GESMER UPDEGROVE LLP
Attorneys at Law

Consortium Standards Bulletin

*A **ConsortiumInfo.org** publication*

JUNE 2004
Vol III, No. 6

FEATURE ARTICLE

CONSORTIA, STANDARDS, AND THE USER EXPERIENCE

Andrew Updegrove

Introduction: In 2003, one of the most active areas of standard setting involved security. In 2004, this trend is continuing, but with a marked difference. Last year, the majority of the action centered on Homeland Security initiatives (see, Standards: the Year in Review.) The focus of much of the effort this year, in contrast, is the end user. And while most efforts in the past involved only standard setting, many of the organizations and initiatives launched this year involve a diverse range of other activities as well.

In some cases, the goal of these new consortia is to make the Web a safer place for customers (thereby facilitating ecommerce opportunities). In others, the intention is to make using the Internet less annoying, both for consumers as well as for the ISPs that carry the billions of email messages (legitimate and otherwise) that are sent every day. And there are also organizations whose goal is to bridge the gap between industry and government, as Washington begins to take a more active interest in what goes on over the Internet and the Web.

In this article, we survey the areas of greatest activity, as well as some of the new organizations that have been launched to help make the Web a better, safer, and more commercially rewarding place for vendors, service providers and customers to meet.

Why Now? Whether you believe that the Spam Age began in 1978 or 1994,[1] one might wonder why it is that 2004 has seen the advent of multiple, overlapping initiatives to curtail the flood of Spam and the incidence of identity theft.

There are a variety of reasons that are worth noting: One is the intervention of state and Federal governments in the effort to curtail Spam. But government intervention always evokes a mixed response from industry, which cannot reliably predict or control the ultimate results of legislation, even if it generally supports the overall thrust of the effort.

A second reason for action now is the potential for adoption of particular methods of Spam blocking to have a competitive effect on the fortunes of specific vendors. A third is that ISPs and carriers are suffering significant, although less widely reported, distress as well as consumers.

But most significant is the fact that, after failing to achieve the initial grandiose projections of the Internet bubble analysts, ecommerce is now growing to significant proportions. At the same time, there is a growing recognition that various forms of Internet abuse will limit commercial opportunities, and raise the costs of promoting and selling goods and services via the Internet and the Web.

The abuses themselves are becoming more troublesome. Those seeking to fleece the public are no longer just sending amateurish emails from Nigeria to their Dear Friends, but also superficially legitimate account confirmation requests ("spoofing") purporting to come from name-brand credit card issuers and other respected sources, sometimes conjoined with realistic looking WebPages ("phishing"). According to

[1] *Opinions differ on what marked the advent of the Spam Age. For the traditional view, which awards the dubious honor of First Spammers to immigration lawyers and Laurence Canter and Martha Siegel, see:* http://www-106.ibm.com/developerworks/linux/library/l-spam/l-spam.html *For the "way back" point of view, see:* www.templetons.com/brad/spamterm.html

some reports, such spoofing and phishing expeditions have fooled as many as 5% of those receiving them.

Force/CounterForce –Canning Spam and Fighting Phish: The intervention of Congress in the Spam wars is in many ways a natural development, given that the Federal Government has a history of acting to curtail telecommunications-based abuse of consumers, once the public uproar reaches a sufficiently defining volume. In 1991, for example, Congress enacted the Telephone Consumer Protection Act of 1991, which assesses fines for sending unsolicited junk faxes. Significantly, this Act addressed some of the more difficult Constitutional issues involving commercial free speech, paving the way for future efforts as new abuses evolved.

In June of 2003, the FCC and the FTC adopted rules under the same Act to create the Federal "no call" list that imposes fines on commercial telemarketers that do not honor telephone customer requests not to be bothered by unwanted solicitations. To most, moving from curbing junk faxes to curtailing junk email represents a logical and appropriate extension of Federal police power.

While the logic may be strong, the practicalities of this extension are far more problematic. In the eyes of most technically savvy observers, the enactment of the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" (popularly known as the CAN-SPAM Act) proved symbolic at best. Given the foreign sources and camouflaging methodologies of many of the most notorious Spammers, the mere defining of a crime represents a necessary, but hardly sufficient step towards actually curbing email abuse. To give the most graphic example of how much greater a challenge is posed by Spam, creating a public "no Spam" list would manifestly prove to be a boon for anonymous Spammers, rather than a useful enforcement tool.

