



Deliverability Year in Review: 2006



January 2007

epsilon[®]



Introduction

The stakes were raised last year as top-tier marketers spent unprecedented effort – and money – to devise truly relevant, integrated marketing campaigns. Customer insight-based marketing gained budget share from traditional mass media efforts, and businesses focused more attention on strategies such as micro-targeting to acquire and retain customers.¹

Email fortified its status as a focal point within the overall targeted marketing mix, outperforming other channels in delivering ROI.² Because of its unrivaled ability to cultivate long-term, valuable consumer relationships, businesses continue to increase their investment in the medium, and U.S. email-driven sales are forecasted to grow at a robust compound annual growth rate of 14.9 percent between 2006 and 2011.³

At the same time, however, over the last twelve months email marketers continued to face an evolving delivery landscape filled with pitfalls, but also new opportunities. As ISPs/email clients (“mailbox providers”) accelerated their adoption of emerging spam fighting and delivery management tools including authentication, accreditation, “Report Spam” buttons, feedback loops and default image suppression, it became more important than ever for marketers to adapt their marketing practices and technological capabilities accordingly, in order to optimize deliverability and ROI.

Epsilon’s *Deliverability Year in Review: 2006* provides email marketers with a comprehensive review and analysis of all the year’s most important challenges, trends, developments and research on the mailbox provider, industry self-regulatory and government policy fronts, and also highlights key lessons learned and new best practices.

1 Epsilon, “U.S. Marketers Shift Toward Trackable Marketing And Media Efforts,” June 21, 2006

2 DMA, “2006 Response Rate Report,” October 2006. According DMA, email returned \$57.25 for every dollar spent in 2005 compared to just a \$7.08 return for print catalog and \$22.52 for non-email Internet marketing ad spend.

3 Ibid.



Table of Contents

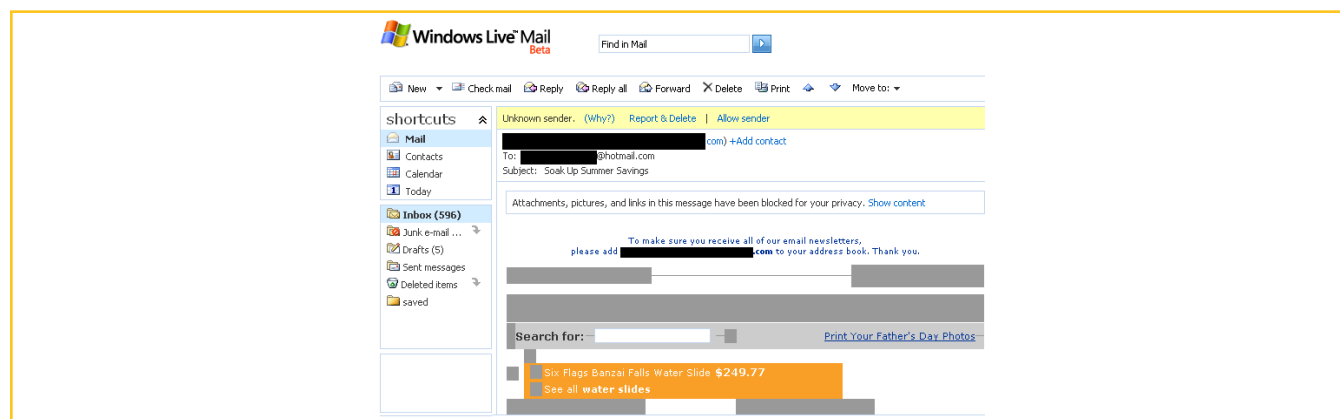
Introduction	2
The Imageless Inbox	4
Email Authentication Goes Mainstream	5
Third-Party Accreditation Sparks Controversy	7
Marketers and Mailbox Providers Unite with Feedback Loops	7
International Mailbox Providers Introduce New Complexities	9
Legislative and Regulatory Developments	9
Epsilon's Deliverability Leadership and Education Activities 2006	10
New Delivery Optimization Best Practices 2006	11
Conclusion	13
Resources	14



The Imageless Inbox

One of the most important trends that shaped deliverability in 2006 was the increased adoption of default image suppression by leading mailbox providers. Default image suppression is an anti-spam/email security technique where mailbox providers deliver email to recipients with images initially hidden, requiring individual end users to take additional, affirmative measures such as clicking a link to activate and view images. Mailbox providers believe this tactic is necessary to counter ever-inventive spammers, who – among other things – are increasingly sending their nefarious messages in image-only format in an effort to evade text scanning-based content filters.⁴

