



UNC
SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 102 | Number 4

Article 6

5-1-2024

Political Spam: Why It Sucks and How to Fix It

Alex Slawson

Follow this and additional works at: <https://scholarship.law.unc.edu/nclr>



Part of the [Law Commons](#)

Recommended Citation

Alex Slawson, *Political Spam: Why It Sucks and How to Fix It*, 102 N.C. L. REV. 1223 (2024).

Available at: <https://scholarship.law.unc.edu/nclr/vol102/iss4/6>

This Comments is brought to you for free and open access by Carolina Law Scholarship Repository. It has been accepted for inclusion in North Carolina Law Review by an authorized editor of Carolina Law Scholarship Repository. For more information, please contact law_repository@unc.edu.

Political Spam: Why It Sucks and How To Fix It*

Email spam is more than just annoying. It is costly, both to the individual and to society. This Comment examines these costs through the lens of one type of spam: political fundraising emails. It also proposes two types of solutions. The first is “front-end” regulation, which could include a do-not-email registry or an outright ban on unsolicited bulk email. This type of regulation would address the spam problem by decreasing the overall amount. The second type of solution is “back-end” regulation, meaning subject-line labeling and a requirement that spammers stick to one sender name. This would tackle the problem by decreasing the costs of receiving each spam email. This Comment weighs the advantages and disadvantages of each approach, ultimately concluding that Congress should pursue back-end regulation first because it is more likely to survive First Amendment scrutiny.

INTRODUCTION.....	1224
I. THE PROBLEM.....	1226
A. <i>Staring Down the Barrel of the Spam Cannon</i>	1226
B. <i>Why Is There So Much Spam?</i>	1230
C. <i>Why Is There So Much Political Spam in Particular?</i>	1232
D. <i>What Makes Political Spam Costly to the Recipient?</i>	1239
II. SOLVING THE PROBLEM OF “WHO” AND “WHAT”	1241
A. <i>Front-End Regulation</i>	1241
B. <i>Back-End Regulation</i>	1245
C. <i>Constitutional Concerns with Back-End Regulation</i>	1247
D. <i>Nonconstitutional Concerns with Back-End Regulation</i>	1251
CONCLUSION	1252
APPENDIX A.....	1254

* © 2024 Alex Slawson.

INTRODUCTION

Every day, billions of spam emails traverse the internet—more than half of all email traffic.¹ These unwanted messages impose costs that far outweigh their benefit. While the cost of an individual email—usually just a few seconds of the recipient’s time—is low, the cost of spam in the aggregate is enormous. One article estimated that someone who receives about 100 emails a day can expect to spend about eighteen hours a year sorting through these unwanted messages.² Multiplied across the economy, the wasted time and other costs are significant: one 2012 analysis estimated that spam robbed the world of \$20 billion every year³—comparable to the gross domestic product of a small country⁴—and that estimate was based on a very narrow definition of spam.⁵ The real cost of spam, if defined as all unsolicited mass email, is likely much higher.⁶

1. The exact amount of spam sent each year varies widely. See Davey Winder, *This Surprisingly Simple Email Trick Will Stop Spam with One Click*, FORBES (May 3, 2020, 6:45 AM), <https://www.forbes.com/sites/daveywinder/2020/05/03/this-surprisingly-simple-email-trick-will-stop-spam-with-one-click/> [<https://perma.cc/TAK3-R7ZT> (dark archive)] (estimating the annual number of spam emails as 320 billion); Stacy Jo Dixon, *Average Daily Spam Volume Worldwide from October 2020 to September 2021*, STATISTA (June 26, 2023), <https://www.statista.com/statistics/1270424/daily-spam-volume-global/> [<https://perma.cc/CJJ6-J574>] (estimating the global volume of spam in July 2021 alone as 283 billion emails); see also JuiHsi Fu, PoChing Lin & SingLing Lee, *Detecting Spamming Activities in a Campus Network Using Incremental Learning*, 43 J. NETWORK & COMPUT. APPLICATIONS 56, 56 (2014) (“Around 90% of email messages are reportedly spam.”).

2. Sead Fadilpašić, *Spam Emails Are Wasting Hundreds of Work Hours Every Year*, TECHRADAR (June 1, 2022), <https://www.techradar.com/news/spam-emails-are-wasting-hundreds-of-work-hours-every-year> [<https://perma.cc/K4ZR-6EYR>].

3. Justin M. Rao & David H. Reiley, *The Economics of Spam*, 26 J. ECON. PERSPS. 87, 87–88 (2012). The cost largely comprises lost productivity.

4. Dino Grandoni, *Spam Costs You a Lot More than You'd Think*, HUFFPOST, https://www.huffpost.com/entry/cost-of-spam_n_1757726 [<https://perma.cc/U697-AVPU>] (last updated Aug. 16, 2012) (noting that, in 2012, the aggregate cost of spam was comparable to the total gross domestic product of Bolivia or Estonia).

5. See Rao & Reiley, *supra* note 3, at 96 (defining “spam” as “messages from economic agents who do not have a previous relationship with the customer and who do not offer opt-out provisions”). Though Rao and Reiley use a much narrower definition of spam than is used in this Comment, their analysis of the “market structure” of email spam is valuable no matter how spam is defined. See *id.* at 96–104.

6. There are many reasons why spam, defined broadly, likely costs more in 2022 than Rao and Reiley estimated it cost in 2012. Their estimate was based largely on average value of the recipient’s time multiplied by the average time it takes a recipient to deal with “spam”—defined narrowly—on a yearly basis. See *id.* at 99–100 (“Suppose, then, that the average value of a user’s time is \$25 per hour, and that each piece of spam takes an average of five seconds to deal with.”). Therefore, if they analyzed the problem again in 2022, accounting for the rise in worker productivity over the last ten years, and if they expanded their definition of spam to include many more messages, their estimate for the cost of spam would certainly be higher. In addition, there are several costs that Rao and Reiley did not include in their estimate: the costs of a “false positive,” meaning the cost of a legitimate, important message landing in the spam folder by mistake and the psychological cost of receiving annoying, offensive, or, in the worst cases, malicious messages. See *id.* at 98–100. These costs, had they been quantified, would have pushed the estimate higher.

In the fight against spam, recipients are largely on their own. While email providers are developing increasingly sophisticated spam filters, they are locked in a “cat-and-mouse game” against ever-more sophisticated spammers—a game they are unlikely to ever win.⁷ The federal government has, for the most part, stood idly by. Congress made one attempt to mitigate the problem with the CAN-SPAM Act of 2003, which requires that email marketers have an unsubscribe link in their emails and prohibits “materially misleading” headers, sender names, and subject lines, among other requirements.⁸ However, the law had little discernible effect on the overall volume and character of unsolicited email.⁹ Many states, to their credit, tried to solve the problem with strict antis spam laws,¹⁰ but they have now been hamstrung by the ineffective CAN-SPAM Act, which explicitly supersedes state law.¹¹

However, even if the CAN-SPAM Act were effective, it would suffer from one glaring deficiency: it does not address political spam.¹² The Act’s drafters were, apparently, wary of the First Amendment scrutiny they would attract if they applied the Act to political speech, so they chose to exclude it.¹³

7. *See id.* at 89–96.

8. *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) of 2003, Pub. L. 108-187, § 5, 117 Stat 2699, 2706–10 (codified as amended at 15 U.S.C. § 7704).

9. *See* John Soma, Patrick Singer & Jeffrey Hurd, *Spam Still Pays: The Failure of the CAN-SPAM Act of 2003 and Proposed Legal Solutions*, 45 HARV. J. ON LEGIS. 165, 165–66 (2008) (“[R]eports show that whereas the worldwide volume of spam in 2003 [before CAN-SPAM was implemented] was just over 50% of all e-mail, the worldwide average volume of spam in 2007 will fall somewhere between 60% and 90% of all e-mail.”).

10. Before the CAN-SPAM Act, many states had laws that were, at least in theory, much stricter on spam than is the CAN-SPAM Act. For example, many states required subject-line labeling, a regulation for which this Comment advocates. *See, e.g.*, TENN. CODE ANN. § 47-18-2501(e) (LEXIS through the 2023 First Extraordinary Sess.) (effective July 15, 1999); Unsolicited Sexually Explicit Email Act, ch. 229, § 3, 2002 Utah Laws 863, 863–64 (repealed 2004); ME. REV. STAT. tit. 10, § 1497 (Westlaw through the 2023 First Reg. and First Spec. Sess. of the 131st Leg.) (effective May 27, 2003); ARIZ. REV. STAT. ANN. § 44-1372.01 (Westlaw through legislation of the First Reg. Sess. of the Fifty-Sixth Leg.) (effective May 16, 2003); *see also infra* Section II.B. However, a majority of these state laws were not in effect for long before the CAN-SPAM Act preempted them, so it is difficult to judge their efficacy. DEBORAH PLATT MAJORAS, ORSON SWINDLE, THOMAS B. LEARY, PAMELA JONES HARBOUR & JON LEIBOWITZ, FED. TRADE COMM’N, SUBJECT LINE LABELING AS A WEAPON AGAINST SPAM: A CAN-SPAM ACT REPORT TO CONGRESS 3–4 (2005), <https://www.ftc.gov/sites/default/files/documents/reports/subject-line-labeling-weapon-against-spam-can-spam-report-congress/050616canspamrpt.pdf> [<https://perma.cc/J465-955Q>].

11. *See* 15 U.S.C. § 7707(b)(1) (“This chapter supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.”).

12. *See id.* §§ 7701–7713 (applying just to *commercial* email); *see also id.* § 7702(2)(A) (defining “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*”) (emphasis added).

13. *See* Seth Grossman, Note, *Keeping Unwanted Donkeys and Elephants Out of Your Inbox: The Case for Regulating Political Spam*, 19 BERKELEY TECH. L.J. 1533, 1551 n.82 (2004) (“The main sponsor of

Thus, even the modest improvements the Act did make¹⁴ (or would make if it were to be diligently enforced) apply only to commercial speech;¹⁵ the political fundraising industry has been left to regulate itself. As one might expect, the self-regulation has been less than draconian.¹⁶

This Comment examines the problem of unsolicited bulk email through the lens of one particular type: political fundraising messages. Part I analyzes why spam—particularly political spam—creates significant problems. Part II begins with one solution to those problems—“front-end” regulations—but concludes that such regulations have a high risk of being struck down by the courts. Part II then outlines two “back-end” regulations that might have better luck: (1) a requirement that all unsolicited mass emails include “ADV” (for “advertisement”) at the beginning of their subject lines, and (2) a requirement that every sender stick to one sender name that is substantially similar to the organization’s name of incorporation. By helping recipients quickly identify and filter out unwanted emails, these regulations would decrease the costs that spam imposes on the recipients. Additionally, because these policies are essentially disclosure requirements, as opposed to front-end limitations on the quantity of speech, they are more likely to survive First Amendment scrutiny.

I. THE PROBLEM

A. *Staring Down the Barrel of the Spam Cannon*

Imagine: It’s fall 2020, and you are a seventy-five-year-old retiree named Bill, browsing the Facebook account you created a few years earlier (with a little help from your children). At the time you made the account, you believed it would be a convenient way to keep track of faraway friends and family. Lately, however, you use it mostly to keep track of the news.

As you scroll, headlines catch your eye. Donald Trump is yelling about the “China Virus.”¹⁷ Donald Trump is accusing Democrats of trying to steal the

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.’ 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.” (alterations in original) (citation omitted)).

14. The CAN-SPAM Act prohibits, for example, subject lines that the sender knows are likely to mislead the recipient. Derek E. Bambauer, *Solving the Inbox Paradox: An Information-Based Policy Approach to Unsolicited E-mail Advertising*, 10 VA. J.L. & TECH. 1, 34 (2005). This provision would certainly help clean up the political email industry, which deploys all manner of misleading subject lines.

