FEDERAL ELECTION COMMISSION
Washington, DC 20463

June 24, 2005

MEMORANDUM

TO: The Commission
General Counsel
Staff Director
Public Information
Press Office
Public Records

FROM: Brad C. Deutsch
Assistant General Counsel

SUBJECT: Untimely Comment on Internet Communications Rulemaking

Attached please find one untimely comment submitted in response to the Notice of Proposed Rulemaking on Internet Communications, Notice 2005-10, published on April 4, 2005 (70 FR 16967). The comment period ended on June 3, 2005.

Attachments

cc: Associate General Counsel for Policy
Congressional Affairs Officer
Executive Assistants

Aristotle

7440 Chummley Court
Falls Church, VA 22043

Tel. 703-846-0078
Fax: 703-846-0576

J. Blair Richardson
General Counsel

June 23, 2005

By Email to:
Mr. Brad C. Deutsch
Assistant General Counsel
Federal Election Commission
999 E Street, NW
Washington, DC 20463

Email: internet@fec.gov

Re: Comment in Support of Commission's Proposed Extension Of Disclaimer Rule to Political "Spam"

Aristotle hereby requests leave to file these late comments in response to the Notice of Proposed Rulemaking on Internet Communications issued by the Federal Election Commission and published beginning at 70 Fed. Reg. 16967 (Apr. 4, 2005).

Aristotle files these comments in support of the Commission's proposed extension of the "disclaimer rule" in 11 C.F.R. § 110.11 to political spam.

These comments are filed after the June 3, 2005 due date for two reasons: 1) An article in the June 8, 2005 issue of *Privacy Times* exposed the political spam

practices of NGP Software and Advocacy Inc[1], raising questions about the need for greater disclosure; and 2) As a result of the article, in the ensuing weeks we have received a number of inquiries demonstrating concern with the issue of political spam and the unique position it holds in online communications.

I. Aristotle's Interest

For over 20 years, Aristotle has been in the business of publishing campaign management software and public record voter list information for lawful uses. Aristotle is non-partisan, with clients across the ideological spectrum.

The Company's stated organizational purpose includes (a) "publishing information used to influence political campaigns, elections, and public policy matters"; and (b) "increasing, in any media, the quality of information reaching the body politic and furthering the goal of the First Amendment to the Constitution of the United States of America of producing an informed public capable of conducting its own affairs." Aristotle does not provide email addresses for unsolicited communications, but has received many inquiries about the practices outlined in the *Privacy Times* article because Aristotle competes with NGP in providing campaign software.

II. Regulatory Goals

We agree with the Comments of the Online Coalition that any new rules should be informed by the regulatory purpose of the Federal Election Campaign Act. Like the Online Coalition, we believe the rules should address corruption, and the appearance of corruption.

[1] The Privacy Times article is appended hereto as Exhibit A.

We also believe that, as a result of the decision in *Shays v. Federal Election Commission*, 337 F. Supp. 2d 28 (D.D.C. 2004), the Commission must be careful to "strike" the proper "balance between provisions of the [Federal Election Campaign] Act," as amended by the Bipartisan Campaign Reform Act ("BCRA"), and the "significant" constitutional and "public policy considerations that encourage the Internet as a forum for free or low-cost speech and open information exchange." 70 Fed. Reg. at 16969.

With this in mind, we address the specific proposal concerning the disclaimer rule.

III. Comments on Disclaimer Requirements, 11 C.F.R. § 110.11

We respectfully, disagree with several of the commenters who have suggested that the Commission's proposed extension of disclaimers through 11 C.F.R. § 110.11(a) to unsolicited e-mail would either be ineffective or unnecessary, or both.

Political spam raises an inordinate number of opportunities for corruption. A disclaimer requirement is a reasonable, affordable, and almost no burden whatsoever on the sender. At the same time, the disclaimer r requirement will impose a discipline on the process that is tailored to addressing the risk of allowing political spam to be sent without such notice.

According to the description of an unsolicited email campaign provided by NGP[2], the purpose of such activity is the "confuse" the opponent:

> *Imagine your opponent's confusion as they try to figure out who you sent it to and how widespread the message was. Do they air a tv ad responding to the attack at the risk of further spreading your message or do they ignore it (not realizing that you sent it far beyond your donor base)?*

[2] See the "Description of Political Email Address Program Offered on NGP Website", attached hereto as Exhibit B.

