Pivotal Veracity LLC

False Positives

A first-hand view of what happens when 100 top-tier enterprises, non-profits, and governmental agencies try to communicate via email with their opt-in customers.

Introduction

By Deirdre Baird, President, Pivotal Veracity

Today, an estimated 70 to 80% of all email traffic is spam. Despite the sheer volume of spam and the generally acknowledged imperfection of today's spam-fighting technologies, many spam-filtering providers and ISPs continue to emphasize the low rate of "False Positives" (legitimate opt-in mail that is erroneously identified or blocked as spam).

According to leading anti-spam providers who service both ISPs and enterprises, the False Positive rate is negligible:

- Message Labs: SLA guarantees "**0.0004% False Positives**"

- Brightmail: "False Positive rate of **fewer than 1 False Positive in every 1 million messages**"

- Postini: "best overall balance of accuracy (97%) and **False Positives (.08%)**"

However, these figures contrast substantially with the average **False Positive rate of 20%** identified by Deliverability Service Providers[1] who are monitoring the deliverability of opt-in communications for the legitimate sending community.

Why are these figures so vastly different? Is the False Positive rate a fraction of a percent or is it closer to 20% or even higher? Are the sending and receiving constituencies – even within the same organization - calculating False Positives differently and, if so, is it time we establish some commonality so that productive and meaningful discourse may take place between the two parties?

Do we even care if there are False Positives? Are legitimate, albeit sometimes over-zealous, retailers who send their customers promotions the only unfortunate companies whose messages are sometimes erroneously treated as spam or is this a universal problem impacting some of the most well-respected brands, non-profits, and governmental agencies? Are False Positives limited to marketing messages and newsletters or are critical transactional emails also being filtered out? Do the opt-in processes, authentication methodologies, deployment methods, etc. that a company implements have any significant bearing on whether their messages will avoid the False Positive hole?

While this study certainly cannot possibly answer all of these questions, the results do definitively shed light on the fact there is a problem – a problem that is, unfortunately, both universal and indiscriminate in its reach. It is our hope by sharing the results of this study with both the sending and receiving community, that we will help engender more open, honest and productive dialog on how we can fight spam together while still preserving email as an essential, effective, and reliable communication medium for companies and individuals.

---

[1] Please see Appendix C for definition.

Table of Contents

I.   About the Study

II.   How the Study was conducted

III.   Important Metrics and Terminology

IV.   Findings

V.   Discussion & Conclusion

Appendices

Appendix A: 100 Companies Monitored
Appendix B: Study Methodology
Appendix C: Miscellaneous Terminology
Appendix D: AOL's CityGuide newsletter

I.   About the Study

In a six-week study, Pivotal Veracity tracked the ability of 100 organizations to communicate effectively and reliably via email with their opt-in customers.

The objectives of the study were to ascertain whether these well-known brands are following best-practice permission and email deployment practices, whether the largest webmail providers are erroneously identifying legitimate emails from these companies to their opt-in customers as spam, and what, if any, impact these companies' policies have on how the webmail providers treated their mail.

II.   How the Study was Conducted

Pivotal Veracity conducted the entire study manually and selected 100 companies at random that purposely excluded all Pivotal Veracity clients. Our goal in so doing was to emulate the "real-world" experiences of:
- an average customer who has actively requested to receive information from a particular company and
- the unbiased activities of that company as they attempt to effectively to communicate with us – their customer – via email.

Specifically for the purposes of the study, personal email accounts were established at three of the largest webmail providers - Yahoo, MSN-Hotmail, and Gmail. All spam-filter settings were left on their default settings and no additions or changes to these or other default settings were made throughout the study.

We then personally and manually signed-up for the email communications offered by each of 100 companies in a variety of industries. A full list of these companies is provided in Appendix A. The emails we signed-up for varied and were often dependent on the company; e.g. publishers often offered newsletters, retailers offered emails on special promotions, business-to-business offered white-papers and sales literature, etc. In all cases, we manually and personally requested emails from the company on their website using our Yahoo, MSN-Hotmail, and Gmail email addresses. For the companies in the study who followed a double-opt-in policy, we 'confirmed' our opt-in by clicking or responding to the confirmation request we received.

We then manually[2] monitored which companies we received emails from and, for those we did, whether all their emails were correctly placed into the inbox or whether some were erroneously flagged by any of the webmail providers as spam and placed into the spam folder[3].

More details on the study methodology may be found in Appendix B.

---

[2] Manual monitoring means we documented the results by logged into our email accounts via the provider's web interface and did not use POP, IMAP, or any other methodology to download the mail.
[3] For simplicity purposes the single term "Spam Folder" refers to mail placed in Yahoo's "Bulk" folder, MSN-Hotmail's "Junk" folder, or Gmail's "Spam" folder.

III. Important Metrics and Terminology

Treatment of non-receipt
The key limitation in this study was our lack of certain knowledge as to which email accounts the company mailed and how frequently. If for example, we received emails from a particular company to our Yahoo account but never to our MSN-Hotmail or Gmail account, we had no way of knowing whether the company purposely excluded MSN-Hotmail and Gmail or whether MSN-Hotmail and Gmail blocked or deleted the company's mail.

We therefore interpreted the results <u>conservatively</u>; if no mail was received, we assumed the company did not mail to that account and did not ascribe the non-receipt to a block or deletion by any of the webmail providers.

Base Metric is Companies not Email Volume
Unless otherwise noted, all study findings are expressed in terms of the number of companies instead of the amount of email volume. This was done purposely in order that we could provide clarity as well as meet the objectives of this study which is to measure what percent of legitimate companies are impacted by False Positives. A full discussion of this base-line metric as well as the different metrics used by Anti-Spam Filtering companies and Deliverability Service Providers is provided in the Discussion Section of this document.

No Mail Received – **the number of companies from whom no mail was received at any of our email accounts throughout the monitoring period.**
While this could be a result of blocking or deletion by the webmail providers (a False Positive), for the purposes of this study it is assumed the companies simply did not mail anything to us as we do not know for certain whether they did. This may result in an <u>understatement</u> of the number of companies in our study impacted by False Positives.

Inbox – **the number of companies for whom 1 or more emails were received at 1 or more of our email accounts and all such emails were placed in the Inbox.**
Note, when emails from a company were only received at 1 email account instead of all 3, we assumed for purposes of this study that the company did not mail to all 3 webmail accounts instead of assuming that the webmail providers deleted or blocked the emails (a False Positive). This may result in an <u>understatement</u> of the number of companies in our study impacted by False Positives.
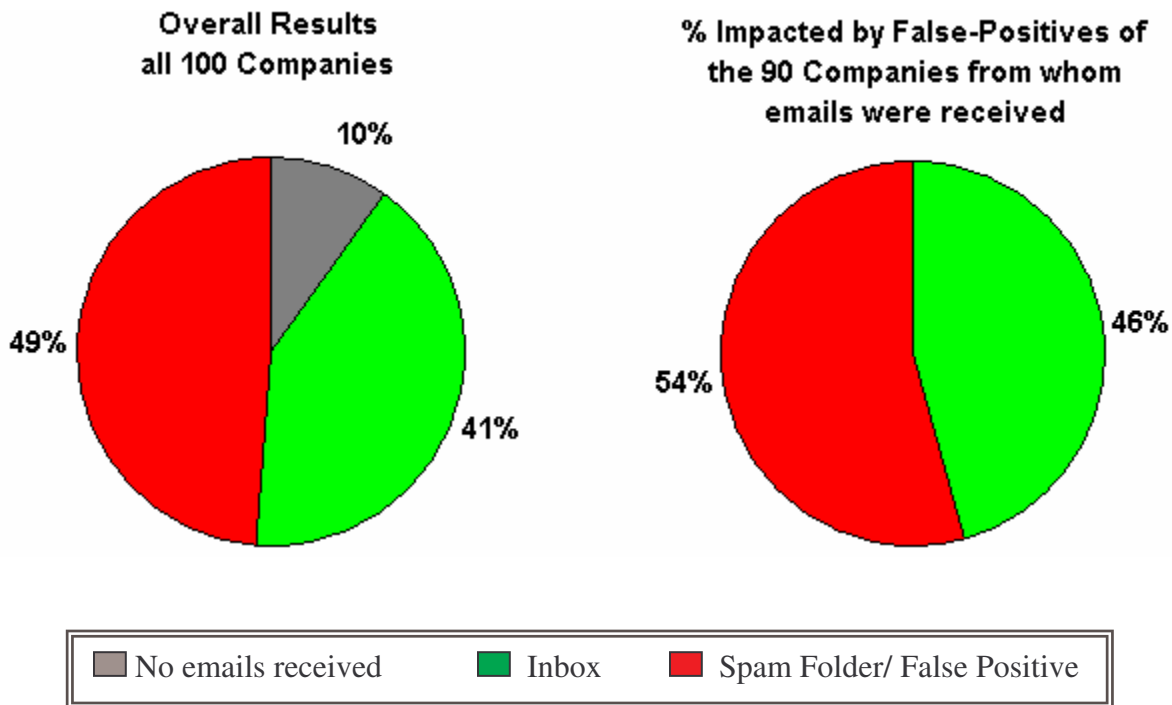
Spam Folder (False Positive)– the number of companies for whom 1 or more emails were incorrectly placed in the spam folder by any of the webmail providers.
None of the companies from whom we received email were spammers; we specifically requested email from them and expected to receive them. Therefore, for purposes of this study, if any email from a company was treated as spam and placed in the spam folder by the webmail provider/s, we are concluding the company is impacted by False Positives. However, this figure may be <u>understated</u> due to the reasons described under the definitions for No Mail Received and Inbox above.