More Email Users Face Inbox Image Suppression



In a first-of-its-kind consumer study conducted by Epsilon and GfK NOP in July 2006, it was revealed that nearly two-thirds of American adult email users (65%) had already received at least some email messages in their inboxes with images suppressed.⁵ This number is expected to grow as mailbox providers, including Microsoft's new WindowsLive Mail, adopt default image suppression, and as more follow in the wake of its ratification as an industry best practice by the influential ISP and communication carrier trade groups MAAWG (the Messaging Anti-Abuse Working Group) and APWG (the Anti-Phishing Working Group) this past July.⁶

Consequently, it has become increasingly important for marketers to become knowledgeable about default image suppression and how it may impact their campaigns. For example, Epsilon's research showed that recipients' responses to receiving email with images suppressed vary by sender, permission-level, content and relevancy.⁷

4 Lisa Lerer, "Hack Attack," Forbes, December 1, 2006.

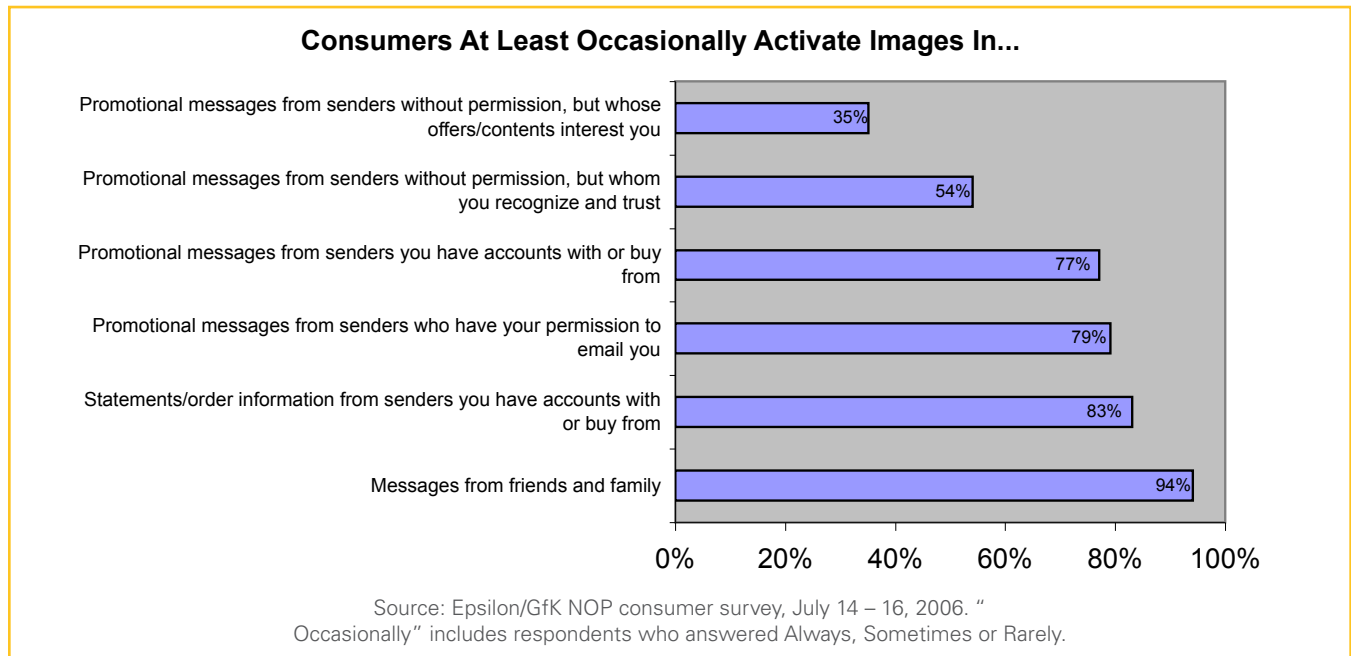
5 Epsilon, "Default Image Suppression Demystified," September 2006.

6 MAAWG & APWG "Anti-Phishing Best Practices for ISPs & Mailbox Providers," July 2006.

7 Epsilon, "Default Image Suppression Demystified," September 2006.



Survey Results: Likelihood of Image Activation



Epsilon’s study demonstrated that increasingly savvy and in-control email consumers are rapidly adapting to image suppression, and that there is no “mass aversion” to activating images – in fact, 94 percent do so at least occasionally.⁸ Consumers are willing and able to activate images in permission-based messaging that they value. By adopting new best practices related to email communication program technology, planning, and execution, marketers can compensate and thrive in the emerging environment despite the challenges posed by default image suppression.

