

KEEPING UNWANTED DONKEYS AND ELEPHANTS OUT OF YOUR INBOX: THE CASE FOR REGULATING POLITICAL SPAM*

By Seth Grossman†

ABSTRACT

This Article focuses on the growing but largely unexamined phenomenon of political spam. Although political spam lies at the nexus of two important developments in recent years—the increasing government regulation of unsolicited communication and the growing use of Internet-based media in political campaigns—it has for the most part been ignored. This Article scrutinizes the reasons underlying lawmakers and commentators’ failure to deal with the political spam problem and argues that leaving the issue unaddressed is a mistake. It contends that political spam can and should be regulated as part of a general measure restricting the use of all unsolicited bulk e-mails.

In order to do so, this Article lays out the scope of the political spam problem by tracing its escalating use in recent elections. It then considers how the various mechanisms contained in current and proposed laws regulating other forms of unsolicited communication, including commercial spam, telemarketing telephone calls, and blast faxing, can be applied to political spam, and evaluates the efficacy of the various measures. Next, this Article examines the constitutional and policy issues surrounding the potential regulation of political spam. Finally, it offers an innovative model piece of legislation that would curb political spam without compromising candidates’ free speech rights or the legitimate use of e-mail in campaigns.

TABLE OF CONTENTS

I.	INTRODUCTION	1534
II.	THE CONCERN: THE POLITICAL SPAM PROBLEM AND ITS COSTS	1536
	A. The Scope of the Political Spam Problem	1536
	B. Reasons for the Political Spam Problem and Why Voluntary Measures Are Not Effective	1539

* Winner of the 2004 Berkeley Technology Law Journal Student Notes & Comments Competition.

© 2004 Seth Grossman

† J.D. Candidate, 2005, Yale Law School; B.A., 2001, University of Pennsylvania. Thank you to Jack Balkin for his assistance in developing this Article. I am also very grateful to Robert Post and Reva Siegel for their guidance and support.

C.	The Costs of Political Spam	1541
III.	POTENTIAL REMEDIES: MECHANISMS FOR REGULATION.....	1545
A.	Opt-in Systems	1547
B.	Opt-out Systems	1548
C.	Labeling Systems	1550
IV.	CONSTITUTIONAL ISSUES: CAN POLITICAL SPAM BE REGULATED?	1551
A.	Content-Neutral Regulations of Political Speech.....	1552
1.	<i>Content-Neutral Regulations</i>	1554
2.	<i>Substantial Interest</i>	1554
3.	<i>Reasonable Fit</i>	1556
4.	<i>Van Bergen v. Minnesota</i>	1559
B.	The Government's Ability to Regulate the Flow of Information	1561
C.	Right to Access Inboxes as Public Fora	1565
D.	Specific Labeling for Political Spam.....	1566
E.	The Right to Engage in Anonymous Political Speech.....	1568
V.	POLICY ISSUES: SHOULD POLITICAL SPAM BE REGULATED?	1569
VI.	THE PROPOSAL: A LEGISLATIVE APPROACH TO REGULATING ALL SPAM	1571
VII.	CONCLUSION	1574

I. INTRODUCTION

You open up your e-mail account to find you have twelve new messages. As you begin to sift through them, you find unsolicited advertisements for Viagra, cheap electronics, quick weight-loss gimmicks, and Joe Lieberman's presidential campaign. While lawmakers and commentators have focused on the type of e-mails represented by the first three messages, the sort of e-mail exemplified by the last message has received relatively little attention, even as it has become increasingly prevalent over recent election cycles.

The first widespread use of unsolicited bulk e-mail for political purposes—political spam—occurred in 1998.¹ Since then, the use of political spam has grown dramatically at all levels of the political process, with utilization by candidates for offices ranging from state representative to state governor to president of the United States. Most individuals consider such unsolicited political bulk e-mail to be spam, analogous to unsolicited commercial bulk e-mail.² Nonetheless, although state and federal governments increasingly have regulated unsolicited commercial e-mail, they

1. People often use the term "spam" to refer to many different concepts. For the purposes of this Article, "spam" refers to unsolicited bulk e-mails. "Political spam" refers to unsolicited political bulk e-mails sent by political campaigns or their affiliates.

2. According to a recent study by the Pew Internet and American Life Project, seventy-six percent of e-mail users consider unsolicited e-mail with political messages to be spam. DEBORAH FALLOWS, PEW INTERNET & AM. LIFE PROJECT, SPAM: HOW IT IS HURTING E-MAIL AND DEGRADING LIFE ON THE INTERNET 10 (2003), available at http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf.

have almost uniformly exempted political spam from any regulation. When legislators and policymakers bother to explain this omission, they usually offer three rationales: politicians would not use spam because of its annoyance factor; political spam constitutes constitutionally protected political speech and thus cannot be regulated; or they do not want to hinder the development of e-mail as a tool in political campaigns.

This Article argues that such beliefs are deeply misguided. Despite the irritation unsolicited bulk e-mails often prompts in recipients, many candidates have employed it as part of their campaigns—and the use of political spam is escalating. In addition, the Constitution does not place this problem beyond the reach of Congress. The Supreme Court has regularly upheld the constitutionality of laws that regulate protected speech, including political speech, as part of general, content-neutral measures. Furthermore, the increasing incidence of political *spam* threatens to undermine the effectiveness of political *e-mail*, which is still underdeveloped as a resource in political campaigns. Preserving this potentially significant tool as a force in the electoral context demands something be done about political spam. Consequently, this Article contends that Congress should not automatically exempt unsolicited political speech from general legislation designed to curb unsolicited communication, as it did with the recent CAN-SPAM Act.³ Instead of ignoring the political spam problem and limiting regulation to unsolicited commercial bulk e-mail, Congress should enact legislation to regulate all unsolicited bulk e-mail, including political spam.

Part II describes the scope of the political spam problem and the costs it entails in order to show that political spam is not a minor issue that should be ignored. Part III explains how different mechanisms proposed to address the problem of unsolicited commercial e-mail, such as various forms of opt-in, opt-out, and labeling systems, could be effectively extended to include political spam. Part IV examines the constitutional issues implicated by regulating political spam as part of a general measure to curb unsolicited communication and describes why such regulation is constitutional. Part V considers the policy arguments made by advocates of political spam and explains that the best way to facilitate the benefits of e-mail in political campaigns is by regulating political spam. Based on the problems, constitutional issues, and policy concerns discussed in the previous sections, Part VI suggests model legislation that would curb political spam as part of a general regulation of unsolicited bulk e-mail.

3. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701-7713.

II. THE CONCERN: THE POLITICAL SPAM PROBLEM AND ITS COSTS

As many everyday users of e-mail are now all too aware, the use of unsolicited bulk e-mail for political purposes is becoming increasingly common. This Part details the escalating use of political spam over the past few election cycles. It then explains the reasons for this increase, why voluntary measures are ineffective in addressing the political spam problem, and the costs imposed by political spam.

A. The Scope of the Political Spam Problem

Many policymakers and commentators who examine the issue of spam dismiss the political spam problem, often on grounds that politicians are unlikely to use a means of communication as unpopular as spam. In arguing that there is no need to bar political spam, one commentator has written that “[w]ith spam less popular than the Ebola virus, savvy politicians aren’t likely to use it.”⁴ However, the actions of campaigns at the local, state, and federal levels demonstrate that, in fact, candidates often use spam for purposes ranging from fundraising to disseminating information to attacking their opponents.

The first widespread use of political spam occurred during the 1998 elections. A state senator running for governor in Georgia sent 500 unsolicited e-mails, prompting a strongly negative reaction.⁵ In Texas, a candidate for the state Court of Criminal Appeals also used political spam on a similar scale to the same off-putting effect.⁶ A more severe form of political spamming occurred in Pennsylvania, where a candidate for state representative sent out 5 million unsolicited e-mails to people all over the world.⁷ His actions likewise provoked a severe backlash and his ISP ultimately disconnected his service.⁸

The most notorious political spamming in 1998 occurred as part of the Florida gubernatorial race. The Democratic candidate, Lieutenant Governor Buddy MacKay, sent out an unsolicited message to almost 250,000 voters entitled “A message from Governor Lawton Chiles” (the sitting

4. Jonathan Turley, *Uncle Sam and Spam*, MILWAUKEE J. SENTINEL, Apr. 28, 2003, at 13A.

5. Dion Nissenbaum, *Politicians Click on to E-mail Spam to Get Message Across*, SAN JOSE MERCURY NEWS, Apr. 7, 2002, available at http://www.staugustine.com/stories/040702/nat_625091.shtml.

6. *Political ‘Spam’ Mail Irks Texas Voters*, CHI. TRIB., Mar. 16, 1998, at C5.

7. Margie Wylie, *In the Age of ‘Spam-paign,’ Politicians Join the Junk E-mailers*, NEWHOUSE NEWS SERV., Mar. 19, 2002.

8. *See id.*

governor at the time) that urged recipients to vote for MacKay.⁹ Also in that race, a volunteer organization sent out unsolicited e-mails on behalf of the MacKay campaign.¹⁰

Candidates continued to use political spam over subsequent election cycles. Elizabeth Dole sent out spam fundraising e-mails to support her fledgling presidential campaign in 2000.¹¹ The 2001 and 2003 Houston mayoral campaigns saw the use of "attack" political spam.¹² Returning to the political scene in 2002, Dole received unwanted publicity when she was sued over her use of political spam in her successful campaign for the United States Senate.¹³ Also in 2002, Steve Biener, a Delaware candidate for the United States House of Representatives attracted a large amount of negative attention for his extensive use of spam in his campaign.¹⁴ Similarly, Katharine Harris, the Florida Secretary of State during the 2000 recount process, used political spam in her 2002 race for Congress. Harris obtained recipients' e-mail addresses primarily from messages they sent her *in her official capacity* as the chief election official during the Florida recount controversy.¹⁵ Also in Florida in 2002, Governor Jeb Bush sent spam fundraising e-mails to supporters of his opponent, Bill McBride. The Bush campaign accessed the e-mail addresses they spammed when a message sent by the McBride campaign unintentionally failed to suppress recipients' e-mail addresses, thus making them public.¹⁶

The 2002 California gubernatorial campaign offered perhaps the most well-known instance of political spam. Secretary of State Bill Jones spammed voters extensively during his campaign for the Republican nomination for governor.¹⁷ After the first two times his campaign sent out large spam mailings, Jones's ISP warned him to stop. Jones then hired an outside company to send even more spam to voters.¹⁸ The campaign itself

9. Jamie Murphy & Stephen McDowell, *A Message From the Governor Breeds Political E-Mail Debate*, WALL ST. J., Jan. 5, 1999, <http://interactive.wsj.com/archive/retrieve.cgi?id=SB91546855489608500.djm>.

10. Samuel Lewis, *Spam Politics: A New Way to Annoy Voters*, N.Y. L.J., Oct. 8, 2002, at 5.

11. Ed Henry, *Heard on the Hill*, ROLL CALL, June 28, 1999.

12. John Williams, *New Mudslinging: Wham, Bam, Spam*, HOUSTON CHRON., Mar. 16, 2003, at A13.

13. *Campaign Notes*, NEWS & OBSERVER, Oct. 8, 2002, at B5.

14. See Katharine Mieszkowski, *Political Spam: Get Used To It*, SALON.COM (Nov. 20, 2002), at http://archive.salon.com/tech/feature/2002/11/20/political_spam/index.html.

15. *Debate on Campaign E-mail Pits Political Speech vs. Spam*, WASH. INTERNET DAILY, Apr. 9, 2002, at Vol. 3, No. 68 [hereinafter *Debate on Campaign E-mail*].

16. *Id.*

17. Wylie, *supra* note 7.

18. Nissenbaum, *supra* note 5.

and the contractor it hired used techniques relied on by large-scale commercial spammers to avoid retaliation and complaints, such as forged headers and false return addresses.¹⁹ Also, the website address provided in the spam linked to a website hosted in Spain—not to Jones’s campaign website—and some of the spam apparently was routed through two unknown Korean schools in order to circumvent common spam filters.²⁰ Moreover, the contractor used “harvesting” techniques to find e-mail addresses.²¹ The 2003 California gubernatorial recall election also prompted widespread use of political spam by various candidates and their supporters. In addition, many e-mails selling products unrelated to the election included phrases such as “Arnold for Governor” or “Terminator for Governor” in their subject lines.²²

The 2004 presidential election prompted additional incidents of political spam. Joseph Lieberman’s campaign acknowledged that it spammed prospective voters, even though the senator was an early, vocal opponent of spam and was one of the original sponsors of the CAN-SPAM Act.²³ Even Howard Dean’s campaign, widely viewed as one of the most savvy about Internet-based campaigning,²⁴ acknowledged that it had e-mailed unsolicited political advertisements to an undisclosed number of people.²⁵ In response to extensive criticism, the campaign pledged not to use political spam again.²⁶ Overall, it has been estimated that registered voters will

19. Wylie, *supra* note 7.

20. *Id.*

21. *Id.* In the report accompanying the CAN-SPAM Act, “harvesting” was described as “obtaining consumers’ e-mail addresses [by] captur[ing] them from websites where users post their addresses in order to communicate with other users of the website. This practice . . . is often done by automated software robots that scour the Internet looking for and recording posted e-mail addresses.” S. REP. NO. 108-102 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2350, 2003 WL 21680759.