Definitions for other Terminology used in this Study may be found in Appendix C.

IV. Findings

► In total, False Positives impacted 54% of the Companies from whom email was received

Overall Results all 100 Companies

10%

49%

41%

% Impacted by False-Positives of the 90 Companies from whom emails were received

46%

54%

| ▨ No emails received | ▨ Inbox | ▨ Spam Folder/ False Positive |

These pie-charts illustrate the overall results for the 100 companies in this study as well as the results for just the 90 companies for whom one or more emails were received.

During the monitoring period, no mail was received from 10 of the companies, all emails were placed in the inbox for 41 of the companies, and one or more emails were treated as spam for 49 of the companies.

Of the 90 companies from whom email was received, a significant 54% were impacted by False Positives with one or more of their emails treated as spam and segregated to the spam folder by at least one of the three webmail provider/s.

The number of companies impacted by False Positives may be understated for two reasons. First of all, for purposes of this study, we did not count 'no mail received' as a False Positive. Second, in some instances mail was only received at one or two of the webmail providers but not at all three. Whether this is the result of their mail being blocked or because they simply only mailed a segment of their customers is unknown. We therefore assumed the latter and did not count these towards the False Positive figure.

► The 54% of Companies impacted by False Positives included a surprising array of some of the world's most recognized commercial, non-profit and governmental agencies.

Companies impacted by False Positives during the 6 week study:

Business to Business • ePiphany • SAS • Webex	**Non-Profit & Government** • American Red Cross • AARP • US Gov.: Dept. of Education • US Gov.: Federal Drug Admin.
Food, Drug, & Pharma • Domino's Pizza • Johnson & Johnson • Walgreens • Wal-mart **Miscellaneous Consumer** • Decision Analyst/ American Consumer Opinion • Home Gain • Postmaster Direct service	**Media** • Agora Publishing • Business Week • CNET • Crain's • Discovery Networks • HBO • National Geographic • Newsweek • The Motley Fool • The Wall Street Journal
Retail • 1800 Flowers • Academy Sports & Outdoor • Bloomingdales • Buy.com • Coldwater Creek • Crutchfield • DVD (Infinity Resources) • LL Bean • Macy's • Marks & Spencer • Neiman Marcus • Polo • Smart Bargains • Target • The Wedding Channel	**Technology & Telecom** • AOL • IBM • Juniper Networks • Nokia • Postini • Verizon **Travel** • Expedia • Hotwire • Orbitz • Travelocity

NOTE: If you are an employee of one of the organizations listed above, examples of the emails that were placed in the spam folder are available upon request.

► **99% of Companies use either Opt-in or Double-Opt-in for consent with a full 18% using Double-Opt-in.**

Primary Consent Method all 100 Companies
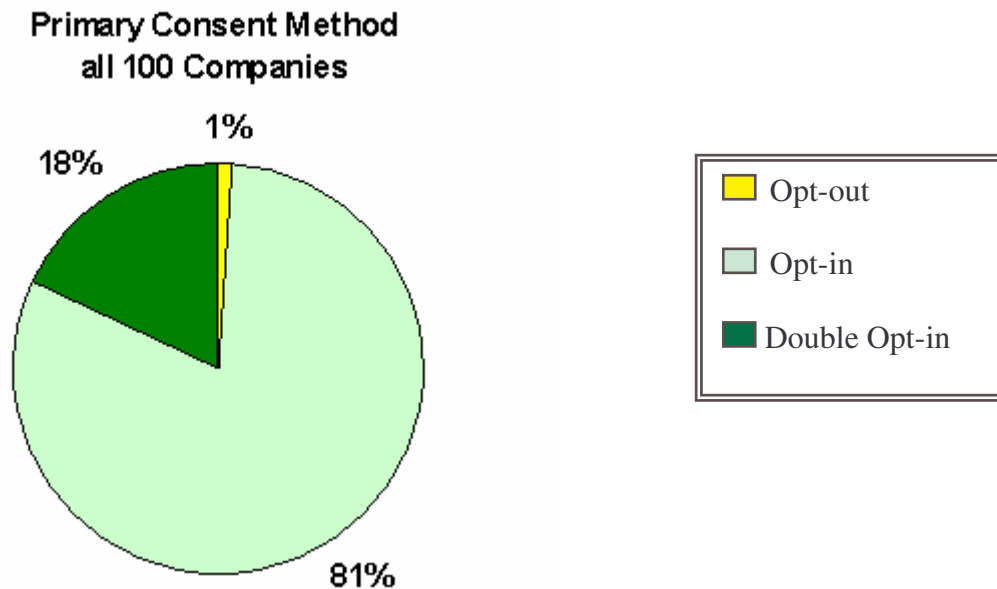
Opt-out: eLoans is the only Company who utilized an opt-out consent form. The primary benefit for which an individual would register at eLoans is not necessarily to receive emails; however, during registration, we were presented with a separate option to consent to receive email communications. This consent was in the form of a pre-checked box.

Opt-in: The vast majority of the companies or 81 out of 100 used Opt-in (both confirmed and non-confirmed) as their primary consent form. This included entry of an email explicitly for the purpose of receiving emails or, in the event email was a potential alternative benefit, a separate un-checked box for receipt of emails was provided.

Double Opt-in: 18% of the companies required double-opt-in. In addition to entering email on the Company's website, we had to confirm our registration with a secondary action of either clicking on the email, replying to the email we received, or logging into the company's website with a specific code. The 18 companies who utilized Double Opt-in as their primary consent vehicle include:

AARP	Decision Analyst	Postmaster Direct
American Red Cross	DM News	Southwest Airlines
Art Select	Keynote (Vividence)	Tiger Direct
Bizrate.com	L-Soft Discussion	Tribe.net
ClickZ	Message Labs	US Gov.: Dept of Defense
CNET	Postini	US Gov.: FDA

► **Only 16% asked for consent for 3rd Party/Partner Offers and, of those, almost half used Opt-out.**

**Companies with a separate 3rd Party Offer/Partner consent form**
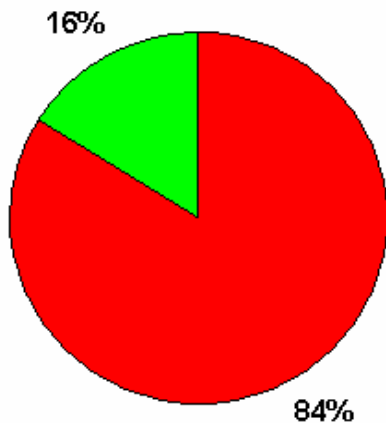
Only 16 out of 100 companies had a separate consent option for receipt of "3rd party or partner" emails.

If a Company sends 3rd party or advertising content to its customers or believes they may at some point in the future, asking customers for separate consent is a best practice. For those who did <u>not</u> provide a separate consent option, it is unknown whether they do not send 3rd Party/Partner offers to their customers or do but choose not to give their customers a choice.

Of the 16 companies who offered a separate 3rd party consent form, 56% provided an Opt-in while 44% only provided an Opt-out.