15. See 15 U.S.C. § 7707–7713.

16. See *infra* Sections I.C, I.D.

17. Maegan Vazquez & Betsy Klein, *Trump Again Defends Use of the Term ‘China Virus,’* CNN, <https://www.cnn.com/2020/03/17/politics/trump-china-coronavirus/index.html> [https://perma.cc/WQN5-7HEL] (last updated Mar. 19, 2020, 4:05 AM). The author does not condone referring to the COVID-19 virus in this way.

upcoming election.¹⁸ Donald Trump is praising Vladimir Putin.¹⁹ You shake your head. A little further down your feed, another post catches your eye: “Urgent Poll for Democrats: SHOULD DONALD TRUMP BE IMPEACHED?” Below is a digital clock counting down to midnight, followed by two large “YES” and “NO” buttons. You click yes. Immediately, you are routed to a new page, which prompts you to enter your email address and answer some questions that, allegedly, will “help set Democrats’ priorities for the rest of the year.”²⁰ You want to help out, so you enter your email and answer a few questions. However, when the last question asks you to donate, you decline. You live on a fixed income, and, in any case, your wallet is in another room.

A few days later, you get an email that alarms you. The sender’s name is “Urgent Update for Bill,” and the subject line is “Social Security Update.”²¹ You read the email and discover, with some relief—but with some annoyance as well—that your social security is not in jeopardy. Rather, the email informs you

18. Richard Cowan, *Trump Says He Will Score a “Big Win,” Accuses Democrats of Trying To Steal Election*, REUTERS, <https://www.reuters.com/article/idUSKBN27K0ME/> [<https://perma.cc/9HPG-PUCK> (staff-uploaded archive)] (last updated Nov. 4, 2020, 3:16 AM).

19. Joseph Gedeon, *Trump Calls Putin ‘Genius’ and ‘Savvy’ for Ukraine Invasion*, POLITICO (Feb. 23, 2022, 10:15 AM), <https://www.politico.com/news/2022/02/23/trump-putin-ukraine-invasion-00010923> [<https://perma.cc/VU3Z-MW3V> (staff-uploaded archive)].

20. This is an example of how political campaigns and committees typically “acquire” email addresses for their fundraising campaigns. Using Facebook’s algorithm, fundraisers “target” potential donors who match specific criteria. See Sara Morrison, *Why Are You Seeing This Digital Political Ad? No One Knows!*, VOX (Sept. 29, 2020, 8:50 AM), <https://www.vox.com/recode/2020/9/29/21439824/online-digital-political-ads-facebook-google> [<https://perma.cc/4GZM-ZS5N>]. By and large, the people targeted are older Americans who are less tech savvy. See Shane Goldmacher, *That ‘Team Beto’ Fund-Raising Email? It Might Not Be from Beto*, N.Y. TIMES, <https://www.nytimes.com/2021/11/26/us/politics/email-political-fundraising-pitches.html> [<https://perma.cc/5Y7G-3SHW> (dark archive)] (last updated June 22, 2023) [hereinafter Goldmacher, *Team Beto*].

21. Mass email blasts typically have an “open rate” of about 20%. See *What Are Good Open Rates, CTRs, & CTORs for Email Campaigns?*, CAMPAIGN MONITOR, <https://www.campaignmonitor.com/resources/knowledge-base/what-are-good-email-metrics/> [<https://perma.cc/Y9J4-Y5E7>]. However, because they are sent to hundreds of thousands, or even millions, pushing that open rate just a little higher can result in thousands more dollars raised. To accomplish this, fundraisers use misleading sender and subject lines they believe will entice more people to open. For example, the Democratic Congressional Campaign Committee (“DCCC”), traditionally one of the most aggressive online fundraising organizations, has sent emails under the name “SOCIAL SECURITY UPDATE (via DCCC).” See Shane Goldmacher, *How Deceptive Campaign Fund-Raising Ensnarers Older People*, N.Y. TIMES (June 26, 2021), <https://www.nytimes.com/2021/06/26/us/politics/recurring-donations-seniors.html> [<https://perma.cc/8KEU-Z44A> (staff-uploaded, dark archive)] [hereinafter Goldmacher, *Deceptive Campaign Fund-Raising*]. Another organization used “‘Your Order Confirmation’ as the sender and ‘Order ID: 73G526S’ as the subject line.” Goldmacher, *Team Beto*, *supra* note 20. It is also common for groups to impersonate other, more popular campaigns in hopes of siphoning off donations from the more popular candidate. For example, on the day Beto O’Rourke announced his campaign for governor of Texas, a group unaffiliated with O’Rourke’s campaign sent messages under the name “Beto O’Rourke Update.” See *id.*

(in a kaleidoscope of red font, flashing graphics, and yellow highlight) that Donald Trump wants to cut social security. At the bottom, the email says:

Figure 1.

We've commissioned this poll of top Democrats like you, Bill, but time is running out, and we still need 20 more responses from people in 27514.

Tell us before midnight: SHOULD SOCIAL SECURITY BE CUT?

Yes	No
-----	----

You're confused. How did they know your name and zip code? You're also concerned about the content of the email. After all, if social security payments are cut, you might have to sell the house. You decide to, as the email suggests, "make your voice heard" by clicking the big flashing NO button. Again, a survey pops up on your screen, followed by a donation page. This time, the donation page is for an organization you've heard of—a prominent committee supporting major candidates—and the donation pitch explicitly mentions protecting social security as a goal of the organization. This time, you decide to donate \$10. You do not notice a small blue checkbox and grey print that says, "Make this a weekly donation."

As November's election approaches, you receive more and more emails. Your inbox has grown so crowded that you sometimes spend thirty to forty-five minutes a day sorting through them.²² Some are from—or seem to be from—

22. Due to the donor-acquisition strategies of many political campaigns and committees, signing up for one email list often results in receiving emails from campaigns you did not sign up for. Campaigns and committees frequently "swap names," meaning they exchange a list of emails with another campaign or committee. See Simone Pathé, *Your Email Address Could Be Worth \$8 to a Political Campaign*, ROLL CALL (Apr. 11, 2019, 12:31 PM), <https://rollcall.com/2019/04/11/your-email-address-could-be-worth-8-to-a-political-campaign/> [<https://perma.cc/6EX7-D5JC>]. The email address, however, continues to receive emails from both lists. Some campaigns will even sell the names of their donors to other groups. See Shane Goldmacher, *Inside the 2016 Black Market for Donor Emails*, POLITICO (Dec. 15, 2015, 5:15 AM), <https://www.politico.com/story/2015/12/inside-the-2016-black-market-for-donor-emails-216761> [<https://perma.cc/KDB4-UDTS>] ("Scott Walker has begun selling access to his email list to pay off his leftover presidential debt, renting out the email addresses of hundreds of thousands of supporters to former rivals, including Marco Rubio, John Kasich, Ted Cruz and Ben Carson."). Some for-profit firms have made a business of buying and selling names. See *Reach Your Ideal Audience with a Targeted Political Email List*, EXACT DATA, <https://www.exactdata.com/quote/form.php?id=17414&campaignid=11207924044> [<https://perma.cc/U3J3-KYT2> (staff-uploaded archive)]. Others have created services wherein political groups will pool their email lists in a common "co-op"; the firm will then analyze lists along with other data, redistributing potential donors between

senders you've heard of: Joe Biden, Beto O'Rourke, the Democratic Senatorial Campaign Committee. Others are from senders you haven't heard of: Democrats Win Together, Blue Wave, Progressive Alliance. Still others are simply sent from Joe, Nancy, Alexandria, or some other common first name. You find these especially aggravating: your son is named Joe, and it's taken you a while to ignore the emails from "Joe," especially those with subject lines like, "This is urgent" or "I really need you, Bill."

One day in early November, you get an email from a committee—the one you first donated \$10 to—asking you to “update your credit card information.” The email explains that, this week, your recurring donation was declined. You have no idea what the email is talking about. You do not remember making a recurring donation. You fish around for the final credit card statement from your recently expired card and discover that the \$10 gift you gave a couple months back had not been a one-time gift like you thought. Rather, the committee had been withdrawing \$10 every week.²³ This is the last straw, you say to yourself, and you resolve to ask your daughter to help you set up a new email account next time she visits. Your existing account is beyond salvation.²⁴

This story illustrates just a small sample of the problems—ranging from minor annoyances to million-dollar frauds²⁵—enabled by the regulatory vacuum in which political organizations operate online. Not mentioned were numerous

the “co-op members” according to which potential donor is most likely to donate to that particular cause. *See, e.g., FAQ*, ADVANTAGE AI, <https://aai.archieplatform.com/faq/> [<https://perma.cc/5JMY-SHPN>] (“How does it work? Organizations pool their supporters, which is what makes up the co-op part. When you want to find new donor prospects, just tell us how many, and we’ll create a model of co-op supporters likely to give to you and *your* cause.”).

23. While most nonprofits include a “make this donation recur monthly” box on their donation forms, the default setting is for the box to be “unchecked.” For political fundraisers, however, it is common to “precheck” this box so that recurring gifts are the default. Because the text notifying donors that they are making a recurring donation is frequently small and confusing, many donors make monthly—or even weekly—recurring gifts without realizing it. *See* Shane Goldmacher, *How Trump Steered Supporters into Unwitting Donations*, N.Y. TIMES, <https://www.nytimes.com/2021/04/03/us/politics/trump-donations.html> [<https://perma.cc/RHN2-9F3U> (staff-uploaded, dark archive)] (last updated Apr. 7, 2021) [hereinafter Goldmacher, *How Trump Steered Supporters*]. While the Trump campaign, which used this tactic to extract as many as six donations in one month from some of its supporters, was arguably the most notorious user of this tactic, its use was not limited to one party. Many Democratic groups relied on the tactic; in fact, when ActBlue—the most commonly used Democratic donation platform—announced its intention to stop allowing prechecked recurring payments, the DCCC began looking for a new donation platform. *See* Goldmacher, *Deceptive Campaign Fund-Raising*, *supra* note 21.

24. While this hypothetical donor is by no means lucky, things could have been a lot worse. For example, one Trump donor, a 63-year-old cancer patient living on less than \$1,000 a month, decided to give a one-time donation for \$500. *See* Goldmacher, *How Trump Steered Supporters*, *supra* note 23. That donation turned into an unwitting weekly contribution which amounted to \$3,000—and it was only discovered after the donor’s rent payments bounced. *See id.*

25. *See* Shane Goldmacher, *Three Men Charged with Running ‘Scam PACs’ That Bilked Small Donors*, N.Y. TIMES (Nov. 10, 2021), <https://www.nytimes.com/2021/11/10/us/politics/pac-operator-charges.html> [<https://perma.cc/YU8V-D49U> (staff-uploaded, dark archive)].

other misleading tactics, such as “matches” that are nothing but accounting gimmicks,²⁶ “memberships” that provide no actual benefit to donors,²⁷ or “Scam PACs” whose whole mission is to raise money to pay the salaries of the fundraisers themselves.²⁸ While these issues should certainly be addressed, this Comment focuses on one specific problem created by spam: its drain on our time and attention.

B. *Why Is There So Much Spam?*

To understand how spam has come to cost us so much time and attention, one must examine why so much spam is sent. The principal reason is that the marginal cost of sending mass email—that is, the cost of sending an email to an additional recipient, or of sending the same email multiple times—is extremely low.²⁹ For spammers, most costs are fixed, meaning the costs do not change depending on the quantity of email the spammer sends.³⁰ Even those costs that are not fixed, such as those involved in message creation or list acquisition, are generally low³¹—and, because of AI models like ChatGPT, they will soon be even lower.³² Thus, because spammers’ costs do not change much regardless of how many emails they send, and because they will almost certainly make more revenue if they send more emails, they are incentivized to send a lot of emails.³³

26. See Mark Sullivan, *How Campaigns Use Manipulative Tricks To Convince You To Open Their Emails*, FAST CO. (Oct. 9, 2020), <https://www.fastcompany.com/90560428/political-emails-trump-dark-patterns> [<https://perma.cc/8BUZ-XYC7>] (“[C]ampaigns that offer donation ‘matching’ are usually just allocating money that’s already coming in to cover the match.”).