22. Tim Lemke, *How Spammers Exploit the News*, WASH. TIMES, Oct. 14, 2003, at A1.

23. Declan McCullagh, *Dean Campaign Says It Spammed*, CNET.COM (Aug. 18, 2003), at http://news.com.com/Dean+campaign+says+it+spammed/2100-1028_3-5065141.htm. At the press conference to unveil the CAN-SPAM bill, Senator Lieberman stated, “After all is said and done, spam is not kosher.” David McGuire, *Six Sanguine Senators Slam Spam*, NEWSBYTES, May 11, 2000.

24. *See, e.g.*, Jeanne Cummings, *The E-Team: Behind Dean Surge: A Gang of Bloggers and Webmasters*, WALL ST. J., Oct. 14, 2003, at A1; Josh Getlin, *Web-Savvy Staff Helps Dean Weave His Way Up*, L.A. TIMES, Sept. 24, 2003, at A10.

25. McCullagh, *supra* note 23.

26. *Id.* The Dean campaign blamed the spamming on two contractors, who it claimed had promised to send the advertisements only to those who had specifically requested them. *Id.*

have received more than 1.25 billion pieces of political spam by the end of the 2004 election.²⁷

These examples of political spam—occurring in races from coast to coast and in campaigns for positions ranging from the most junior local office to the presidency—demonstrate the extent of the political spam problem.

B. Reasons for the Political Spam Problem and Why Voluntary Measures Are Not Effective

The widespread use of political spam can be attributed to the same factors driving its use for commercial purposes: its cost relative to other forms of advertising, its efficiency and ease of use, and the increasing numbers of regular e-mail users. Compared to television or radio advertisements, direct mail, telemarketing, or blast faxing, political spam is a very cheap way to reach voters. The production costs for a piece of unsolicited political e-mail are significantly less than those for a television or radio advertisement or a piece of direct mail, as are the costs of distribution. Another reason that spam is cheaper than other forms of communication is its ease of distribution. Whereas a telemarketing call or blast fax requires a phone line for each communication, millions of e-mails can be sent at once over a single Internet connection.²⁸ Furthermore, unlike other forms of political communication, a campaign can often engage in political spam completely in-house, without turning to outside contractors. As a result, it is unsurprising that many of the campaigns that used political spam cited its low cost and ease of distribution as key motivations for its use.²⁹ Finally, with more and more people using e-mail, its attractiveness as a tool for political advertising or solicitation increases.³⁰

27. Jeffrey H. Birnbaum, *Consultants Deliver Politics To Voters' Inboxes, At a Price*, WASH. POST, Aug. 29, 2004, at A1.

28. David E. Sorkin, *Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991*, 45 BUFF. L. REV. 1001, 1012 (1997) [hereinafter Sorkin, *Unsolicited Commercial E-Mail*].

29. Nissenbaum, *supra* note 5 (citing an official for Bill Jones' gubernatorial campaign who said the cheapness and ease of distribution of political spam was an important reason they used it); Mieszkowski, *supra* note 14 ("Politicians appear to spam for the same reasons that hawkers of 'amazing love potion that works' do. It's a cost-effective way to get their message out.").

30. Mike McCurry and Larry Purpuro, former high-ranking Democratic and Republican staffers, respectively, discussed this dynamic when they stated, "[w]ith more than 60 percent of all potential voters in this country possessing e-mail accounts, it makes sense that political candidates use this medium." Mike McCurry & Larry Purpuro, *A Vote for Political Spam*, BOSTON GLOBE, Aug. 23, 2002, at A27.

Political spam resembles unsolicited commercial bulk e-mails in another way as well: self-help and self-regulatory measures are not sufficient to address the problem. In arguing against governmental regulation of spam in general and political spam in particular, critics often suggest that an easy self-help measure exists—the delete key. They claim that all it takes for a recipient to deal with the spam is to read the subject line and delete the e-mail if it is unwanted.³¹ However, frequently it is not that simple. Because of unclear or misleading subject headings, a recipient often must open and read an e-mail before she can tell if it is unsolicited bulk e-mail or a personal communication. For instance, a New York network management firm official received the infamous e-mail from the Democratic candidate for governor in Florida in 1998,³² which had the subject line, “A message from Governor Lawton Chiles.” The official, believing the e-mail related to work he had done for the Florida Internet Service Providers Association, opened it only to discover it was a bulk e-mail urging him to vote for the Democratic candidate in the upcoming Florida gubernatorial election.³³ This e-mail user’s experience exemplifies the problem facing political spam recipients—they often cannot identify unsolicited political bulk e-mail simply based on the subject line; instead, they have to spend much of their time reading through unsolicited messages in order to find personal or requested e-mails.

Critics of government regulation of unsolicited bulk e-mails (and specifically political spam) also assert that self-regulation is adequate to deal with the spam problem. They often cite opt-out measures that spammers voluntarily include in spam, such as the ability to reply to the sender with a request to not receive any further e-mails or links to a website that allow a user to unsubscribe, as examples of such self-regulation.³⁴ However, these measures are largely ineffective because spammers are often unresponsive to requests not to receive further unsolicited communication. Many spammers, including political spammers, use false return addresses—either “spoofs” of real addresses or entirely fictitious ones—which makes it impossible for recipients to contact spammers and request removal from their mailing lists.³⁵ Additionally, some spammers offer

31. *Id.* (“When a political candidate sends a voter an e-mail, that recipient can choose to delete the message without opening it . . .”).

32. Murphy & McDowell, *supra* note 9.

33. *Id.*

34. See e.g., Mark Sweet, *Political E-mail: Protected Speech or Unwelcome Spam?*, 2003 DUKE L. & TECH. REV. 1, 6 (2003).

35. S. REP. NO. 108-102 (2003), *reprinted in* 2004 U.S.C.C.A.N. 2348, 2350, 2003 WL 21680759.

links to websites that seem to allow a recipient to unsubscribe from the unsolicited e-mail list, but actually are inactive, unconnected to the spammer, or serve only to confirm to the spammer that the recipient possesses an active address for future spamming.³⁶ Bill Jones' gubernatorial campaign in California exemplified many of these problems.³⁷ Its spam employed forged headers and false return addresses. Also, its spam linked to a website hosted in Spain, not the Jones' campaign website. Thus, while it may seem that many spammers voluntarily provide recipients with the means to opt-out of future communication, these measures are often either fake or ineffective.

Even when spammers offer legitimate opt-out procedures, such measures are frequently futile because the spammers often do not share the addresses of those who wish to opt-out with affiliated organizations. This problem is particularly acute with political spam, in which contractors, political action committees, volunteer organizations, other entities connected to a campaign, and the campaign itself often do not share opt-out requests with each other. As a result, when an individual responds to an e-mail from someone affiliated with a campaign, such as the state party, and asks not to receive any future e-mails, she may believe that she has successfully opted-out of receiving any future e-mail from that particular campaign. However, she may, to her surprise and unhappiness, continue to receive e-mails from other organizations associated with the campaign or the campaign itself.³⁸ Thus, even functioning voluntary opt-out systems are ineffective if the information is not shared between coordinated organizations working on behalf of one candidate.

C. The Costs of Political Spam

Political spam increasingly contributes to the significant costs and burdens imposed by the explosion in unsolicited bulk e-mailing. As Congress noted in its report for the recent CAN-SPAM legislation, spam imposes numerous expenses on ISPs, consumers, and businesses, while cost-

36. *Id.*, reprinted in 2003 U.S.C.C.A.N. 2348, 2350-51, 2003 WL 21680759. Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 398 (2000) ("Responding to an advertisement confirms that one's address is valid, and often does nothing more than encourage the marketer to increase the number of messages. In fact, the addresses of those who request to be removed from a mailing list may simply be added to a database for sale to other spammers.")

37. See *supra* notes 17-21 and accompanying text.

38. For example, one contractor working for a campaign admitted that it did not pass on to the campaign complaints it received from recipients about getting unsolicited political e-mail. Murphy & McDowell, *supra* note 9.

ing senders virtually nothing.³⁹ In this sense, spam results in similar kinds of cost-shifting as other types of unsolicited communication, such as blast faxing. Spam dramatically increases costs for ISPs, who must enlarge capacity to deal with the volume of spam, pay for sophisticated filters and other technologies to reduce the influx of spam, and bear the costs of additional customer service personnel to handle subscriber complaints related to spam.⁴⁰ ISPs typically have passed on these costs to consumers and businesses.⁴¹ Congress cited one report finding that spam costs Internet subscribers worldwide \$9.4 billion each year and another that estimated fighting spam adds an average of \$2 per month to an individual's Internet costs.⁴²

Spam exacts a particularly heavy price from consumers in rural areas, business travelers, and others who must pay per-minute access fees or long-distance charges to access the Internet. These consumers incur significant costs from the time spent having to sort through and delete spam in order to access their desired e-mail.⁴³ As one frustrated e-mailer stated, "I cannot afford to subscribe to unlimited online time and instead chose the more economical 5 hours per month for a nominal annual fee. About 3 of those hours per month are spent deleting unsolicited junk e-mail."⁴⁴

Unsolicited bulk e-mail also imposes considerable costs on businesses. According to a Ferris Research report, the cost of spam to businesses in terms of lost productivity, upgrading infrastructure, unrecoverable data, and increased personnel costs will exceed \$10 billion in 2003.⁴⁵ Of that total figure, the report estimates productivity losses resulting from sifting through and deleting spam alone amount to almost \$4 billion. These expenses represent a 300 percent increase from two years ago.⁴⁶ As dis-

39. S. REP. NO. 108-102, *reprinted in* 2003 U.S.C.C.A.N. 2348, 2352-53, 2003 WL 21680759.

40. *Id.*

41. *Id.*

42. *Id.*

43. *Id.*

44. FALLOWS, *supra* note 2, at 16.

45. S. REP. NO. 108-102, *reprinted in* 2003 U.S.C.C.A.N. 2348, 2353, 2003 WL 21680759.

46. *Id.* First-person accounts collected by the Telecommunications Research and Action Center, which are included in the Pew Internet and American Life Project, also highlight the cost of spam to businesses. One small business owner stated, "Our business spends about 1 hour per day erasing spam messages. At \$10 per hour (it costs more than that) the annual cost is \$2500 per year. That is not insignificant for a very small business." FALLOWS, *supra* note 2, at 20. An IT consultant who is frequently employed by businesses to implement spam protection measures gave some sense of the cost for larger businesses. He stated,

cussed above, political spam is becoming more widespread, and therefore increasingly contributes to these financial costs. Mitigating the economic burdens of spam thus demands addressing not only the explosion of commercial spam, but the growth of political spam as well.

Furthermore, spam inflicts major non-financial costs as well. It threatens the continued viability of e-mail as a means of communication. The glut of spam, and the fact that it represents an increasing percentage of total e-mail, causes some people to reduce or eliminate e-mail use.⁴⁷ According to a recent study by the Pew Internet and American Life Project, twenty-five percent of e-mailers have reduced their overall use of e-mail because of spam, for most to a significant extent.⁴⁸ Commentators also have noted this dynamic. For instance, one writes, “[f]ew people have the time or inclination to sort through hundreds of spam messages to find the one e-mail that is not marketing discount Viagra or a Russian wife. As a result, some people are abandoning e-mail and returning to conventional mail and telephone communications.”⁴⁹ This trend could be particularly dangerous in the political arena, as recent campaigns have demonstrated that legitimate uses of solicited e-mail are increasingly valuable.⁵⁰ The advantages of using e-mail in politics could be lost if people decrease their e-mail use.⁵¹ Spam also poses technical dangers to the electronic infrastruc-

“A tremendous amount of money is spent both in paying for my services, as well as equipment costs. Considering that the design and implementation of such a system is likely to be a minimum of four weeks of work (~\$5000/week), and require two moderate powerful servers (~\$4000/each), that is a cost of \$28,000.”

Id. at 22.

