False Positives:
The Baby in the Bathwater
&
Placing Responsibility for Spam Where it Belongs:
The Case for Vendor Liability

Anne P. Mitchell, Esq.
President & CEO, Institute for Spam and Internet Public Policy

Presentation to 3rd AP Net Abuse Workshop
August 25, 2003
Busan, Korea

Section I – False Positives: The Baby in the Bathwater

False Positive. ***n*****. 1. A test result that erroneously assigns an improper value to a test subject, due particularly to insufficiently exact methods of testing. 2. A legitimate, wanted email which is incorrectly identified as "spam".**

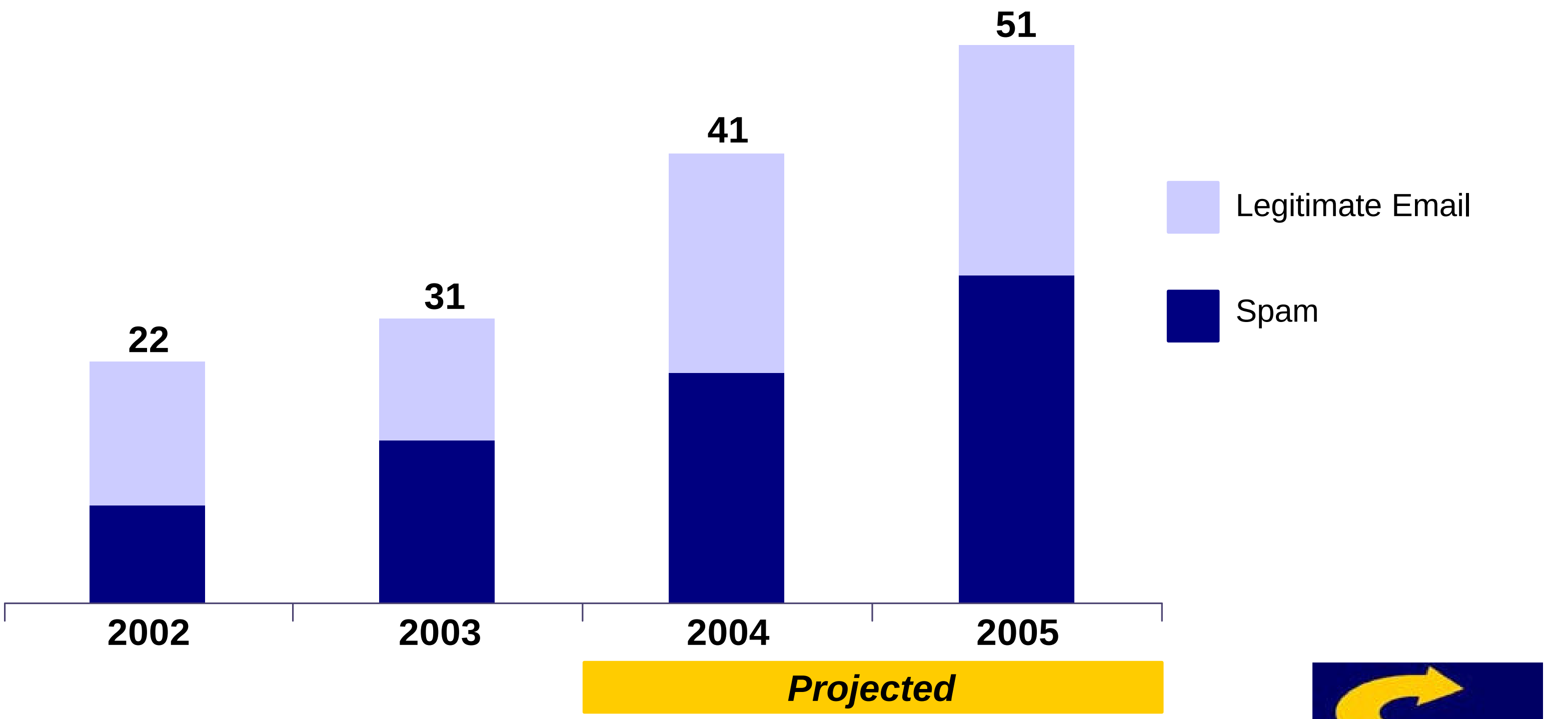
False positives are on the rise.

