simply standard email addresses, Email Channels technology interoperates with all RFC-compliant email servers, features, and applications, such as MTAs, address books, mailing lists, autoresponders, forwarders, workflow engines, and even filters. By virtue of this standards compliance, Channels-protected users seamlessly interoperate with all others.

Generalizations and Enhancements. Many variants of the basic Channels behavior can be implemented within the PCA and bouncer. For example, each Channel can have associated a user-controlled set of rules for how to treat messages received on that channel. Examples of such special treatment can include restriction to certain senders; time-based status changing from "public" (messages from anyone may be received on it) to "restricted" (only messages from a designated set of correspondents may be received on it) or "closed" (messages may no longer be received at all on it); limitation of the total number or frequency of messages accepted; or special routing to other processing programs like autoresponders, folders, or workflow agents. Another useful capability implemented in some embodiments is per-channel automatic encryption of outgoing and decryption of incoming messages flowing on the channel.

A Channels-based system can be used in many different email architectures. In addition to the ISP- and web-mail configurations mentioned above, the idea can be used in corporate and governmental messaging applications, which may have special requirements relating to organizational functions and structure. For example, it could be used as the basis for a high security messaging application enforcing prioritization and quality of service guarantees based upon the channels idea. And beyond email, the Channels idea of a

user controlled set of address variants can even extend into other telecommunications domains, such as telephony or instant messaging.

2 Introduction and The Directory Problem

Obviously, there must be ways for a Channels user to give out valid addresses for use by desired correspondents the first time such a correspondent wishes to send a message. This is termed *introduction*. Since channelized addresses are simply email addresses, all well known (and several not so well known) introduction methods can be used, if desired. However, some such methods will attract usage by spammers and should be avoided.

Suppose Alice wants to send email to Bob. The first introduction scenario, and the easiest way for Alice to get Bob's address, is for Bob to send to Alice first. Whenever the PCA notices Bob has not sent to someone before, it opens a new channel and puts it into the return address of the message. Alice needs only to hit *Reply*.

Another scenario starts with Alice asking Bob over the phone for his email address. For this purpose, Bob gives Alice a memorable, easily typed channelized address, such as `tiger@bob.zoemail.com`. Since Bob gives this address to friends only, he can give out the same one to each. The friends can be switched to other (distinct) channels by the PCA later as necessary.

Another common scenario concerns what address Bob fills into forms. For example, world-wide web sites often require this. In this case, if Bob wishes to, he can easily create a new channel for each web site. The PCA tracks the source of any undesired messages sent through one of these addresses.

If Bob is not quite so energetic, he can allocate a single "commercial" channel and use it for all web sites. If too much undesired traffic builds up on such a channel, he can simply close it once in a while and make a new one. This is less precise in managing unwanted traffic from commercial companies, but mirrors what many people already do today using multiple ISP accounts. If the user wishes to, he could use the PCA's database to selectively notify some of the entities currently using the closing channel of a switch.

Finally, *directories* are the logically trickiest introduction technology. After all, by publishing in a directory (either a centralized directory or on a web page, for examples) one is attempting to let anyone who wants to contact them do so. However, this *per force* gives a spammer a way to do so as well.

Many introduction approaches have been proposed and implemented,

such as challenge/response systems, trust webs, and computation-based schemes. Email Channels can be used with any or all of these.

One interesting technique enabled by channels technology is the *single-use, limited-lifetime (SULL) channel*. Such channels will accept at most one message, from a particular email address, and only for a limited time period, such as 30 minutes. These channels cannot be usefully stored in spammer databases nor burned into spammer CDs because of the timeout feature. And they cannot be used at a particular time to send a “burst” of spam due to the single-use property.

One can use SULL channels for introduction in a couple of ways. First, one could establish a well-known autoresponse channel such as `contact@bob.zoemail.com` (not itself SULL). If a message is sent to that address, a tailored response message is automatically generated which has within it a SULL channel. This will allow the correspondent to use that channel to get a message to the protected user once, after which the protected user can reply, causing the PCA to set up a regular channel. Note that for spammers to exploit this, (a) they must have a valid return address to receive the response, and (b) they must send their message immediately (i.e., within the limited lifetime of the channel, say on the order of 30 minutes). Note that the spammer must *receive* one message for each spam message sent out this way. Thus, to send out a million messages per day, his ISP must receive a million and deliver them to him. While not inconceivable, such a large volume could attract attention of system administrators at the spammer’s own ISP. Thus, two spammer tools, total anonymity and the ability to save and pass around lists of addresses, are defeated by this method.