This is precisely the problem. "Widespread" dishonest attacks can be sent at the eleventh hour, and the source of the attack must be identified immediately to avoid corruption. In addition, "widespread " corruption could result if dirty tricks were to include spamming large numbers of swing voters with offensive messages that seem to come from supporters of an opponent.

The difficulty of tracing the source of email addresses is only part of the problem. This is exemplified by the fact that a political spammer such as NGP does not even identify its physical location on its own website. (Although NGP lists its mailing address as a post office box at Mailboxes, Inc. at 5505 Connecticut Ave NW, PMB 277, Washington, DC 20015, NGP actually appears to operate a large scale operation with many employees out of a home in Washington, DC, at 5305 Connecticut Avenue, NW, and no record of a permit to run a business at that location has been found.) NGP's true location is not disclosed at its website, so voter recourse to offensive spam is difficult and burdensome.

The example of US-based spammers such as NGP and Advocacy Inc. contradicts the claim by one commenter, English First, that "the true spammers set up shop outside the jurisdiction of American law, just like the on-line gambling sites do." The fact is that political spammers located in the U.S. should be required to include the disclaimer, and the existence of some offshore spammers should not give those in the U.S. a free ride to engage in unfair practices.

This is merely an example an actual problem that could be rectified if a spammer were required to include a disclaimer.

In the same vein, we note that "the burden of complying with a disclaimer requirement" in the case of spam email is insignificant. The benefit of the disclosure far outweighs the burden of inserting the required notice into the text of each email.

Moreover, we believe that the figure of 500 emails trigger limit is arguably too high. Recent gubernatorial and presidential races have turned on final tallies of only a few hundred votes. The Privacy Times reveals that political email addresses are bought from spammers in relatively small amounts for unsolicited email "blasts":

> *In Colorado a State Senate candidate now taps into a nationwide database of 26 million e-mail addresses appended to voter file records and pulls out the 5,228 Democrats and 5,952 Independents in his district," [Roger] Stone [of Advocacy, Inc.] wrote in a September 2004 edition of his company newsletter.*

Therefore, where email addresses have been purchased for the purpose of engaging in a controversial and easily corruptible practice such as unsolicited political spam, we believe that the rationale for a non-burdensome disclaimer is strong, regardless of how many emails are involved. The seriousness and degree of corruption involved in the particular practice should be the touchstone for regulation, rather than focusing on the number of emails sent.

I am grateful for the opportunity to submit these comments.

Respectfully submitted,

/s/ J. Blair Richardson

J. Blair Richardson
General Counsel
Aristotle

June 24, 2005

Exhibit B

PRIVACY TIMES

EDITOR: EVAN HENDRICKS

Volume 25 Number 11 June 8, 2005

LIVE STRATEGY: E-MAIL SOLICITATION FOR POLITICAL GAIN

Despite the public's professed dislike of "spam," some political consultants, anxious to help their clients achieve or maintain success, appear to be promoting unsolicited e-mail as a central strategy. Some think the strategy could backfire, particularly against politicians who have publicly railed against spam.

A look at NGP Software and Advocacy, Inc., two Washington consultants which service Democratic politicians and liberal groups, provides a window into the world of politically-oriented e-mail solicitation.

When *Privacy Times* began its work on this story, the NGP Software Web site indicated that it maintained opt-in e-mails. "We now have email addresses for registered voters who have agreed to receive information from political candidates," the Web site stated. http://www.ngpsoftware.com/voteremail.html

Just below, however, the NGP Web Site more specifically stated, "**Where the email addresses came from:** Working with partners, we've matched the entire national voter file against multiple email databases nationwide. We then sent each of those people an email saying that political candidates and organizations were interested in communicating with them and giving them the opportunity to opt-out. In some states and districts we got up to a 20% match rate. You can buy email addresses for voters targeted by party, geography, age, gender and/or voting frequency and in most cases we can have them in your hands within 24 hours."

Previously, the NGP Web site said it had about 25 million e-mail addresses and gave a state-by-state breakdown. http://www.ngpsoftware.com/stateslist.html However, NGP Software recently revamped its Web site, taking visitors to www.ngpsystems.com. The site only has an obscure reference to the 25 million e-mails; its privacy policy is silent on the source of the e-mails.