Email Authentication Goes Mainstream

Designed to help mailbox providers more effectively verify the legitimacy and integrity of email communications, many believe that authentication solutions represent a much-needed foundation for reducing spam and phishing. By supporting an email delivery framework based on sender transparency and reputation, authentication can help mailbox providers tailor their deliver, non-deliver and folder placement decisions more squarely around individual end-user preferences, as opposed to legacy, more arbitrary heuristics and methods used to distinguish legitimate email from unwanted spam. Authentication also has been found to reduce spam filtering false positives (when legitimate, non-spam email is blocked or routed to a junk folder) by as much as 80 percent.⁹

In 2006, authentication became a thoroughly entrenched feature of the email delivery landscape, with a critical mass of legitimate marketers compliant with at least one standard. In fact, as consensus formed within the industry that IP-based solutions such as SIDF and SPF are complementary to – not competitive with – cryptography-based solutions like DomainKeys and DKIM, many marketers began to adopt multiple forms of authentication for their outbound messaging.

The relatively easy and inexpensive-to-implement SIDF/SPF experienced almost four-fold growth in sender adoption between December 2005 and November 2006. By the end of the year Microsoft reported that approximately

⁸ Ibid.

⁹ Microsoft, “Microsoft Furthers Email Protection Efforts,” April 18, 2006.



40 percent of all legitimate, non-spam email being sent on a daily basis was compliant with SPF/SIDF, and that approximately 6 million domains published their SPF/SIDF records, up from 1.6 million in December 2005.¹⁰ Mailbox providers and anti-spam companies using SPF/SIDF include: MSN/Hotmail, BellSouth, Gmail, Symantec, SecureComputing and others.

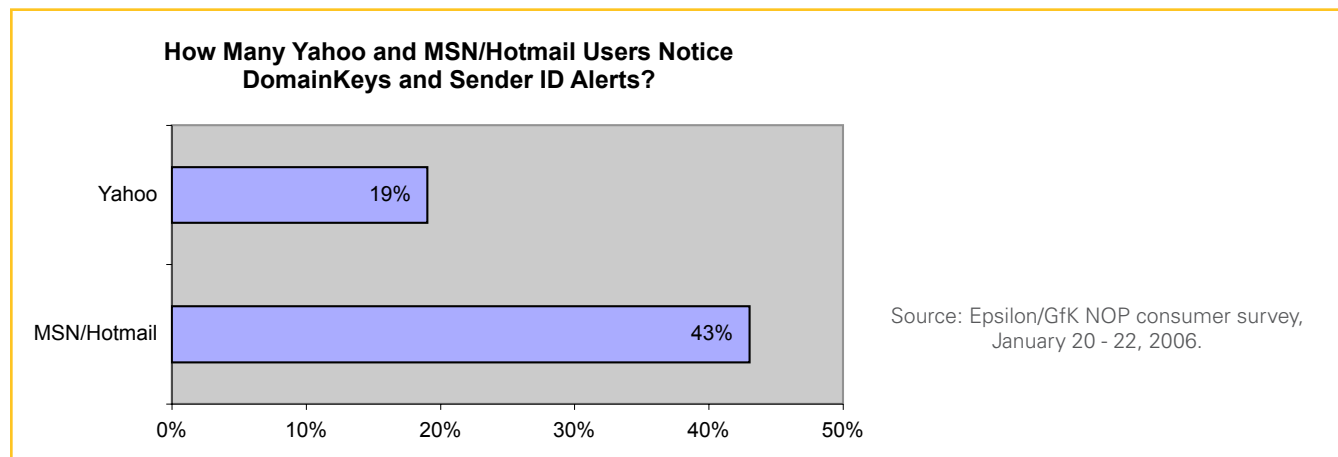
Implementation of more complex, cryptographic signature-based methods of email authentication also grew in 2006. Whereas adoption of DKIM was so small that it was virtually immeasurable in the spring of 2005, by April 2006's Email Authentication Summit II, it was reported that 9 percent of total email volume was being signed.¹¹

In use at major mailbox providers including Yahoo, SBC and others, DKIM received additional, important support in January when the Internet's leading global standards body, the Internet Engineering Task Force (IETF) chartered the DKIM Working Group to seek refinement and ultimate standardization of the specification. (Note: parallel to this, SIDF and SPF were approved by the IETF as "experimental standards" in the summer of 2005).