One can also use SULL channels in a web based directory. The directory user would supply a valid email address to the directory form, and then the directory system would email a message to him with a SULL channel as return address for the looked-up user.

3 Comparison and Possible Synergies

Email Channels has advantages over existing anti-spam technologies.

- *Channels gives the individual a way to positively stop spam.* Part of the frustration of spam is the feeling of helplessness a user feels in not being able to stop it. If spam is received on a channel, the Channels

system empowers a user to close the channel, positively stopping spam from that source.

- *Channels tolerates individual definitions of spam and changing tastes of its users.* There is no universal agreement on what is spam, and yet content-based rule systems and collaborative filtering systems are totalitarian regimes defining what is spam for everyone. If a user actually wants to see advertising about cars (say because she is in the market for one), there is no way to do it if the filter has decreed it spam. With Channels, each individual controls his or her own definition of spam.
- *Channels avoids false positives.* Approaches that filter messages by using rules to judge whether the content of a message contains spam are notorious for filtering out desirable messages as well as spam messages. While their false positive rates for many users are low, many people feel that even one false positive could be critical to their business or other concerns. And, according to industry reports, users who have *specifically requested* advertisements or product information have much higher false positive rates (as high as one sixth of these requested messages are rejected by filters). Email Channels avoids these altogether.
- *Channels does not penalize innocent users.* Blacklists can deny mail service to people simply because they try to send from a range of IP addresses that was once used by a spammer. Reverse DNS checking can remove a person's right to send email because his system administrator made a mistake in configuring the domain name system. These "autoimmune responses" penalize innocent victims and degrade email service worse than spam does. Channels avoids this, because a channel is closed at the discretion of the individual recipient.
- *Channels does not classify all "have-nots" as spammers.* Technologies like cryptographically signed email and pay-per-message ("stamped") schemes require that users reject all mail that does not take part in the scheme. For example, users of the cryptographic scheme must reject all unsigned email. Since the Internet *never* adopts a new technology all at once, these schemes will create a class of "have-nots" and lump them together with spammers. Even worse, more than one such scheme could be adopted by different camps, thereby balkanizing the Internet into non-interoperating zones. This would surely degrade service as

much or more than spam already does. Channels, on the other hand, interoperates seamlessly with all RFC-compliant email technology, so does not have this effect.

There are occasions where Email Channels can work with other anti-spam technologies to solve problems. For example, if one wishes to publish an address widely in a free directory or on one's web page, one could use the rule-based heuristic filters on *only the published channel*. This would cut down the spam received through it significantly, and yet false positives on this introduction channel are probably tolerable. All daily email with known correspondents would take place on unfiltered channels not subject to false positives of filtering nor to spam.

There are many other synergies possible that exploit the power and fine-grained control possible with Channels. For example, in reference[1], I propose a payment-based introduction scheme where *only messages sent to an introductory contact channel must have a payment (or verified IOU)*. Such a pay-per-view introductory channel can be widely published without fear of abuse by bulk emailers. Another example would marry a channels system with an existing *challenge/response* system. Only messages sent without valid channel addresses are met with the challenge.

4 Limitations

All anti-spam approaches have weaknesses as well as strengths; Email Channels is no exception. Its primary limitation is that it is not totally transparent to the user. That is, the user's behavior must change from current patterns of email usage. This could typically start out with the user simply managing two channels, one for friends and one for all others. As the user understands more the limitations of the two-address usage pattern, he can learn more and gradually use more of the power of the approach. Note that many people today maintain several distinct email addresses "by hand", so this is not a totally alien idea. A Channels system allows a smooth transition from one-address user to multi-address power user, with various types of automated support. And of course, a well designed user interface can facilitate this behavior transition.

It should also be remembered that the so-called "transparent" anti-spam approaches are not really so transparent when one considers the impact of their false positives and other service degradations, as well as their high

maintenance costs. Diagnosing these types of difficulties and finding out how to work around them can be extremely frustrating to the user.

While Email Channels is effective at protecting day-to-day communications from the incursion of spam, it does not, in itself, provide a solution to the Directory Problem mentioned earlier. This is a fundamentally difficult problem, due to the logical conflict between wanting both to publish a way by which strangers can reach you, and yet not wanting to publish a way for spammers to reach you. There are, as briefly reviewed above, a number of solutions to this problem, and Email Channels works with all of them. It can provide mechanisms, such as SULL channels and pay-per-view channels, which facilitate them as well.

5 Conclusion

The power of Email Channels stems from the simple idea that a spammer cannot send you email if he does not know your address. Channels allows you fine control over who can send you email, with the PCA managing the bookkeeping, letting you set whatever definition of spam is appropriate to you at a particular time. If you want to receive car ads, you can.