27. See, e.g., Archived E-mail from DASS, info@democraticsecretaries.org (Jan. 20, 2022, 1:48 PM), <https://politicalemails.org/messages/568453> [<https://perma.cc/62RU-ESPR>]; Archived E-mail from 2022 Membership Services, news@pelosi4never.com (Jan. 20, 2022, 9:08 PM), <https://politicalemails.org/messages/568957> [<https://perma.cc/9PCA-S9XP>].

28. See Jarrett Renshaw & Joseph Tanfani, *How ‘Scam PACs’ Fall Through the Cracks of U.S. Regulators*, REUTERS, <https://www.reuters.com/article/idUSKBN1ZS29B/> [<https://perma.cc/5W9Z-KL77> (staff-uploaded archive)] (last updated Jan. 29, 2020, 12:11 PM) (defining “Scam PACs” as groups that “gobble up most of the money they raise rather than using it for the charitable or other causes they profess to support”).

29. In this section, an “email” is the individual chunk of data that reaches each recipient’s inbox. A “message” is a piece of unique content. For example, if the author sent the word “hey” to 500 of his friends, he would have sent 500 emails but only one message.

30. See Bambauer, *supra* note 14, at 11 (“Most of [the costs of sending email] are fixed (hardware, addresses, revenue capture) and others are generally low (Internet access, message creation). Thus, sending additional spam incurs trivial marginal costs.”).

31. *Id.*

32. See *infra* Section I.C.

33. See Bambauer, *supra* note 14, at 11 (“[S]ending additional spam incurs trivial marginal costs. Even if marginal revenue is low, spammers have an incentive to send more messages to cover fixed initial investments. Thus, an advertiser who transmits spam tends to send a lot of it.”); see also Soma et al., *supra* note 9, at 169 (“The marginal cost of adding additional e-mail addresses to a recipient list is minimal, meaning that there is only a negligible cost difference between sending, for example, 1,000 and 10,000 spam e-mails.”).

Contrast this with other forms of advertising. With direct mail, for example, the marginal cost of sending each piece of additional material—the cost of printing, packaging, and paying the postage for it—is much higher than the cost of sending an additional email.³⁴ Therefore, direct-mail marketers are incentivized, to a much greater extent than are email marketers, to only send messages to their “best” prospective customers. Whereas for an email marketer “there is only a negligible cost difference between sending, for example, 1,000 and 10,000 spam e-mails,”³⁵ such an expansion in a direct-mail campaign could turn a profitable campaign into a net loss. This dynamic applies in most other advertising mediums as well, including print, TV, and radio: to get in front of more eyeballs, the advertiser will have to pay significant costs.³⁶ This is not so with the email marketer. Because of email’s low marginal costs, spammers are free to carpet bomb the world’s inboxes, knowing that they will receive little flack in return.

This carpet-bombing approach causes more uninterested people to receive the spammers’ messages. In traditional marketing mediums, this would be a bad result for both the marketer and the recipient: the marketer has wasted resources advertising to someone who is uninterested, and the recipient has wasted a small amount of time dealing with the ad. In email, however, the burden falls mostly on the recipient.³⁷ These costs primarily include the time wasted by recipients sifting through unwanted emails³⁸ and the negative psychological effect of receiving annoying, offensive, or, in the worst cases, malicious messages.³⁹ They

34. For a direct mail campaign, most marketers will spend between \$0.30 and \$3 per piece of mail. See *How Much Does Direct Mail Cost in 2023?*, TARADEL (Aug. 23, 2022, 1:01 PM), <https://www.taradel.com/blog/how-much-does-direct-mail-cost-in-2022> [https://perma.cc/D5D3-KBBG]; Dennis Kelly, *Direct Mail Costs Made Easy—How To Understand Direct Mail Pricing*, POSTALYTICS (Aug. 13, 2023), <https://www.postalytics.com/blog/direct-mail-cost/> [https://perma.cc/RD55-9VFK]. Within those costs, marginal costs—printing and postage, which vary based on the number of pieces—make up between \$0.71 and \$3.50, or between about 24% and 116% of the total average cost. See *How Much Does Direct Mail Cost in 2023?*, *supra* (estimating print costs as between \$0.05 and \$2.00 per piece and postage costs between \$0.66 and \$1.50 per delivery). In contrast, email marketers incur only negligible marginal costs; nearly all their costs are “fixed.” See Bambauer, *supra* note 14, at 11.

35. Soma et al., *supra* note 9, at 169.

36. Pricing for TV commercials, for example, varies according to the number of expected viewers. See George Alger, *How Much Does a TV Commercial Cost?*, SKYWORKS MKTG. (Dec. 18, 2023), <http://skyworksmarketing.com/tv-commercial-cost/> [https://perma.cc/QW7X-4S2G] (estimating that a thirty-second time slot in a medium-sized market “can be purchased for as little as \$15–\$25 per 1,000 viewers”).

37. See Bambauer, *supra* note 14, at 12 (“Recipients, unlike senders, face non-trivial marginal costs for additional messages.”).

38. See Rao & Reiley, *supra* note 3, at 98.

39. See Bambauer, *supra* note 14, at 12 (noting that “psychological effects on users, such as from viewing pornographic spam or from the annoyance of managing large volumes of unwanted mail” is part of spam’s cost).

also include the costs Internet Service Providers (“ISPs”) incur from processing spam⁴⁰—some of which are presumably passed on to the consumer.

While society does receive some benefit from unsolicited bulk email—the sender receives some revenue, and the recipient occasionally learns about a product or opportunity in which they are interested⁴¹—such benefits pale in comparison to the costs. According to research scientists at Microsoft and Google, the ratio of spam’s costs to its benefits is about 100:1, meaning that for every dollar of benefit spam generates, it generates \$100 of costs to society.⁴² They compare this “externality ratio” to that of car theft, which they estimate as somewhere between 6.7:1 and 30:1, meaning for every dollar of benefit to the thief, society pays between \$6.70 and \$30.⁴³ Though their definition of spam is narrower than that used in this Comment, the conclusion holds true for all types of unsolicited mass email: the costs far outweigh the benefits. Until the costs of receiving spam are lessened, or until spammers themselves incur a greater percentage of the costs that they currently defray to the recipients, spam will continue to be a problem.

C. *Why Is There So Much Political Spam in Particular?*

In the early days of email, some policymakers thought that political groups would not add to the spam problem.⁴⁴ After all, politicians have goals more important than raising money: winning elections. Political spam, the thinking went, risked annoying people to the point of losing their votes.⁴⁵ Therefore, the hope was, political groups would use such email sparingly, if at all. It was a hope that proved naïve.

The opening salvo of political spam took place from 1998 to 2004.⁴⁶ In the beginning, there was significant negative backlash against the spammers, including ISPs blocking or threatening to block the offenders’ emails.⁴⁷ The

40. See Rao & Reiley, *supra* note 3, at 98–99 (estimating that ISPs must employ “more than five times as much [server] capacity as would be required in the absence of spam”).

41. See Bambauer, *supra* note 14, at 63.

42. See Rao & Reiley, *supra* note 3, at 103 (defining “costs” as time waste and resources spent on antispam measures and “benefits” as revenue to the spammers).

43. See *id.* (defining “costs” as “uninsured losses to the victims, insurance premiums, law enforcement patrol costs, and the cost of prosecuting and incarcerating offenders who are caught” and “benefits” as the value the thief gains from the car).

44. See Grossman, *supra* note 13, at 1534–35 (explaining that, when policymakers explain why they exempted political email from regulation, they frequently argue that “politicians would not use spam because of its annoyance factor”).

45. See *id.* at 1570 (“As a spokesman for the RNC stated, ‘it is counterproductive to send unsolicited mass e-mail; people view it as junk mail and [it] will turn off more voters than gain supporters.’ 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.’”).

46. See *id.* at 1536 (discussing candidates’ use of spam in various 1998 state elections).

47. See *id.* at 1536–37.

backlash even led Howard Dean's 2004 Presidential campaign, "viewed as one of the most savvy about Internet-based campaigning," to promise not to use the tactic again.⁴⁸ However, public outcry was not enough to stop the gathering storm. By the end of the 2004 elections, registered voters had received an estimated 1.25 billion unsolicited political messages.⁴⁹ That number would only grow in the years to come.

The 2008 election brought fundraising into the digital era. With the support of most party bigwigs and immense (for the time) financial resources, the Democratic nomination should have been Hillary Clinton's.⁵⁰ And it probably would have been, had Barack Obama not revolutionized political fundraising.⁵¹ Clinton was still operating with the old fundraising model, which depended almost exclusively on wealthy "bundlers."⁵² The Obama campaign, building off Howard Dean's methods in 2004,⁵³ adopted a new approach, using the internet to tap a sea of small-dollar donors.⁵⁴ The campaign did this by, among other things, amassing a thirteen-million-person email list—to which the campaign sent over one billion emails, including "8,000 to 10,000 unique e-mail messages targeted to specific segments."⁵⁵ The Clinton campaign, seeing Obama's success, tried to adapt, but it was too little, too late: after Super Tuesday, her campaign was out of cash.⁵⁶ Barack Obama, meanwhile, raised a

48. *Id.* at 1538.

49. *Id.* at 1538–39.

50. See Joshua Green, *The Amazing Money Machine: How Silicon Valley Made Barack Obama This Year's Hottest Start-Up*, ATLANTIC (June 2008), <https://www.theatlantic.com/magazine/archive/2008/06/the-amazing-money-machine/306809/> [<https://perma.cc/J7JL-RERA> (staff-uploaded, dark archive)] ("What's amazing," says Peter Leyden of the New Politics Institute, "is that Hillary built the best campaign that has ever been done in Democratic politics on the old model—she raised more money than anyone before her, she locked down all the party stalwarts, she assembled an all-star team of consultants, and she really mastered this top-down, command-and-control type of outfit.").

51. Some commentators, such as Ariana Huffington, have postulated that Barack Obama's 2008 victory would not have happened without the internet. See Christoph Pagel, *New Media--Flashback Arianna: "Were It Not for the Internet, Barack Obama Would Not Be President,"* HUFFPOST, https://www.huffpost.com/entry/flashback-ariana-were-it-n_156730 [<https://perma.cc/9SYA-J6WP>] (last updated May 25, 2011).

52. See Green, *supra* note 50.

53. Many of the tools pioneered by the Obama campaign were created by Blue State Digital, a company founded by veterans of the Dean campaign. See VALENTINO LARCINESE & LUKE MINER, *THE POLITICAL IMPACT OF THE INTERNET IN US PRESIDENTIAL ELECTIONS* 8 (2017). The company continues to provide technology services, including email capabilities, to many Democratic campaigns and nonprofits. See *Case Studies*, BLUE STATE, <https://www.bluestate.co/case-studies/> [<https://perma.cc/ZTF5-V4K6>].

54. See Green, *supra* note 50.

55. JENNIFER AAKER & VICTORIA CHANG, *OBAMA AND THE POWER OF SOCIAL MEDIA AND TECHNOLOGY* 1 (2009), <https://www.gsb.stanford.edu/faculty-research/case-studies/obama-power-social-media-technology> [<https://perma.cc/H89M-JKPT> (staff-uploaded archive)].

56. See Green, *supra* note 50; see also Aaron Smith & Lee Rainie, *The Internet and the 2008 Election*, in PEW INTERNET & AM. LIFE PROJECT 1, 14 (2008) (finding that, among those who use the internet,

record-breaking \$745 million that cycle, about half of which came from small-dollar donations over the internet.⁵⁷

Four years later, Obama's reelection campaign doubled down on digital, raising \$700 million—70% of its record-breaking \$1 billion raised—online.⁵⁸ About \$500 million of that came from email.⁵⁹ By 2012, any fear the campaign had about annoying its supporters had been abandoned.⁶⁰ As digital director Teddy Goff explained, even if the Obama emails sounded like “sketchy pleas from Internet con artists,” the most a recipient would do is unsubscribe; they would still vote for Obama.⁶¹ Thus, the only consideration for how many emails to send was how much those emails stood to raise. Was there any possibility that sending too many emails could cause the campaign to raise *less*, by causing too many unsubscribes or generally disillusioning the campaigns supporters? To find out, the Obama campaign ran a “More Emails Test,” which showed, simply, that more messages resulted in more money.⁶² In fact, the test showed that, if the campaign had switched to a lower volume of messages, it would have

17% of Obama supporters donated to the candidate online, compared to just 8% of Clinton supporters). Seeing the success Obama was having online, Hillary Clinton's 2008 campaign “belatedly sought to mimic Obama's Internet success.” *See id.* But the Clinton campaign was too late. By the old model of politics, it should have been a juggernaut, but it could not keep up with Obama's online fundraising machine. *See id.* (“What's amazing,” says Peter Leyden of the New Politics Institute, “is that Hillary built the best campaign that has ever been done in Democratic politics on the old model—she raised more money than anyone before her, she locked down all the party stalwarts, she assembled an all-star team of consultants, and she really mastered this top-down, command-and-control type of outfit. And yet, she's getting beaten by this political start-up that is essentially a totally different model of the new politics.”).