As part of the IETF's effort, industry is also exploring ways to maximize the value of DKIM for the Internet ecosystem through the development of the corresponding Sender Signing Policy ("SSP") protocol. In the future, senders may be able to use SSP to indicate to mailbox providers their desire to either have blocked or routed to the junk folder all messages claiming to be from their domains that are unsigned, or even to convey policies as specific as "email from our domain is never sent in text-only format," – providing an additional layer of control and defense against would-be domain spoofers and phishers.

In the meantime, mailbox providers continue to push forward with integrating authentication into their delivery technologies and policies, including by providing end users with visual legitimacy cues in their email browsers. A consumer survey conducted by Epsilon and GfK NOP in January 2006 revealed that nearly half of all MSN/Hotmail users, and a fifth of all Yahoo users, noticed recently introduced Sender ID alerts and DomainKeys confirmations in their browsers.¹² These numbers are expected to grow as solutions such as SPF, the Sender ID Framework (SIDF) and DKIM continue to enjoy boosts in market penetration.

Consumers Aware of Sender ID and DomainKeys Alerts



¹⁰ Microsoft/Mark Monitor data provided by Microsoft to Epsilon, November 22, 2006.

¹¹ Email Authentication Summit II, April 19, 2006. Authentication & Online Trust Alliance, see: http://www.aotalliance.org/summit_archive/pdfs/2_Summit_Scorecard_final.pdf

¹² Epsilon/GfK NOP, "Email & Spam: Consumer Attitudes & Behaviors," January 2006.



Third-Party Accreditation Sparks Controversy

The implementation of Goodmail Systems' CertifiedEmail accreditation solution at AOL sparked a national debate to kick off 2006. Consumer advocacy groups – most prominently the Electronic Frontier Foundation (EFF) with their “Dear AOL” media campaign – voiced concerns that the solution’s “pay-per-email” schema was akin to an “email tax” that could potentially lead to “unintended consequences” including the limitation of free speech.¹³

Following CertifiedEmail’s initial launch, AOL further extended its overall accreditation program, announcing in March that it partnered with two additional providers – Habeas and ISIPP SuretyMail – to offer free accreditation services for nonprofit and charitable organizations that would provide similar benefits to participating in CertifiedEmail. In addition, AOL emphasized that it was committed to maintaining its legacy free Whitelisting and Enhanced Whitelisting programs for all senders, which also are attached to delivery optimization benefits, and this helped to address initial concerns.¹⁴

Other highlights related to third-party accreditation in 2006 include:

- In December, Goodmail confirmed that a limited number of senders began participating in the phase-one rollout of CertifiedEmail at Yahoo, for transactional messages only. Goodmail anticipates that Yahoo will eventually allow promotional marketing messages to be certified at Yahoo as well. The company also continues to negotiate similar partnerships with additional mailbox providers, which may be announced in the months ahead.
- As of the publication of this document, the Beta release of Microsoft’s next generation webmail client, WindowsLive Mail, offers ReturnPath SenderScore Certified senders similar benefits to being in an end-user’s address book or safelist, including bypassing certain levels of filtering and overriding the default image suppression which may be applied to other, non-accredited or non-address-book listed high-volume senders (Note that this policy can change at any time at Microsoft’s sole discretion, and that WindowsLive Mail is slated to fully replace MSN and Hotmail in 2007).

To date, marketer adoption of fee-based third-party accreditation solutions has been tepid, as many take a “wait and see” approach to assess these solutions’ consequences for the overall landscape and for their own organizations’ email marketing ROI. In addition, some marketers may be finding it difficult to qualify for some programs because of their stringent participation requirements.

The ultimate success of fee-based third party accreditation solutions will hinge on their accessibility, and – most of all – on their ability to consistently deliver to marketers incremental ROI above and beyond their cost and the results achieved using current best practices and technologies.

Marketers and Mailbox Providers Unite with Feedback Loops

Feedback loops don’t just help mailbox providers reduce member spam complaints – they also have proven tremendously valuable to marketers seeking to improve their email “reputation scores” and optimize deliverability by providing critical insights into how mailbox providers are interpreting messaging (e.g., as “spam,” “legitimate email” or “something in between”). In addition, they indicate how many end-users are reporting a marketer’s communications as spam via clicks of “Report Spam” buttons or links. Leveraging feedback loops, marketers are better equipped to identify the root causes of delivery failures and make corrections to improve their deliverability, customer relationships, and overall email marketing ROI going forward.