Channels is not susceptible to the wide range of problems to which other anti-spam tools are prone, including false positives, rule set maintenance, guilt by association, yielding control of one's personal or business communications to third parties, or balkanizing the Internet into "haves" and "have-nots". These "autoimmune responses" risk degrading email service worse than spam does.

References

- [1] R.J. Hall; How to avoid unwanted email; *Comm. ACM* 41(3), 88–95, March 1998.
- [2] R.J. Hall, "Channels: Avoiding unwanted electronic mail", in *Proc. 1996 DIMACS Symposium on Network Threats*, Amer. Math. Soc., 1997.
- [3] R.J. Hall, "Communications addressing system", U.S. Patent #5,930,479.
- [4] ZoEmail, LLC. www.zoemail.com

COMPANY OVERVIEW

ZoEmail, LLC (“Company” or “ZoEmail”) has acquired and is commercializing AT&T Labs’ email authentication technology that eliminates all unsolicited email (“spam”) and thereby privatizes email. The technology is compatible with prevalent PC client-based and Webmail systems.

The Company acquired this breakthrough, patented technology in a cash and equity agreement because AT&T Labs recognized that ZoEmail’s technologies, management team and significant depth of marketing expertise would enhance the commercialization of its patented anti-spam technology. AT&T Labs remains an equity holder and partner in supporting both further technology development and marketing opportunities.

Intelligent Messaging To Transform eMail: The AT&T Labs solution is a system that automatically assigns unique “virtual keys” as part of one’s email address for all outside correspondents — in a way that is foolproof, simple, user friendly, and managed automatically. The use of these unique alphanumeric keys in the address field of a message enables the system to intelligently act on that message to effect delivery or non-delivery. This is the foundation of the AT&T patent acquired and enhanced by the Company.

Elimination of Spam: ZoEmail’s initial market entry is as an intelligent email addressing authentication system that completely eliminates unsolicited email and enables user-controlled management of email applications.

The unique alphanumeric keys (“SenderID™”) inserted into the protected user’s “from” address allows the specific outside party to mail back to the protected user. As such, ZoEmail is not a filtering system, but an email address authentication system, which allows the user to simply and easily control what mail he or she receives.

The system far surpasses current filter technologies in capability, user friendliness and effectiveness. With this intelligence at the edge

of the provider’s network, all undesired messages are prevented early on from negatively impacting the service provider’s infrastructure.

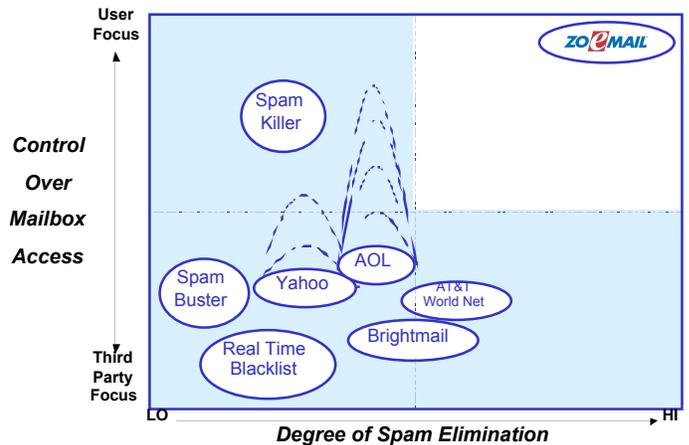
ZoEmail offers an intelligent email system using breakthrough, patented technology to completely eliminate unsolicited messages using a method totally different from the ineffective spam filtering products on the market today.

ZoEmail believes that conventional spam filtering techniques are in an arms race as spammers quickly morph to slip past the latest filtering rules. ZoEmail offers differentiated anti-spam messaging that is not subject to spammer decoding... helping service providers deliver *truly private email* to their customers.

Importantly, because of the unique digital key, ZoEmail users’ addresses are non-transferable and cannot be harvested, shared or resold by spammers.

ZoEmail, with AT&T Labs’ patented technology, is a foundational “market standard” and presents a significant opportunity for teaming with service providers, software integration and other firms, large and small. This technology is also broadly applicable to any message over any network, including Wireless, Instant Messaging, SMS and IP Telephony for potential future applications.

Comparison of Common Techniques



ZOEMAIL BENEFITS TO ISPS AND THEIR CUSTOMERS

ISP's are caught between increasing costs and decreasing revenues. The proliferation of spam has resulted in significant increases in capital investment and operating expenses directly proportional to the amount of unwanted messages processed. Spam's impact on the cost of customer retention is considerable.