57. *See Barack Obama (D)*, OPENSECRETS, <https://www.opensecrets.org/pres08/candidate?id=N00009638> [https://perma.cc/CRP8-9K8M]. While Obama's 2008 campaign was a leader in the transition to online fundraising, his was not the only campaign to find success in this medium. Another notable example is Ron Paul, who used the internet to raise \$6 million in 24 hours, breaking the single-day record then held by John Kerry. Kenneth P. Vogel, *Ron Paul Becomes \$6 Million Man*, POLITICO, <https://www.politico.com/story/2007/12/ron-paul-becomes-6-million-man-007421> [https://perma.cc/JV6R-QHUW] (last updated Dec. 17, 2007, 11:34 AM). In contrast, John McCain, Obama's general election opponent, did not emphasize digital fundraising. *See Green, supra* note 50 (“John McCain's online fund-raising has been abysmal.”). Of McCain-supporting internet users, only 5% contributed online, compared to 13% of Obama-supporting internet users. Smith & Rainie, *supra* note 56, at 14.

58. Ed Pilkington, *Obama's Re-election Campaign Topped 2008 Efforts To Raise \$700m Online*, GUARDIAN (Nov. 20, 2012, 11:42 AM), <https://www.theguardian.com/world/2012/nov/20/obama-re-election-2008-700m-online> [https://perma.cc/PQ33-9Q4M].

59. Scott Detrow, *Bill Wants To Meet You: Why Political Fundraising Emails Work*, NPR (Dec. 15, 2015, 9:02 AM), <https://www.npr.org/2015/12/15/459704216/bill-wants-to-meet-you-why-political-fundraising-emails-work> [https://perma.cc/SBC6-7EMC].

60. *See* Jonathan Alter, Opinion, *Annoying Emails Work Way Better than You'd Think: A Lesson from the Obama Campaign*, WIRED (June 5, 2013, 9:30 AM), <https://www.wired.com/2013/06/dont-dismiss-email-a-case-study-from-the-obama-campaign/> [https://perma.cc/6K72-33PP (dark archive)].

61. *See id.*

62. *Id.*

raised \$100 million less over the course of the campaign.⁶³ Goff, and political fundraisers everywhere, learned a lesson: to succeed, you must “ignor[e] the human desire not to be annoying.”⁶⁴

Other candidates and organizations quickly learned the lessons of the Obama campaigns. The most notable was Bernie Sanders, who raised over \$200 million from a whopping 2.4 million individual donors in his campaign for the 2016 nomination.⁶⁵ And while Democrats “dominated” the early days of online fundraising, Republicans have begun to catch up, in no small part because of the development of WinRed, a donation platform on par with the Democrats’ ActBlue.⁶⁶ In 2020, nearly half of Donald Trump’s fundraising came from small-dollar donations, largely over the internet⁶⁷—a total that would have been unthinkable for any Republican just eight years earlier. Veterans of campaigns on both sides of the aisle have leveraged their campaign experience for career opportunities: after the campaigns ended, many started or joined companies that offer to run candidates’ online fundraising operations for them.⁶⁸ Even

63. *See id.*

64. *See id.*

65. Walter Shapiro, *The Limits of Bernie Sanders’ Fundraising Juggernaut*, BRENNAN CTR. FOR JUST. (June 21, 2016), <https://www.brennancenter.org/our-work/analysis-opinion/limits-bernie-sanders-fundraising-juggernaut> [<https://perma.cc/K923-YNR6>]. While Clinton’s 2016 campaign did not depend on small-dollar, online donations to the same extent as Sanders, her email fundraising program was nevertheless prolific. At its height, the Clinton campaign sent her supporters eight emails a day. *See* Jeff Broxmeyer & Ben Epstein, *The (Surprisingly Interesting) Story of E-mail in the 2016 Presidential Election*, 17 J. INFO. TECH. & POL. 232, 239 (2020).

66. Alex Seitz-Wald & Ben Kamisar, *Big Problems with Small Money? Republicans Catch Up to Democrats in Online Giving*, NBC NEWS, <https://www.nbcnews.com/politics/elections/big-problems-small-money-republicans-catch-democrats-online-giving-n1275605> [<https://perma.cc/8N7W-YQ34>] (last updated Aug. 2, 2021, 9:41 AM) (“Like an Amazon for causes and candidates, the platforms streamline the giving process by saving donors’ credit card information to allow for one-click contributions, providing a central hub for the parties and their allied groups.”). As Walter Shapiro points out, political parties gain a significant advantage from having a common donation platform. *See* Shapiro, *supra* note 65. When a donor donates to any candidate on ActBlue (or, now, WinRed), their credit card information is saved. *See id.* This means that, the next time *any* Democratic candidate who uses ActBlue asks that donor for money, the donor will be able to donate with one click, thereby avoiding the hassle of reentering credit card information. *See id.* Thus, with every new donor a campaign receives, it becomes easier for that same campaign—or any other campaign of the same party—to solicit money from that donor. *See id.*

67. *See* Krystal Hur, *Small Donors Ruled 2020; Will That Change Post-Trump?*, OPENSECRETS (Feb. 3, 2021, 8:54 AM), <https://www.opensecrets.org/news/2021/02/small-donors-dominated-2020-will-that-change-in-midterms/> [<https://perma.cc/P8KS-USWK>].

68. *See, e.g.*, MOTHERSHIP STRATEGIES, <https://mothershipstrategies.com/> [<https://perma.cc/G2ZW-TASD>]; MISSIONWIRED, <https://missionwired.com/> [<https://perma.cc/5YJY-DJ65>]; RISING TIDE INTERACTIVE, <https://www.risingtideinteractive.com/> [<https://perma.cc/CLG6-XY9X>]; NEW BLUE INTERACTIVE, <https://www.newblueinteractive.com/> [<https://perma.cc/DWP4-HDXT>]; AISLE 518, <https://aisle518.com/> [<https://perma.cc/RZU2-GV3H>]; BULLY PULPIT INTERACTIVE, <https://www.bpimedia.com/> [<https://perma.cc/GH24-LXNH>]. If you’ve noticed two different candidates sending emails that look eerily similar, it’s probably because the same firm, or maybe even the same person, is responsible for both emails.

more isolated from any constituent backlash, but very aware of their fundraising totals, these companies often urge their clients to be even more aggressive.⁶⁹ Why? Because they know that when you send more emails, you raise more money.

However, there are some constraints holding political spam in check, at least to an extent. One is the unsubscribe button, which all major campaigns and organizations include in their emails.⁷⁰ Campaigns know that, with every message, some percentage of recipients will unsubscribe. If the rate of unsubscribes rises above the rate at which the organization can acquire new names for the email list, that list—and therefore its earning potential—will shrink.

However, the unsubscribe button loses its deterrent effect as campaigns get closer to the election. Campaigns know that their list won't do them much good if they lose, so they "ramp up" their email volume to an unsustainable rate to raise as much as possible before election day.⁷¹ By the end, their lists will be a fraction of their original sizes, but they know that, if they win, they will have time to build them up again before the next election season (at which point the process will repeat itself). This, in industry parlance, is called "churn and burn."⁷²

69. See, e.g., Michelle Ye Hee Lee & Anu Narayanswamy, *How a Little-Known Democratic Firm Cashed In on the Wave of Midterm Money*, WASH. POST (Jan. 8, 2019, 5:44 PM), https://www.washingtonpost.com/politics/how-a-little-known-democratic-firm-cashed-in-on-the-wave-of-midterm-money/2019/01/08/f91b04bc-fef5-11e8-862a-b6a6f3ce8199_story.html [<https://perma.cc/6BJF-RE7F> (dark archive)] (discussing Mothership Strategies' high volume and aggressive tactics).

70. Because nonprofit organizations are not subject to the CAN-SPAM Act, political organizations are not legally required to include unsubscribe links in their emails. See 15 U.S.C. §§ 7701–7713 (applying just to *commercial* email and defining "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*" (emphasis added)). However, it is the author's experience that most of them do, even if the link borders on microscopic. See *All Messages*, ARCHIVE POL. EMAILS, <https://politicalemails.org/messages> [<https://perma.cc/YRP3-S9XZ>], for a random sample. This may be because some Customer Relationship Management systems ("CRMs") require that unsubscribe links be included. See, e.g., *Why We Require an Unsubscribe Link*, MAILCHIMP, <https://mailchimp.com/help/why-we-require-an-unsubscribe-link/> [<https://perma.cc/KBH8-Y54X>].

71. See Laura Putnam & Micah L. Sifry, Opinion, *Fed Up with Democratic Emails? You're Not the Only One*, N.Y. TIMES (Aug. 1, 2022), <https://www.nytimes.com/2022/08/01/opinion/democrats-2024-election.html> [<https://perma.cc/8CCL-7YZ2> (staff-uploaded, dark archive)]; Adriel Hampton, *From Fear Comes Loathing: A Guide to Email Fundraising That Respects Your List*, CAMPAIGNS & ELECTIONS (Dec. 15, 2017, 6:05 PM), <https://campaignsandelections.com/campaigntech/from-fear-comes-loathing-a-guide-to-email-fundraising-that-respects-your-list/> [<https://perma.cc/3EAN-KLJE>].

72. See, e.g., Putnam & Sifry, *supra* note 71 ("Inside Democratic fund-raising circles, this tactic is known as 'churn and burn': a way of squeezing money out of individual donors that reliably produces brief spikes in donations but over the course of an election cycle overwhelms their willingness to keep giving."); Hampton, *supra* note 71 (advocating for an alternative to the "churn-and-burn approach that requires continually pulling in 'fresh' emails").

A second mitigating factor is the need for campaigns to maintain “deliverability” with the ISPs that host recipients’ inboxes.⁷³ Each ISP uses a proprietary algorithm to automatically sort some emails into your spam folder or, in extreme cases, to not deliver the email to your inbox at all.⁷⁴ Too many people unsubscribing or not enough people opening a sender’s messages sends a negative signal to the ISP, causing it to block that sender’s messages.⁷⁵ Therefore, organizations must be wary of emailing too many annoyed or unengaged people lest they be blocked by Gmail, Outlook, or another email platform.

But, as with the unsubscribe button, ISP filters will never fix the problem on their own. That’s because these filters will always be somewhat underinclusive. There may be political reasons for this,⁷⁶ but there are practical reasons as well. Any algorithm for identifying spam will make some errors. It will let some spam into the main inbox (a type II error)⁷⁷ and will mark some legitimate mail as spam, relegating it to the junk folder (a type I error).⁷⁸ In theory, a highly aggressive filter could capture *all* spam; however, this filter would be extremely prone to type I errors, which have the potential to be much more costly than type II errors.⁷⁹ A few type II errors may cost someone thirty extra seconds to filter out the unwanted email. A type I error, on the other hand, may send an important email from your boss to the spam folder, where you do not find it until it is too late. This error is much more costly—and much less likely to be forgiven by the user—than letting a few extra spam emails (or a few hundred extra spam emails) into your main inbox.⁸⁰ As a result, spam filters

73. See *Email Deliverability*, CAMPAIGN MONITOR, <https://www.campaignmonitor.com/resources/glossary/email-deliverability/> [<https://perma.cc/R9N5-GQUA>].

74. See Piotr Malek, *Email Deliverability: Everything You Need To Know*, MAILTRAP (Jan. 5, 2024), <https://mailtrap.io/blog/email-deliverability/> [<https://perma.cc/8TYH-VMQR>].