¹³ Electronic Frontier Foundation, see: <http://www.eff.org/spam/aolmail/>

¹⁴ America Online Postmaster, see: <http://postmaster.aol.com/whitelist/nfpdoc.html>



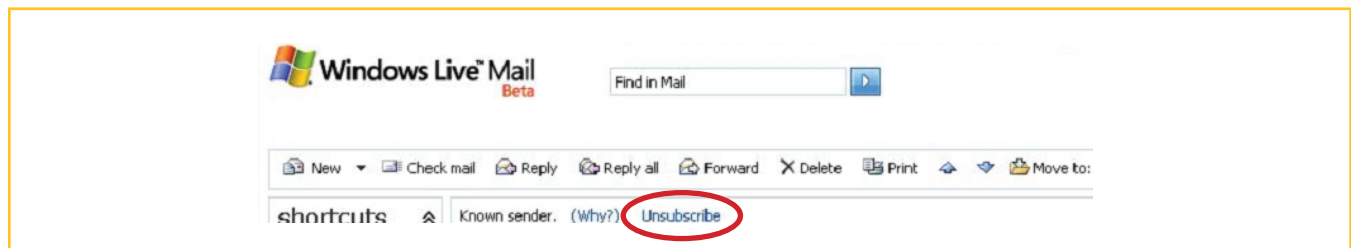
In Epsilon's *Deliverability Year in Review: 2005*, we were pleased to highlight that the industry had developed and coalesced around a single open standard for feedback loop reporting, called the Abuse Reporting Format ("ARF"), which we predicted would open the doors to much wider adoption of feedback loops beyond the pioneering implementers, AOL and Juno/NetZero. Our forecast came true, and 2006 saw many additional mailbox providers establish feedback loops with senders, including, for example, MSN/Hotmail, Earthlink, Outblaze and RoadRunner.

Browser-Based Unsubscribe

Over the last year, mailbox providers also began to explore providing end-users with more granular and precise browser-based feedback reporting options besides "Report Spam." Microsoft unveiled a browser-based "Unsubscribe" link within the Beta of its next generation webmail service, WindowsLive Mail. In a survey conducted by Epsilon and RoperASW in February 2005, 86 percent of American adult email users said they would prefer their mailbox provider to include an unsubscribe option that would safely remove them from email lists¹⁵ – with WindowsLive Mail, Microsoft became the first to offer its users such functionality.

Although the criteria for displaying the Unsubscribe link to WindowsLive Mail users is still evolving and can change at any time at Microsoft's sole discretion, currently the link is displayed for messages where the sender is in the end-user's address book or safelist, or is SenderScore Certified, and where the sender has also included an additional RFC-compliant, standardized unsubscribe header in its messages.¹⁶

Microsoft Introduces the Browser-Based Unsubscribe



While Microsoft can also change the effect of consumers' clicking the Unsubscribe link at any time, its current thinking highlights that mailbox providers continue to seek new ways to help legitimate marketers distinguish their messages from spam – for example, clicking the new "Unsubscribe" link will have no negative impact on a marketer's "reputation score" with Microsoft, whereas clicking "Report Spam" will diminish it. Microsoft is also exploring ways to enable clicks of the new Unsubscribe link to route users to a marketer's specified Online Preference Center rather than only working as a "one-stop shop" opt-out mechanism. This will help address concerns and objections from leading marketers whose corporate policies may require them to only accept and process opt-out requests directly from end users, not via third-parties.

Growing adoption of ARF and the testing of new features and technologies like Microsoft's Unsubscribe link are positive developments that should help improve deliverability. However, those marketers without the technical and professional staff in place to constantly monitor and implement new feedback protocols will, by the same token, find themselves at an increasingly disadvantaged position relative to competitors.

¹⁵ Epsilon/RoperASW, "Email & Spam: Consumer Attitudes & Behaviors," February 2005.

¹⁶ RFC 2369, see <http://www.faqs.org/rfcs/rfc2369.html>



International Mailbox Providers Introduce New Complexities

With the majority of spam originating from the U.S. and China,¹⁷ Epsilon's global Email Delivery Management team reported that a growing number of leading mailbox providers in Europe began responding by more aggressively filtering bulk email that is sent in English, Chinese and other non-native languages. These include, most prominently, Spain's Ya.com, Germany's GMX, France's Free.fr and Russia's Mail.ru. As a result, an increasingly important best practice for international marketers is to localize messages by using the native languages of European recipients.