NGP President Nathanial Pearlstein said the previous site's statements about e-mails were provided by one of the company's partners. Although he declined to specify which one, he suggested that *Privacy Times* contact Advocacy, Inc. for more information.

Pearlstein said that unsolicited e-mails did not work very well, and that his company was moving away from them.

In fact, the *Washington Post* reported last September that Advocacy, Inc. matched its email address file with the 155 million-person voter file of Voter Contact Services (VCS), headed by William Daly. Advocacy Inc.'s President is Roger Alan Stone. *Privacy Times* was unable to find a privacy policy on Advocacy's Web site.

Stone denied to the Post he was spamming anyone, arguing that Internet anti-spam filters did not consider his company's e-mail to be spam because of the kind of servers that sent it. He said e-mail recipients can click a link if they don't want to receive political communications. He also said that since he launched the lists in 2004, the complaint rate had been low and customer satisfaction high. "Now any candidate or interest group can call us up and ask, 'How many Democratic voters do you have e-mails for in Ohio?' or 'How many non-registered voters do you have emails for in Florida between the ages of 18 and 24?' we can get it to them in a couple hours,"

So where did Advocacy obtain 25 million e-mails? The company is not saying, and would not respond to *Privacy Times'* queries. It is worth noting, however, that before Stone founded Advocacy, Inc. in August 2002, "he previously founded the Juno Advocacy Network (JAN) in 1998 and built it into a $5 million business," according to the firm's Web site.

JAN's parent company, Juno, launched in the late 1990s by offering free Internet service in exchange for customers granting permission for use of their e-mails. Sources said that Juno was a possible source of Advocacy's e-mail address database. But Sylvia Goeffrey, of Juno's Security & Abuse Dept., said, "Juno prohibits unsolicited email, and we would never share our members email address with others." However, Goeffrey did not respond to a follow up e-mail asking if Juno customer e-mails could have migrated with Stone to Advocacy, Inc.

"In Colorado a State Senate candidate now taps into a nationwide database of 26 million e-mail addresses appended to voter file records and pulls out the 5,228 Democrats and 5,952 Independents in his district," Stone wrote in a September 2004 edition of his company newsletter. "The candidate surveys these voters and sends targeted messages based on their responses. Testing the messages by the rate at which a recipient opens the message, the candidate blasts out the best message to the rest of the list."

"What we're talking about here is political spam," Pam Fielding, co-author of "The Net Effect: How CyberAdvocacy is Changing the Political Landscape," told the *Washington Post.*

Several leading Democrats have favored strong anti-Spam proposals. Sen. Charles Schumer (NY) said in 2003, "The e-mailing public has been at the mercy of spammers for way too long," he said. "This survey confirms that people are screaming out to be

empowered with the ability to stop the constant flow of unsolicited e-mails in their in-boxes."

June 24, 2005

Exhibit B

Description of Political Email Address Program Offered on NGP Website

SEND EMAIL TO YOUR REGISTERED VOTERS

We now have email addresses for registered voters who have agreed to receive information from political candidates.

Where the email addresses came from:
Working with partners, we've matched the entire national voter file against multiple email databases nationwide. We then sent each of those people an email saying that political candidates and organizations were interested in communicating with them and giving them the opportunity to opt-out. **In some states and districts we got up to a 20% match rate.** You can buy email addresses for voters targeted by party, geography, age, gender and/or voting frequency and in most cases we can have them in your hands within 24 hours. Click here to see how many email addresses we have in your area.

What you can do with them:
- Engage your contacts and constituents in local opportunities to volunteer and donate.

- Put your messages and ads directly into the hands of your swing voters.

- Put info about your opponent directly in the hands of voters during the critical homestretch. Imagine your opponent's confusion as they try to figure out who you sent it to and how widespread the message was. Do they air a tv ad responding to the attack at the risk of further spreading your message or do they ignore it (not realizing that you sent it far beyond your donor base)? [

- Email vote by mail requests to your ID'd supporters pre-filled with their information and a pre-addressed envelope. Track who has downloaded and printed it, send reminders and re-allocate your more expensive phone and door to door GOTV efforts accordingly.

Call or email us if you would like specific counts of email addresses available in your state/district.