While only 1 company out of 100 used an opt-out for the primary consent form a total of 7 companies used opt-out (a pre-checked box) as it pertained to consent to 3rd party/partner offers. Why would a Company have a less rigorous consent policy as it pertained to 3rd party offers than their primary consent methodology? While we believe this is contrary to best practices, it does not appear to be uncommon, particularly among publishers. The methodologies followed by the 16 companies are illustrated below.
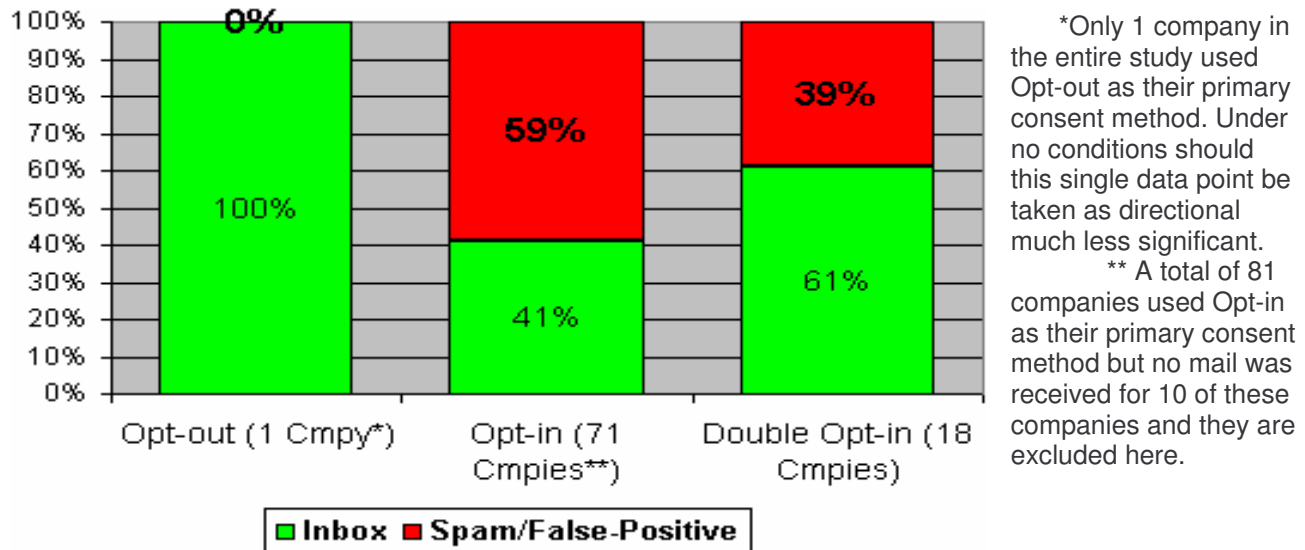
Type of 3rd Party/Partner consent form provided (16 companies)
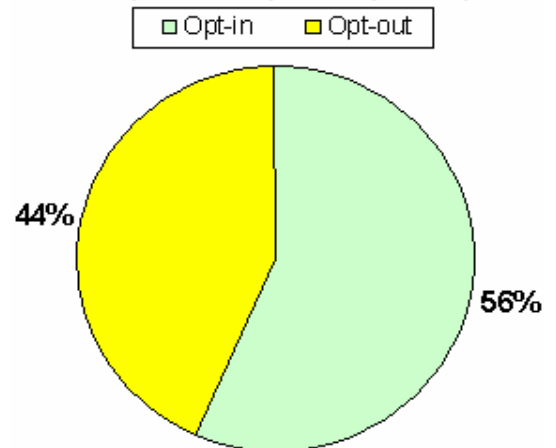
Company	Primary	3rd Party	Company	Primary	3rd Party
Business Week	Opt-in	Opt-out	Discovery Networks	Opt-in	Opt-in
CNET	Double Opt-in	Opt-out	Homegain	Opt-in	Opt-in
Crains	Opt-in	Opt-out	IBM	Opt-in	Opt-in
Motley Fool	Opt-in	Opt-out	National Geographic	Opt-in	Opt-in
Alitalia	Opt-in	Opt-out	The Wall St Journal	Opt-in	Opt-in
Art Select	Double Opt-in	Opt-out	Clickz	Double Opt-in	Opt-in
Match.com	Opt-in	Opt-out	eDiets	Opt-in	Opt-in
			Montgomery Ward	Opt-in	Opt-in
			Washington Post	Opt-in	Opt-in

► Companies are impacted by False Positives regardless of their use of Opt-in versus Double Opt-in

90 Companies from whom mail was received broken-down by primary consent method.

*Only 1 company in the entire study used Opt-out as their primary consent method. Under no conditions should this single data point be taken as directional much less significant.

** A total of 81 companies used Opt-in as their primary consent method but no mail was received for 10 of these companies and they are excluded here.

Earlier in this report, the primary consent methods used by the Companies in this study were delineated. This graph details which of these Companies were impacted by False Positives broken-down by the primary consent method they used. While the results indicate a directional correlation between the consent method used and whether or not the Company was impacted by False Positives this does not necessarily imply a causal relationship.

The most useful interpretation of these results is that it reveals that companies that use both methods were impacted by False Positives. Companies should carefully consider the implications of False Positives on the effectiveness of the consent method they choose:

- **Opt-in (unconfirmed)** – False Positives have no implication as to whether this method is effective as no confirmation email is sent.
- **Opt-in (confirmed)** – the purpose of a confirmed opt-in is to provide a means to ensure that the email address entered at sign-up is valid and belongs to the person who signed-up. This is accomplished by sending a confirmation email that "confirms" the registration and provides an unsubscribe mechanism. However, if this confirmation email is identified as spam, the actual owner of the email address may never see it and, therefore, the intended goal of the confirmation is not met and this consent method becomes no better than an unconfirmed opt-in.
- **Double Opt-in** – a double opt-in requires the registrant to take some secondary action as instructed in the email sent to the registrant. However, if this email is identified as spam, the registrant may never see it and therefore cannot complete the registration process.

► 18% of the Companies had critical <u>Transactional</u> messages erroneously identified as spam. Included in this figure are almost 1/3rd of the Companies who use Double Opt-in as their primary consent methodology.

18% or 16 of the 90 Companies for whom mail was received had one or more transactional emails identified as spam. In most cases, the transactional emails were registration confirmations. However, for two companies (American Red Cross and Postmaster Direct) the double opt-in request that required a response was identified as spam. In all cases, these emails are critical and their identification as spam is not only erroneous but undermines the customer's ability to exercise their consent.

Examples of the Transactional emails identified as spam

Academy Sports & Outdoor	Welcome to Academy Sports & Outdoors
Agora Publishing	Welcome to Early to Rise
American Red Cross **	Subscription Confirmation Requested
Buy.com	Thank you for signing up for our FREE Weekly Newsletter!
Crutchfield	Your Crutchfield E-Mail Subscriptions
Decision Analyst**	American Consumer Opinion®
Domino's Pizza	Thank You!
US Government - FDA **	You are now subscribed to the FDA-NEWSDIGEST-L list
Hotwire	Hotwire Registration Confirmation
IBM	You're all set. Here's helpful information re: your iSource subscription.
Marks & Spencer	Welcome to the Marks & Spencer eClub!
Nokia	Press release subscription
Orbitz	Details About Your Orbitz Membership Benefits
Postini **	Welcome to the Postini Insider
Postmaster Direct **	Confirmation Required - Just one more step
Verizon	Thank You For Registering at Verizon Online Courses

**** Of the 18 total Companies who used Double Opt-in as their primary consent method, these 5 had their Transactional emails identified as spam.**

► **Over 1/3rd of the Companies pay for Accreditation and/or Certification programs. Not only did these programs not provide protection against False Positives but those using them faired slightly worse.**

37% of the Companies from whom mail was received paid for either certification by Truste and/or membership in the Bonded Sender program. [4] The percent of Companies who had mail erroneously identified as spam despite paying for these solutions is provided below and compared against those who used neither.
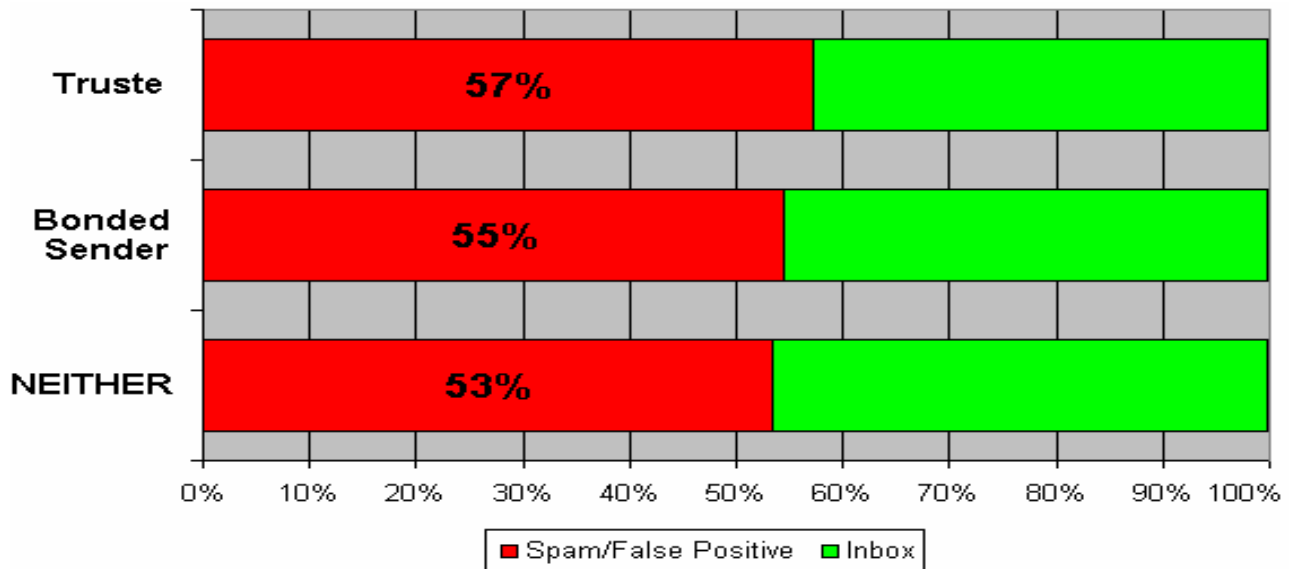

TRUSTe - a for-profit enterprise that sells a "Web Privacy Seal". According to Truste, if you display their seal on your website, "**you build confidence with consumers and drive revenue by letting your customers know that they can trust you with their personal information**". TRUSTe does **not** promise better inbox delivery but the seal is intended to connote solid customer permission practices. Since spam is defined on the basis of whether permission has been granted to the mailer, it is relevant to consider whether the TRUSTe seal has any bearing on one's delivery.