Meanwhile, similar to their counterparts in the U.S., for the first time marketers in Asia were exposed to a fee-based delivery assurance solution when China's largest consumer mailbox provider, Netease, launched its in-house "Green Channel" program. By adhering to the program's requirements, and paying a steep CPM, Green Channel participants are assured delivery without significant volume or sending speed restrictions. On the other hand, non-participating high-volume senders are not guaranteed delivery and may have to reduce their sending speed and volume to below 1,000 messages per hour to optimize deliverability.

The past year's developments in China and in Europe underscore that the global email delivery landscape remains a very fluid and rapidly evolving one. Mailbox providers around the world are likely to continue to test a variety of new approaches to fighting spam and modify their delivery procedures, which in turn will have ramifications for marketers.

Legislative and Regulatory Developments

CAN-SPAM Act Rulemaking. More than a year-and-a-half has passed already since the FTC issued its May 2005 CAN-SPAM Act Notice of Proposed Rulemaking (NPRM) in which the agency controversially proposed to – among other things – reduce the allowable opt-out processing period from ten to three business days.

Because the NPRM was discretionary, rather than mandated by Congress within CAN-SPAM, the FTC can issue final rules – or not – anytime it chooses to do so. In the year ahead, marketers should continue to closely monitor FTC developments including the potential issuance of critical final rules related to the allowable opt-out processing period, and multiple-sender obligations.

China Introduces New "Regulations on Internet Email Services." On March 30, 2006, complicated new regulations governing commercial email went into effect in the People's Republic of China. Epsilon issued guidance to clients on the new regulations, highlighting in particular their "affirmative consent" framework (in contrast to the more lenient opt-out permission framework in the U.S.), "AD" labeling, and other requirements. The introduction of the new regulations in China reminded marketers that – like mailbox provider policies – the global legislative and regulatory landscape around email and spam is diverse, and still very much in its infancy. In the year ahead, for example, Germany will begin enforcing updated, more restrictive laws around email marketing, while Hong Kong is expected pass its first piece of legislation targeting spam. [Click here](#) to access Epsilon's in-depth, exclusive briefing on the new Chinese anti-spam regulations.

¹⁷ David Utter, "U.S. Slithers Atop Spam Producing Heap," SecurityProNews, November 8, 2006.



Spotlight on Security and Privacy. As additional public and private sector entities were revealed to have lost or exposed millions of records containing personal customer and employee information, lawmakers continued to focus attention on the hot issues of data security and privacy in 2006. In 2002, California became the first state to enact a data breach notification law – but its leadership spread like wildfire and by January 1, 2007, 36 states adopted similar laws.¹⁸ Now Congress is pondering a number of federal data security breach and privacy bills, including some that are preemptive in nature and which could result in a single national standard for corporate privacy and security. Marketers should continue to closely monitor these developments on the Hill and in the states, as well as audit their own data acquisition, usage, handling and security policies and procedures to ensure consistency with best practices.

FTC Holds “Protecting Consumers in the Next Tech-Ade” Hearings. The FTC held three days of hearings in November 2006, entitled “Protecting Consumers in the Next Tech-Ade,” to examine the key technological and business developments that will shape consumers’ experiences in the coming 10 years. The hearings built on “The Global Hearings” hosted by the FTC in 1995, which helped the agency establish its consumer protection agenda for the past decade.

Of extra importance to marketers, in her opening remarks at the hearings, FTC Chairman Deborah Platt Majoras emphasized her belief that the agency already has enough authority under existing laws to protect consumers from emerging online privacy threats such as spyware. She cautioned against the potential passage of new laws that could chill innovation and result in negative, unintended consequences for legitimate businesses. “The Commission’s existing legal authority is often elastic enough to cover a specific case,” said Chairman Majoras.

In addition, Majoras argued that today’s savvy online consumers are, themselves, a powerful force for changing business practices, without the need for government intervention. “Consumers believe quite strongly that it is their Internet, and they will have a strong voice in how it is used,” she said. “... The power of the collective consumer voice to cause changes in business behavior and move markets must be considered in assessing what policies to adopt.”¹⁹

Epsilon’s Deliverability Leadership and Education Activities 2006

In 2006, Epsilon continued to spearhead original and high-impact efforts designed to promote the most responsible, effective use of email for marketing purposes.