- A false positive occurs when legitimate, wanted email is incorrectly identified as spam.
- On average, 15% of wanted messages do not get through to the inbox because of the false positive problem.[1]
- David Ferris of Ferris Research estimates false positives will cost US companies alone $10 Billion in 2003.

Note[1]: Assurance Systems, August 2003..

The rate of false positives is increasing along with the volume of spam.

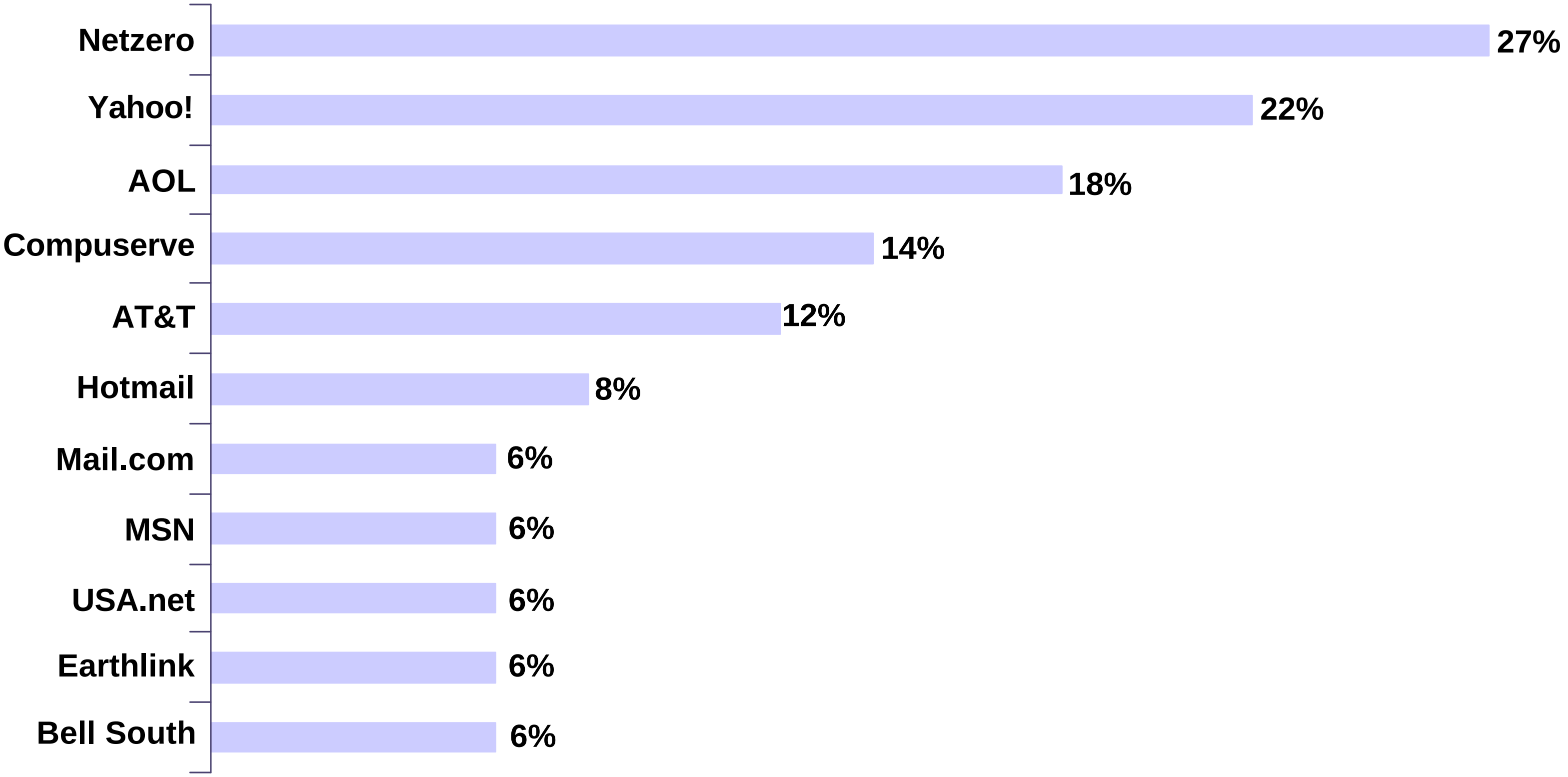
World-Wide Email Messages
(Billions)