Bonded Sender– a for-profit enterprise that sells an "accreditation" program whose specific stated benefit is improved email delivery. Unlike TRUSTe whose stated benefit is not related to deliverability, Bonded Sender states they "**help deliver email directly into the inbox**" and that their "**program *ensures legitimate email gets delivered*"**. Bonded Sender does not publish a full list of all the ISPs against which this claim is applicable. However, in this study a guarantee of inbox delivery was not supported at Yahoo, Gmail or MSN-Hotmail and as a group those using Bonded Sender faired slightly worse than those not using it.

---

[4] The Better Business Bureau offers a web privacy seal similar to Truste. Habeas offers "accreditation" similar to Bonded Sender. Neither was evaluated in this report as only 2 and 4 companies respectively could be identified as using them.

► **Half the Companies out-sourced the deployment of their emails and had a slightly lower False Positive rate than those who deployed from in-house systems.**
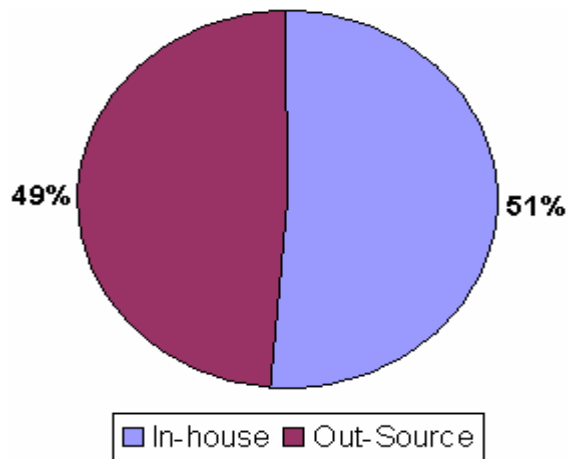

51% of Companies out-sourced the deployment of their emails to ESPs.

ESPs are companies who deploy emails for other companies. Approximately half the companies from whom we received emails were identified as having used an external deployment vendor or ESP. This identification was made by looking up the registered party for the mail server or IP used to deploy the mail.

The # of Companies impacted by False Positives was slightly lower for those who out-sourced deployment. **
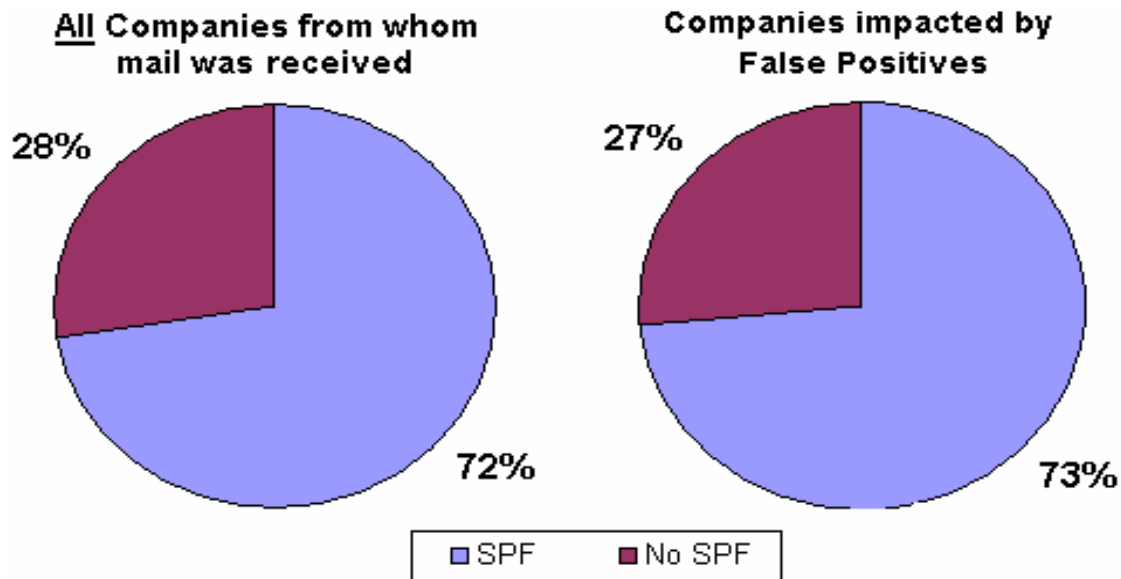
Many believe that outsourcing deployment will improve deliverability. The overall results in our study would support this although the results varied by ESP. Some ESPs whose clients were included in this study had no False Positives issues; some of them had all False Positive issues and, in most cases, the percent of their clients who had issues versus those who did not was split down the middle.
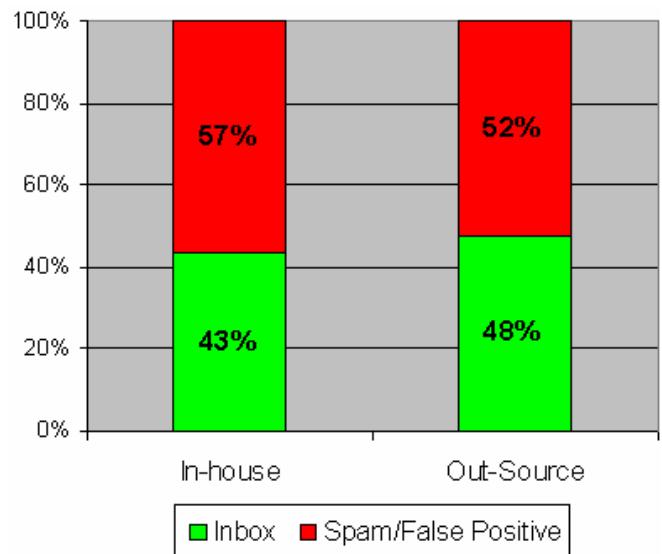
** Note of caution:
This was not an evaluation of ESPs nor should this statistic be interpreted to unconditionally espouse the out-sourcing of email deployment. The quality and capabilities of ESPs varies dramatically, particularly as it pertains to the means they use to independently track and successfully optimize inbox versus spam folder placement. Where you deploy your emails from, has been and continues to be only **one factor** affecting email deliverability.

► SPF Authentication implemented by just shy of 75% of Companies .

All Companies from whom mail was received

28%

72%

Companies impacted by False Positives

27%

73%

☐ SPF   ■ No SPF

72% of the 90 companies from whom mail was received had SPF[5] configured. SPF is one of three main authentication methodologies espoused by various parties in the internet community. The other two include Sender-ID and Yahoo Domain Keys although there are also a variety of other methods espoused by various constituencies. No single method has been espoused by all and the "best method" is still a topic of hot debate.

Authentication may be more accurately categorized as an anti-phishing mechanism as opposed to anti-spam. Executed in isolation, authentication will not reduce the amount of spam and, despite a wide-spread believe to the contrary, is not intended to. Rather, in general, it is intended to provide accountability and assurance regarding the sender of the message. In layman's terms, one of the primary purposes of authentication methodologies is to verify "the email is from who it says it's from". As such, authentication is a key mechanism for reducing the number of consumers who unwittingly click or respond to an email they believe to be from a trusted party when in fact it's from somebody else pretending to be that trusted party ("phishing").

Not surprisingly, the results in this study illustrate SPF had no significant influence on which companies were impacted by False Positives and which were not. The penetration of SPF amongst those impacted by False Positives (73%) closely paralleled the penetration of SPF across all companies in the study (72%).

---

[5] SPF stands for Sender Policy Framework

► **Special Spotlight on the "Recipient" community -> What happens when the tables are turned?**

The 100 companies we monitored included 2 ISPs (Verizon and AOL) and 3 companies who develop and sell anti-spam filtering technology (Postini, Message Labs, and IBM). These organizations are critical parties on the recipient-side and have a direct influence via their spam filtering on the False Positive problem. However, instead of monitoring them as "recipients", we monitored them as "senders" since, like most organizations today, they are both senders and receivers of email. Our purpose in calling out these five organizations is to illustrate the practices implemented by the traditional recipient community when they are deploying emails..

