UNITED STATES OF AMERICA

FEDERAL TRADE COMMISSION

WASHINGTON, D.C. 20580

Division of Marketing Practices

Spam Forum

Panel: The Economics of Spam

Time: Thursday, May 1, 2003 – 8:30 - 10:00 a.m.

Moderator: Renard C. François, Staff Attorney, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission

Panelists:

Laura Atkins, President, SpamCon Foundation
Laura Betterly, President, Data Resource Consulting, Inc.
Al DiGuido, CEO, Bigfoot Interactive
Chris Lewis, Security Architect, NortelNetworks
Dale W. Mailk, Director, BellSouth Internet Group
Lisa Pollock Mann, Senior Director of Messaging, Yahoo!, Inc.
Carl Shivers, Systems Architect, Aristotle, Inc.
Steve Smith, President, Mindshare Design, Inc.

Key Issues: What is the definition of spam? Email is a cost-effective means of marketing. The costs of spam has risen over the past few years, and the cost of addressing the spam has risen over the past few years. Business incur significant costs processing spam. ISPs are incurring significant costs to address spam, and losing customers because of their frustrations with spam. Will spam significantly affect email as a tool for marketing?

Discussion Questions (intended to prompt thoughts):

(1) ALL- What is spam? Has that view changed over the past couple of years? If this has changed, what was the cause of it? Your customers?

It has changed for us somewhat. We used to define spam as email that was not "opt-in", meaning that the recipient never gave consent to being mailed to. We've had to expand our definition of spam though, and what we are now seeing is that what it really boils down to is that spam can be any email which irritates, annoys, offends, or inconveniences recipients. We, just like ISPs, are accountable for recipient complaints. Even if it is "confirmed opt in"—considered the "gold standard" by many in the anti-spam community—if it is ill-timed, or not well targeted, it may be considered spam. This is why we are spending more and more time working with customers on improving their mailing practices to keep their mail timely and relevant, as well as opt in.

(2) AL DIGUIDO- What is the appeal of email marketing? How is this different from the other forms of marketing? What are the benefits and the burdens of email marketing? How has unsolicited email affected email marketing over time (for better and for worse)?

Have these effects changed over time? How so? If spam continues unabated, hopw will that impact email marketing and communications via email?

(3) LAURA BETTERLY- What are the benefits that you see from email marketing? For a consumer side and from a small business side? How did you get involved in marketing? Was it the low barrier to entry that caused you to get involved? How many email addresses do you market to on a weekly basis? How many ads do you send out on a daily basis? What is the response rate where you consider a successful campaign? How much does it cost you to set up the system from soup to nuts (the computers, the distribution software, the collection of address via purchase or relationships, etc, the servers, the ISP connection)? How has your business grown over time? What are the products or services that you find have the higher response rates? On average how long do you work with a client to craft the email campaign?

(4) YAHOO AND BELLSOUTH- What do you consider spam? Has this definition changed over the past few years? If so, why? How much spam do you get on a daily basis? Has spam been increasing? What accounts for this growth? What are the resources that you devote to limiting the amount of spam you receive?

A. how much has the spam that you received in the past two years increased?
B. how much have your costs in addressing spam risen in the same amount of time?
C. has the number of customer complaints risen in the past two years?
D. what accounts for the increase in the cost?
E. have you found that the features that many customers find interesting, such as HTML, have made it more costly or burdensome to address spam?

(5) CARL SHIVERS- How many customers do you have? How much email do your customers generally receive? On a daily basis how much email traffic do you have? What percentage of that is spam? Has this percentage been static for the past year or two? How large is your staff to handle spam and customer complaints? How much do you spend in hardware and software to provide some sort of protection for spam?

(6) ALL ISPs- How much do you spend to maintain your architecture? How often do you make significant adjustments to you architecture because of spam? Is that because of volume or invasions, or both? Does the volume of spam (and software meant to filter or to intercept the spam) significantly affect your systems? If there is an impact, is this in a way that affects the consumer (functionality)?

(7) What is the amount of churn? How much is due to spam? Has this number increased significantly in the past two years? Is your churn being off set by new customers?

(8) CHRIS LEWIS- How does spam affect your business? I know that you have done a study and estimated how much it costs for each piece of spam that gets to your system? What goes into that calculation? Is this because of the amount of spam or the expense of the tools to combat spam? What are the things that tend to make it through the filters? What are the steps that your company has taken to try to diminish the amount of spam? Are there legal concerns about people receiving pornographic spam?

(9) LAURA ATKINS- What are consumers saying about spam? What do they consider spam to be? How does it affect them (not getting email they really want, getting pornography, the volume)? How many have complained about spam vis-a-vis marketing

that they really want? Who do they blame for receiving the spam? How often do they complain to their ISPs? Has this affected consumer participation on the Internet or in e-commerce? If so, how (are they afraid to join in newsgroups or purchase items from websites)?

(10) LAURA ATKINS- As an industry, how much spam are ISPs seeing on a daily or yearly basis? How much does this cost them? How has this changed over time? How does the increase of spam affect the ISPs' ability to project expenses and provide services to their customers? What are the tradeoffs that ISPs are making to combat spam (more resources vs. value added services)?

(11) STEVE SMITH- There are costs that are more than economic?