47. Turley, *supra* note 4.

48. FALLOWS, *supra* note 2, at i. A researcher at the Telecommunications Research and Action Center elaborated on this problem: “The ever-increasing flood of spam is causing consumers to turn away from e-mail as a means of communication Many people we hear from are contemplating getting off the Internet altogether.” Katie Hafner, *A Change of Habits To Elude Spam’s Pall*, N.Y. TIMES, Oct. 23, 2003, at G1 (quoting John Breyault). The *Times* article highlighted an example of this dynamic, Daleena Garrelts, who “has not abandoned the Web, but she has curtailed her use of e-mail. These days, [she] . . . is far more willing to give out her cellphone number than her e-mail address.” *Id.* Ms. Garrelts said this represented a dramatic shift in her behavior from even just two years ago, when she would have freely given out her e-mail address but hesitated to give out her cellphone number. *Id.* Now, she “discourages people from sending me general e-mail these days.” *Id.*

49. Turley, *supra* note 4.

50. See *infra* Section V.

51. As the chairman of the FTC recently stated, “Spam is threatening to destroy the benefits of e-mail.” Shelley Emling, *Anti-Spam Sentiment Sweeps Congress*, ATLANTA J. CONST., May 1, 2003, at 1C. Similarly, the director of the FTC’s Bureau of Consumer

ture, as it is often a key avenue through which viruses are spread.⁵² For instance, Senator Lieberman's presidential campaign sent spam that inadvertently contained a virus.⁵³

In addition, unsolicited bulk e-mail constitutes a particularly invasive form of communication that impinges upon people's right to privacy. Unsolicited bulk e-mail often invades people's home, where many people check their e-mail. Individuals usually cannot avoid spam simply by deleting messages based on the subject line. Spammers often employ misleading or unclear subject lines, such as "Re: Hi" or "Re: Your order," which force recipients to read through an e-mail before they recognize it is unsolicited. By the time readers realize a message is unwanted or objectionable, it is too late—they have already been forcibly exposed to the contents of the message. As a result, e-mail recipients cannot simply avert their eyes, which the Supreme Court has stated is adequate protection in the context of direct mail.⁵⁴ Rather, spam more closely resembles television, radio advertisements, or telemarketing calls, in which an individual must view or hear the objectionable content before she has an opportunity to avoid it (by changing the channel or hanging up the phone).⁵⁵ In fact, the Pew Internet and American Life Project study discovered that e-mail

Protection testified before Congress, "E-mail provides enormous benefits to consumers and businesses as a communication tool. The increasing volume of spam to ISPs, to businesses, and to consumers, coupled with the widespread use of spam as a means to perpetrate fraud and deception, put these benefits at serious risk." *Legislative Efforts to Combat Spam: Joint Hearing Before the Subcomm. on Commerce, Trade, and Consumer Prot. and the Subcomm. on Telecomm. and the Internet of the House Comm. on Energy and Commerce*, 108th Cong. (2003) (statement of J. Howard Beales III, Director, Bureau of Consumer Protection, Federal Trade Commission).

52. S. REP. NO. 108-102 (2003), *reprinted in* 2003 U.S.C.C.A.N. 2348, 2352, 2003 WL 21680759.

53. Sonia Arrison, *You've Got Spam*, L.A. TIMES, July 8, 2002, at 11.

54. *Consol. Edison Co. v. Pub. Serv. Comm'n*, 447 U.S. 530, 542 (1980).

55. The Court spoke to this issue in its discussion of offensive material sent through other media in the *Pacifica* case:

Patently offensive, indecent material presented over the airwaves confronts the citizen, not only in public, but also in the privacy of the home, where the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder To say that one may avoid further offense by turning off the radio when he hears indecent language is like saying that the remedy for an assault is to run away after the first blow. One may hang up on an indecent phone call, but that option does not give the caller a constitutional immunity or avoid a harm that has already taken place.

FCC v. Pacifica Found., 438 U.S. 726, 748 (1978).

users find spam to be as intrusive as telemarketing calls and much more intrusive than door-to-door solicitations or junk “snail” mail.⁵⁶

Although unsolicited commercial e-mail currently constitutes the majority of spam, political spam is becoming increasingly prevalent. According to Brightmail, which tracks spam, while politically-oriented spam accounted for only one-quarter of one percent of total spam in 2001,⁵⁷ it now accounts for two percent of all spam.⁵⁸ This figure promises only to grow as campaigns increasingly look to Internet-based communications as a key tool,⁵⁹ and the problem will be further exacerbated if political spam is one of the few categories of spam that remains unregulated.

III. POTENTIAL REMEDIES: MECHANISMS FOR REGULATION

As the previous Part demonstrates, political spam presents many of the same problems as unsolicited commercial e-mails, and it, like commercial spam, cannot be addressed adequately with voluntary measures. These parallels suggest another similarity between the two types of unsolicited e-mail: various proposed mechanisms for dealing with commercial spam could be applied effectively to the problem of political spam.

Commentators and policymakers have suggested a range of potential legislative solutions to address the problem of unsolicited commercial bulk e-mail, and states and the federal government have enacted some of these measures. Congress, for instance, recently passed the CAN-SPAM Act, which is specifically limited to commercial spam.⁶⁰ Among its various regulatory provisions, the law prohibits the transmission of commercial e-mail containing deceptive subject headings⁶¹ or false or misleading information in its header.⁶² It further requires commercial e-mail to have a functioning return address or other comparable mechanism that allows a

56. FALLOWS, *supra* note 2, at 27.

57. Wylie, *supra* note 21.

58. Spam Statistics, Brightmail, at <http://web.archive.org/web/20040201223519/http://www.brightmail.com/spamstats.html> (last visited Dec. 20, 2004). On June 21, 2004, Brightmail, Inc. was acquired by Symantec Corp. Brightmail Acquired by Symantec, at <http://brightmail.com> (last visited Dec. 20, 2004).

59. The example of the Howard Dean campaign’s successful use of e-mail, in particular, will likely fuel an increase in the use of political spam.

60. CAN-SPAM Act of 2003, 15 U.S.C. §§ 7701-7713. The Act defines “commercial electronic mail message” as “any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.” *Id.* § 7702(2)(A).

61. *Id.* § 7704(a)(2).

62. *Id.* § 7704(a)(1).

recipient to opt-out of future messages from that sender.⁶³ Once a recipient has opted-out, the transmission of any additional e-mails by that sender is prohibited.⁶⁴ The CAN-SPAM Act also calls on the Federal Trade Commission (FTC) to report to Congress, within six months after the law's enactment, on how a "Do-Not-E-Mail" registry could be established and on possible concerns with creating such a registry.⁶⁵ Within 18 months of CAN-SPAM's enactment, the agency must also report on a plan for identifying commercial spam by its subject line, such as with an "ADV" identifier.⁶⁶

This Part's discussion draws on some of the more promising features of the CAN-SPAM Act, as well as useful state regulatory mechanisms and other proposed measures, and analyzes how they could be successfully extended to political spam, particularly as part of a comprehensive regulation of all unsolicited bulk e-mail.⁶⁷ Using the analysis in this Part, as well as an examination of relevant constitutional and policy issues, this Article proposes a model federal statute to regulate all forms of unsolicited bulk e-mail, including political spam.⁶⁸ Because it can implement uniform national rules, a federal statute is the best legal means to address the problem of unsolicited bulk e-mail. However, it is worth noting that poorly crafted federal legislation can be less effective than better-designed, albeit piecemeal, state legislation. In fact, the CAN-SPAM legislation preempted many state measures that contained more desirable provisions for the regulation of unsolicited bulk e-mails.⁶⁹ As a result, the best solution is not *any*

63. *Id.* § 7704(a)(3).

64. *Id.* § 7704(a)(4).

65. *Id.* § 7708(a).

66. *Id.* § 7710 (2). The characters "ADV" are an abbreviation of "advertisement."

67. Numerous technical solutions to the issue of commercial spam have also been proposed. The "e-stamp" represents one such proposal. Under one type of this "micropayment" system, companies could create a system that allowed senders to attach e-cash to an e-mail. A user could put those whose e-mails she wants to receive, such as friends and family, on a personal do-not-charge list. For everyone else, the system would be configured to reject any messages that did not include a certain fee, such as 25 cents. If, after the e-mail from the unknown party was received the user decided she wanted to communicate with that person, she could place that person on the do-not-charge list and return the money. *See* Arrison, *supra* note 53; *see also* Lawrence Lessig & Paul Resnick, *Zoning Speech on the Internet: A Legal and Technical Model*, 98 MICH. L. REV. 395, 428-29 (1999); Sorkin, *Unsolicited Commercial E-Mail*, *supra* note 28, at 1030-31. While these technical solutions may have some promise, numerous obstacles to their implementation exist. Nonetheless, these issues are beyond the scope of this Article, which is focused on legislative solutions to the problems of political spam.

68. *See infra* Section VI.

69. *See, e.g.,* Tamara Loomis, *Effect of New Anti-Spam Statute Is Uncertain*, N.Y. L.J., Dec. 29, 2003, at 1 ("Opponents counter that the law is more lenient than many of

federal statute, but rather one that implements the most effective means for regulating spam.

A. Opt-in Systems

An opt-in system constitutes one proposal for dealing with commercial spam that can be applied to its political counterpart. Under an opt-in system, specified entities cannot contact an individual unless the individual has requested such contact. This type of system prohibits even initial contact if the recipient has not permitted such contact to be made. Opt-in proposals vary on what constitutes permission. The most rigorous require that a potential recipient give specific assent to receiving a specific communication. Less stringent forms of opt-in systems infer permission from established relationships. For example, if an individual previously bought an item from a retailer or previously contacted an advertiser, those actions can be considered constructive permission to be sent what would otherwise be classified as unsolicited communication. Therefore, opt-in systems place a premium on affirmative consent *prior* to the occurrence of communication.

Rules governing unsolicited messages sent via another type of communication—faxes—demonstrate an existing opt-in system. Under the Federal Communications Commission (FCC) facsimile rules, promulgated pursuant to the Telephone Consumer Protection Act of 1991 (TCPA), unsolicited commercial faxes can only be sent to those individuals who have given prior consent.⁷⁰ The previous version of the rules assumed that those with whom the sender had an “established business relationship” had provided constructive consent. In July 2003, however, the FCC issued new rules that eliminated this provision and required senders to secure all recipients’ express written permission before sending unsolicited faxes.⁷¹ The new rules represent one of the stricter varieties of opt-in systems.

the state statutes it is designed to preempt, and will permit spam previously banned by those laws. At least 34 states have passed anti-spam laws, several of which are much tougher than the new federal law.”).

70. See 1992 TCPA Order, 7 F.C.C.R. 8752, 8779, ¶ 54 n.87.

71. *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, FCC 03-153, Report and Order (rel. July 3, 2003), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-153A1.doc. The FCC delayed implementation of these guidelines until January 1, 2005, to permit those sending fax advertisements to secure the permission of recipients and to allow the FCC to consider any petitions for reconsideration. *Id.*, Order on Reconsideration (rel. Aug. 18, 2003), http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-208A1.doc. These guidelines apply to political solicitations.

The European Union has adopted a less strict opt-in policy for e-mail, which became effective on October 31, 2003.⁷² Under this system, an individual must give prior affirmative consent to receiving an e-mail before the e-mail can be sent. The rules make exceptions when a prior customer relationship exists, but require that an opt-out option be provided in those cases.⁷³

As applied to political spam, an opt-in system could take various forms. A strict version would prohibit any campaign or affiliate from sending e-mail to any individual unless that individual specifically requested such communication before it was sent. Under this type of opt-in system, even if a person had previously requested communication from the state Republican Party, for instance, a Republican candidate for governor could not send her any e-mail unless she gave prior permission to that candidate's specific campaign. A less-restrictive system would allow a campaign or affiliate to send e-mail to those individuals with whom it had an "established relationship." Thus, in the previous hypothetical, an individual's contact with a gubernatorial candidate's state party could constitute constructive permission to receive e-mails from that candidate. Of course, the breadth of this exception would depend on how broadly one defines "established relationship"—it could range from previous contact with a particular candidate in the context of another campaign or her official duties to previous contact with a candidate's political party.

B. Opt-out Systems

Another method for regulating unsolicited bulk e-mail is opt-out systems. Unlike opt-in systems, these presume consent to receiving unsolicited e-mail unless a recipient indicates otherwise. Such systems take two primary forms—one allows for opting-out of receiving unsolicited e-mail on a case-by-case basis and the other allows for opting out of all, or all of a certain type of, unsolicited e-mail.⁷⁴ In a case-by-case system, senders are required to provide a means for the recipient of an unsolicited e-mail to indicate that she does not want to receive any further communication from that particular sender. Depending on the rules, this can mean either having a valid return address to which a recipient can reply in order to un-

72. See Privacy and Electronic Communications Directive, Council Directive 2002/58, 2002 O.J. (L201) 37-47, http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf. European Union directives, such as this one, establish broad policy, but each EU member country must enact its own laws on how to implement the policy.