An independent research study estimates churn directly related to spam costs an ISP \$7 per year per subscriber (at one million subscribers this translates to \$7 million). New York based ISP PANIX reports that 15% of revenue goes to deal with the spam problem.

ZoEmail will help service providers reduce message storage and bandwidth costs. Customer satisfaction will be enhanced and churn reduced, along with the costs to replace lost subscribers.

End-user loyalty to the ISP will increase with ZoEmail's ease of use and unique capabilities.

For Service Provider, Portal and Enterprise

Product and Service Features

- Webmail and Client-based configuration
- Real-time spam detection — messages are bounced *before* they enter your mail network
- Robust and scalable architecture — designed to support email networks of any size — from regional to international
- Eliminates the need to endlessly update filtering rules
- Optimizes network performance — operating in front of your email system

Benefits

- Reduced subscriber churn and acquisition costs
 - Eliminate spam — increase customer satisfaction
 - Strengthens brand image
 - Re-establishes customer loyalty, value, differentiation
- Reduce network system and storage costs
 - Prevents spam from taking up space in your message storage
 - Reduces time and system resources processing spam traffic
- Lower total cost of ownership
 - Fewer customer service calls, formal/legal complaints to resolve
 - Minimal intervention by system administrator
 - Eliminates need for resources dedicated to manual spam blocking
 - Eliminates need to endlessly update filtering rules
- Control message volume and protect bandwidth
 - Removes unsolicited emails from message traffic — *at the edge, not in your network*
- Simple, user friendly mail management
 - Range of security — under user control

- Fully transparent
- Secure platform
 - Users' mail is never opened, protecting privacy
- Patented, scalable technology
 - Easily scales to more than 10 million mailboxes
 - Protected under U.S. Patent No. 5,930,479
- Shifts the burden of liability (re: "false positives")

For End Users

Product and Service Features

- Works seamlessly with prevalent email applications (Outlook, Eudora, Netscape Mail, etc.)
 - Works on multiple operating platforms — Windows, Linux, Mac OS
- Open, close, change sender's key (allowances and restrictions)
- Automatic routing of child-targeted mail to parents
- Simple, wide range of implementation options
 - Automated "change of address" through user's address book
 - "Business Card" one time use key
 - Website key generation
 - User-defined "white list"

Benefits

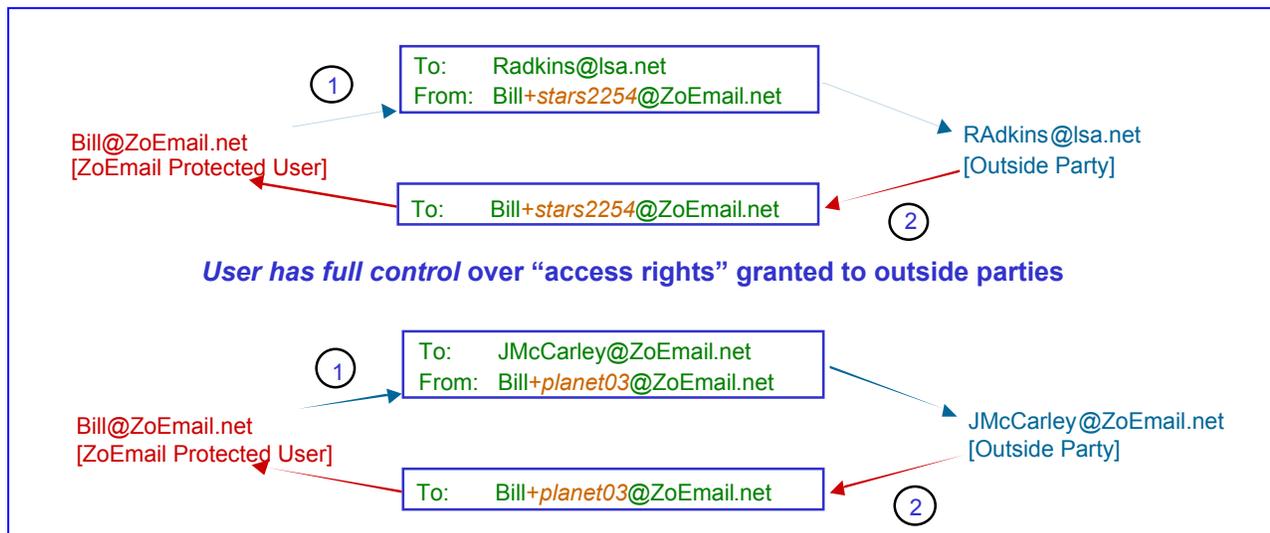
- Eliminates unsolicited commercial emails
- Addresses cannot be harvested from public groups and chat rooms or by spider programs
- Addresses cannot be passed along without approval
- Protects users and their families from unwanted solicitations (e.g., pornography)
- Eliminates potential filtering out of desired email
- Eliminates need to endlessly update filtering rules
- No time wasted reviewing/cleaning out inbox