75. See Nupur Mittal, *Everything You Need To Know About Email Deliverability*, MAILMODO (Dec. 14, 2023), <https://www.mailmodo.com/guides/email-deliverability/#difference-between-email-delivery-and-email-deliverability> [<https://perma.cc/F96H-QU6U>].

76. See Ashley Gold, *Scoop: Google Moves To Keep Campaign Messages Out of Spam*, AXIOS (June 27, 2022), <https://www.axios.com/2022/06/27/google-campaign-email-spam-gmail> [<https://perma.cc/EGJ8-WGC7> (staff-uploaded archive)] (describing how, in response to pressure by Republican lawmakers, Google is developing a system to exempt campaign-related emails from its spam filter).

77. Also called “false negatives.” *False Positive and False Negative Junk Submission*, PENN INFO. SYS. & COMPUTING (June 23, 2020), <https://www.isc.upenn.edu/how-to/false-positive-and-false-negative-junk-submission> [<https://perma.cc/TY7G-P3YD>].

78. Also called “false positives.” *Id.*

79. See Soma et al., *supra* note 10, at 168–69 (“In attempting to separate the wheat from the chaff, these filtering systems inevitably filter legitimate e-mails by mistake . . . [thus,] potentially important communications are lost.”); Bambauer, *supra* note 14, at 29 (discussing some of the problems caused by “overinclusive filters”).

80. Sharon Gaudin, *False Positives: Spam’s Casualty of War Costing Billions*, DATAMATION (Aug. 7, 2003), <https://www.datamation.com/security/false-positives-spams-casualty-of-war-costing-billions/> [<https://perma.cc/NB3G-YUEG>] (“Analysts say that’s why many IT managers have chosen to go easy

make many type II errors for every type I error.⁸¹ Type II errors, in the aggregate, cost consumers a lot, but because each individual error creates only a minor inconvenience, most consumers overlook them.

A third mitigating factor—present in all email marketing but especially for cash-strapped campaigns—is the supply of new content. While political organizations will repeatedly send the same message, especially if the content succeeds at driving donations,⁸² re-sent messages will eventually lose their effectiveness. When that happens, fundraisers must write new content, which takes time and resources.

However, advancements in generative AI could make this constraint as trivial as the others. To illustrate, see ChatGPT’s response to the author when prompted to write a fundraising email in the style of Joe Biden:

Dear [Recipient’s Name],

Our democracy is at risk, and I’m reaching out with urgency. I’m trailing in the polls and falling short in fundraising.

We’re fighting for crucial issues like healthcare, climate action, and economic fairness, but we’re running out of time and resources. Without your help, we can’t win these battles.

Donate now, and your gift will be doubled. We can’t afford to miss this critical deadline.

[Donate Now]

Your support isn’t just about my campaign; it’s about protecting our democracy and the values we hold dear.

Please act now. Democracy is on the line.

on spam. More offers of wild porn, hair regrowth tonics and body enhancers get through to users’ inboxes, but at least they’re not missing the big emails.”).

81. *Type 1 and Type 2 Errors*, MATT RICKARD (Apr. 1, 2022), <https://matt-rickard.com/type-1-and-type-2-errors> [<https://perma.cc/7K2F-BBVP>] (“[S]pam email classifiers could aggressively filter spam and reduce the amount of emails that arrive. But, the cost of identifying a legitimate email as spam could be very costly, so spam classifiers often accept more false negatives . . . than false positives . . .”); *Type II Error*, SPLIT, <https://www.split.io/glossary/type-ii-error/> [<https://perma.cc/TUU9-MH7D>] (“[T]he goal of email spam filtering systems should be to bring down the number of type II errors while keeping the number of type I errors at near-zero.”).

82. See Lauren Minning, *Resending Email: To Do or Not To Do? Here’s How To Decide (and What To Do After)*, ACTIVECAMPAIGN (Sept. 13, 2023), <https://www.activecampaign.com/blog/resending-email> [<https://perma.cc/6CH8-P8N6>].

With gratitude,

Joe Biden⁸³

By prompting the model and then refining that prompt based on the model's output, the author was able to produce a serviceable fundraising email in minutes. With practice, fundraisers may be able to do so in seconds. This will lower the cost of sending new content, thereby increasing the quantity and variety of spam.

D. *What Makes Political Spam Costly to the Recipient?*

Having covered why there is so much spam in general—and so much political spam in particular—this Comment now turns to why political spam is costly to the recipient, in terms of time spent identifying and disposing of it. There are a few features of all spam, but particularly of political spam, that add to these costs. These are the problems of “who” and “what,” meaning the difficulties of determining who the messages are from and what they are (i.e., that they are fundraising emails, as opposed to another type of message).

Political campaigns and organizations, even legitimate ones, often try to obscure their identity when they hit your inbox.⁸⁴ Mass email blasts typically have an “open rate” of about 20%.⁸⁵ However, because they are sent to hundreds of thousands—or even millions—of people, pushing that open rate just a little higher can result in thousands more dollars raised. To accomplish this, fundraisers use misleading sender names, which will entice—or trick—more people into opening the message.⁸⁶ This includes varying the sender name with every email,⁸⁷ trying to resemble a news alert,⁸⁸ using the first name of the candidate, or even of a campaign staffer, if that name is sufficiently common in

83. This passage is based on a query to ChatGPT-3.5: “Please write an email in the voice of Joe Biden based on this outline . . .” on September 20, 2023. See *infra* Appendix A (providing the full text of this conversation).

84. As one commentator memorably put it, “The greasy-smocked minion who cooks up these [emails] tries to slip them past not just your spam filters, but your internal filters.” John Dickerson, *Hey! Do You Want To Save America? Give Me \$5*, SLATE (Oct. 8, 2014, 12:21 PM), <https://slate.com/news-and-politics/2014/10/political-fundraising-emails-are-insulting-and-deceitful-why-they-represent-whats-wrong-with-american-politics.html> [<https://perma.cc/2A4L-YEWE>].

85. See *What Are Good Open Rates, CTRs, & CTORs for Email Campaigns?*, *supra* note 21.

86. See *supra* note 18 and accompanying text.

87. See ARCHIVE POL. EMAILS, <https://politicalemails.org/messages?query=%40dsc.org> [<https://perma.cc/5VR4-HEXM>], to sample the many different senders the Democratic Senatorial Campaign Committee has used.

88. See, e.g., Archived E-mail from Trump Endorsement Tracker, news@actblue4never.com (May 29, 2022, 3:16 PM), <https://politicalemails.org/messages/676616> [<https://perma.cc/JEK9-8TMV>].

the general population.⁸⁹ It is even common for groups to impersonate other, more popular campaigns or organizations in hopes of siphoning off donations from the more popular candidate.⁹⁰ For example, on the day Beto O'Rourke announced his campaign for governor of Texas, a group unaffiliated with O'Rourke's campaign sent messages under the name "Beto O'Rourke Update."⁹¹ The organizations who use these tactics hope that, even if recipients open the email under false pretenses, some percentage of those recipients will be inspired to give by the message within.

The second, somewhat related issue is the difficulty in determining whether an email actually is a fundraising email. This difficulty begins with the sender and subject line: when someone receives an email from "Joe" with the subject line "this is urgent," they might not identify the message as a fundraising email—at least without opening it. However, even opening the message does not always end the confusion because, frequently, the email will not ask for a donation. Instead, it will prompt the recipient to take a survey or sign a petition.⁹² And, contrary to what the surveys or petitions claim, the campaign does not use the responses to "help build [the campaign's] strategy."⁹³ In fact, the survey's only purpose is to prime the recipient for the last survey question: the request for a donation.⁹⁴ Organizations use "petitions" in a similarly deceptive fashion, either as a way to entice someone into "signing" the petition (after which they will be routed to a survey and then to a donation page) or as a cheap way to collect names to "swap" with other political organizations who

89. See, e.g., Archived E-mail from Megan, info@dsc.org (May 25, 2020, 10:31 PM), <https://politicalemails.org/messages/170251> [<https://perma.cc/JCS7-PT3T>]; E-mail from Laura, info@democraticgovernors.org, to Alex Slawson, the author of this Comment (Dec. 15, 2022, 12:25 PM) (on file with the North Carolina Law Review). The idea is that recipients will be more likely to open an email from "Megan" or "Laura" because the recipient is more likely to think a real person—maybe even someone they know—as opposed to a political organization, is sending them the message.

90. See Goldmacher, *Team Beto*, *supra* note 20.

91. See *id.* Other instances of misleading sender names abound. For example, the Democratic Congressional Campaign Committee ("DCCC"), traditionally one of the most aggressive online fundraising organizations, has sent emails under the name "SOCIAL SECURITY UPDATE (via DCCC)." See Goldmacher, *Deceptive Campaign Fund-Raising*, *supra* note 21. Another organization used "Your Order Confirmation" as the sender and "Order ID: 73G526S" as the subject line." *Id.*

92. See, e.g., Archived E-mail from Bobby Maggio, info@johnfetterman.com (Jan. 7, 2022, 9:30 PM), <https://politicalemails.org/messages/559514> [<https://perma.cc/Y6CT-PMX2>]; Archived E-mail from Megan, *supra* note 89. For an example of a typical survey, see *Official Democratic Priorities Survey*, DEMOCRATIC SENATORIAL CAMPAIGN COMM., <https://surveys.signforgood.com/official-website-survey> [<https://perma.cc/ZGJ8-RXAH>].

93. See *Official Democratic Priorities Survey*, *supra* note 92.

94. See Arunesh Mathur, Angelina Wang, Carsten Schwemmer, Maia Hamin, Brandon M Stewart & Arvind Narayanan, *Manipulative Tactics Are the Norm in Political Emails: Evidence from 300k Emails from the 2020 US Election Cycle*, BIG DATA & SOC'Y, Jan.–June 2023, at 1, 10.

are “sponsoring” the same petition.⁹⁵ Again, the groups who use these tactics hope that some percentage of recipients who had no intention of donating will, after completing a petition or survey, donate anyway.⁹⁶

At their best, the difficulties of determining “who” and “what” add a few seconds to the time it takes a recipient to recognize the email as a fundraising email and to transfer it to the junk folder. At their worst, they defraud donors of their money by leading them to believe they are donating to one organization when, in fact, they are donating to another. Somewhere between those two extremes are the costs paid by the recipients who sign the phony petitions and surveys—people who, if they knew the true purpose of those devices, might spend their time on something else. These costs are, individually, small, but to a person who receives thousands of these emails a year, they can amount to a death by a thousand digital papercuts.

II. SOLVING THE PROBLEM OF “WHO” AND “WHAT”

A. *Front-End Regulation*

Faced with a clear market failure, government should step in. In theory, many solutions are possible. One set of “front-end” regulations would involve trying to decrease the overall volume of spam by stopping spam at its source. One example of this would be a “do-not-email” registry, allowing people to sign up and be excluded from all marketing or fundraising emails. A more radical example would be to simply prohibit all bulk emails to recipients who have not affirmatively consented to receiving them.⁹⁷

However, front-end regulations have significant flaws. For one, the Federal Trade Commission has said that a do-not-email registry would likely

95. These petitions are called “joint actions.” After an organization signs up to sponsor the joint action, it will send the petition to its email list asking recipients to sign. *See Simone Pathé, supra* note 22. When the joint action “closes” after about a month, all the sponsoring organizations pool the email addresses of the supporters who signed and then redistribute them amongst the sponsoring organizations according to how many signatures each provided to the total. *See id.* For example, a sponsor who gained 3,000 signatures from emails to their own list could expect to receive about 3,000 new email addresses from the other sponsors in return. *See id.* As noted above, the fact that your email address has been traded from one organization to another does not mean it ceases to be on the original list. It means that you are likely to be on more lists.

96. Because the last question of the survey is often “will you donate,” and because the answers often do not include a “no” option, some respondents may donate because they think their responses to the survey will not count unless they make a donation. *See Mathur et al., supra* note 94, at 2, 11.