In consequence, CAN-SPAM is not likely to actually decrease Spam for the foreseeable future. Rather, its principal benefit has been to facilitate legitimate commercial email solicitation by defining what email format a vendor must use in order to avoid violating the law, and by preempting the multiple (and sometimes more restrictive) definitions of acceptable solicitation that had been springing up on a state-by-state basis.

At the same time, the limited nature of the Act and the practical limitations on government investigative techniques underline the fact that if anything effective can be done (at least in the near term), it will need to be done by private industry.

Multiple Approaches: The new initiatives formed to protect the public come from a variety of distinct constituencies, and adopt a range of approaches. None of the new organizations will exclusively use standards to reach its goals, and some will not create standards at all. Instead, these new initiatives involve creating codes of conduct, seeking the prosecution of abusers, and influencing public policy.

While production of best practices and standards has long been part of the consortium playbook, engaging in some other types of joint action has been largely avoided, in part because of the greater degree of antitrust care that must be exercised when competitors (and especially competitors controlling a majority of a given industry segment) act together. Similarly, while individual companies have hired lobbyists, and traditional trade associations have usually had a public policy agenda as an important part of their program, cutting edge technology initiatives have rarely looked to Washington for assistance.

This historical lack of interest in influencing legislation is not surprising, given that the time between conception and realization of lobbying efforts can exceed the useful life of the technology in question. Rather, investments in public policy are more likely to reward industries, instead of individual technologies or product opportunities.

But with the maturation of the Internet and the Web and the proliferation of security related issues, an environment has evolved that suggests the need for joint effort, in order to focus government attention on protecting and nurturing ecommerce. The result is a sudden proliferation of consortia formed solely, or in significant part, to inform and influence public policy to bolster cyber security.

Who they are: The new consortia addressing security needs are a varied group. Some of the more interesting are the following:

- ***Cyber Security Industry Alliance:*** CSIA **www.csialliance.org/home** was announced in February at this year's RSA security conference by an impressive list of cyber security software, hardware and services companies. The fact that its board is made up of the CEOs of member companies is indicative of both the gravity of the situation that the organization was formed to address, as well as the seriousness with which the member companies regard the challenges at hand. Similarly, CSIA took care to recruit an Executive Director that is also a heavyweight in cyber security: prior to accepting the position, Paul Kurtz was a Special Assistant to the President and the Senior Director for Critical Infrastructure Protection on the White House Homeland Security Council. Before that, he served as the Senior Director for National Security of the Office of Cyberspace Security and a member of the White House National Security Council. One reason for the high membership fees is the fact that public advocacy is the primary activity of CSIA, with the mission of improving cyber security through public policy initiatives. Its many current and planned programs include coordination with the Department of Homeland Security to promote information-sharing between business and government on cyber-threats; identifying gaps in cyber security R&D; collaborating with U.S. and international standards development organizations to support emerging technology standards and specifications that will serve to enhance cyber security; and pursuing U.S. Senate ratification of the Council of Europe's Convention on Cyber-Crime. CSIA currently has 13 members listed at its site.

- ***Messaging Anti-Abuse Working Group:*** MAAWG **maawg.kavi.com/home** was formed not by product vendors, but by the ISPs that must deal with the practicalities of Spam and related email-based forms of abusive behavior. Spam dramatically overloads ISP systems, and decreases the overall value proposition of purchasing and upgrading ISP services. Moreover, consumers have come to expect Spam blocking as an included service from many ISPs, and keeping pace with the enemy represents an ongoing challenge and expense. Moreover, email is the carrier of worms, viruses and other Internet assaults launched by hackers, which also can tax carrier resources. Finally, ISPs find themselves in the difficult position of deciding what to do when it becomes evident that abuse is occurring. All of this provided incentives for ISPs to band together to seek common solutions, based on collaboration, technology and policy initiatives. Not surprisingly, MAAWG's goals include developing an ISP code of conduct for dealing with abusive practices, defining reference architectures and network standards for combating spoofing and identity forgery, and influencing public policy. As of this writing, the MAAWG website discloses the names of 10 carrier members.