HOW ZOEMAIL WORKS

The ZoEmail system is based on a simple solution of issuing a self-authenticating virtual key (a specific word and an alpha-numeric token) which is automatically appended to the user's email address. Given this key-based approach, the system puts a virtual gate in front of the user's email address for each outside party — simply and effortlessly.

Whenever a ZoEmail-protected subscriber sends an email, the recipient of that message is automatically given a unique key as a part of the protected user's address. This key opens the authentication gate and gives the recipient permission to email back to the ZoEmail user. Of course, there are appropriate and easy means of access for a legitimate sender who does not have a private key to the protected ZoEmail user. The user has full control over access rights granted to outside parties vs. third party filter services that decide such on their own.

The ZoEmail user has nothing more to do. This key is self-authenticating -- it operates in real time, which means that the email system is neither burdened or slowed down in processing. And, the ZoEmail server does all of this transparently. Sophisticated spammer tactics, such as creating random email addresses, are ineffective against ZoEmail. A ZoEmail user's email address is non-transferable: spammers cannot effectively harvest, share or resell it. Protected users do not have to remember these "virtual keys" — that is done automatically for them.



WHY FILTERS DON'T WORK

Filters are largely reactive and operate principally by attempting to screen on the basis of header / address, subject line or content — either filtering out too much ("false positive") or too little ("false negative").

A number of these filtering systems are augmented by the use of "White Lists" (addresses of acceptable message sources) and "Black Lists" (addresses of known spammers). These lists require constant maintenance and ongoing, somewhat tedious user involvement to remain effective, yet can be circumvented by spammers.

In addition, the spam in these filtered systems is typically not rejected, but diverted and stored in another folder to await further action by the user or administrator. These systems frequently allow the user to turn off the spam filter or regulate it to a less strict level of filtering -- decreasing significantly the benefit to users and service providers.

Spammers use a whole portfolio of tricks: fake subject lines, hijacking of legitimate email addresses, sending from multiple addresses, same "to" and "from" lines, etc. All such spammer tactics are ineffective against ZoEmail's technology.

PRODUCT COMPARISON: ZOEMAIL VS. MAJOR FILTER-BASED SYSTEM

Feature/Benefit	Filter-based	ZoEmail w/AT&T Channels
100% effective blocking of unwanted senders	No	Yes
Prevents unauthorized transfer of addresses	No	Yes
Effective against all unsolicited e-mail	No	Yes
Complete end-user control	No	Yes
Avoids errors due to filtering based on headers, addresses and/or content	No	Yes
Self-authentication checking for fast delivery	No	Yes
Unnecessary to store and review pending file of bulk/ unsolicited e-mail for reliability	No	Yes
Ability to define duration, frequency and other "access rights"	No	Yes
Maintenance requirements	High	Low
Scalability	High	High
Reduces Spam's impact on bandwidth, storage and CPU usage	Possible, but only with tradeoffs	Yes
Eliminates ISP liability for "false positives" and "false negatives"	No	Yes
Loses Mail	Always at risk	<i>Never makes such an error</i>
Permanent solution	Temporary at best	<i>Permanent solution</i>
Costs to administer	Giant and growing	<i>Permanently inexpensive</i>
Allows user to escape (opt out) of problems	No help at all	<i>Provides a simple, complete solution</i>
Allows temporary address (e.g., online purchases)	Can't support at all	<i>Supports fully</i>
Supports parental control	Can't do anything to help this	<i>Supports fully</i>
Can integrate with virus control	Yes	Yes
Identity protection	Can't support this	<i>Can fully support</i>
Protects the user when he signs up at a Website or for a newsletter	Can't support this	<i>Fully protects the user in all situations</i>
Requires a 24/7 staff of pattern matching experts	Requires an ever growing staff	<i>No extra support staff is required</i>
Third party control	3 rd party determines what is "spam" (differing user requirements averaged)	<i>Each user has full control</i>
Stability / predictability	Filtering criteria may change without notice	<i>User in full control</i>

Contact: Mike Oyster, President and COO — 270 Lafayette, Suite 1202, New York, NY 10012
(office) 212.941.8344; (cell) 908-391-4595; e-mail: moyster-3publickey-@zoemail.com