97. Under this law, marketers, fundraisers, and other publishers of email could still send to people who, for example, went to the publisher’s website and signed up for emails. The law could also include an exception for people who have a preexisting business relationship with the publisher.

be hard to enforce and ultimately counterproductive.⁹⁸ In their report to Congress on the feasibility of a do-not-email registry, the FTC wrote that such a program “would likely result in registered addresses receiving more spam because spammers would use such a registry as a directory of valid email addresses.”⁹⁹ Second, both the registry and the ban would have enforceability problems. The registry would require those most vulnerable to email spam—older, less tech-savvy people—to sign up for the registry. If they sign up at all, they may not do so until their inboxes are swamped, and by then they may have already been tricked into, for example, giving erroneous recurring donations. A ban on unsolicited email, for its part, suffers from the fact that fundraisers can mislead people into consenting, as with the fake petitions and surveys discussed above.¹⁰⁰

Most importantly, front-end regulations have a high risk of being struck down as unconstitutional under the First Amendment, at least as applied to political emails. Front-end restraints on *commercial* emails—those offering to exchange a good or service in exchange for money—would have a better chance of survival because commercial speech has less First Amendment protection.¹⁰¹ Restraints on commercial speech are judged merely by the *Central Hudson* test, a form of “intermediate scrutiny.”¹⁰² Though regulation on commercial speech is not guaranteed to pass the test, many restraints on commercial speech, including the CAN-SPAM Act,¹⁰³ have done so.¹⁰⁴

Regulation of *political* email is different. Because political speech is at the “core” of the First Amendment, courts more readily strike down laws that

98. Press Release, Fed. Trade Comm’n, New System To Verify Origins of E-Mail Must Emerge Before Do Not Spam List Can Be Implemented, FTC Tells Congress (June 15, 2004), <https://www.ftc.gov/news-events/news/press-releases/2004/06/new-system-verify-origins-e-mail-must-emerge-do-not-spam-list-can-be-implemented-ftc-tells-congress> [https://perma.cc/PV9T-A67S].

99. *Id.*

100. *See supra* notes 92–96 and accompanying text.

101. *See* Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n of New York, 447 U.S. 557, 562–63 (1980) (citing *Ohralik v. Ohio State Bar Ass’n.*, 436 U.S. 447, 456–57 (1978)) (“The Constitution . . . accords a lesser protection to commercial speech than to other constitutionally guaranteed expression.”).

102. *See id.* at 573 (Blackmun, J., concurring) (“Under this four-part test a restraint on commercial communication that is neither misleading nor related to unlawful activity is subject to an intermediate level of scrutiny . . .”).

103. *See* Aitken v. Commc’ns Workers of Am., 496 F. Supp. 2d 653, 665 (E.D. Va. 2007) (“It is . . . clear that application of the CAN SPAM Act to misleading union speech does not . . . pose any difficult First Amendment questions about the Act’s validity . . .”).

104. *Compare* Friedman v. Rogers, 440 U.S. 1, 15–16 (1979) (holding that the State can restrict the use of trade names in certain industries), and *Ohralik*, 436 U.S. at 449 (upholding the punishment of an attorney for face-to-face solicitation of an accident victim), with 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 516 (1996) (striking down a state law prohibiting price advertising of alcoholic drinks).

proscribe it.¹⁰⁵ In *Buckley v. Valeo*,¹⁰⁶ for example, the Supreme Court struck down parts of a law limiting campaign expenditures.¹⁰⁷ The Court wrote that “[i]t is clear that a primary effect of these expenditure limitations is to restrict the *quantity* of campaign speech” and that “[t]he restrictions, while neutral as to the ideas expressed, limit political expression ‘at the core of our electoral process and of the First Amendment freedoms.’”¹⁰⁸ Though it is unclear what standard the Court applied in *Buckley*,¹⁰⁹ the Court was more definitive in *Citizens United v. FEC*,¹¹⁰ when it declared that “[l]aws that burden political speech are subject to strict scrutiny,” meaning they must be “narrowly tailored” to further a “compelling interest.”¹¹¹ Very few laws pass this test.¹¹²

Would front-end regulation of unsolicited email face strict scrutiny if it were applied to political emails? If *Buckley* and *Citizens United* are to be believed, then probably yes, because front-end regulation would “burden” political speech—or at least “restrict the quantity.”

However, there are reasons to believe the seeming prohibition on restricting political speech is not as literal as it seems. For example, in *Rowan v. U.S. Post Office Department*,¹¹³ a 1970 Supreme Court case, the Court upheld a law that gave mail recipients the right to block certain mailers which the recipient found objectionable.¹¹⁴ The law purported to apply only to “lewd and salacious” mail; however, the recipient alone could determine whether the mail was lewd and salacious, so the law ostensibly empowered recipients to block any mailer for any reason.¹¹⁵ If a recipient wished to be removed from a mailer’s list, they would notify the Postmaster General, who would then direct the mailer to delete the recipient’s address.¹¹⁶

105. See *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 346 (1995) (“Discussion of public issues and debate on the qualifications of candidates are integral to the operation of the system of government established by our Constitution. The First Amendment affords the broadest protection to such political expression” (quoting *Buckley v. Valeo*, 424 U.S. 1, 14–15 (1976) (per curiam))).

106. 424 U.S. 1 (1976).

107. *Id.* at 58–59. The Court struck down provisions limiting overall spending by campaigns, by self-financing candidates, and by independent groups. *Id.*

108. *Id.* at 39 (emphasis added) (quoting *Williams v. Rhodes*, 393 U.S. 23, 32 (1968)).

109. See *id.* at 260 (White, J., concurring).

110. 558 U.S. 310 (2010).

111. *Id.* at 340 (2010) (citing *Fed. Election Comm’n v. Wis. Right to Life, Inc.*, 551 U.S. 449, 464 (2007)); see also *Ariz. Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721, 741 (2011).

112. “In order to survive strict scrutiny, a statute must be narrowly tailored to advance a compelling state interest.” *State v. Roundtree*, 952 N.W.2d 765, 770 (Wis. 2021) (citing *In re Zachary B.*, 2004 WI 48, ¶ 17, 271 Wis. 2d 51, 678 N.W.2d 831). “Strict scrutiny is an exacting standard, and it is the rare case in which a law survives it.” *Id.* (citing *State v. Baron*, 2009 WI 58, ¶ 48, 318 Wis. 2d 60, 769 N.W.2d 34).

113. 397 U.S. 728 (1970).

114. *Id.* at 729–31, 740.

115. See *id.* at 731, 737.

116. *Id.* at 729–30.

The Court held that this law did not violate the First Amendment, rooting its decision in the right to be left alone.¹¹⁷ Though the Court acknowledged that the right to communicate is “highly important,” it held that such a right “must stop at the mailbox of an unreceptive addressee.”¹¹⁸ “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.”¹¹⁹

An Eighth Circuit case, *Van Bergen v. State of Minnesota*,¹²⁰ offers another example. In that case, the court upheld a Minnesota law—even as applied to political candidates—that banned the use of machines that automatically dial telephone numbers and play prerecorded messages.¹²¹ In reaching that decision, the court determined that the law was a “content-neutral time, place or manner restriction,” because the law applied to all prerecorded messages—regardless of their content—and merely regulated the manner in which they were transmitted.¹²² Therefore, the court applied intermediate scrutiny, not strict,¹²³ and upheld the law.¹²⁴ Though *Van Bergen* does not reference *Buckley*, the two opinions can be read as somewhat contradictory. Part of the Eighth Circuit’s justification for upholding the ban on auto-dialers was that campaigns had “ample alternative[s]” to auto-dialing machines, such as “[l]ive telephone calls” and “door-to-door distribution of information.”¹²⁵ But, even with these alternatives, the ban still “restricts” political speech. The alternatives are more costly than the banned auto-dialers, so the total amount of speech a campaign can engage in is lessened by the ban. This is in seeming tension with *Buckley*, which decried regulations that “limit” or “restrict” the quantity of political speech.

Rowan and *Van Bergen* may help pave the way for front-end regulation of political spam. If the Constitution allows for the blocking of mail and the banning of auto-dialing machines, it might also allow for a ban on unsolicited bulk email or a do-not-email registry. However, optimism should be tempered. For one, the law in *Rowan* is narrower than the front-end solutions discussed

117. *See id.* at 737–38.

118. *Id.*

119. *Id.* at 738.

120. 59 F.3d 1541 (8th Cir. 1995).

121. *Id.* at 1551.

122. *Id.* at 1553.

123. *Id.* Because “time, place, or manner” restrictions do not alter or discriminate based on the content of the speech, they are judged less harshly than content-based restrictions. *Compare* *Ward v. Rock Against Racism*, 491 U.S. 781, 803 (1989) (upholding a New York City ordinance—which required performers in a public amphitheater to use the city’s sound equipment instead of their own—as a reasonable time, place, or manner restriction), *with* *Police Dep’t. of Chi. v. Mosley*, 408 U.S. 92, 94 (1972) (striking down an ordinance—which forbade all picketing near a school *except* picketing that concerned labor disputes—as an unconstitutional content-based distinction).

124. *Van Bergen*, 59 F.3d at 1556.

125. *Id.*

above. As the Court noted, the *Rowan* law applied only to “an affirmative act of the [recipient] giving notice that he wishes no further mailings from *that mailer*.”¹²⁶ The *Rowan* law is more akin to a law mandating unsubscribe links in all mass emails—and less akin to a blanket ban on unsolicited email or a do-not-email registry, which would not require recipients to affirmatively opt-out of specific mailers. A court might view these solutions as broader and therefore more injurious to First Amendment rights. *Van Bergen*, for its part, is distinguishable because phone calls are, arguably, more invasive than emails—and therefore more worthy of regulation.¹²⁷ Lastly, *Van Bergen* never reached the Supreme Court, and both cases predate speech-protective cases like *Citizens United*.¹²⁸

The bottom line is that, though *Rowan* and *Van Bergen* provide reason to hope that front-end regulation could survive judicial scrutiny, they may not be enough to counterbalance the Supreme Court’s more speech-protective decisions.¹²⁹ This does not mean that policymakers should not try front-end regulation; it does mean, however, that they should not put all their eggs in the front-end basket. Fortunately, there is another, surer path to reform: a back-end approach, grounded in the Supreme Court’s “disclosure” jurisprudence.

B. Back-End Regulation

Rather than lessening the amount of spam a recipient receives, back-end regulation would work by decreasing the cost of receiving each message. This can be achieved through two simple policies: (1) requiring all senders of unsolicited bulk email to stick to one sender name that is substantially similar

126. *Rowan v. U.S. Post Off. Dep’t*, 397 U.S. 728, 737 (1970) (emphasis added).

127. Mark Sweet, Note, *Political E-Mail: Protected Speech or Unwelcome Spam?*, 1 DUKE L. & TECH. REV., Jan. 14, 2003, at 1, 4–5.

128. See, e.g., *Ariz. Free Enter. Club’s Freedom Club PAC v. Bennett*, 564 U.S. 721, 755 (2011) (striking down a public financing system that gave publicly funded candidates a dollar-for-dollar match for every dollar their privately funded opposition spent above a certain amount). Some argue that the Court has made “a decisive move towards free-speech absolutism” in the last three decades. See Spencer Bradley, Comment, *Whose Market Is It Anyway? A Philosophy and Law Critique of the Supreme Court’s Free-Speech Absolutism*, 123 DICK. L. REV. 517, 530 (2019).