73. *Id.*

74. Fisher, *supra* note 36, at 411-12.

subscribe from future mailings, providing a link to a website to unsubscribe, or including instructions about alternate means of unsubscribing. Some opt-out systems require senders to provide a non-e-mail method for recipients to opt-out, such as a toll-free number.⁷⁵ The new federal law, for example, requires commercial spam to contain a valid return address, opt-out instructions, and a sender's physical address.⁷⁶ Before the federal law largely preempted the state measures, some states, including California, Delaware, and Tennessee, also required senders to honor the recipient's opt-out request.⁷⁷

In a comprehensive opt-out system, there is a central list to which individuals can subscribe in order to indicate they do not want to receive *any* unsolicited e-mail. Once a certain period of time passes after a person has submitted her e-mail address to a central "do-not-spam" list, no unsolicited e-mail can be sent to that individual without penalty. All senders of unsolicited advertisements must check their intended recipients against this list before sending their message. The Do-Not-Call registry serves as an example of this type of opt-out system. Individuals can submit their phone numbers to the Do-Not-Call registry either over the phone or through a website. Beginning no more than three months after a number is submitted to the registry, no telemarketer can call that number without incurring penalties.⁷⁸ This form of an opt-out system eases the burden on the recipient because she only has to act once to stop the transmission of all unsolicited communication of a certain type (that is, telemarketing calls or spam) instead of individually responding to each instance of communication she receives. These opt-out systems are often limited to certain types of a particular unsolicited communication. The Do-Not-Call registry, for instance, exempts political and charitable solicitations from its rules.⁷⁹

An opt-out procedure applied to political spam could assume different permutations. In a case-by-case model, all unsolicited e-mail, including

75. David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 374 (2001) [hereinafter Sorkin, *Technical and Legal Approaches*].

76. 15 U.S.C. § 7704(a).

77. Fisher, *supra* note 36, at 404, citing CAL. BUS. & PROF. CODE § 17538.4(c) (West 2000); DEL. CODE ANN. tit. 11, § 938(a) (2004); TENN. CODE ANN. § 47-18-2501(c) (2004); see also COLO. REV. STAT. § 6-2.5-103(1) to -103(3) (2000); IOWA CODE § 714E.1(2)(d) (2003); ME. REV. STAT. ANN. tit. 10, § 1497(2) (West 2003) for other examples of state laws enacted prior to CAN-SPAM.

78. Telemarketing Sales Rule, 16 C.F.R. § 310.4(b)(3)(iv) (2003). A revision to the statute that became effective on January 1, 2005, will decrease this time frame to 31 days.

79. See Don Oldenburg, *Do Not Call: A Simple Idea Gets Complicated*, WASH. POST, Aug. 5, 2003, at C9.

politically oriented e-mail, could be required to provide a valid return address that recipients could use to opt out of further communication or to include instructions on how one could unsubscribe from future mailings. As part of a comprehensive opt-out mechanism, the FTC also could create a "Do-Not-Spam" registry that political spammers, as well as commercial spammers, would have to respect. Both of these opt-out approaches differ substantially from opt-in systems in that they allow a sender to make the initial contact without permission from the recipient (as long as the potential recipient has not preemptively requested to not be contacted).

C. Labeling Systems

Labeling is a third method for regulating unsolicited commercial e-mail that could be applied to political spam. Under a labeling system, senders of unsolicited e-mail are required to include a predetermined label, such as "ADV", in the subject line of the message. The label is often required to be the first characters in the subject line. One variation on this system is to require a special label, such as "ADV:ADLT" for unsolicited e-mails that advertise or promote adult content. Both Maine and Tennessee required that an "ADV:" label appear at the beginning of the subject line of unsolicited commercial e-mail and "ADV:ADLT" appear at the beginning of unsolicited commercial e-mail advertising materials that only adults could legally view or purchase.⁸⁰ This labeling performs two functions. First, it allows recipients to identify an e-mail as an unsolicited advertisement without having to open the message and read it. Second, it facilitates filtering by individuals or ISPs.⁸¹

A labeling requirement applied to political spam could take two forms. As part of a general labeling requirement, senders of political spam could be required to place "ADV:" at the beginning of the subject line of any unsolicited bulk e-mail. Alternatively, they could be required to include "ADV:POL" at the beginning of any unsolicited political bulk e-mail. This type of labeling would assist people in differentiating political spam from commercial spam. Those who wanted to receive political spam but not commercial spam would be able to readily distinguish between the two when reading e-mail subject lines or when setting filters. On the other hand, those who did not want to receive any spam could just as easily de-

80. See, e.g., ME. REV. STAT. ANN. tit. 10, § 1497(A) (West 2003); TENN. CODE ANN. § 47-18-2501(e) (Supp. 2003). These state laws requiring labeling have likely been preempted by the CAN-SPAM Act. 15 U.S.C. § 7707(b)(1) (preempting any state law that expressly regulates the use of e-mail to send commercial messages except to the extent it prohibits false or deceptive practices).

81. Sorkin, *Technical and Legal Approaches*, *supra* note 75, at 376-77.

lete messages labeled “ADV:” or “ADV:POL” or set their filter to delete both types of messages.

IV. CONSTITUTIONAL ISSUES: CAN POLITICAL SPAM BE REGULATED?

In addition to the conviction that politicians do not or would not use it, one of the primary barriers to the regulation of political spam has been the belief that it is constitutionally protected and thus immune from regulation.⁸² While it is undoubtedly true that political speech receives greater protection than commercial speech, political speech is not beyond the reach of all regulation. The Supreme Court has frequently recognized the right of the government to regulate political speech as part of content-neutral measures.⁸³ Furthermore, the Court has often deferred to Congress’s judgment about the necessity of specifically regulating political speech for the achievement of important goals.⁸⁴ “Political speech” is not a talismanic label that renders whatever it includes immune from regulation. This Part will demonstrate that although political spam contains political speech, it can be regulated without violating the Constitution.

In order to do so, this Part reviews five areas of constitutional concern related to the regulation of political spam as part of a general scheme to regulate all unsolicited bulk e-mail: (1) the constitutionality of content-neutral regulations of political speech; (2) the constitutionality of regulating the flow of information to certain recipients; (3) whether e-mail inboxes are public fora that spammers have a constitutional right to access; (4) whether political spammers can be constitutionally required to label

82. The main sponsor of the CAN-SPAM Act in the House stated, “[T]he real reason we do not address political speech [in the spam laws] is because we want to make sure this law stands up to any court challenge.” Congressman Gary Miller, *How to Can Spam: Legislating Unsolicited Commercial E-mail*, 2 VAND. J. ENT. L. & PRAC. 127, 130 (2000). Senator Schumer also suggested that First Amendment concerns explain, at least in part, the reason political spam was not included in the recent spam legislation. *Senator Charles Schumer of New York and Roberta Combs, president of the Christian Coalition, Discuss Their Proposed Bill on Capitol Hill That Would Place Limits on Unsolicited E-mail*, CNBC, July 9, 2003, LEXIS, Nexis library, CNBC News Transcript.

83. See, e.g., *Ward v. Rock Against Racism*, 491 U.S. 781 (1989); *Frisby v. Schultz*, 487 U.S. 474 (1988); *Lehman v. City of Shaker Heights*, 418 U.S. 298 (1974); see also *City of Cincinnati v. Discovery Network, Inc.*, 507 U.S. 410, 428 (1993) (“[A] prohibition against the use of sound trucks emitting ‘loud and raucous’ noise in residential neighborhoods is permissible if it applies equally to music, political speech, and advertising.”).

84. See, e.g., *McConnell v. FEC*, 540 U.S. 93 (2003) (upholding most parts of the Bipartisan Campaign Reform Act).

their messages; and (5) whether regulation of political spam violates individuals' rights to engage in anonymous political speech. Within each of these areas, this Article argues that the proposed regulations of political spam would survive constitutional scrutiny, and thus, the Constitution should not be considered a roadblock to the regulation of political spam.

A. Content-Neutral Regulations of Political Speech

Legislation that regulates political spam as part of a general regulation of unsolicited bulk e-mail likely would survive constitutional scrutiny as a content-neutral restriction on the time, place, and manner of protected speech. Restrictions on the time, place, and manner of speech, including political speech, have long been held valid by the Supreme Court so long as they are content-neutral⁸⁵ and promote a "substantial government[al] interest that would be achieved less effectively absent the regulation."⁸⁶ This Section discusses the Court's standards for identifying and evaluating content-neutral laws and applies these principles to the proposed measures for regulating political spam.

Over the years, the Supreme Court has offered a framework for determining whether a law qualifies as a constitutional content-neutral regulation. The Court has stated that, the "principal inquiry . . . is whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys."⁸⁷ The Court has further explained, "[a]s a general rule, laws that by their terms distinguish favored speech from disfavored speech on the basis of the ideas or views expressed are content based."⁸⁸

Under *United States v. O'Brien*, a content-neutral regulation of protected speech will be subjected to intermediate scrutiny.⁸⁹ The Court in *Turner Broadcasting Systems, Inc. v. FCC* ("*Turner II*") described the *O'Brien* test as follows: "A content-neutral regulation will be sustained under the First Amendment if it advances important governmental interests unrelated to the suppression of free speech and does not burden sub-

85. See, e.g., *Discovery Network*, 507 U.S. at 428 ("The Court has held that government may impose reasonable restrictions on the time, place, or manner of engaging in protected speech provided that they are adequately justified without reference to the content of the regulated speech.") (internal quotation marks omitted).

86. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 662 (1994) [hereinafter *Turner I*] (quoting *Ward*, 491 U.S. at 799).

87. *Ward*, 491 U.S. at 791.

88. *Turner I*, 512 U.S. at 643.

89. *United States v. O'Brien*, 391 U.S. 367, 377 (1968); see also *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 189 (1997) {hereinafter *Turner II*} (noting that *O'Brien* enunciated the intermediate scrutiny standard for content-neutral regulations).

stantially more speech than necessary to further those interests.”⁹⁰ A content-neutral regulation does not demand the same tight fit between the regulation and its purpose that is required of a content-based regulation. As the Court stated, “[u]nder intermediate scrutiny, the Government may employ the means of its choosing ‘so long as the . . . regulation promotes a substantial governmental interest that would be achieved less effectively absent the regulation,’”⁹¹ The Court has also stated repeatedly that this “reasonable fit” requirement for a content-neutral regulation does not demand the government use the least-restrictive alternative.⁹²

Under these standards, the Court has upheld numerous laws and regulations that have impacted people’s ability to engage in protected speech on the grounds that the measures were content-neutral. For instance, in *Heffron v. International Society for Krishna Consciousness, Inc.*, the Court upheld state fair regulations limiting the distribution or sale of any merchandise, including printed or written material, even though it impinged on ISKCON’s ability to distribute religious literature.⁹³ In its ruling, the Court noted that although the regulation limited ISKCON’s ability to engage in religious speech, the purpose of the regulation was not intended to and did not specifically target protected speech. Instead it “applie[d] evenhandedly to all who wish[ed] to distribute and sell written materials or to solicit funds.”⁹⁴ Similarly, the Court in another case upheld a ban on the use of sound trucks that emitted loud noises on public streets despite the effects of such regulation on highly protected speech.⁹⁵

The Court’s jurisprudence on content-neutral time, place, and manner restrictions indicates that many of the spam-regulating mechanisms discussed above could be extended to include political spam without constitutional difficulty. As the following discussion will demonstrate, the purpose of regulating all unsolicited bulk e-mail stems from a desire to limit not the content of their messages, but their negative effects. The government possesses a substantial interest in regulating unsolicited bulk e-mail to ad-

90. *Turner II*, 520 U.S. at 189.

91. *Id.* at 213-14 (quoting *Turner I*, 512 U.S. at 662).

92. *Turner II*, 520 U.S. at 217. (“This less-restrictive-alternative analysis . . . has never been a part of the inquiry into the validity of content-neutral regulations on speech.”) (internal citations omitted); see also *Ward*, 491 U.S. at 800; *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 299 (1984).

93. 452 U.S. 640 (1981). Religious speech, like political speech, is highly protected under the First Amendment.

94. *Id.* at 649.