Source: The Radicati Group.

False positives are also increasingly problematic for ISPs.

Non-Delivery of Legitimate Email Messages



Source: Assurance Systems, August 2003..

To demonstrate how false positives are a problem, these opt-in messages were recently delivered to the Yahoo! junk-mail folder.

- 1-800 Flowers
- American Airlines
- Barnes & Noble
- Bid4Vacations
- Buy.com
- Clickz
- Dell
- Direct Magazine
- eBags
- eMarketer
- eWeek
- Fidelity
- Frontier Airlines
- Gorp.com
- Harvard University
- iGo
- MediaPost
- Midwest Express
- Morningstar
- Microsoft Carpoint
- MyPoints
- Frommer’s
- 11thHour Vacations
- New York Times
- Orbitz
- Palm
- Starwood
- Topics
- United Airlines
- Venture Wire
- Wall Street Journal
- Wired Magazine
- Yesmail Network

Each piece of email in this study was requested and not received by the intended recipient.

Source: Assurance Systems, August 2003..

Why do false positives exist at all?

- As the administrators of inbound mail servers draw their spam filters ever tighter in an effort to cope with the burgeoning flood of spam, it is inevitable that more and more legitimate email will get caught by the filters as well.
- The trick is to minimize the false positives while maximizing the amount of spam stopped at the border.
- Many inbound email policy makers are not aware of the existence, let alone the severity, of the false positive problem. Others are aware of the phenomena, but don't necessarily see it as a "problem".
- Some anti-spam measures, such as some DNS blocklists, create false positives by design, the intent being that the pain caused to a site by having their legitimate email blocked will lead to the site taking care of their spam problem in order to have the block removed.
- For ISPs, false positives can be particularly problematic as their customers – the users who are paying them – expect to receive the the email they want and have requested.
- False positives are more than just a nuisance, they can lead to serious business and personal hardships.

False positives cause harm to ethical, non-spamming businesses

“We have learned that our ownership of the macslash.com domain did in fact expire without our knowledge. The reason we never received any of the domain renewal notices from Dotster is … that the folks at mac.com have at some point classified all mail from Dotster as spam, therefore trashing our domain renewal notices without our knowledge.” -- Macslash.com is now macslash.org, Macslash.org website, May 21, 2003

“In one week alone, a whopping 10 percent of TidBITS recipients - 4,000 readers - failed to receive the news they had requested simply because a TidBITS writer made a passing reference to Viagra. Worse yet, in writing about the filtering fallout Duncan was reduced to referring to Viagra as "a well-known Pfizer drug for men," lest repeating the brand name cause his report to again run afoul of the filters.” -- ‘Net Buzz, Reseller News Online, August 5, 2002

“What causes some email systems to misinterpret TidBITS as spam or malicious email? … Jeff Carlson's article on the Palm i705 in TidBITS-635 made a passing reference to a well-known Pfizer drug for men, technically known as sildenafil citrate. Our mail error logs indicate over 2,500 TidBITS issues were rejected by over 1,000 sites because they contained the drug's name; many of the rejections were from relatively high-profile sites like the Association for Computing Machinery (ACM) and VeriSign.” – Email Filtering: Killing the Killer App, TidBITS, July 7, 2002

A few companies have created solutions that help combat the false positive problem.