### *Spotlight on consent and authentication methodologies*

	AOL	**Verizon**	**IBM**	**MessageLabs**	**Postini**
Signed up for:	Cityguide Newsletter	Online Learning	i-Source Newsletter	Intelligence Newsletter	Insider Newsletter
Primary Opt-in	**Opt-in (confirmed)**	**Opt-in (confirmed)**	**Opt-in (confirmed)**	**Double Opt-in**	**Double Opt-in**
3rd Party Opt-in	None	None	None	None	None
Authentication (SPF, Sender ID, Domain Keys)	**SPF and Sender ID**	**None**	**SPF**	**None**	**SPF**

AOL, Verizon, and IBM provided a single step opt-in just like the vast majority or 82% of companies monitored. In addition, all three sent an email confirming the registration. Message Labs and Postini, two leading spam-filter organizations, took the more conservative approach and required a double opt-in. Message Labs requires registrants to click on a link in a confirmation email. Postini sends the registrant a password and requires login on their website with this password in order to complete the registration.

Authentication: 3 of the 5 ISPs and spam filtering companies used SPF. In addition, AOL also had Sender ID implemented as identified by the SPF2 and PRA record published for their domain. None of the 5 used Yahoo Domain Keys as identified by Yahoo's check in the message header of their emails to the Yahoo account.

Spotlight on False Positives

4 of the 5 had one or more of their legitimate emails erroneously flagged as spam. Additionally, as documented earlier in this report, both Postini and IBM had transactional emails flagged as spam.

4 out of 5 were impacted by False-Positives
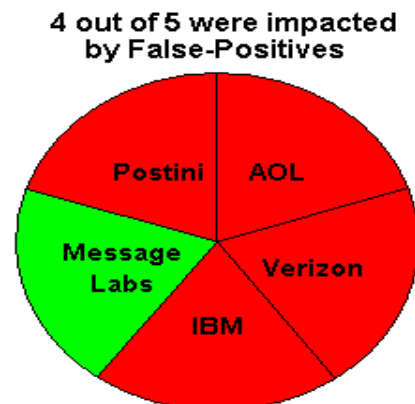
Spotlight on AOL: does AOL the "mailer" comply with AOL the "ISP"?

AOL is the world's largest consumer ISP. They process over 1 billion email messages a day and, unequivocally, represent the front line in the battle against spam. Just like MSN-Hotmail, Gmail, and Yahoo, AOL identifies spam emails and takes a variety of actions upon them, including segregating them to the spam folder or blocking them altogether.

AOL clearly documents its policies for mailers and provides extensive information intended to guide and help companies who are trying to communicate with their customers who have AOL email addresses. AOL also provides channels to communicate with AOL postmasters in the event email to AOL customers are being blocked or placed in spam folders. AOL is both unique and a leader in this respect as many major ISPs still do not provide clearly documented policies and resolution channels for mailers.

However, in this case study, AOL was monitored not as an "ISP" but as a mailer or just 1 company in 100 trying to effectively communicate with its customers via email. In the prior section AOL's consent practices were documented; below is a brief examination of whether the AOL Cityguide newsletter complies with some of the best practices and polices that AOL the "ISP" espouses. The purpose of this examination is simply **to illustrate** the differences in opinion and practice that exist between sending and receiving constituencies, even when such constituencies work for the same exact organization.

AOL Postmaster Best Practice Recommendations for Incoming Mail	AOL's Cityguide newsletter (see Appendix D for a sample)
► All e-mail servers connecting to AOL's mail servers must have valid reverse DNS records.	✓ Reverse DNS is enabled. (newsletter was mailed via an ESP named DoubleClick and this issue applies to them)
► All e-mail servers connecting to AOL's mail servers must be secured to prevent unauthorized or anonymous use.	✓ The mail server has no open relays, no open proxies, and no insecure web forms. (applies to DoubleClick)
► Direct connections from dynamically assigned IP addresses or residential customers to AOL's mail servers may not be accepted.	✓ The IP is static. (applies to DoubleClick)
► Persons transmitting mail.. must not do anything that tries to hide, forge or misrepresent the sender of the e-mail and sending site of the e-mail.	✓ The Envelope and Message From were: AOLCityGuide@dc.aol.com. The mail server: mta.member.aol.com [198.31.62.16]

► All bulk e-mail to AOL members must be solicited, meaning that the sender has an existing and provable relationship with the e-mail recipient and the recipient has not requested not to receive future mailings from the sender.	✓ Pivotal Veracity staff opted-in to receive the CityGuide newsletter.
► Bulk mailings **must specifically state how the AOL members' e-mail addresses were obtained** and **must indicate the frequency of the mailing**.	☒ AOL's Cityguide email newsletter does **not** state where our email address was obtained and ☒ **nor** does it state how frequently we will receive it.
► Bulk mailings should contain simple and obvious unsubscribe mechanisms. We **recommend that this be in the form of a working link to a one-click unsubscribe system**; however, a valid "reply to:" address may be used instead.	☒ AOL's Cityguide email newsletter does **not** have a one-click unsubscribe. You must 1) first click on the link, 2) then enter your email address, and 3) then select the unsubscribe button on the page that is loaded in order to unsubscribe. **
► **All subscription based e-mail must have** valid, non-electronic, contact information for the sending organization in the text of each e-mail including **phone number and a physical mailing address**.	☒ AOL's Cityguide email newsletter does **not** have a postal address **nor** does it have a telephone number. Note: there is a link at the bottom of the email that, if clicked on, will bring the customer to a site that provides this information but the data is not contained in the email itself.

** **Pivotal Veracity note on the Unsubscribe Page**: Insofar as AOL offers multiple types of Cityguide newsletters (city-specific), it is the opinion of Pivotal Veracity that AOL's Cityguide newsletter is following the best practice. When you click to the unsubscribe page, AOL provides an option to unsubscribe not only from the specific newsletter the recipient has just received but an option to unsubscribe from any other Cityguide newsletter. In so doing, AOL Cityguide actually improved our ability to exercise our consent by providing us the option to pick and choose which newsletters we'd like to unsubscribe from while still providing us the ability to unsubscribe from all. CAN SPAM requires that an option to unsubscribe from all communications be made available in all commercial messages. Thus, if AOL Cityguide had followed AOL the ISP's specific guidelines and used only a 1 click unsubscribe, then AOL would have had to unsubscribe us from all newsletters even if our intent was only to unsubscribe from this particular city's newsletter. This is why we believe the best practice in this case is that followed by AOL Cityguide.

V.   Discussion & Conclusion

False Positives impact a broad array of commercial and non-profit enterprises as well as governmental agencies.

In this six-week study, 54% of the companies from whom mail was received had one or more emails erroneously identified as spam. Interestingly, no single company had all their emails identified as spam by all the webmail providers all of the time.

What we learned is that on any given day regardless of whether you have your customers' permission, are an authenticated sender, are sending marketing or transactional messages, or even if you are the largest consumer ISP in the world or the Government of the United States of America, there is a risk that your legitimate emails may be identified as spam.

Undermining consent

Both commercial and transactional emails were incorrectly identified as spam in this study. In defining what constituted commercial vs. transactional messages, we interpreted CAN-SPAM's Primary Purpose narrowly and only considered registration confirmations and welcome emails as transactional (see Appendix C for more details) whereas all other messages including newsletters were identified as commercial even though some may be considered transactional under CAN-SPAM.

In this study, 18% of the companies had their transactional emails erroneously identified as spam.

Since we did not buy any products for which we expected an order confirmation, or book flights for which we expected an airline confirmation number, or engage in a business transaction with a company from whom we were expecting our statement, these particular transactional messages were merely those confirming our registration or, in some cases, the second step required to complete our registration. One of the reasons confirmed opt-in and double-opt-in are considered best practices is because they are intended to prevent somebody signing up for emails with someone else's address by providing the underlying addressee the opportunity to opt-out of the messages (confirmed opt-in) or requiring them to take an additional step (double opt-in). Ironically, the erroneous flagging of these particular transactional messages as spam undermined the effectiveness of the very mechanisms that have been instituted in order to ensure a customer does not receive emails they did not consent to receiving. Is this protecting consent or undermining it?

What about the commercial or marketing messages?

Is it okay if these messages are treated as spam? The answer is very obviously "it depends on who you ask".