95. *Kovacs v. Cooper*, 336 U.S. 77 (1949) (upholding a regulation that prohibited appellant from using his sound truck to comment on a pending labor dispute).

dress these effects, and any of the mechanisms discussed above would reasonably fit the furtherance of this interest.

1. Content-Neutral Regulations

First, a general regulation of unsolicited bulk e-mails that includes political spam would not be based on the content of the message, a key element for determining whether a measure constitutes a content-neutral regulation. Congress' reasons for regulating unsolicited bulk e-mail, including political spam, would have nothing to do with the content of the e-mails or the views they express. The adoption of an opt-in, opt-out, or labeling system for all unsolicited bulk e-mail would not be related to the content of the political spam nor would it be an attempt to disfavor the specific political views expressed in any message or political views in general relative to other kinds of speech. Rather, the rationale for such measures would be to address the problems posed by any unsolicited bulk e-mail, including its cost-shifting and privacy-violating effects as well as its impact on business productivity and e-mail use in general. The regulations would apply equally to all unsolicited bulk e-mail, regardless of the content of the message or the viewpoint of the spammers. Consequently, the Supreme Court would likely find the government's interest in a regulation of all unsolicited bulk e-mail, including political spam, to be unrelated to the suppression of protected speech.

2. Substantial Interest

Second, Congress's interests in regulating political spam as part of a general regulation of unsolicited e-mail would be sufficiently substantial to pass constitutional muster. As discussed in Part II.C, spam imposes a number of costs—both financial and otherwise—on individuals (at home and work), on businesses, and on the electronic infrastructure. These significant costs, including cost shifting from senders to recipients, the threat it poses to the viability of e-mail as a communication medium, its impact on privacy rights, and its harm to the productivity of businesses, belie the claim of critics of spam regulation that the most effective means of dealing with spam is the “delete key.” The ever escalating amount of spam in general, political spam's increasing role in fueling that growth, and the large costs it imposes on consumers, business, and ISPs demonstrate that the scope of the problem is too large to be dealt with solely by individual action. This indicates that Congress has substantial interests in regulating unsolicited bulk e-mails.

Courts have already recognized these interests as important in related cases dealing with similar forms of unsolicited communication sent via

other media. In cases challenging the constitutionality of regulations of unsolicited faxes, courts have recognized the substantiality of Congress's interest in preventing cost-shifting between senders and recipients of unsolicited advertisements.⁹⁶ For example, the Eighth Circuit ruled on a case challenging the constitutionality of the opt-in system for unsolicited fax communications and determined that the government asserted a substantial interest in "restricting unsolicited fax advertisements in order to prevent the cost shifting and interference [that] such unwanted advertising places on the recipient."⁹⁷ In other challenges to the regulations of unsolicited faxes, various district courts found the government's interest in preventing cost shifting to be substantial as well.⁹⁸

Courts have also recognized that the government's interest in protecting individuals' privacy rights, particularly in the home, justifies regulation of unsolicited communication. For instance, in a challenge to the constitutionality of the Do-Not-Call registry, the Tenth Circuit recognized Congress's declared interest in protecting privacy in the home as sufficiently substantial to justify that legislation.⁹⁹ In other types of cases, the Supreme Court has recognized that the government's interest in protecting residential privacy is substantial. It has stated, "[t]he State's interest in protecting the well-being, tranquility, and privacy of the home is certainly of the highest order in a free and civilized society . . . a special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions."¹⁰⁰ In addition, in a

96. See, e.g., *Missouri v. Am. Blast Fax, Inc.*, 323 F.3d 649, 655 (8th Cir. 2003).

97. *Id.* at 655.

98. See *Texas v. Am. Blast Fax, Inc.*, 121 F. Supp. 2d 1085, 1092 (W.D. Tex. 2000); *Destination Ventures v. FCC*, 844 F. Supp. 632, 635-37 (D. Or. 1993). In their appeal of the latter, the plaintiffs stipulated that the government's interest in preventing cost shifting was substantial, 46 F.3d 54, 56 (9th Cir. 1995), as did the plaintiffs in *Kenro, Inc. v. Fax Daily*, 962 F. Supp. 1162, 1167 (S.D. Ind. 1997).

99. *FTC v. Mainstream Mktg. Servs., Inc.*, 345 F.3d 850, 854-55 (10th Cir. 2003) (recognizing "protecting privacy" as one of the "substantial government interests" justifying the regulation), *cert. denied*, No. 03-1552, 73 U.S.L.W. 3206 (U.S. Oct. 4, 2004).

100. *Frisby v. Schultz*, 487 U.S. 474, 484-85 (1988) (internal quotation marks omitted); see also *Watchtower Bible & Tract Soc'y of N.Y. v. Vill. of Stratton*, 536 U.S. 150, 164-65 (2002) (stating that residents' privacy is an "important interest [] that the Village may seek to safeguard through some form of regulation"); *Rowan v. U.S. Post Office Dep't*, 397 U.S. 728, 737 (1970) (upholding a statute that allowed an individual to request the Postmaster General to direct a particular sender to cease sending that individual any further mail and stating that "[t]he ancient concept that 'a man's home is his castle' into which 'not even the king may enter' has lost none of its vitality, and none of the recognized exceptions includes any right to communicate offensively with another").

case dealing with the regulation of the use of automatic dialing-announcing devices, the Eighth Circuit recognized as significant the government's interest in protecting the efficient operation and productivity of businesses.¹⁰¹

As a result, whether it is to prevent cost shifting, defend privacy in the home, or facilitate the productivity of businesses, Congress could articulate a sufficiently substantial interest to satisfy that prong of the test for determining the constitutionality of a content-neutral regulation of protected speech.

3. *Reasonable Fit*

Finally, a general regulation of all unsolicited bulk e-mail would also satisfy the "reasonable fit" requirement for content-neutral restrictions of protected expression. As the Court has stated, "[u]nder intermediate scrutiny, the Government may employ the means of its choosing 'so long as the . . . regulation promotes a substantial governmental interest that would be achieved less effectively absent the regulation,' and does not 'burden substantially more speech than is necessary to further' that interest."¹⁰² An opt-in, opt-out, or labeling system, each of which facilitates Congress's goals without impeding the use of bulk e-mail between interested and willing parties, likely would be found to meet this standard for content-neutral regulations. A clear nexus exists between any of the regulatory mechanisms and the government's interests. Moreover, as the earlier discussion of the problems associated with spam demonstrates, these substantial governmental interests would not be achieved as effectively without legislation enacting any of the proposed systems.

Courts' treatment of restrictions on other forms of unsolicited communication indicate the likelihood that the proposed spam regulation would be found to "reasonably fit" the government's interest. Circuit courts have already upheld against "fit" challenges existing opt-in requirements for unsolicited faxing and opt-out requirements for telemarketing calls.¹⁰³ Although courts performed this analysis under the *Central Hudson* standards

101. *Van Bergen v. Minnesota*, 59 F.3d 1541, 1554 (8th Cir. 1995).

102. *Turner II*, 520 U.S. 180, 213 (1997) (quoting *Turner I*, 512 U.S. 622, 662 (1994)).

103. *See, e.g.*, *FTC v. Mainstream Mktg. Servs.*, 345 F.3d 850 (10th Cir. 2003) (telemarketing calls); *Missouri v. Am. Blast Fax, Inc.*, 323 F.3d 649 (8th Cir. 2003) (blast faxes); *Destination Ventures, Inc. v. FCC*, 46 F.3d 54 (9th Cir. 1995) (same); *see also infra* Part IV.A.4 (discussing a particularly relevant Eighth Circuit case, *Van Bergen*, that examined the regulation of a type of unsolicited communication used for political purposes).

for commercial speech,¹⁰⁴ their reasoning is still useful for analyzing the validity of content-neutral restrictions. As the Court noted in *Board of Trustees v. Fox*, “the application of the *Central Hudson* test [for the constitutionality of commercial speech] was ‘substantially similar’ to the application of the test for validity of time, place, and manner restrictions upon protected speech.”¹⁰⁵

Furthermore, the criteria used by the Supreme Court to determine whether a restriction on protected speech “reasonably fits” the government’s interest in other types of cases also indicate that any of the proposed spam regulations would satisfy this requirement. For instance, the Court has held that empowering an individual to decide whether she wanted to receive unsolicited communication, instead of banning it altogether, was an important element in determining that a law regulating speech “reasonably fit” the government’s stated interest.¹⁰⁶ All of the proposed regulations of unsolicited bulk e-mails rely on individual choice, not a government-imposed total ban, to determine the messages that are cut off. Even the most restrictive mechanism, an opt-in system without a constructive assent exception, does not ban all bulk e-mails.¹⁰⁷ Instead, it allows senders to transmit bulk e-mails to those who desire to receive such communication, and thus is unlikely to be found to burden substantially more speech than is necessary to further the asserted governmental interests.

104. See *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 563 (1980) (noting that commercial speech receives less constitutional protection than other types of protected expression, such as political speech).

105. 492 U.S. 469, 477 (1989); see also *Van Bergen*, 59 F.3d at 1553 n.11 (“The intermediate level of scrutiny applied in *Ward* and *Clark* also closely resembles the test applied to regulations that restrict solely commercial speech.”).

106. See *Rowan v. United States Post Office Dep’t*, 397 U.S. 728, 736-37 (1970) (emphasizing the importance of the law giving individuals, and not the government, the power to decide they do not want to receive information from certain senders); *Mainstream Mktg. Servs.*, 345 F.3d at 860 (“We find it relevant that the national do-not-call list is of an opt-in nature, which provides an element of private choice and thus weighs in favor of a reasonable fit.”); see also *United States v. Playboy Entm’t Group, Inc.*, 529 U.S. 803, 815 (2000) (noting that recipient-initiated “targeted blocking enables the Government to support parental authority without affecting the First Amendment interests of speakers and willing listeners” and that “[t]argeted blocking is less restrictive than banning, and the Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests”).

107. As a result, it avoids the concern expressed by the Court, in *City of Ladue v. Gilleo*, with “laws that foreclose an entire medium of expression.” 512 U.S. 43, 55 (1994).

In addition, any of the proposed mechanisms for spam would “leave open ample alternative channels for communication,”¹⁰⁸ another important factor in evaluating content-neutral regulations of protected speech. Under any of the proposed regulations, bulk e-mailers, including political spammers, would still be able to use direct mail, television or radio advertisements, billboards, leafleting, and door-to-door canvassing, among other means, to engage in information distribution, solicitation, or other functions of unsolicited bulk e-mail. As a result, these factors also indicate that the general spam regulations would be considered “reasonably fit” to achieving the government’s interests.

The Court’s jurisprudence in this area demonstrates that a challenge to the general spam regulations as not being the least-restrictive available alternative would not be successful. The Court has repeatedly noted that the “fit” requirement for a content-neutral regulation does not demand that the government use the least-restrictive alternative. In *Turner II*, for example, the Court stated, “This less-restrictive-alternative analysis . . . has never been a part of the inquiry into the validity of content-neutral regulations on speech.”¹⁰⁹ No matter whether Congress chooses the opt-in, opt-out, or labeling method, or some combination thereof, instead of some plausibly less restrictive means such as private filtering, its decision would not render the regulation unconstitutional. Any of these methods would still be reasonably related to the achievement of its goals and would meet the relatively permissive “fit” standard demanded by the test for content-neutral restrictions.

Moreover, by including political spam as part of a general regulation of unsolicited communication, the constitutionality of the law actually would be strengthened against a “fit”-related challenge. Many of the existing regulations of unsolicited communication, including the Do-Not-Call registry and the blast-faxing rules, have been challenged on “fit” grounds because they do not apply to unsolicited political communication, which the parties claim equally contributes to the problems cited by Congress as the rationale for regulating commercial communications.¹¹⁰ Many of these

108. *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984).

109. *Turner II*, 520 U.S. 180, 218 (1997) (internal citations omitted); *see also* *Ward v. Rock Against Racism*, 491 U.S. 781, 800 (1989); *Clark*, 468 U.S. at 299.

110. *See, e.g., Destination Ventures v. FCC*, 46 F.3d 54, 56 (9th Cir. 1995) (“Destination argues that the FCC failed to sustain its burden of demonstrating a ‘reasonable fit’ between this interest and the ban on fax advertisements. Specifically, it contends that the government has not shown that faxes containing advertising are any more costly to consumers than other unsolicited faxes such as those containing political . . . messages.”).

challenges cite *City of Cincinnati v. Discovery Network, Inc.*¹¹¹ for the proposition that the government cannot single out commercial speech for regulation when other, noncommercial types of speech equally contribute to the problems that the government cites as the rationale for restricting commercial speech.¹¹² Although the laws have survived these challenges, the addition of political spam to regulation of other unsolicited bulk e-mails would bolster such a regulation against attacks on its constitutionality.¹¹³ Thus, whether the regulation employs an opt-in, opt-out, or labeling system, it is likely to meet the “reasonable fit” standard for content-neutral regulation of protected speech.