The way I would look at it is that there are short-term and long-term economic costs. Spam in general has a negative long-term economic cost. Spam negatively affects legitimate marketers' response rates, and, long term, it will drive their marketing dollars towards other media down the road, and impact our business. This is why it's important for those of us who want to provide services to legitimate opt-in email marketers to help get rid of the porn, get-rich-quick, penis enlargement, Viagra and mortgage offers. Reputation and good will directly impact our ability to send mail into ISPs, as ISPs still factor reputation and others' perception very heavily when deciding who they will grant sending access to. As mail delivery is the core of our business and a major part of what our customers pay us for, reputation and good will amongst ISPs clearly translates into economic value.

I know that you have had to deal with loss of good will and reputational injury on the Internet, please tell us about that?

Probably every few months we have some sort of incident where a spammer either tries to assume our identity or uses our email address removal instructions in their messages. One particularly nasty example was someone trying to assume our identity asking people to fax their social security numbers to an e-fax number, presumably for identity theft. We've also had international spammers clone our company web site and offer services under a similar name to confuse us with them.

Describe some of the efforts that you had to undertake to repair that injury?

When something like this happens, we end up spending the most time communicating with major ISPs, our upstreams, and major backbone providers to make sure our customers' delivery channel is not impaired. We also try to investigate as much as possible, however it's very difficult and time consuming to track down the offenders, and usually it's a dead end. The spammers use open relays, stolen ISP accounts, and they register domains with false information. One time our search ended up with a South African tire company who had their IP address range hijacked and used by spammers. We also try to report illegal activity, however it's hard to get employees up to speed on who to report which types of activity to. Local police, the SEC, the FBI, the FTC… it's hard to keep it all straight. And the times we have reported incidents haven't given us a lot of confidence that anything even gets done.

How many customers did you lose as a result of that?

Customer attrition due to these incidents is long-term, and it's hard to quantify, but we know it has an impact. In one forged header incident we had 4 major ISPs mistakenly block us, representing 6% of our customers' recipient base. While we ended up getting unblocked quickly, customers sending that day saw a noticeable drop in delivery rates. It is impossible for us to proactively contact smaller ISPs, so invariably there will be a number of small ISPs who block us each time something like this happens. Invariably there will be a handful of customers who use these small ISPs who will stop getting their own messages, which does an incredible amount of damage with our relationship with our customers.

Was there any damage to your systems?

Forged headers can cause performance problems and even outages on our bounce handling systems as the deluge of undeliverable mails get re-routed back to our servers. And then you have retaliatory hacking. After one incident of someone forging our headers to send out spam we had to fend off a DOS attack from a hacker who didn't take the time to make sure they were even retaliating against the actual sender of the email.

How much did it costs for you to litigate this issue? What was the result?

First we would have to find someone to litigate against. But as we've found, the people sending these messages are experts at cloaking their identity. Assuming we did litigate and win, we would need to be able to collect the judgment afterwards, which probably wouldn't happen as the spammer would likely declare bankruptcy and start over. With litigation expensive as it is, it's not a good business decision to try and litigate. That's why in places like Utah with poorly conceived spam laws, the courts are clogged with suits against companies with deep pockets, while the porn, get-rich-quick, penis enlargement, Viagra and mortgage rate spammers keep pumping their trash into people's inboxes.

The costs we see are in maintaining relationships, reviewing and managing our customers, developing technology to detect and prevent abuse, and to assist our customers in keeping their lists clean. In 2002 we probably spent $.20 to $.30 for every dollar our customers paid us in ISP relations and spam prevention.

(12) Is instant messaging spam a significant problem?

(13) How would the Burns Wyden Bill affect your economic interest as a small marketer, a business, a large/small ISP, a consumer advocate, a large marketer, etc? Can any type of legislation strike that balance between protecting consumers from the onslaught of spam and preserving a cost effective opportunity for small business and marketers?

The economic impacts of Burns Wyden on our business will be based on two things: the introduction of risk of frivolous lawsuits to legitimate senders hurts us and our customers, while its ability to combat spam will benefit us and our customers in the long run.

Since the majority of states have spam laws in place, some of which are poorly conceived and written, we don't see Burns Wyden introducing a lot of additional risk. The consolidation of a diverse patchwork of state laws into a single federal law may in fact lessen the potential liability of frivolous lawsuits. Utah is a great example of a state in

which a poorly crafted law which is being abused. We were named in a suit in Utah that came about when one of our customers sent mail to a recipient in Utah who claimed the mail was spam. When we investigated our customer's claim that the mail was, in fact, opt in, we examined the IP address, date, time, and URL provided by our customer for the subscription, and found that they were all consistent with the recipient actually subscribing to the mailings that they later claimed were spam.

An article in DM News on April 29th showed that we are not the only ones which feel that Utah's law is being abused. Al Mansell, President of the Utah Senate, and Martin R. Stephens, Speaker of the Utah House of Representatives were quoted as saying that Utah's current law "… has resulted in the proliferation of over 1500 lawsuits in the last 10 months. Two Utah law firms are taking unfair advantage of our legal system."

As for combating spam, Burns Wyden is still an opt-out standard, which takes some of the teeth out of the law, however we think the provisions against forging headers, truth in subject line, and working opt-out links could be significant for combating the worst of the spammers. By the FTC's own estimates, nearly 2/3 of spam emails have invalid removal instructions, which alone would be actionable under Burns Wyden. Couple that with people actually being able to remove themselves from spam lists due to the threat of prosecution, and there is a real possibility for significantly reducing spam.

All in all, we see the Burns Wyden bill as positive for our business.

(14) Besides the complete elimination of spam, what is the solution that can positively affect the economic issues that you and your business face?

Make senders identifiable and accountable, and allow recipients to automatically discard mail that isn't from an identifiable, accountable sender. That will go a long way.