Default Image Suppression Research. As part of Epsilon’s ongoing commitment to maximize marketer insight into the latest industry trends and state-of-the-art best practices, we conducted research exploring consumers’ experiences with – and reactions to – growing mailbox provider adoption of default image suppression. In an exclusive white paper entitled, “Default Image Suppression Demystified,” Epsilon published results from its proprietary consumer study and educated marketers about the latest deliverability and rendering optimization best practices. [Click here](#) to request a complimentary copy of Default Image Suppression Demystified.

TRUSTe and Epsilon Best Practices White Paper and Webinar. TRUSTe, the leading nonprofit online privacy organization, teamed up with Epsilon to produce a white paper and corresponding webinar entitled, “Your Customers Hold the Key to Deliverability: Best Practices that Minimize Email Complaints.” The unprecedented joint effort updated marketers about the latest, largely end-user controlled spam filtering solutions, as well as emerging industry standards like the ARF feedback loop protocol. In addition, it offered a series of practical recommendations and best practices

¹⁸ Direct Marketing Association, June 22, 2006.

¹⁹ FTC, Opening Remarks of Chairman Deborah Platt Majoras, “Protecting Consumers in the Next Tech-Ade,” November 6, 2006. See: <http://www.ftc.gov/speeches/majoras/061106dpmtech-aderemarksltrhd.pdf>



for providing consumers notice and choice, capturing consent, collecting marketing preferences through preference centers and technology, monitoring and putting to use ISP spam complaint feedback data, and many other essential practices designed to keep complaint rates low and consumer satisfaction high. [Click here](#) to request a complimentary copy of Your Customers Hold The Key To Deliverability.

Email Authentication Summit II. Epsilon, an original founder and the only ESP on the steering committee of the inaugural Email Authentication Implementation Summit (July 2005), was proud to once again lead the charge in organizing Email Authentication Summit II. In Chicago in April 2006, a sold-out crowd of more than 500 email marketers, ISPs and technologists converged to learn about, and accelerate adoption of, authentication solutions. Epsilon is currently programming the third annual authentication summit - the Authentication and Online Trust Summit 2007, to be held in April in Boston. [Click here](#) for more information on the upcoming Summit.

New Delivery Optimization Best Practices 2006

Successfully navigating the complex email delivery landscape requires adjusting practices and technologies to correspond to rapidly evolving mailbox provider policies, technologies and anti-spam solutions.

What did marketers learn in 2006? And a look ahead...

Regarding Authentication:

- **Comply With Both!** Mailbox providers are implementing IP-based solutions such as SPF and SIDF, or cryptography-based solutions like DomainKeys and DKIM... or both. To optimize deliverability across multiple receiving mailbox providers, marketers also must implement both types of solutions.
- **We're Not Done Yet.** Marketers and mailbox providers have joined forces over the past few years to promote authentication solutions – but the job isn't finished yet. With the upcoming third annual Authentication and Online Trust Summit, and through other initiatives, industry must continue to intensify efforts to develop broad-based online security policies and procedures, and to explore two-factor authentication and emerging technologies and best practices to combat online fraud and identity theft – especially as omnibus privacy and security legislation looms over Washington.

Regarding Feedback Loops:

- **They're Blessings, But Also Headaches (Depending On How You Look At It).** By now, most marketers are well aware that increasing mailbox provider adoption of feedback loops is a delivery optimization blessing, but few understand the requirements for participation. Fully taking advantage of feedback loops necessitates implementing the Abuse Reporting Format (ARF), RFC-compliant unsubscribe headers, access to integrated complaint reporting, and having the technology resources and team of ISP relations specialists in place to identify and physically establish new feedback loops with mailbox providers as they are launched.

Regarding Image Suppression:

- **It's Not an Insurmountable Challenge.** According to Epsilon's research, four out of five consumers will, at least occasionally, activate images in messages that are transactional/service oriented, in promotional messages from companies they do business with, and in promotional messages that they request to receive. In addition, further



investigation of client campaign data revealed that, although image suppression may slightly diminish HTML open rates, click-through rates are unaffected. Image suppression presents marketers with new challenges, but the sky is not falling. Relevancy, value, and the employment of industry best practices hold the key to breaking through the clutter, getting into the inbox, and getting images activated by end users.