- **Habeas**. Their Sender Warranted Email product line identifies email that is promised not to be spam, thereby helping to ensure delivery of the email you want, and doesn't stop other mail from getting through. Email senders can license the copyrighted and trademarked Habeas mark to include in their outgoing email, and thus "warrant" that their email is not spam. In turn, receiving systems can recognize the Habeas mark in inbound email, and deliver it with confidence that it is not spam.

- **Ironport**. Ironport's Bonded Sender and Bonded Sender Plus programs work in a manner similar, although not identical, to Habeas. Ironport identifies for receiving systems senders of email who have posted a bond as a guarantee against the email they send being spam.

Many sending and receiving sites apply a “do it yourself” approach to addressing false positives.

- Sending sites may contact ISPs and other sites or companies which are blocking their legitimate email, one at a time, and try to negotiate more reliable delivery of their email. This is a tedious, time-consuming, and expensive process.
- Receiving sites may maintain an internal “whitelist" - a list of the IP addresses or domains of sending sites whom they trust to send only legitimate email. This is helpful for those senders of which the receiving site is aware, but does nothing to help those of which it is not, and does not scale well.

False positives have been recently featured in many publications.

“But that stringency has its own costs: complaints from people who say their e-mail is being blocked unfairly. AOL now has 18 people in its postmaster department, who set the spam filters and take the calls from aggrieved mailers” – Totaling Up the Bill For Spam, New York Times, July 28, 2003

“… e-mail improperly blocked by stringent filters at ISPs represented a major challenge for the e-mail marketing industry, as the consumer backlash against spam leads ISPs to aggressive action against bulk e-mail. Many e-mail marketers have complained that the filters swoop up their legitimate e-mail messages along with spam. ” – Report: ISPs block 17% of legit e-mail, Internet News, August 13, 2003.

"Of great importance to corporate is that 70 percent of people have not gotten email that was expected," says Vincent Schiavone, president of Philadelphia-based ePrivacy Group Inc. "When it comes to blocked email, the consumer is inconvenienced. The enterprise could be losing an expensive deal ...False positives damage business." -- False Positives: Spam's Casualty of War Costing Billions, IT Planet.com, August 8, 2003

Policy recommendations for Email Senders for diminishing false positives.

1. Adhere to the highest level of permission possible when subscribing people to your mailing list. While this may not help up front, it will help immensely when working with a receiving site to get your mail unblocked.
2. Insist that any organizations for whom you send email also adhere to the highest levels of permission possible.
3. Refrain from sending the email of several different organizations through one IP address. Instead, assign a separate IP address to each organization for whom you send mail. That way if the mail from one organization causes a problem, you can isolate the problem and help to ensure that the rest of the mail you send gets through.
4. Learn what are the most common indicia considered to be "spam signs", and don't use them. These include such words and phrases as 'financial success' 'free' 'money-back guarantee' 'new and improved' and, ironically, "you are receiving this mail because" and "click here to unsubscribe". Yes, you shouldn't have to do this, but it's reality.
5. Run your outgoing mailing through one of the more popular spam-filter packages before you send it out, to see whether the spam-filter tags it as spam. If so, get rid of the offending elements of your message. Or use one of the systems available online to help you determine the "spaminess" of your mailing (see, for example http://www.assurancesys.com/hm/mcheck).
6. Subscribe to an assured email delivery service such as Habeas or Ironport's Bonded Sender Plus.

Policy recommendations for Email Receivers for diminishing false positives.

1. Be familiar with the policies and practices of any anti-spam service to which you subscribe! Make sure that their definition of “spam” comports with your own, and that you are comfortable with how they identify “spammers” and with what actions they take attendant thereto.
2. When installing any new anti-spam software, make it a policy to err on the side of allowing more mail through, rather than adjusting settings to the strictest levels available, until you have some familiarity with how well the product works on your own system.
3. Never delete sight unseen any incoming mail before delivering it to your user’s account unless you have expressly advised your users that this is your policy (virus detection excepted). Rather, segregate suspected spam into a separate area to which the user has access.
4. Know who you are blocking, and why.
5. Regularly review blocking processes and lists, and set an aging policy such that a block is removed after a certain period of time with no spam having been received from the blocked site.