4. *Van Bergen v. Minnesota*

The constitutionality of including political spam in a general spam regulation finds particular support in a Eighth Circuit case, *Van Bergen v. Minnesota*.¹¹⁴ This case concerned a gubernatorial candidate’s use of a machine that automatically dialed home telephone numbers and played a campaign-related recorded message. The court upheld a Minnesota law that regulated all uses of such a device as a valid content-neutral time, place, or manner restriction of speech, even as applied to the gubernatorial candidate’s use in a campaign context.¹¹⁵ In its decision, the court found that the government had a significant interest in protecting residential privacy, which justified the law.¹¹⁶ This case strongly indicates that the regulation of political spam as part of a general spam regulation likely would survive constitutional scrutiny.

111. 507 U.S. 410 (1993).

112. See, e.g., *Missouri v. Am. Blast Fax, Inc.*, 323 F.3d 649, 655 (8th Cir. 2003) (“[The defendant] contends that this case is just like *City of Cincinnati v. Discovery Network, Inc.*”); *Destination Ventures*, 46 F.3d at 56.

113. It is important to note that the failure to include unsolicited charitable e-mails would mean general spam regulation remained underinclusive. While unsolicited charitable e-mails should also be included as part of a general ban on spam, any discussion on this point is beyond the scope of this Article. Furthermore, the failure to include charitable spam, even in a general measure to regulate spam, would not undermine the regulation. Courts have been willing to uphold regulations of other specific types of unsolicited communication despite the fact the regulations do not include all forms of unsolicited communication. As the Eighth Circuit noted in one of the blast-faxing cases, “Congress is not required to ‘make progress on every front before it can make progress on any front.’” *Am. Blast Fax*, 323 F.3d at 658 (quoting *United States v. Edge Broad. Co.*, 509 U.S. 418, 434 (1993)).

114. 59 F.3d 1541, 1546 (8th Cir. 1995).

115. *Id.* at 1551.

116. *Id.* at 1554-55.

Some have suggested this case is not relevant to regulation of political spam because telephone calls are more invasive than e-mail.¹¹⁷ One critic argued that on e-mail “the recipient has an opportunity to screen any message she receives by merely pressing ‘Delete,’ without reading more than the author’s name and message title.”¹¹⁸ However, the suggestion that spam is less invasive than a telemarketing call or other forms of unsolicited communication is incorrect. As described above, spammers often use false or misleading return addresses and subject lines, which force recipients to open and read a message to determine whether it is spam. By the time they have done so, they have been assaulted by the spam’s message. Furthermore, the overwhelming volume of spam indicates its invasiveness. Spam now accounts for almost 50 percent of all e-mail traffic.¹¹⁹ As a result, individuals must spend a significant amount of time sifting through spam in order to locate legitimate e-mails. The relevance of the quantity of unsolicited communication to the government’s interest in regulating it was recognized by the *Van Bergen* court, which noted that the volume of telemarketing calls bolstered the government’s interest in protecting privacy.¹²⁰ Thus, the suggestion that spam is not invasive because one can simply delete it without reading it reflects a naïve view of the practices of spammers and the sheer amount of spam individuals receive.

Others suggest that the logic of *Van Bergen* should not be applied to political spam because recipients of spam have a better ability to respond to that form of unsolicited communication than those who receive a prerecorded telephone call. Some claim that a political spam recipient can easily send an “unsubscribe” message to the sender or otherwise opt-out of future communications.¹²¹ This, too, reflects an unrealistic view of how spammers currently operate. Many use false return addresses or provide no opt-out options at all, which prevents recipients from being able to con-

117. See Sweet, *supra* note 34, at 5.

118. *Id.* at 6.

119. S. REP. NO. 108-102 (2003), *reprinted in* 2003 U.S.C.C.A.N. 2348, 2349, 2003 WL 21680759.

120. *Van Bergen*, 59 F.3d 1541 at 1555 (“The sheer quantity of telemarketing calls further supports the government’s interest in regulation protecting privacy.”). In its opinion, the *Van Bergen* court referenced the Supreme Court’s decision in *Breard v. Alexandria*, 341 U.S. 622 (1951), upholding a regulation that allowed door-to-door commercial solicitation only if the resident had given her prior consent. In *Breard*, the Court cited the growth in door-to-door solicitation as a reason for its decision. It stated, “Door-to-door canvassing has flourished increasingly in recent years with the ready market furnished by the rapid concentration of housing. The infrequent and still welcome solicitor to the rural home became to some a recurring nuisance in towns when the visits were multiplied.” 341 U.S. at 626.

121. Sweet, *supra* note 34, at 6.

tact them and unsubscribe from future unsolicited e-mails.¹²² In reality, recipients of spam, like recipients of prerecorded telephone messages, often lack a means to respond to the unsolicited communication. Consequently, the *Van Bergen* case offers a valuable precedent for the constitutionality of regulating political spam as part of a general regulation of unsolicited bulk e-mails.

A general regulation of unsolicited bulk e-mails which includes political spam, is likely to be upheld under the Court's jurisprudence on content-neutral restrictions of protected speech. The government can assert multiple interests for the legislation, which would likely be considered substantial. These interests would be unrelated to the suppression of speech or the targeting of particular views. Moreover, the scope of the legislation, under any of the discussed systems, would meet the "fit" requirements.

B. The Government's Ability to Regulate the Flow of Information

Limitations on unsolicited bulk e-mail that include political spam would also survive a challenge based on the constitutionality of the government regulating the flow of information to certain recipients. The Court has specifically empowered the federal government to facilitate a mailing recipient's wish to not receive any messages from designated senders. In *Rowan v. U.S. Post Office Department*, the Supreme Court upheld a federal statute that allowed a resident to contact mailers, through an order of the Postmaster General, and compel them to not send any more mailings to the resident.¹²³ The Court's decision offers language particularly relevant to the proposed general regulation of all types of spam:

In effect, Congress has erected a wall—or more accurately permits a citizen to erect a wall—that no advertiser may penetrate without his acquiescence. The continuing operative effect of a mailing ban once imposed presents no constitutional obstacles

. . . If this prohibition operates to impede the flow of even valid ideas, the answer is that no one has a right to press even 'good' ideas on an unwilling recipient The asserted right of a mailer . . . stops at the outer boundary of every person's domain.¹²⁴

122. See *supra* note 35 and accompanying text.

123. 397 U.S. 728, 729-31 (1970).

124. *Id.* at 738.

This case strongly indicates that the federal government may, without constitutional difficulty, assist individuals in preventing messages they do not wish to receive, such as spam, from reaching them in their homes.

Spam advocates may challenge this point by citing two cases that seem to restrict the government's ability to regulate the flow of information to certain recipients. However, these cases are easily distinguishable. In *Consolidated Edison Co. v. Public Service Commission*, the Court held that the Commission could not prohibit ConEd from including messages about controversial issues of public policy in their regular bills to customers.¹²⁵ The Court rejected the Commission's argument that concern for protecting clients' privacy justified the rule.¹²⁶ Similarly, in *Bolger v. Youngs Drug Products Corp.*, the Court invalidated a federal statute prohibiting the mailing of unsolicited advertisements for contraceptives on the grounds the First Amendment does not permit the government to ban the flow of certain messages because people may be offended by them.¹²⁷

A general regulation of unsolicited bulk e-mail including political spam can be readily differentiated from the regulations at issue in these cases. First, in both cases, the Court pointed to the ease with which an individual could avoid the unwanted communication as a reason the government should not be able to prohibit the intrusive speech. In *Consolidated Edison*, the Court wrote:

Where a single speaker communicates to many listeners, the First Amendment does not permit the government to prohibit speech as intrusive unless the 'captive' audience cannot avoid objectionable speech . . . customers who encounter an objectionable billing insert may 'effectively' avoid further bombardment of their sensibilities simply by averting their eyes.¹²⁸

Similarly, the Court declared in *Bolger*, "the short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned."¹²⁹ However, when it comes to spam, as described above, recipients cannot easily avoid the objectionable speech. In addition, unlike traditional bulk mail, which imposes some costs on the sender, unsolicited bulk e-mail essentially costs the senders nothing and, as a result, individuals receive significantly more unsolicited bulk e-mail, including political spam, than direct mail. Consequently, re-

125. 447 U.S. 530 (1980).

126. *Id.* at 541.

127. 463 U.S. 60 (1983).

128. *Consol. Edison*, 447 U.S. at 541-42.

129. *Bolger*, 463 U.S. at 72.

ipients must spend much of their time on e-mail sorting through unwanted, and often objectionable messages, just to find legitimate and desired communication. This heavy burden is readily distinguishable from the more negligible one imposed on recipients of unsolicited bulk regular mail.

Second, in both *Consolidated Edison* and *Bolger*, the Court expressed concern that the disputed regulation totally cut off the flow of certain communication.¹³⁰ None of the possible mechanisms discussed in this Article, however, completely bans spam. Under either the opt-in, opt-out, or labeling systems, entities can still send out spam. The restrictions only require that spammers, alternatively, send e-mail solely to those who give prior consent, provide the means for recipients to opt-out of further communication, or include an unobtrusive label on their messages that facilitates filtering. As a result, any of the spam regulations under consideration would not result in an outright ban on political or any other form of spam, and thus are not susceptible to either the *Consolidated Edison* or *Bolger* analysis.

Instead, the situation of e-mail users more closely resembles that of the bus riders in *Lehman v. City of Shaker Heights* or the homeowner in *Frisby v. Schultz*. In the former case, the Court upheld a city policy permitting the display of commercial but not more “controversial” political or public issue advertisements in the interior of city buses based on a captive-audience analysis.¹³¹ In the latter case, the Court upheld an ordinance that banned picketing in front of single residences, also based on a captive-audience rationale.¹³² The *Frisby* Court stated, in particularly relevant language, “we have repeatedly held that individuals are not required to welcome unwanted speech into their own homes and that the government may

130. *Id.* at 75 (stating “the justifications offered by appellants are insufficient to warrant the sweeping prohibition on the mailing of unsolicited contraceptive advertisements”); *Consol. Edison*, 447 U.S. at 541-44.

131. 418 U.S. 298, 302 (1974) (“The streetcar audience is a captive audience. It is there as a matter of necessity, not of choice.”) (internal quotation marks omitted).

132. 487 U.S. 474, 484-85 (1988). The *Frisby* Court stated:

Although in many locations, we expect individuals simply to avoid speech they do not want to hear . . . the home is different. That we are often “captives” outside the sanctuary of the home and subject to objectionable speech . . . does not mean we must be captives everywhere. Instead, a special benefit of the privacy all citizens enjoy within their own walls, which the State may legislate to protect, is an ability to avoid intrusions.

Id. (internal quotation marks and citation omitted).

protect this freedom.”¹³³ Similar to the bus riders in *Lehman* or the homeowner in *Frisby*, e-mail users are a captive audience because many must encounter the content of the unwanted messages at home when they check e-mail. One commentator has stated, in a more general discussion of Internet use, “arguably the Internet has more of the captive audience features of a bus. Like a bus, when one is surfing the Internet, he is typically online for a purpose other than viewing advertisements and, thus, may not be able to avoid unwanted Internet advertisements without curtailing his other activities.”¹³⁴

The degree of spam’s intrusiveness serves as another relevant consideration for determining which line of cases is most applicable to political spam. One of the differences between the *Consolidated Edison* and *Bolger* cases, on the one hand, and *Lehman* and *Frisby*, on the other, appears to be the degree of intrusiveness from the unwanted communication.¹³⁵ As discussed above, the techniques of spammers and the overwhelming volume of unsolicited bulk e-mail renders spam particular intrusive. In this respect, it is more equivalent to the bus advertisements or picketing in front of single residences than to direct mail. Thus, spam’s high level of intrusiveness indicates that the *Lehman* and *Frisby* cases offer more relevant precedent than *Consolidated Edison* or *Bolger*.

The criteria used by the Court to evaluate the constitutionality of government efforts to regulate the flow of information thus suggest that any of the mechanisms for regulating all unsolicited bulk e-mail—including political spam—would survive constitutional review. All of the proposed regulations facilitate individuals’ ability to control the flow of information they receive in their homes, and none effectuates a complete ban on e-mail communication. Furthermore, spam can be distinguished from regular mail because it is significantly harder to avoid and presents a greater intrusion. As a result, any limitations on the flow of information imposed by the regulatory mechanisms would likely be considered within the government’s constitutional authority.