- **Don't Just Slap Print Creative into Email.** The fine art of email creative design and rendering optimization has never been more important. Marketers must optimize how they construct messages to improve their chances of success in the event of image suppression by maintaining an appropriate balance between images, plain-text and ALT-tags – never images only – and by using the text and ALT-tags to provide recipients with a better understanding of the email's benefit, and to help motivate them to view suppressed images. It also is wise to include links at the top of messages to view them in web page format.

Regarding Compliance:

- **Don't Assume You Know All the Rules.** Over the last year, a few marketers learned the hard way that it's not safe to assume you're compliant when it comes CAN-SPAM's "gray areas." In particular, over the last year the FTC engaged in high-profile enforcement actions against marketers for alleged violations related to insufficient opt-out processing, as well as non-compliant forward-to-a-friend campaign practices. Marketers should seek additional legal counsel to verify that their practices are in-synch with the law and with FTC staff opinion before deploying forward-to-a-friend, multiple sender, and mixed messaging campaigns (e.g., transactional email that contains some promotional content), as there are additional, complicated rules involved. In addition, they should audit opt-out processing capabilities.
- **Beware Before Deploying Overseas.** Marketers expanding their email marketing programs beyond U.S. borders should seek legal counsel and learn about the spam laws that are on the books in the countries of their intended recipients. Many have already enacted, or are in the process of crafting, spam legislation that is more restrictive than the law in the U.S.
- **Audit Security and Privacy Policies.** Lawmakers and regulators on the Hill and in the states are considering new laws and rules, and the privacy and security practices of leading marketers are under more intense scrutiny than ever before. Marketers should audit their security and privacy policies and procedures, ensure they're adequate, and strive to implement best practices.

Regarding the Marketer-Service Provider Relationship:

- **Marketers with Best-in-Class Deliverability Work with Best-in-Class Providers.** In 2006, marketers who sent their campaigns using an in-house or inferior provider's email deployment engine suffered from low delivery rates and were unable to maximize ROI. Optimizing deliverability in 2006 required deploying email from a specialized mail relay server with advanced bounce logic. It was also about having the creative and rendering expertise to design email campaigns that were optimized for image suppression. And, perhaps most important, in an era of increased consumer control, having access to actionable data and the tools to sort through it was critical to gaining meaningful customer insights and to devising compelling, relevant campaigns that truly engage the recipient and mitigate the potential for deliverability-damaging spam complaints.



Conclusion

With a critical mass of senders now authentication compliant, leading mailbox providers' spam filtering technologies are becoming more accurate, and more squarely tailored around individual end-user preferences, rather than arbitrary legacy heuristics.

Fortunately, today deliverability success is more dependent on getting customers to add you to their address books and activating images than it is about adjusting contextual elements to score well enough to "pass" spam content filter checks.

We have every reason to believe that, in 2007, the email environment will continue to improve. Consumers will find an inbox less cluttered by the nuisances of spam and phishing, and increasingly filled with relevant offers they want to receive.

However, it is prudent for marketers to keep in mind that the delivery landscape remains in a state of continuous, rapid evolution. Just as marketers had to implement new deliverability best practices in 2006, they must continue to actively monitor and effectively respond to whatever new developments may come in 2007.

Best-in-class marketers will continue to migrate their email communication campaigns to providers like Epsilon that have the scalability, flexibility, industry thought leadership and the depth of offering required to help clients stay a step ahead of the competition by ensuring the strongest delivery rates and developing the most timely, relevant and wanted communications.



Resources

Request your complimentary copies of the following key deliverability resources published by Epsilon in 2006. (Just ask your sales/client services representative, or visit our Resource Center at www.epsilon.com)

Epsilon's Delivery Optimization White Papers and Best Practices

- The Era of Consumer Control
- Default Image Suppression Demystified
- Your Customers Hold the Key to Deliverability: Best Practices that Minimize Email Complaints (co-published with TRUSTe)

Epsilon's Exclusive International Mailbox Provider and Legislative/Regulatory Issues Briefs

- What China's New Anti-Spam Regulations Mean for You
- Email Delivery Management Update: European Providers Implementing Aggressive Language-Based Filters

Epsilon's Ongoing Proprietary Research

- Image Suppression (July 2006)
- Executive Survey: Marketing Technology & Spending Trends (June 2006)
- Email and Spam: Consumer Attitudes and Behaviors (January 2006)
- Retailer Email Communication (January 2006)

For more information, contact

Epsilon
info@epsilon.com
(212) 995-7500
www.epsilon.com



Customer Insight Realized.™