129. There are a few other cases that front-end proponents could look to for support. See, e.g., *Barr v. Am. Ass’n of Pol. Consultants, Inc.*, 140 S. Ct. 2335, 2343 (2020) (considering a challenge to a national ban on robocalls to cell phones). The *Barr* Court addressed only whether an exception to the ban—for debt collectors—rendered the ban an unconstitutional content-based restriction. *Id.* at 2346. It held that the exception was unconstitutional, but it did not address whether the law as a whole impermissibly burdened political speech. See *id.* at 2356. Another possible analogy would be the FTC’s do-not-call registry, were it to be applied to political speech and were it to be challenged in the Supreme Court. However, the registry isn’t applied to political speech, at least partially because the FTC is afraid of running afoul of the First Amendment. See Jerry Carnes, *Why Are Political Campaigns Exempt from the Do Not Call Registry?*, 11ALIVE, <https://www.11alive.com/article/news/why-are-political-campaigns-exempt-from-the-do-not-call-registry/85-611616109> [https://perma.cc/L6WQ-ZXBZ] (last updated Nov. 6, 2018, 8:17 AM).

to the organization's actual name of incorporation (the "sender requirement"), and (2) requiring all senders of such email to put "ADV," for "advertisement," in their subject line (the "subject line requirement").¹³⁰ For political emails, this could be taken a step further by requiring all such emails to have "ADV:POL," for "political advertisement," in the subject line. This back-end approach is preferable for the simple reason that it is more likely to survive constitutional scrutiny because it does not limit or restrict anyone's speech. Political organizations would still be free to send as many emails to as many people as they please; they would just have to follow these additional requirements when they do.

Figure 2: An example of how subject line labeling could enable people to easily identify advertising emails.

<input type="checkbox"/>	☆	»	DCCC HQ	[ADV:POL] get your FREE sticker - It's up to STRONG grassroots Der
<input type="checkbox"/>	☆	»	Amazon Prime	[ADV] Alex, your Prime picks for this week
<input type="checkbox"/>	☆	»	[REDACTED]	Hey! - Hey man, it's been a long time! Are you planning on coming hor
<input type="checkbox"/>	☆	»	Quora Digest	If a fully armed Nimitz class aircraft carrier were present on D-
<input type="checkbox"/>	☆	»	Biden and Harris' C.	[ADV:POL] Alex, have you seen the news? - Alex, Last night, Donald
<input type="checkbox"/>	☆	»	NCBA	Government & Public Sector Digest for Thursday January 12, 2023

These requirements would lessen the cost of receiving spam by solving the problems of "who" and "what." The sender requirement would enable recipients to identify the sender, thereby curbing the issue of certain organizations impersonating others,¹³¹ of using misleading names like "SOCIAL SECURITY UPDATE,"¹³² and of rotating through common names to confuse recipients into opening their emails.¹³³ The subject line requirement would alert recipients to the fact that an email is indeed a fundraising email, enabling them to either ignore it or, if they wished to read it, to do so with their "internal filter" on.¹³⁴ The labels would even enable recipients to proactively filter all political emails—or all advertising emails—out of their inboxes, using the custom filters that most email providers allow users to create.¹³⁵ Currently, to create such an all-encompassing filter, a user would need to individually input the email addresses of the organizations which the user wished to filter out, and the user

130. This is similar to a policy tried by a few states before the Federal CAN-SPAM Act preempted state regulation. See *supra* note 10 and accompanying text.

131. See *supra* notes 90–91 and accompanying text.

132. See *supra* notes 21, 91, and accompanying text.

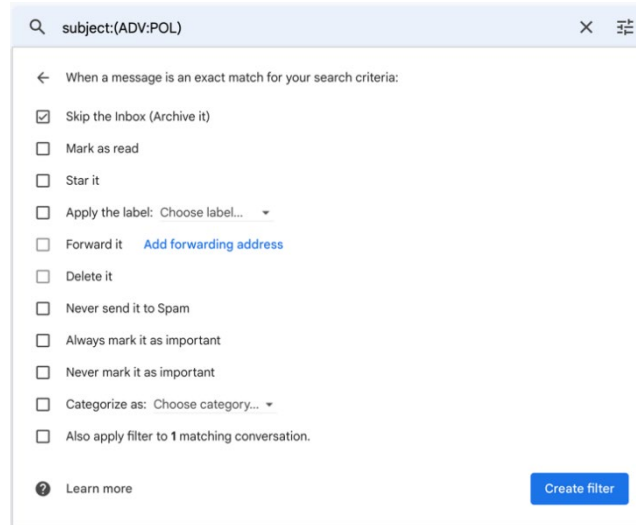
133. See *supra* notes 86–89 and accompanying text.

134. See Dickerson, *supra* note 84.

135. See *infra* Figure 3.

would need to update that list every time a new organization added the user's email to the organization's distribution list. But, with the subject line requirement implemented, that user would simply need to input "ADV:POL," and they could then instantly screen out all future political fundraising emails.

Figure 3: An example of Gmail's email filtering system which, if coupled with a common label on all advertising emails, would enable recipients to filter and, if they wished, delete, all political emails.



C. Constitutional Concerns with Back-End Regulation

These back-end regulations have a fighting chance at survival because they fall into one of the few categories of regulation that the Supreme Court has allowed to be applied to political speech: mandatory disclosure laws.¹³⁶ Such laws are subject to, at most, "exacting scrutiny."¹³⁷ For a law to survive under this standard, the government would need to prove "a substantial relation between the disclosure requirement and a sufficiently important governmental interest."¹³⁸ Residing somewhere between strict and intermediate scrutiny,¹³⁹

136. See *Buckley v. Valeo*, 424 U.S. 1, 84 (1976) (upholding a law requiring campaigns to disclose the names and addresses of all donors who gave more than \$10).

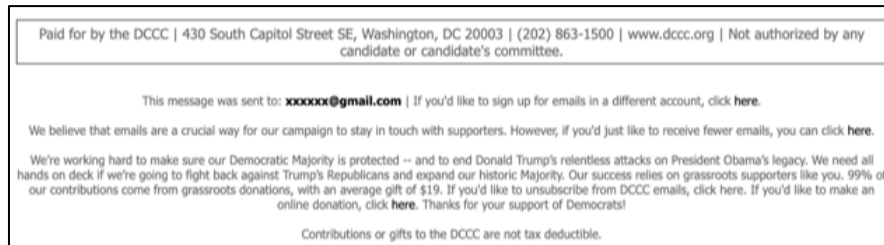
137. See *id.* at 64 (citing *NAACP v. Alabama*, 357 U.S. 449, 463 (1958)).

138. *Doe v. Reed*, 561 U.S. 186, 196 (2010) (citing *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 366–67 (2010)).

139. See David L. Hudson Jr., *Exacting Scrutiny*, FREE SPEECH CTR., <https://www.mtsu.edu/first-amendment/article/1959/exacting-scrutiny> [<https://perma.cc/99NK-5NN5>] (last updated Sept. 19, 2023).

exacting scrutiny is demanding; however, it is not a death sentence.¹⁴⁰ Indeed, laws similar to the one proposed in this Comment, such as laws requiring “paid-for” disclaimers in political advertisements, have been repeatedly upheld,¹⁴¹ which is why political organizations already have to include a disclaimer within the body of their mass emails.¹⁴²

Figure 4: An example of what you might find at the bottom of a typical fundraising email. Note the disclaimer. Also, note how difficult it is to find the “unsubscribe” link.



This does not mean back-end regulations are guaranteed to survive. By forcing spammers to stick to one sender name and to include “ADV:POL” in their subject lines, the policies would compel, or place conditions on, political speech. This would implicate the “compelled speech” doctrine, as recognized in *West Virginia Board of Education v. Barnette*,¹⁴³ which stated that the First Amendment “includes both the right to speak freely and the right to refrain from speaking.”¹⁴⁴ These policies would also implicate the right to speak anonymously, as established in *McIntyre v. Ohio Elections Commission*,¹⁴⁵ and the right not to disclose membership to an organization, as established in *NAACP v. State of Alabama, ex rel. Patterson*.¹⁴⁶ Political spammers would argue that the sender requirement unconstitutionally compels spammers to disclose their organization’s identity, as barred by *McIntyre* and *NAACP*, and that the subject

140. See *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021) (“While exacting scrutiny does not require that disclosure regimes be the least restrictive means of achieving their ends, it does require that they be narrowly tailored to the government’s asserted interest.”).

141. *McConnell v. Fed. Election Comm’n*, 540 U.S. 93, 201 (2003); *Citizens United*, 558 U.S. at 366.

142. See 52 U.S.C. § 30120(a) (requiring disclaimer of certain information in “any . . . type of general public political advertising or . . . electioneering communication”); see also 11 C.F.R. § 110.11(a)(1) (2024) (“The following communications must include disclaimers . . . electronic mail of more than 500 substantially similar communications when sent by a political committee.”).

143. 319 U.S. 624 (1943) (striking down a law requiring public school students to stand and recite the pledge of allegiance).

144. *Id.* at 645 (Murphy, J., concurring).

145. 514 U.S. 334 (1995) (striking down a law prohibiting anonymous pamphleteering).

146. 357 U.S. 449 (1958) (overturning the contempt conviction of an NAACP chapter that refused a court order to disclose its membership list).

line requirement unconstitutionally “alters the content”¹⁴⁷ of the organization’s speech, as forbidden by *Barnette* and its progeny.

However, the sender and subject line requirements should survive these challenges. First, the sender requirement does not violate an organization’s right to speak anonymously because political organizations are already required to disclose their identity in the “paid-for” disclaimer at the bottom of the email.¹⁴⁸ The law would simply require them to display their identity in a more obvious way: in the sender line. In fact, when considered alongside the existing “paid-for” requirement, the sender requirement should be judged as a content-neutral “time, place, or manner” restriction.¹⁴⁹ The requirement does not alter the *content* of the speech because the paid-for disclaimer already discloses the speaker’s identity. The sender requirement simply designates the *place* in which that disclosure must take place: the sender line, in addition to the footer. Viewed thusly, the sender requirement might receive only intermediate scrutiny and would therefore have an even better chance at survival than most disclosure laws, which undergo exacting scrutiny.¹⁵⁰

Challenges to the subject line requirement should fail for a similar reason. It is true that existing disclaimer requirements¹⁵¹ do not require political emails to literally say “this is a political advertisement,” which is what the subject requirement (“ADV:POL”) is meant to denote. Therefore, opponents could argue that the subject requirement, unlike the sender requirement, is compelling the disclosure of new information and thus should be judged more strictly. However, as noted above, existing requirements do, at the very least, require disclosure of the advertiser’s identity, which will usually alert the reader to the fact the email is a political ad.¹⁵² Even if the nature of the email is not obvious from the name of the organization, it would become obvious after rudimentary research, such as a simple Google search of the organization’s name. This research is made easier by the fact that some disclaimer requirements require

147. See *Nat’l Inst. of Fam. & Life Advocs. v. Becerra*, 138 S. Ct. 2361, 2371 (2018) (citing *Riley v. Nat’l Fed’n of the Blind of N.C., Inc.*, 487 U.S. 781, 795 (1988)) (invalidating a California law requiring certain medical facilities to notify clients that California provides free or low-cost abortion services).

148. See *supra* notes 145–46 and accompanying text.

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

150. See *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (“[T]he government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions ‘are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.’” (quoting *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984))); see also *City of Austin v. Reagan Nat’l Advert. of Austin, LLC*, 142 S. Ct. 1464, 1475 (2022) (explaining that content-neutral “time, place, or manner” restrictions are subject to intermediate scrutiny).

151. 11 C.F.R. § 110.11 (2024).

152. Why else would the DCCC be sending you an email?

advertisers to include their website and address in the footer, in addition to their name.¹⁵³ Thus, the subject line requirement would not actually mandate new disclosure. It would simply elucidate information that was already implicit in existing disclaimers.

But, even if the sender and subject line requirements were viewed as compelling new disclosures, they could still survive exacting scrutiny because they are justified by a “sufficiently important” interest.¹⁵⁴ In upholding similar disclaimer requirements in the past, the Supreme Court has said that helping citizens “make informed choices in the political marketplace” is a sufficiently important interest to justify the burdens that disclaimer requirements place on speech.¹⁵⁵ In coming to one such decision, the Court cited the “independent groups [that] were running election-related advertisements ‘while hiding behind dubious and misleading names.’”¹⁵⁶ The Court’s rationale in that case would apply just as much to a challenge of the legislation proposed here. Currently, the use of dubious and misleading sender and subject lines is impeding the ability of citizens to make informed choices. Sender and subject line requirements would help solve that problem.