133. *Id.* at 485.

134. Sharon K. Sandeen, *In For a Calf Is Not Always in For a Cow: An Analysis of the Constitutional Right of Anonymity as Applied to Anonymous E-Commerce*, 29 HASTINGS CONST. L.Q. 527, 568 (2002).

135. See Joshua A. Marcus, *Spam and the Internet*, 16 CARDOZO ARTS & ENT. L.J. 245, 300-01 (1998) (“*Lehman*, like *Frisby*, seems to involve a greater degree of intrusion than was present in *Consol. Edison* and *Bolger*.”)

C. Right to Access Inboxes as Public Fora

A related constitutional argument that may be lodged against the proposed regulations of all unsolicited bulk e-mail, including political spam, is that people's e-mail inboxes are public fora to which spammers have the right to access.¹³⁶ This objection seems unlikely to succeed. Although the Supreme Court has not ruled on whether e-mail inboxes are public fora, they have explicitly ruled that traditional mailboxes are not.¹³⁷ Similarly, a federal appeals court has ruled that the telephone system constitutes a private channel of communication.¹³⁸ These rulings suggest that e-mail inboxes are also unlikely to be considered public fora.¹³⁹ In fact, e-mail inboxes are even less likely to be considered public fora than traditional mailboxes because the former are neither owned nor approved by an entity of the U.S. government.¹⁴⁰ Nor do e-mail inboxes meet the criteria generally used by the courts for determining whether something is a traditional or designated public forum. E-mail inboxes have not traditionally been used for assembly and expression. Similar to the airport terminal in *International Society for Krishna Consciousness v. Lee*, e-mail inboxes have not existed long enough to have developed such a tradition.¹⁴¹ In addition, the policies of many ISPs to prohibit the distribution of unsolicited mass e-mail to their account holders indicate that e-mail inboxes have not been guided by a policy of being a public forum. Consequently, whether based on their parallels to traditional mailboxes or applying the requirements for

136. The classic definition of a public forum comes from *Hague v. Committee for Industrial Organization*, in which the Supreme Court described it as a location that has "immemorially been held in trust for the use of the public and, time out of mind, [has] been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions." 307 U.S. 496, 515 (1939). The Court has noted that in public fora, "the government's ability to permissibly restrict expressive conduct is very limited." *United States v. Grace*, 461 U.S. 171, 177 (1983).

137. *U.S. Postal Serv. v. Greenburgh Civic Ass'ns*, 453 U.S. 114 (1981).

138. *Van Bergen v. Minnesota*, 59 F.3d 1541, 1553 (8th Cir. 1995).

139. See R. Jonas Geissler, *Why Robert Redford May Call Your House to Get Your Vote, But He May Not Send You an E-mail*, 2001 J. ONLINE L., art. 8, para 17 (2001) ("The Court has ruled that conventional home mailboxes do not constitute public fora. By analogy, then, individual e-mail boxes are not public fora either.").

140. See, e.g., *Hudgens v. NLRB*, 424 U.S. 507, 520-21 (1976) (holding that the First Amendment does not create a right of access to private property for speech purposes).

141. See 505 U.S. 672, 681-83 (1992) (noting that airport terminals cannot be considered public fora because "given the lateness with which the modern air terminal has made its appearance, it hardly qualifies for the description of having 'immemorially . . . time out of mind' been held in the public trust and used for purposes of expressive activity").

public fora, e-mail inboxes are unlikely to be found to be public fora which spammers have the right to access.

D. Specific Labeling for Political Spam

Unlike the opt-in or opt-out regimes, which do not single out political spam but instead target all unsolicited bulk e-mails, some versions of the labeling regime—those which require that political spam be labeled “ADV:POL” instead of being labeled “ADV”—would regulate political spam specifically.¹⁴² Nonetheless, a political spam-specific labeling regime would also likely survive constitutional scrutiny. For many years, political communication has been subject to special disclosure and identification requirements, which are significantly more burdensome than the labeling system proposed here. Rules promulgated under the Federal Election Campaign Act (FECA) mandate that advertisements funded by independent expenditures that expressly advocate the election or defeat of clearly identified candidates include identification of who paid for the advertisement.¹⁴³ In the Bipartisan Campaign Reform Act (BCRA), which the Court recently upheld in the face of a vigorous challenge on First Amendment grounds,¹⁴⁴ Congress expanded the scope of FECA’s disclosure rules by implementing strict disclosure requirements for those who sponsor a broad category of advertisements known as “electioneering communication,” including so-called “issue advocacy” advertisements.¹⁴⁵

142. This system requires defining the “political” aspect of political spam in order to identify which messages require the specific “ADV:POL” label. One possibility would define political spam as “an e-mail message that refers to a clearly identified candidate for public office.” See *infra* notes 149-52 and accompanying text (suggesting possible definitions of the “unsolicited” and “bulk” aspects of the message).

143. See Communications Disclaimer Requirements, 60 Fed. Reg. 52,069 (Oct. 5, 1995) (describing the “paid for by” requirements implemented by the Federal Election Commission pursuant to FECA). The Federal Election Campaign Act originally required disclosure for any independent expenditure spent for “the purpose of . . . influencing” a nomination or election. The Court narrowed this provision to apply only to communications that “expressly advocate the election or defeat of a clearly identified candidate.” *Buckley v. Valeo*, 424 U.S. 1, 79-80 (1976).

144. *McConnell v. FEC*, 540 U.S. 93 (2003).

145. Bipartisan Campaign Reform Act of 2002, Pub. L. No. 107-155, § 201(a), 116 Stat. 81, 88-90 (codified at 2 U.S.C. § 434(f) (2000 & Supp. II 2002)). Under the new rules, non-corporate or non-union people or entities that spend more than \$10,000 on electioneering communication during a calendar year must file disclosure reports detailing those who made the disbursements, those who control the person or entity who made the disbursements, the custodians of the records, all contributors who gave more than \$1,000 to finance the communications, the recipients of disbursements of more than \$200, the elections to which the communications pertain, and the names of the candidates identified. *Id.*

As a result, under current rules, public political advertisements must clearly state who paid for the communication and whether a candidate authorized it. If the advertisement is not sanctioned by a candidate or an authorized political committee of a candidate, it must clearly state the name and permanent street address, telephone number, or web address of the person who paid for the communication.¹⁴⁶ BCRA also added the requirements that any advertisement paid for or authorized by the candidate must meet specific minimum standards to enhance the visibility of candidate identification.¹⁴⁷ Although the constitutionality of many sections of BCRA was litigated, critics of the law did not feel the identification aspects of it were susceptible to challenge.¹⁴⁸

The requirement that political spam include “ADV:POL” at the beginning of its subject lines is a significantly less onerous burden on political speech than the restrictions contained in either FECA or BCRA, which the Court upheld. First, senders of the political spam do not have to identify themselves; rather, they must only indicate that they are sending a bulk political advertisement with a minimally intrusive label. Second, requiring political spam to be labeled “ADV:POL” does not inhibit candidates, political organizations, affiliates, or interested third parties from engaging in political speech. While a concern could arise if ISPs install mechanisms that automatically filter out all messages labeled “ADV:POL” before they reach recipients, this potential issue could easily be addressed. The legislation requiring the “ADV:POL” label could include a provision that bans ISPs from automatically filtering “ADV:POL” labeled messages unless individual recipients specifically request such filtering. Although probably not constitutionally necessary, such a provision would ensure that individuals, not ISPs, ultimately decided whether to receive political spam. In fact, creating separate labels for political and other forms of spam could

146. 2 U.S.C. § 441d(a) (2000 & Supp. II 2002).

147. Under these rules, an advertisement paid for or authorized by a candidate must include a statement that identifies the candidate and states that she has approved of it. The statement must either be conveyed by a full-screen view of the candidate making the statement or a candidate voice-over accompanied by a clearly identifiable image of the candidate. The statement must also appear in writing in a “clearly readable manner with a reasonable degree of color contrast between the background and the printed statement, for a period of at least 4 seconds.” *Id.* § 441d (c), (d) (2000 & Supp. II 2002).

148. See Jim Rutenberg, *Fine Print Is Given Full Voice in Campaign Ads*, N.Y. TIMES, Nov. 8, 2003, at A1 (“Though the law is being challenged before the Supreme Court, the advertising regulation was not a target.”). Furthermore, the Court refused to invalidate on First Amendment grounds other significantly more speech-restrictive sections of BCRA, including the limits on “electioneering communications” by unions and corporations in the 30 days before a primary or 60 days before a general election. *McConnell*, 540 U.S. at 204-09.

facilitate political communication; individuals who wanted political, but not commercial spam, would not have to choose between filtering out both or neither type of spam as they would under a single “ADV” labeling system.

The “ADV:POL” requirement for political spam would be significantly less intrusive than existing, constitutionally permissible rules on identification and disclosure for political communications. In addition, it would not inhibit political speech. Thus, such a requirement is likely to survive constitutional scrutiny.¹⁴⁹

E. The Right to Engage in Anonymous Political Speech

Political spam regulations may also be challenged based on people’s rights to engage in anonymous political communication. Such a challenge would be without merit. The Supreme Court’s rulings on whether individuals enjoy a right to engage in anonymous speech have not always been consistent, although the Court has often protected the rights of individuals to remain anonymous when engaging in political speech.¹⁵⁰ However, these cases are irrelevant to any of the proposed spam regulations discussed above because none requires a sender to disclose her identity. One of the opt-out mechanisms proposed in this Article mandates that a sender include a valid return address, but it does not demand that the address identify the sender in any way. Similarly, opt-out proposals that require senders to provide a non-e-mail way to opt-out, such as through a telephone number or address, do not demand that the senders disclose their identities—senders can use a non-listed telephone number or a P.O. Box for their address. Under an opt-in system in which senders need to preemptively secure permission to contact someone, potential senders can use numerous mechanisms that do not reveal their identity, such as an anonymous website or a non-identity-revealing e-mail address, as a means to allow people to indicate their consent to be contacted. Furthermore, the labeling requirement does not demand a sender reveal her identity; it only requires that she indicate the e-mail she is sending is political spam. Thus,

149. A more general requirement that all unsolicited bulk e-mail, including political spam, contain the “ADV” label in their subject line likely would be upheld as a content-neutral time, place and manner restriction. *See supra* section IV.A.

150. *See, e.g.*, *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334 (1995) (striking down a statute that prohibited the distribution of anonymous campaign literature, but noting that mandated identification requirements are not impermissible in all circumstances); *Buckley v. Valeo*, 424 U.S. 1 (1976) (upholding the FECA disclosure requirements despite their effects on speakers’ anonymity); *Talley v. California*, 362 U.S. 60 (1960) (striking down an ordinance that prohibited the distribution of anonymous handbills).

none of the proposed regulations of political spam implicate the possible rights of individuals to engage in anonymous political speech.

Despite the beliefs of many policymakers, commentators, and others that regulation of political spam could not be constitutional, this review of the relevant issues demonstrates that the Constitution poses no barrier to the regulation of political spam as part of a general measure regulating all forms of unsolicited bulk e-mail.

V. POLICY ISSUES: SHOULD POLITICAL SPAM BE REGULATED?

In debating whether to regulate political spam, it is critical to distinguish the benefits of political *e-mail* from those of political *spam*. E-mail can play an important role in political campaigns,¹⁵¹ but the increasing use of political spam actually threatens the continued development of e-mail as an effective electoral tool. As a result, attempts to regulate spam, including through the proposed opt-in, opt-out, or labeling systems, seek to save rather than undermine e-mail as a viable campaign resource. This Part of the Article identifies and responds to common arguments made against regulating political spam in order to demonstrate the need for such regulation.

Proponents of political spam often argue that e-mail provides a low-cost way for campaigns to communicate with voters, which permits candidates with fewer resources to compete¹⁵² and provides campaigns with the opportunity to engage voters directly.¹⁵³ While it is undoubtedly true that e-mail can function as a low-cost and interactive means to communicate with voters, taking advantage of these features does not require using spam. The campaigns that have most successfully used e-mail have relied on *solicited* e-mail communication. Jesse Ventura, whose use of the Internet is viewed as a critical factor in his 1997 Minnesota gubernatorial victory,¹⁵⁴ relied exclusively on opt-in lists when e-mailing voters.¹⁵⁵ Howard

151. See, e.g., Seth Grossman, Note, *Creating Competitive and Informative Campaigns: A Comprehensive Approach to "Free Air Time" for Political Candidates*, 22 YALE L. & POL'Y REV. 351, 384-85 (2004).