If I am a busy business executive who relies on my Wall Street Journal email subscription as my primary source of news, I surely care when I don't receive it. If I am a voracious consumer of shoes but have a minimal budget, I surely care when I miss my special sale notice from Bloomingdales. If I am a progressive teacher who wants to stay abreast of changes in the 'no child left behind' program, I surely care when I miss the updates from the Department of Education. If am a retired person living alone in Florida, the AARP newsletter may be the one thing in my week that makes me feel a part of things.

When we do not permit customers to receive emails they've requested we are not permitting them to make decisions in respect to the mail they receive, we are making them for them.

False Positives – Is it math or is it a matter of opinion?

In the introduction to this report we shared a variety of statistics quoted by different companies in respect to the rate of False Positives. Not only did they vary substantially from one another but in this report we've introduced a third and higher statistic of 54%.

Why is there such a difference? Unlike many of the questions posed in this study, this one is fairly easy to answer. It is both a mathematical issue and an opinion issue.

The rate of False Positives is a metric and, like any statistic, how you calculate it will dictate the story it tells.

- "**54%**": **False Positives as calculated in this study = % of legitimate companies impacted by False Positives.** In this study we very clearly stated one of our key objectives was to measure <u>what percent of legitimate companies were impacted by False Positives</u>. This objective dictated the math used and in this study the math was simply the # of legitimate (non-spamming) companies whose emails were erroneously identified by spam divided by the number of legitimate (non-spamming) companies from whom we received emails. The key difference between this method and the two described below is that the numerator and denominator were the number of <u>companies</u> affected instead of the number of emails. The results of this study are very clear but by no means can we state that they can be extrapolated to the world. This study involved 100 companies across a six-week period across three different webmail providers. Nothing more, nothing less.

- "**less than < 0.01%**":   **False Positives as calculated by many Spam Filtering Companies =False Positives as a percent of <u>ALL</u> mail (spam and legitimate).** Companies who develop and sell spam-filters typically take the quantity of emails they believe have been mis-identified as spam and divide it by all email received. However, given that this same group also estimates that 70 to 80% of all email is spam, the denominator in this case would include 70 to 80% of the mail that is spam. This statistic sheds light on the percent of False Positives across all mail but does not provide much clarity in respect to what percent of legitimate mail is being misidentified as spam.

- **"Average of 20%":** **False Positives as calculated by Deliverability Service Providers = False Positives as a percent of legitimate mail.** This group uses email samples and divides the number of legitimate emails misidentified as spam by the number of legitimate emails expected. However, the key difference is that the denominator in this case is intended to be legitimate (non-spam) emails and not all emails. It is also based on a sample of legitimate mail versus the entire mail volume of all legitimate mailers.

Given the inordinate amount of spam mail (70 to 80%) that is being included in the calculations used by some but removed from those made by others, it is not difficult to figure out why the numbers are so different. However, if False Positives are defined as legitimate mail that is misidentified as spam, then by including non-legitimate mail in the denominator, the metric that results may lead one to conclude that False Positives are insignificant. We believe the more accurate interpretation of the oft-quoted metric of less than .01% would simply be there is a tremendous amount of spam out there and that legitimate mail and the portion thereof that is misidentified as spam is insignificant in comparison. This does not make this metric untrue it simply does not make it particularly useful if you are a sender or receiver hoping to gauge and minimize the number of legitimate emails misidentified as spam.

False Positives are also a matter of opinion

All the above metrics required somebody or something to determine what constitutes a false-positive.

In this study, we defined legitimate mail as emails we signed up to receive or, in other words, we used the customer's consent as the defining criteria between legitimate and spam mail.

If, however, a receiving party uses anything other than consent as the defining criteria between legitimate and spam email then the emails they consider false-positives would be quite different. For example, if a recipient enterprise believes..
- any emails sent from servers without Reverse DNS are spam or
- any emails that come from un-authenticated senders are spam or
- any emails with big red fonts and salesy-words in the content are spam or
- any emails that are sent in high volume are spam …

than any such email by their definition is correctly being identified as spam and is not in their view a False Positive regardless of whether the customer asked for it.

If it looks like a duck, walks like a duck, and quacks like a duck….

…well, maybe it is a duck. But what if it just lets out a little quack? The sum total of the results in this study make one thing quite clear, while none of these companies are spammers, 54% were treated like one at some point or another. Did these companies mail something that justified this treatment?

If your customers have asked for your email, should it matter if you make liberal use of flashy colors and salesy words? Just because your email looks like spam that does not mean it is spam. Unfortunately, content filters cannot tell the difference and by their definition spammy-looking content **is** spam.

If you send a lot of mail, are you spamming? Many receiving constituencies, most notably some large ISPs, have documented volume filters. If you send a lot of mail, you could be spamming, but you could also be a large successful company with a lot of happy customers. Unfortunately, volume filters cannot tell the difference and by their definition bulk mail **is** spam.

In every case, we requested emails from these companies. If spam is defined by a lack of permission and in all cases permission was granted, what does it matter if these companies might have been dressed like a duck, walking like a duck, and quacking at the top of their lungs?

CAN-SPAM and the Wild, Wild West.

No reputable organization will claim that spam-filters are perfect at identifying spam. This fact is not a matter of debate, although as has been discussed so far, the degree to which they are imperfect and the metrics used to calculate that imperfection are.

To revisit the corny duck analogy, there is universal agreement on the fact nobody is perfect at identifying a duck on the basis of how it looks, walks, or quacks. However, regardless of how it looks, walks, and quacks, the bigger and far more important question is: **is it actually a duck**?

In otherwords, whose laws define spam?

CAN-SPAM – the mailer's law.

Regardless of whether CAN-SPAM's goal was to clearly delineate what is and is not spam, mailers turn to CAN-SPAM for guidance on this subject if, for no other reason, because the federal government can prosecute those who fail to comply.

The challenge with CAN-SPAM as the mailer's law is only one of interpretation.

For example, Pivotal Veracity does not deploy mail for companies, but we do work with the legitimate mailing community and while we have every reason to advocate their side, we disagree frequently as to what CAN-SPAM prohibits. While we are not lawyers and every lawyer we have met has had a different opinion, some of the practices that we believe may butt against the spirit if not the literal definition of affirmative consent, include:
- Companies who follow strict permission policies on their own site but then rent email lists and conduct at best cursory inquiries as to whether permission was granted by those recipients to receive third party offers. The justification: it is the list owner's problem because they do the mailing and their mail will be blocked not ours.

- Companies who pay to have email addresses appended to their customer file because they could not obtain the email directly or quickly enough from their customers. The justification: the ephemeral "pre-existing relationship" – a term which is still widely used by many in the messaging community even though no such term exists in CAN-SPAM.
- Companies who pay 3rd party companies to provide them new email addresses for their own customers (email Change Of Address or "eCOA") without much consideration to the fact that one reason folks change their email address is to specifically avoid the email they have been receiving. The justification: prior to the sharing of the email, the person is sent an email that allows them to opt-out of having their address shared. As we saw in this study, there is a chance the person may never see this message.

We pointed out that we work with the mailing community, but our views are ours alone and certainly not necessarily shared by all our clients much less all of those in the recipient community. For example, at least one ISP sometimes relies upon a for-profit enterprise to examine or "accredit" other companies' policies for them – this arbiter of whether other companies have good permission and mailing practices is a company that sends high volumes of mail themselves, has a database of email addresses they sell to others for eCOA, and has another database of emails they sell to advertisers.

CAN-SPAM is the law mailers turn to for guidance as to what is and is not spam. While there may be dispute on how to interpret this law, at the very least it is a single documented law with which all US mailers must comply.

Recipients and the Wild Wild West

Whereas mailers use CAN-SPAM as their guide for defining spam, the recipient community use another "law" altogether to establish what can and cannot be blocked as spam: their own.

Examples of various ISPs' definitions of and justifications for blocking or identifying emails as spam are illustrated below.

From Earthlink's Spaminator FAQ:
- What is spam? spam is the common term for unsolicited commercial email (UCE)—the Internet version of junk mail. "spam" can also be a verb, used to describe **the method of flooding the Internet with many copies of the same message**.

From Verizon's Anti-Spam Policy:
- You may send **a single e-mail message to a maximum of 100 recipients in one mailing, not to exceed 500 recipients within a one hour period**. All single e-mails sent to over 100 addressees will not be delivered. No notice will be given to you in this case.

From Road Runner's Inbound Sender Policy:
- If an organization **generates complaints**, **bounces 20% or more of the total recipients on its mailings**, or has **difficulty accepting those bounces**, the Road Runner Security Operations group may implement blocks until a reconfirmation mailing is sent.

From Excite's FAQ on spam blocks
- Messages to an @excite.com account may be blocked by us if **they had characteristics similar to "spam"** (unsolicited commercial email),
- reject: header Subject: This **subject line is on our "black list" of subject lines**, or is on the black list of one of the spam filter lists we use to lessen the amount of Spam our users receive.