Section II - Making those who advertise in spam as legally responsible as the people actually sending the spam

Senders v. Vendors

- Senders of spam are often not the people who are actually driving the spam; rather the spammer's clients - those whose products or services are advertised in the spam (collectively referred to herein as "vendors") – are the ones driving the campaign. They are the ones paying the spammer's bills.
- Vendors typically accept no responsibility for the spam which is sent on their behalf. Until now they have been able to shrug their shoulders and claim "it wasn't me who sent it".
- Senders – those who actually inject the spam into the Internet stream - often obfuscate their identity, making it difficult and costly to identify and find them.
- Many senders are offshore, making them both more difficult to find, and to prosecute.
- By contrast, most vendors are easy to find. In order for people to send them money, which is usually the purpose of the spam being sent, they must be able to be contacted.
- The vast majority of spam which is sent in the English language advertises a product, service or website with connections to the United States, making prosecution under U.S. law relatively straightforward and easy. The same is true for other languages and other countries.

Making Vendors Liable

- Holding vendors accountable for the methods used to advertise their goods or services via email, where they know or should know what methods are being used, is practical, logical, and makes for good public policy.
- Vendors who are willing to pay to have their marketing and advertising messages sent via spam are a core part of the spam problem.
- Finding and prosecuting the responsible vendors is easier, faster, less time and money intensive, and more viable than trying to find and prosecute the spam-senders.
- With no clients, the spam-senders will have far less reason to send spam.
- There is already precedent for this in other areas of law, such as contributory trademark infringement and contributory negligence.

Sample Vendor Liability Legislation

- **In June of 2003, ISIPP's Anne Mitchell worked closely with Senator John McCain's office to help develop and draft legislation which would hold vendors liable for advertising in spam.**
- **This legislative draft was introduced as an amendment to the Burns-Wyden CAN-SPAM Act, and adopted by committee as part of the bill. Vendor liability is now part of the Burns-Wyden bill.**
- **The proposed legislation makes liable any vendor who advertises in spam which violates the general provisions of the law.**
- **Exceptions are made if the vendor truly did not know, and could not have been reasonably expected to know, that their information would go out in spam.**

Text of the McCain Amendment

SEC. ———. BUSINESSES KNOWINGLY PROMOTED BY ELECTRONIC MAIL WITH FALSE OR MISLEADING TRANSMISSION INFORMATION.

(a)IN GENERAL.—It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of section 5(a)(1) if that person —

(1) knows, or should have known in ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;

(2) received or expected to receive an economic benefit from such promotion; and

(3) took no reasonable action —

(A) to prevent the transmission;or

(B) to detect the transmission and report it to the Commission.

- Holding vendors accountable for the method by which they market and advertise through email
  - helps to reduce the incidence of spam
  - helps receiving systems to differentiate between legitimate email and spam as vendors will have to either utilize only legitimate methods of email marketing, or abandon email marketing rather than face legal liability and penalties
  - makes good sense.

What is the ISIPP and how are we helping?

- The Institute for Spam and Internet Public Policy is a California Limited Liability Corporation headquartered in California's Silicon Valley.
- Founded in 2003 and privately funded, ISIPP sponsors and hosts such industry policy and working groups as the Email Management Roundtable, and the Email Deliverability Summit.
- ISIPP's advisors provide expert analysis and consulting services to governmental and regulatory agencies, industry leaders, educational institutions, and the press.

Thank you.

Anne Mitchell
President & CEO
Institute for Spam and Internet Public Policy (ISIPP)
Contact: amitchell@isipp.com

(Many thanks to Janice Wuttke, of myjanice.com, for her assistance with this presentation.
I couldn't have done it without her.)