152. McCurry & Purpuro, *supra* note 30 ("When a candidate lacks a large war chest, he or she can use the Internet to provide constituents with information to prepare them to perform their civic duty of casting educated votes.").

153. Sweet, *supra* note 34, at 8.

154. See, e.g., Greg Miller, *Web Helped the Decision Go To Jesse 'The Body' Ventura*, L.A. TIMES, Nov. 9, 1998, at C3.

155. Murphy & McDowell, *supra* note 9.

Dean, whose campaign attracted tremendous attention for its use of e-mail and other Internet-based forms of campaigning, also primarily sent e-mail only to those who requested such communication. In addition, both the Democratic and Republican National Committees only send e-mail to those who request it.¹⁵⁶ As a spokesman for the RNC stated, "it is counter-productive to send unsolicited mass e-mail; people view it as junk mail and [it] will turn off more voters than gain supporters."¹⁵⁷ A co-founder of Mindshare Internet Campaigns, which helps political candidates use the Internet, said of political spam, "[i]t's a bad way to campaign You annoy the very people you are trying to woo."¹⁵⁸ Unsurprisingly, those campaigns that have used unsolicited e-mail communication have been subjected to major criticism and backlash.¹⁵⁹ Thus, taking advantage of e-mail's price advantage over television, radio, or direct-mail advertising and its interactivity does not require using unsolicited bulk e-mail. Moreover, the hostility that comes from the use of political spam likely mitigates or eliminates any benefits it may offer.

Besides general apprehension with any regulation of political spam, its advocates are also concerned with specific proposed measures. For instance, they suggest that certain methods of regulation, such as a labeling system, could result in ISPs blocking all political spam before it reaches individuals, thus depriving citizens of the opportunity to decide for themselves whether they wish to receive it.¹⁶⁰ Although this potential problem does not raise a constitutional concern, it is a legitimate issue—but one that is easily addressed by a provision that prevents ISPs from automatically filtering political e-mails labeled as such and thus allows an individual to choose for herself whether to receive political spam, filter it on her own, or have the ISP block it.¹⁶¹

Political spam proponents also object to opt-in systems because they do not allow campaigns to make first contact with voters without their express permission. They claim that voters are often unaware of certain kinds of candidates, particularly challengers or those without the resources to promote themselves in other media, and thus voters do not know that

156. *Id.*

157. *Id.*

158. Nissenbaum, *supra* note 5.

159. *See supra* Part II.A.

160. *See, e.g.,* Larry Purpuro, *The Big Push: The Case for Political E-mailing*, CAMPAIGNS & ELECTIONS, Oct. 2002, at 47 ("A political candidate must have access to spreading a message through e-mail This freedom cannot be undermined by commercial ISPs that attempt to block these e-mails from ever being delivered to the voters.").

161. *See supra* Part IV.D.

there are candidates about whom they would want to receive more information.¹⁶² Without the ability to make an unsolicited first contact, voters may never learn about these candidates. While this issue is not of a constitutional dimension,¹⁶³ it is a valid concern that suggests an opt-in-only system may be too restrictive to be desirable as a policy alternative. Policy concerns thus dictate that a form of opt-out or labeling system, or some combination thereof, is the best means for addressing the problem of political spam and protecting e-mail as a tool in political campaigns.

VI. THE PROPOSAL: A LEGISLATIVE APPROACH TO REGULATING ALL SPAM

Political spam should not be considered beyond the reach of regulation, either for policy or constitutional reasons. Through its exemption of political spam, current federal law creates numerous problems that would be solved by an approach that encompasses all types of unsolicited bulk e-mail regardless of its content. The present federal law's focus only on unsolicited commercial e-mail ignores the increasing prevalence of political (and other forms) of unsolicited bulk e-mail and its contributions to the costs imposed by spam. Furthermore, a general regulation that includes all types of unsolicited bulk e-mail would better protect the viability of e-mail as a communication medium, which, while particularly valuable in the political context if used properly, is currently threatened. As a result, this Part offers a legislative proposal that would implement a general regulation of all unsolicited bulk e-mail.

The most important part of the legislation would be to define the e-mail subject to regulation as *all* unsolicited bulk e-mail. The new legislation would modify the definition contained in the CAN-SPAM Act by defining an "unsolicited message" as any message other than one "the recipient expressly consented to receive either in response to a clear and conspicuous request for such consent or at the recipient's own initiative."¹⁶⁴ Defining "bulk e-mail" is more challenging. Most agree that bulk e-mail should encompass identical or substantially similar messages sent to a large number of people within a certain period of time. The key areas of disagreement lie in what number of recipients and what timetable should serve as the threshold for determining bulk e-mail status. State laws provide relevant examples of the range of approaches. For instance, Idaho

162. See *Debate on Campaign E-Mail*, *supra* note 15.

163. As explained above, including political spam as part of an opt-in system applied to all unsolicited bulk e-mail would likely survive constitutional scrutiny.

164. See 15 U.S.C. § 7702(1)(A).

defines "bulk e-mail" as "an electronic message, containing the same or similar advertisement, which is contemporaneously transmitted to two (2) or more recipients, pursuant to an Internet or intranet computer network."¹⁶⁵ On the other hand, Louisiana defines bulk e-mail as "any electronic message which . . . is sent in the same or substantially similar form to more than one thousand recipients."¹⁶⁶ And Virginia offers a sliding scale of penalties based on different amounts and timetables of unsolicited bulk e-mailing.¹⁶⁷ A reasonable compromise among these various alternatives, which is neither too restrictive nor too permissive, would be to define bulk e-mail as identical or substantially similar messages sent to fifty or more recipients over a week.

Once unsolicited bulk e-mail is defined, the next challenge is determining the best mechanism for regulating it. Based on the problems posed by political spam, the constitutional issues, and policy considerations discussed in earlier sections, the ideal legislation would implement a regulatory system consisting of three parts. First, it would require all unsolicited commercial bulk e-mails to include "ADV" and all unsolicited political bulk e-mails to include "ADV:POL" at the beginning of their subject lines. Second, it would mandate that all senders of unsolicited bulk e-mail, including political spam, offer a valid return e-mail address as well as a working opt-out mechanism, and that they heed all opt-out requests. This section of the legislation would require that spammers share the opt-out requests with all their affiliates and marketing partners, who would also be required to respect these opt-out requests. Third, it would mandate the creation of a nationwide "do-not-spam" registry. Any individual who wished to send unsolicited bulk e-mail would first have to check whether any of the addresses on her list are on the registry and, if so, refrain from e-mailing those addresses.¹⁶⁸

165. IDAHO CODE § 48-603E (Michie 2003).

166. LA. REV. STAT. ANN. 14:73.1(13) (West Supp. 2000).

167. Under Virginia law, a person is guilty of a Class 6 felony if "[t]he volume of [unsolicited bulk e-mail] transmitted exceeded 10,000 attempted recipients in any 24-hour period, 100,000 attempted recipients in any 30-day time period, or one million attempted recipients in any one-year time period." VA. CODE ANN. § 18.2-152.3:1(B) (Michie 2003).

168. In order to deal with concerns that disreputable spammers would use the do-not-spam registry as a source for new recipients, the law could require the FTC to set up a remailer system. Under this type of system, senders of unsolicited bulk e-mail have to send their e-mail through a database that would remove anyone on the registry from the recipient list. As a result, the spammers themselves would never have access to the list of addresses. *See, e.g.,* Lessig & Resnick, *supra* note 67, at 427.

This suggested system offers numerous advantages. It in no way affects a campaign's ability to continue to send bulk e-mails to those who have requested them, which has proved to be the most effective type of political e-mailing. In addition, the use of an opt-out as opposed to an opt-in system allows unsolicited bulk e-mailers, including political spammers, to make initial contact with unaware but potentially willing recipients, while the requirement of a valid return address and a working opt-out mechanism ensures that those who do not want to continue to receive mailings beyond the first contact have an effective way to unsubscribe. Spammers would not be able to contact individuals who include themselves on the "do-not-spam" registry, but those individuals, by placing themselves on the registry, would be indicating they are not willing recipients of even an initial contact by a campaign. Furthermore, the labeling scheme would allow recipients to easily identify both commercial spam and political spam and facilitate filtering. If an individual wanted to receive political, but not other forms of spam, she could set her e-mail client to only filter out messages beginning with "ADV." On the other hand, those who do not want to receive any spam could set their filters to delete all e-mails starting with either "ADV" or "ADV:POL" or request their ISP to do so. As a result, this legislation, through the imposition of general regulation of unsolicited bulk e-mail and labeling requirements, preserves legitimate e-mailing as a tool for campaigns while addressing the problems of political spam.

Nonetheless, this model legislation clearly is not perfect. Setting a specific threshold for what constitutes bulk e-mail creates certain problems, including the possibility that spammers will adjust their volume or timing to meet the threshold.¹⁶⁹ Also, a certain proportion of spam is sent from overseas and thus remains largely beyond the reach of American law.¹⁷⁰ Despite these obstacles, legislation such as that proposed here is worthwhile. No legislation will be able to completely and perfectly eliminate the

169. See Sorkin, *Technical and Legal Approaches*, *supra* note 75, at 331 n.22. Sorkin noted that:

Among the arguments against a precise threshold are . . . spammers would respond to a clearly disclosed threshold by adjusting their message volume to accommodate it (for example, by sending one message fewer than the threshold within the specified time period) [and] the existence of a fixed threshold would encourage spammers to find ways to circumvent it (for example, by sending spam under different names, or by spreading their message traffic over a slightly longer time period) . . .

Id.

170. Miller, *supra* note 82, at 130-31.

problems posed by unsolicited bulk e-mails. However, a more comprehensive, general regulation of all forms of unsolicited bulk e-mail, including political spam, would better reduce and manage the occurrence of spam than the current focus on only commercial varieties. This would, in turn, reduce the heavy costs that spam in all its varieties imposes on consumers and businesses.¹⁷¹ Furthermore, whereas current legislation only addresses one type of spam that causes people to become frustrated with e-mail and reduce their use of it, the general regulation would cover many more types of spam that fuel this problem. Although not an ideal solution, the legislation proposed in this section goes much further toward dealing with the problems posed by spam than current statutes. As with so many problems that one seeks to address through legislation, one cannot allow the perfect to be the enemy of the good.

VII. CONCLUSION

For over ten years, people have believed that Internet-based communication would play a transformative role in political campaigns.¹⁷² Early indications of the potential impact of the Internet came with Jesse Ventura's victory in the Minnesota gubernatorial race in 1997; in 2004, Howard Dean's presidential campaign seemed to vindicate the promise of the Internet on a national scale. However, the growing use of Internet-based communication by candidates has a dark side: the escalating incidence of unsolicited political bulk e-mail. Despite the negative reaction its past use has consistently elicited, political candidates over the last five years have increasingly used unsolicited political bulk e-mails as part of their campaigns. They are turning to unsolicited bulk e-mail for the same reasons as commercial spammers—its low cost relative to other forms of communication, the ease with which it can be distributed, and the growing number of people who can be reached via e-mail. And, like commercial spam, political spam imposes numerous costs on the public—including on using the Internet, on individuals' privacy rights, on business productivity, and, not least of all, on people's confidence in e-mail itself—that are not readily susceptible to self-help solutions.

Despite these problems, policymakers have refrained from regulating political spam even as they have moved aggressively to address commercial spam. Some have attributed this failure to politicians' own self-

171. See Jerry Berman & Paula J. Bruening, *Can Spam Be Stopped?*, LEGAL TIMES, June 16, 2003, at 76.

172. See, e.g., Charles A. Radin, *MIT Plugs Citizens into President Race*, BOSTON GLOBE, Nov. 2, 1992, at 23.

interest. The politicians themselves, when they bother to explain this important policy choice at all, have alternatively clung to the clearly erroneous beliefs that political candidates do not spam, cited readily addressable constitutional concerns as complete barriers to regulation, or declared that protecting e-mail as a campaign tool requires they leave political spam untouched. Whatever the reason, the decision to not regulate political spam as part of a general regulation of *all* unsolicited bulk e-mail constitutes a serious mistake. By exempting political spam from regulation, current law fails to address a growing contributor to the costs of unsolicited e-mail. In enacting a comprehensive regulation of all spam, such as the one this Article suggests, Congress would more effectively address the problems posed by spam as a whole, while also protecting the effectiveness of e-mail as a communication tool among senders and willing recipients. The latter accomplishment would be particularly important to facilitating e-mail's continuing, and perhaps increasing, role in political campaigns. Only time will tell if e-mail will become a key force in reshaping how political campaigns are conducted. But we do not need to wait to understand the costs of not regulating political spam along with other unsolicited bulk e-mail.