From United Online's Email Delivery Guidelines:
- United Online will consider refusing connections from servers based on criteria including, but not limited to, the following: Have **our spam filters been triggered** in any way?

From MSN Acceptable Use Guidelines for emails sent to MSN
- After given a numeric **SMTP error response code between 500 and 599** (also known as a "permanent non-delivery response"), the sender must not attempt to retransmit that message to that recipient. **
- After multiple non-delivery responses (see #2), the sender must cease further attempts to send e-mail to that recipient.

    *** Pivotal Veracity note: a 500 to 599 SMTP error response can pertain to a number of things that have nothing at all to do with an invalid or non-existant email address, such as an SMTP command line that is too long or a recipient's mailbox being full or a bad sequence of SMTP commands.*

While above are just a subset of some of the rules posted by some of the ISPs, perhaps the most difficult type of these to comprehend as it pertains to False Positives are those that equate being identified as spam by spam filters to being spam. Spam filters are not 100% accurate. Thus, this is no different than saying "I don't have perfect eyesight but if I say you look like a duck then you **are** a duck".

Regardless of whether or not one agrees with the recipient communities' rules, all have some impact on False Positives as these rules are used to define spam and/or determine whether mail will be blocked, redirected to spam folders, or delivered to the inbox.

Whose law is the law of the land?

Most recipient ISPs post policies and rules that have a basis in CAN-SPAM but are rarely limited to CAN-SPAM. Are recipient enterprises within their rights to establish any rules and guidelines they want similar to how the territories in the old west defined their own laws? **Yes**.

Section 8 of CAN-SPAM is labeled "**Effect on other Laws**". It has only 3 parts: part (a) refers to other Federal Laws, part (b) refers to State Laws, and part (c) refers to Internet service providers. According to CAN-SPAM, Section 8, part (c), nothing in CAN-SPAM prohibits an Internet service provider from establishing their own rules and, regardless of whether you comply with CAN-SPAM, there is no requirement that the Internet service provider deliver your mail.

The downside to not complying with CAN-SPAM is federal prosection. The upside to complying with CAN-SPAM is avoiding federal prosecution. If, however, a company would

like to ensure their legitimate communications reach their customer's inbox, the only law that applies is the "law" of the recipient enterprise and each recipient enterprise is entitled to establish whatever they want.

Impossible compliance?

Recipient enterprises are free to establish anything they want in respect to what is spam and what is not, what mail will be delivered and what will not.

One would therefore expect that if all mailers must comply with the rules established by recipient enterprises, recipient enterprises might be best served by clearly documenting what those rules are. The excerpts from policies of various ISPs' policies provided above may lead one to conclude that these policies are easy to find and are thoroughly documented. This, however, is not always the case. Many large ISPs have yet to publish their policies and those who do usually provide a provision similar to that below provided by MSN:

> **The MSN Services also utilize other blocking or filtering mechanisms. Microsoft is under no obligation to publish the particulars of any such mechanism, device, or process, and Microsoft makes no representation, warranty or commitment that any message you send to users of the MSN Services will be delivered.**

ISPs and recipient enterprises unquestionably shoulder the majority of the burden and cost associated with spam. However, legitimate companies are being asked to shoulder the majority of the burden in ensuring their emails are not erroneously identified as spam. Some of the sometimes insurmountable challenges faced by legitimate companies in trying to comply with this requirement may be summarized by the following:

► **Mailers must comply with the rules of hundreds if not thousands of recipient enterprises if they want to successfully communicate with their customers.**

► **Each of these recipient enterprises may establish any definition of spam and any rules they would like in respect to what mail they deliver.**

► **Recipient enterprises usually do not publish all their policies but do expect mailers to comply with them whether published or not.**

► **If a legitimate mailer manages to comply with each recipient enterprises' requirements, the recipient enterprise may still call the email spam and/or choose to block it at their sole and exclusive discretion.**

► **When mistakes occur, as they often do, the legitimate mailer lacks a defined and accessible 'judge' at the recipient enterprise to which they can present their case and, even when one can be found, lacks a common 'law' or definition of spam upon which to argue that case.**

Conclusion

In this study Pivotal Veracity set out to research and evaluate the impact of false-positives with respect to a mere 100 legitimate companies across three major email providers. No matter how limited in scope, this study clearly illustrated that false-positives are a potentially more serious issue than certain industry-espoused metrics have historically implied.

Is spam a tremendous problem? Absolutely. Should ISPs and enterprises be blamed for using all means at their disposal to stem the onslaught of this plague? Absolutely not. Should we expect and even understand that in the fight against spam some legitimate emails will erroneously and inadvertently be misidentified as spam? In our opinion, absolutely. However, if we continue to devalue the importance of False Positives, due in part to our use of metrics that dilute their occurrence relative to the volume of legitimate mail, it is unlikely we will ever solve the problem much less minimize its impact.

As commonly reported in the media, the cost of spam includes the processing costs borne by the ISPs and enterprises and the time required by recipients to delete it. We believe the cost of spam also includes the cost borne by legitimate companies and their customers whose ability to communicate reliably and effectively via email is threatened by it.

How do we solve the problem?

Spam is a cost borne by and a problem that can only be solved by both receivers and legitimate senders. Unfortunately, there is a wide divide between these two parties and communication, empathy and cooperation are often lacking even within the same organization. One of our most important challenges is improving communication and transparency between these parties.

There is however a bigger problem.

While the industry continues to debate more effective methods for identifying spam and reducing False Positives, the fact remains we have yet to agree upon a single set of criteria for establishing what spam is. While mailers follow one set of common rules, recipients create and apply another.

Until we all agree on what actually defines spam, better methods for identifying it will fail and False Positives will continue.

VI.   Appendix A: 100 Companies Monitored

1800 Flowers	Fidelity	Polo
AARP	Ford	Postini
Academy Sports & Outdoors	Fox sports	Procter & Gamble
Agora Publishing	GE	REI
Alitalia	Geico	Postmaster Direct
American Eagle Outfitters	Harris Interactive	SAS
American Red Cross	HBO	Sears
AOL (cityguide)	HomeGain	Sidestep
ArtSelect	hotwire.com	Smartbargains
Bass Pro Shops	IBM (isource news)	Southwest Airlines
bizrate.com	Intel	Starwood Resorts
Bloomingdales	J&J Babycenter	Synovate
Brooks Brothers	Juniper Networks	Target
Brookstone	Keynote (Vividence)	Tesco
Business Week	Lego	The Motley Fool
buy.com	Linen & Things	Ticketmaster
Classmates	Lions Gate Films	Tigerdirect
ClickZ	LL Bean	Travelocity
Cnet	Lyris / L-soft discussion	Tribe.net
Coach Leatherware	Macy's	UNICEF
Coldwater Creek	Marks & Spencer	United Nations
Crain's	Match.com	US Gov.: Department of Defense
Crutchfield	Message Labs	US Gov.: Federal Drug Administration
Decision Analyst / American Consumer Opinion	Montgomery Ward	US Gov: Department of Education
Discovery Networks	National Geographic	Verizon
DM News	Neiman Marcus	Walgreen
Dollar Rent A Car	Newsweek	Wall Street Journal
Domino's Pizza	Nokia	Wal-mart
DVD (Infinity Resources)	Nordstrom	WashingtonPost
eDiets.com	Omaha Steaks	Webex
eLoans	Oracle/ PeopleSoft	WeddingChannel
ePiphany	Orbitz	Williams Sonoma
Expedia	Performance Bike	
Exxon Mobile	Pfizer	

Appendix B: Study Methodology

Yahoo, MSN-Hotmail, and Gmail
Account Setup
Three personal email accounts were setup with one each at the largest webmail providers: Yahoo, MSN-Hotmail, and Gmail. These providers were selected due to their market share, because they are free of charge, and are used by individuals around the world as primary and secondary email accounts.

Account & Spam Filter Configuration
In all cases, absolutely no changes were made to the default settings provided by Yahoo, MSN-Hotmail, and Gmail. No black-lists or white-lists were created, no custom filters were added, and no changes to existing filters were made. Additionally, no received emails were ever identified as "spam" or "not spam" via the buttons provided in the interface.

Interaction with Email Received
Throughout the monitoring process, interaction with emails received at these accounts was kept to an absolute minimum. The only emails that were "clicked-on" were the Opt-in-Confirmation requests from those organizations that required double-opt-in. Additionally, for the purpose of this report, some emails had to be opened to identify the senders and to capture header information. Finally, where automatic spam-folder deletion by the webmail provider would have erased emails contained in the spam-folder, a secondary folder was created and emails were moved to this folder to avoid automatic deletion.