- ***Trusted Electronics Communications Forum:*** The newest entrant into the anti-abuse consortium club is TECF www.tecf.org, which was announced just last week at the first ever Email Technology Conference, held in San Francisco. TECF was launched by yet another interest group with its own unique concerns and (therefore) action program. The focus of TECF is combating identity fraud and brand abuse, and the 14 members listed at its site represent a range of retail, telecommunications, financial services, banking and technology companies, including founding members IBM, BestBuy, E*Trade and Fidelity Investments. The goal of the organization is to curtail spoofing, phishing and other types of identity fraud that threaten the credibility and utility of e-mail marketing and e-commerce. TECF's announced initiatives involve not only the promotion of standards for technology and best practices, but also the prosecution of phishers and other offenders. The initial four working groups of TECF are intended to formulate and/or validate techniques and tools that specifically address the high-risk threats identified by the organization.

- ***Anti-Phishing Working Group:*** APWG www.antiphishing.org/index.html was officially launched in November of last year, and reportedly has 400 members (most of whom are individuals), representing over 250 companies. The actual membership roster does not appear at the member website, in order to avoid providing a target for retaliatory attacks. The public portion of the site provides a particularly useful resource for information on the nature and frequency of phishing attacks, as well as methods to recognize and combat such assaults. Recently, the organization announced a joint initiative with the Financial Services Technology Consortium http://fstc.org aimed at defining the technical requirements for counter-phishing measures.

- ***Global Infrastructure Alliance for Internet Safety (GIAIS):*** www.microsoft.com/serviceproviders/giais. This initiative has a far different point of origin. Rather than being a membership organization launched by a core group of companies, GIAIS is a

working group organized and hosted by Microsoft to promote and deploy its CallerID for E-Mail and related anti-SPAM initiatives. Like CSIA, GIAIS was also announced at the 2004 RSA security conference. Its goal is to increase Internet security for consumers by attempting to reduce the impact of viruses and worms. Its proposed methodologies include identifying potential threats, developing response tactics, creating longer-term remediation solutions, and communicating with and educating end customers. After an initial burst of publicity, it had not been much in the news. However, recently Microsoft announced that it would blend its CallerID proposal with another popular authentication scheme, the Sender Policy Framework (SPF), which would then be presented to the Internet Engineering Task Force as a single proposed specification for adoption.

Conclusions: The proliferation of consortia aimed at protecting the user, and thereby fostering further robust consumer use of the Internet and the Web, is a testament to the coming of age of ecommerce. On the positive side, the opportunities for advertising and closing sales via the Internet, as well as redeploying services more economically (everything from confirming flight schedules to enabling home banking), are growing enormously, fueled by a robust technology platform, a large and skilled technical work force, and the fact that a huge number of consumers have become experienced and comfortable with the Web. On the negative side, the increased online exchange of financial information has not gone unnoticed by those that see expanded criminal opportunities in ecommerce, and enforcement capabilities are failing to keep pace with technical innovation.

As we have so often noted before, the consortium approach provides a proven, low cost, easily deployed method for companies with similar concerns and interests to band together to seek common solutions. But – while the strength of this approach is that multiple groups can achieve rapid, targeted solutions for problems that they are uniquely able to understand and address, the concomitant weakness is the potential for disparate, poorly coordinated and (therefore) less effective solutions. The burden, therefore, is on these organizations to quickly explore and establish effective liaison relationships with each other so that the sum of their various worthwhile efforts adds up to the most effective, rapidly adopted, and pervasively deployed security solutions.

Comments? updegrove@consortiuminfo.org

Disclosure: *The Cyber Security Industry Alliance and the Message Anti-Abuse Working Group were each formed with the advice and legal assistance of Gesmer Updegrove LLP, the sponsor of this site.*

For further Information:

ConsortiumInfo.org has a variety of resources to help you locate and investigate new and existing consortia:

- The ***Consortium and Standards List /*****www.consortiuminfo.org/ssl /links** includes descriptions of over 300 consortia and accredited standards development organizations. Links are included to each organization's web site, as well as to their specifications and intellectual property policies, if they appear at public portions of the site. The list is searchable by geography, type of organization, and subject matter. For a list of over 20 organizations involved solely or significantly in ***Security*** issues, click **www.consortiuminfo.org/links/security.** For ready reference on any area of standard setting, bookmark the master list. If you know of an organization that is not listed, please let us know.

- The ***News Section*** **www.consortiuminfo.org/news** of the site is a portal providing ongoing, up to date news relating to consortia, SDOs and standards, searchable by category, one of which is ***New Consortia*** www.consortiuminfo.org/news/nc.php Bookmark the News home page or a category page, or take advantage of our ***RSS Feed:*** **www.consortiuminfo.org/rss/**