Opponents will argue that these sender and subject line requirements are more burdensome than other disclaimer requirements. Unlike the “paid-for” disclaimers, they will say these requirements affect the recipient’s first impressions of the speech, thereby enabling recipients to ignore political emails in a way that they can’t with a TV or radio ad. This argument is accurate: one of the main goals of this policy would be to make fundraising emails easier to ignore. That, however, does not make the policy unconstitutional. Disclaimer requirements can be constitutional even if they lower the effectiveness of the ads to which they are attached. For example, in *Citizen’s United v. FEC*,¹⁵⁷ the petitioner argued that a disclaimer law was unconstitutional because it “decrease[d] both the quantity and effectiveness of the group’s speech by forcing it to devote four seconds of each advertisement to the spoken disclaimer.”¹⁵⁸ The Court rejected this argument.¹⁵⁹ The Court reasoned that certain requirements “may burden the ability to speak,”¹⁶⁰ but, as long as they “impose no ceiling on campaign-related activities . . . and do not prevent

153. 11 C.F.R. § 110.11(b)(3) (2024).

154. *Doe v. Reed*, 561 U.S. 186, 196 (2010) (citing *Citizens United v. Fed. Election Comm’n*, 558 U.S. 310, 366–67 (2010)).

155. *See McConnell v. Fed. Election Comm’n*, 540 U.S. 93, 197 (2003) (quoting *McConnell v. Fed. Election Comm’n*, 251 F. Supp. 2d 176, 237 (D.D.C.), *rev’d in part*, 540 U.S. 93 (2003)).

156. *See Citizens United*, 558 U.S. at 367 (quoting *McConnell*, 540 U.S. at 197).

157. 558 U.S. 310 (2010) (upholding a law requiring that mass media ads disclose the identity of the “payer”).

158. *Id.* at 368.

159. *Id.*

160. *Id.*

anyone from speaking,” they will receive no more than exacting scrutiny.¹⁶¹ This is a strong defense for the sender and subject line requirements: though they would likely make political spam less effective, they would place no ceiling on the quantity of speech—thereby avoiding the pitfall of the *Buckley* expenditure limits—nor would they prevent anyone from speaking.

Opponents may retort that these policies, by enabling recipients to effectively block all political communication from their inboxes, are no different from restricting speech at its source and that, therefore, strict scrutiny should apply. This is not a winning argument. Giving people the option to ignore a speaker does not violate that speaker’s First Amendment rights. The Constitution guarantees a person the right to stand in the public square and speak about nearly anything they wish, but it will not force others to stop and listen.

D. *Nonconstitutional Concerns with Back-End Regulation*

The Constitution, of course, is not the only barrier to the successful implementation of these policies. Another is the feasibility of administering them. The sender requirement would require a federal agency—likely the Federal Trade Commission, since it is already in charge of administering the CAN-SPAM Act¹⁶²—to maintain a registry of each sender’s designated name. Agencies or, if they wish, the lawmakers themselves, will need to make tricky decisions, such as whether the same name can be used by multiple organizations, how to prevent organizations from acquiring misleading names, and if, or how often, an organization can change the sender name it uses. For the subject line requirement, lawmakers will need to give guidance on what counts as an advertising or fundraising email. For both requirements, the agency will need to ensure compliance in an area—cyberspace—that is far too broad for it to monitor alone.

These are hard problems, but they are not insurmountable. Regarding the name registry, trademark law would provide a good starting point, and agencies should have little trouble developing coherent rules for what sender names are “substantially similar” to their names of incorporation. Under these rules, “The Committee to Elect George Costanza” could not register as “Art Vandelay,” but it could register as “the Costanza Campaign.”¹⁶³ With regard to defining “political,” “advertising,” or “fundraising” email, lawmakers and, if necessary, courts, can look to other legal doctrines that have already defined these terms,

161. *Id.* (first quoting *Buckley v. Valeo*, 424 U.S. 1, 64 (1976); then quoting *McConnell*, 540 U.S. at 201).

162. 15 U.S.C. § 7706.

163. *See Seinfeld: The Stake Out* (NBC television broadcast May 31, 1990).

or they could adopt a type of “predominant purpose” test from contract law.¹⁶⁴ Regarding enforcement, it is true that no agency could scrutinize every political email. In fact, due to privacy concerns, we might prefer that agencies not have such capacity. That is why it would be important for the agency to set up an easy reporting system and, if necessary, offer bounties to people who do report. One defining aspect of mass email is that it goes to a lot of people—people who would be willing to turn in offenders, especially if they are particularly annoyed by the volume of spam and *especially* if they could receive a reward for doing so.¹⁶⁵

Of course, this enforcement regime will have cracks. One cannot expect the true outlaw spammers—those peddling outright scams and phishing schemes—to start putting “ADV” in their subject lines *en masse*, no matter how severe the penalties. However, the perfect should not be the enemy of the good. With even moderate enforcement, most legitimate campaigns and political organizations will comply, just as they have with existing disclaimer laws.¹⁶⁶ They have too much on the line—and too many opponents waiting to pounce on any misstep—to do otherwise.

CONCLUSION

The political email industry is trapped in a race to the bottom. Unfortunately, misleading and annoying tactics work, so very few political campaigns or organizations would willingly forgo those tactics (and the millions of dollars they rake in). To do so would be to unilaterally disarm, putting their candidates and causes at an extreme disadvantage. In addition, recipients alone will never force campaigns to change their ways. Campaigns know that only a fraction of recipients will unsubscribe, and the ones that do will still end up voting their way on election day.

This situation calls for government action.

There are many forms this action could, and should, take, most of which are beyond the scope of this Comment. For example, privacy laws should be bolstered so that personal data cannot be so freely traded between campaigns and organizations. Election laws should be amended so that email “swaps” count

164. See Gary D. Spivey, Annotation, *Applicability of UCC Article 2 to Mixed Contracts for Sale of Business Goods and Services: Manufacturing, Construction, and Similar Contracts*, 15 A.L.R.7th Art. 7 (2016).

165. One advantage of the back-end regulations compared to the do-not-email registry is that, for the back-end regulations, more people would be able to report violations. Whereas enforcement of the registry would depend on those who registered to report violations, anyone with access to the emails could report an organization for using a misleading name.

166. For proof that campaigns and political organizations do comply with existing disclaimer laws (and therefore would presumably comply with new disclaimer laws), see *All Messages*, *supra* note 70. In a random sample of emails, most, if not all, will include a “paid for” disclaimer at the bottom.

as contributions and are regulated as such.¹⁶⁷ The content of the emails themselves should, to whatever degree is constitutional, be monitored so that fake matches,¹⁶⁸ surveys,¹⁶⁹ and “membership” campaigns are snuffed out.¹⁷⁰ If possible, front-end regulation, like prohibiting mass email to anyone who has not affirmatively opted in, or implementing a do-not-email registry, should be pursued.¹⁷¹

However, the solution policymakers should pursue first is the one at the nexus of what is possible and what is effective: “back-end” regulation to make political emails more recognizable. While this solution would not directly decrease the quantity of new emails, it would make those emails easier to deal with, and it would lessen the likelihood of people being scammed. It is true that, by enabling people to ignore political emails more easily, the sender and subject line requirements would decrease the visibility and effectiveness of certain political communication. But this is a loss that few will mourn. If political spammers’ best argument against these regulations is that, if the spammers could not trick people into opening their emails, then nobody would open them, maybe that’s an admission that these emails are closer to fraud than they are to valuable political discourse.

ALEX SLAWSON**

167. *See supra* note 22 and accompanying text.

168. *See supra* note 26 and accompanying text.

169. *See supra* notes 92–94 and accompanying text.

170. *See supra* note 27 and accompanying text.

171. *See supra* Section II.A.

** J.D. Candidate, North Carolina School of Law, 2024. I want to thank Rachel Jones and Steven Constantin for their editorial guidance, Professor William Marshall for his insights on the First Amendment, and Anna Fraser for her love and support. I also want to thank my former colleagues in the digital fundraising industry. I’m proud to have worked with you. I hope the laws change soon, but until they do, “send a lot of emails, raise a lot of money.”

APPENDIX A

The author:

Write a political fundraising email in the style of Joe Biden. Please include common talking points, including the right to an abortion. Please also include that all gifts will be matched.

ChatGPT:

Subject: Stand with Joe: Defend Our Values Together

Dear [Recipient's Name],

I hope this message finds you and your loved ones in good health and high spirits. It's been a challenging time for our nation, but I know that when we come together, there's nothing we can't overcome. That's why I'm reaching out to you today.

As we look ahead, we face critical battles on the horizon. The values we hold dear, the progress we've made, and the future we envision for our country are at stake. But I firmly believe that, with your support, we can stand strong and protect the principles that define us as a nation.

First and foremost, we must safeguard the right to make our own healthcare choices. This includes ensuring that every person has the right to make decisions about their own body. I've always been a staunch supporter of a woman's right to choose, and I will continue to fight to protect and expand this fundamental right. Our daughters, sisters, mothers, and friends deserve nothing less than the full autonomy to make the best choices for their health and future.

But we can't do it alone. We need your help to make a difference. Today, I'm excited to announce that every gift you make will be matched, doubling the impact of your contribution. Your support will help us defend our values, protect our rights, and build a brighter future for all Americans.

Whether it's preserving access to healthcare, combating climate change, strengthening our economy, or advancing civil rights, your contribution will

2024]

POLITICAL SPAM

1255

play a crucial role in our efforts. Together, we can continue the work of building a more just, equitable, and inclusive America.

Please consider making a donation today. Your generosity will not only support our campaign but also send a powerful message that we are united in our commitment to a better tomorrow.

[Donate Button]

Thank you for your unwavering support. Together, we can overcome any challenge and shape a future that reflects the best of who we are as a nation.

With hope and determination,

Joe Biden

P.S. Don't forget, every gift you make today will be matched, so your impact will be twice as powerful. Please contribute now to help us defend our values and protect our rights.

[Contribute Now Button]

The author:

Please write an email in the voice of Joe Biden based on this outline:

- This is urgent. If we don't win, Democracy is at stake
 - Right now, I'm behind in the polls and behind in fundraising
 - I need your help. Donate now, and your gift will be doubled.
 - There are so many important issues at stake, such as . . .
 - If we can't hit this fundraising deadline, we won't be able to fight for these issues.
 - Donate now
-

ChatGPT:

Subject: Urgent: Democracy at Stake - I Need Your Help

Dear [Recipient's Name],

I hope this message finds you well, but I need to be frank from the start. Our democracy is facing an unprecedented challenge, and the stakes couldn't be higher. Right now, we're up against a critical moment in our nation's history, and we can't afford to lose.

I'll be honest; I'm behind in the polls, and we're falling short in fundraising. This is not where we want to be, and I need your help to turn the tide. Time is running out, and every moment counts.

Our campaign stands for so much—important issues that affect the lives of every American. We're fighting for affordable healthcare, meaningful action on climate change, a fair economy that works for everyone, and so much more. But without the resources to back our vision, these vital issues hang in the balance.

This is where you come in. I need you to step up and make a donation right now. The urgency cannot be overstated, and to make it even more impactful, every dollar you give will be matched, effectively doubling your contribution.

[Donate Now]

If we can't hit this critical fundraising deadline, we won't have the means to fight for these issues that matter deeply to you and countless others across the nation. We can't let that happen.

Your support isn't just about helping me win; it's about preserving our democracy and making sure that our values and priorities guide our country's future.

So, please, don't wait. Donate now, and let's ensure that our democracy thrives, our values prevail, and our nation moves forward together.

With gratitude and determination,

Joe Biden

The author:

Could you shorten that?

2024]

POLITICAL SPAM

1257

Chat GPT:

Subject: Urgent: Democracy in Peril - I Need Your Help

Dear [Recipient's Name],

Our democracy is at risk, and I'm reaching out with urgency. I'm trailing in the polls and falling short in fundraising.

We're fighting for crucial issues like healthcare, climate action, and economic fairness, but we're running out of time and resources. Without your help, we can't win these battles.

Donate now, and your gift will be doubled. We can't afford to miss this critical deadline.

[Donate Now]

Your support isn't just about my campaign; it's about protecting our democracy and the values we hold dear.

Please act now. Democracy is on the line.

With gratitude,

Joe Biden