100 Organizations Tracked
Selection of 100 Organizations
100 organizations across a broad range of industries were selected randomly within the following criteria:
- representation of b2b and b2c commercial, non-profit, and government entities with an emphasis wherever possible on well-known brands
- the organization could not be a Pivotal Veracity client
- the organization must have a feature that permits the public to opt-in at no charge and online. The communication or benefit to which the opt-in pertained was not relevant (e.g. in some cases it was sales literature, in some a newsletter, in others access to site features and specific types of alerts). *

*due to criteria 3, we were unable to include a significant sample of financial services companies as many require the individual to open and fund an account.

For a full list of these 100 companies, please see Appendix A.

Opt-in Process
A Pivotal Veracity staff member manually "opted-in" to receive email communications from each of the 100 organizations with the three personal email addresses from Yahoo, MSN-Hotmail, and Gmail. The opt-in procedures (opt-out, opt-in, double-opt-in) followed by each of these organizations was documented.

Monitoring of Email Received

On a routine basis, a Pivotal Veracity staff member logged into each of the email accounts at Yahoo, MSN-Hotmail, and Gmail to determine whether any double-opt-in confirmation requests required a response. In total, 18 of the 100 organizations required confirmation of opt-in and required either a click on a link to confirm the opt-in or a reply to the confirmation email; these confirmations were executed manually.

Through-out the monitoring period, the IP address from which the email originated and other basic information regarding the message was documented on one of the emails received from each organization. Additionally, every email received in the spam folder at each of the email accounts was documented in detail on a spreadsheet.

At the end of the monitoring period, the data was summarized and is presented in this report.

Appendix C: Miscellaneous Terminology

Authentication Methodologies

In this report, three authentication methods were mentioned. More information is available on these three methods at the links provided below. Please, note this is not an exhaustive list of the various authentication methodologies being explored within the internet community.

► SPF (Sender Policy Framework): http://spf.pobox.com/
► Sender-ID: http://www.microsoft.com/senderid
► Yahoo! Domain Keys: http://antispam.yahoo.com/domainkeys

CAN-SPAM Act

http://www.ftc.gov/bcp/conline/edcams/spam/rules.htm

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) went into effect on January 1, 2004. The Act establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. The Act may be accessed by visiting the above site or clicking here: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

The Primary-Purpose definitions applicable to CAN-SPAM went into effect March 28, 2005 and define the criteria used to establish whether a message's primary purpose is transactional or commercial. These rules may be accessed by visiting the above site or clicking here: http://www.ftc.gov/os/2005/01/050112canspamfrn.pdf

Deliverability Service Providers (DSP)

Organizations that track the inbox deliverability of email communications. This term is intended to differentiate these organizations from Email Service Providers (ESPs) who provide deployment services and/or deployment technology to companies. DSP services do not typically include the deployment of emails, rather the core DSP service is the tracking of the deliverability of mail deployed by the end-mailer or the end-mailer's ESP. DSPs track whether emails are placed into the Inbox, placed into the Spam Folder, or blocked and/or bounced by the ISP or enterprise.

How deliverability tracking works: Most DSPs provide their clients a representative seedlist of emails at a variety of recipient enterprises (e.g. AOL, Yahoo, etc.). The seedlist email accounts are setup, paid for, and accessed exclusively by the DSP. The client then mails their messages to the seedlist and the DSP monitors what percent of their client's expected mail is received and where it is placed. Insofar as the seedlist constitutes

legitimate, active email accounts, mail that is expected but not received purposely excludes mail that is bounced or blocked as a bad-address.

In addition to inbox versus spam folder tracking, DSPs typically provide a full range of complimentary technology and services such as Blacklist monitoring, Content Scoring, ISP Relations and Remediation, Whitelisting, etc.

Pivotal Veracity is a Deliverability Service Provider. There are also a number of other companies with whom we compete who also provide deliverability services including: eDiagnostix, Enhance Rate, Piper Software, and Return Path. If you are considering a Deliverability Service Provider, please consider all options and conduct full due-diligence on the solutions each company has available.

Appendix D: AOL's CityGuide newsletter

The Opt-in consent page for AOL's CityGuide newsletter
(note, below is the full web-page; no other content or links were on this page but white space has been cut in order to minimize the size of the image for this report)

AOL cityguide
Weekender

Explore Your City

Enter your e-mail address to sign up or access your preferences.

Your E-mail Address:

[ ] Submit

Return to CityGuide

The confirmation email sent after registration.

Date:	Sat, 19 Mar 2005
From:	"AOL CityGuide" <AOLCityGuide@dc.aol.com> Add to Address Book
To:	████████████
Subject:	Welcome to the AOL CityGuide Weekender

Thank you for subscribing to AOL CityGuide's Weekender newsletter, the free weekly update on new restaurants, upcoming concerts, hot clubs and top events in and around your city.

We'll soon begin sending your New York Weekender with what's new and happening near you. We'll pick the best stuff going on and deliver it to your email box, each week.

If you feel you're receiving this message in error, please click here.

Thanks for signing up!
The editors at AOL CityGuide

A sample of the CityGuide newsletter

Date:	Thu, 14 Apr 2005
From:	"AOL CityGuide" <AOLCityGuide@dc.aol.com> 📇 Add to Address Book
To:	▬▬▬▬▬▬▬▬▬▬
Subject:	NYC Weekender: Animals, Orchids and Beer...

WEEKENDER
cityguide.com
New York

| Music & Nightlife | Restaurants | Movies | Tickets | City's Best | Personals |

Weekend Event Picks:

1 Greater New York Orchid Show
Rockefeller Center is in bloom.

2 Gotham Motorcycle Classic
Go hog wild at the USS Intrepid.

3 Int'l Arts & Antiques Show
Evaluate treasures at the Armory.

4 Brewtopia at Metro Pavilion
Not Oktoberfest, but pretty close.

5 Poetry Safari at Bronx Zoo
Go wild for Nat'l Poetry Month.

▸ **Check Out Your Top Clicks**

☑ **Zoo Boom! Get Your Wild On...**
Cool Zoos & Aquariums Near You

Search AOL CityGuide:
[_____] [Go]

Music & Nightlife   ▸ More Choices

Tracy Morgan
April 15-17, Caroline's Comedy Club, New York
The former 'SNL'-er turned sitcom star takes a break from the tube for a three-night stand of raw zingers at Caroline's.

Brendan Benson at Bowery
April 15, Bowery Ballroom, New York
Detroit power-popper unveils crafty hits.

Restaurants   ▸ More Choices

Dine In Brooklyn
April 14-20, Dine In Brooklyn, Brooklyn
This restaurant week boasts a $19.55 prix-fixe at some of the hottest spots in town, like Stone Park and Frankie's 457.

Shea Gallante is F+W Best New Chef
24 5th Ave, New York
Reserve at Cru before word gets out.

This restaurant week boasts a $19.55 prix-fixe at some of the hottest spots in town, like Stone Park and Frankie's 457.

Shea Gallante is F+W Best New Chef
24 5th Ave, New York
Reserve at Cru before word gets out.

You Like Us, You Really Like Us...
We're up for a Webby Award for best travel site. Vote for AOL CityGuide.

How Safe is Your State?
Nevada tops this year's list of most dangerous states. See the 2005 rankings.

Movies ▸ More Choices

'The Amityville Horror' (R)

A couple thinks they've found a perfect home for a perfect price until they discover the house is full of evil spirits.

▸ **'Fever Pitch' (PG-13)**
▸ **'Sahara' (PG-13)**
▸ **'Sin City' (R)**

Tickets ▸ More Choices

Summer Concert Guide
Get your summer music plans in check with our guide to the best concerts, tours and festivals. Scan dates and buy tickets.

David Copperfield
Dates are on sale all across the country, including two weeks in Branson, MO. Grab tickets before they disappear.

Family Activity Planner
Kids bored? Find big fun for little ones.

Big Hunger, Little Wallet?
Get more for less with great cheap eats.

City's Best ▸ More Choices

New York Nightlife Picks

Boogie man? Dancing queen? Lounge lizard? Get out and get funky at one of your city's hottest dance clubs or coolest bars.

▸ **Best Dance Clubs**
▸ **Best Bars**
▸ **More City's Best 2005**

Personals ▸ More Choices

2 Sweet 2 Be Single?
Love is in the air! Spark a fine romance with local personals. Check out pictures and profiles and find someone special tonight.

I am a [M ▾] seeking [W ▾]
in Zip / Postal code [ ] Go

aolcityguide.com
personals
powered by
match.com

CityGuide News Flash
Get alerts on new features & specials.

Hot Spots & Roads Less Traveled
Plan with travel info from all 50 states.

Real Estate

- **Find a Realtor**
- **Find a Home**
- **Find an Apartment**
- **Get Mortgage Rates**
- **Find a Home Builder**
- **More Real Estate**

SUBSCRIBE, UNSUBSCRIBE OR CHANGE PREFERENCES
If you were forwarded this newsletter and want to subscribe, **click here**.
If you want to cancel or subscribe to another city, **click here**.

Important Information About Commercial E-mail from AOL