

ROBOCALLS HAVE BEEN BLOCKED, BUT BUSINESSES CAN-SPAM EMAILS WITH LITTLE REGULATION

INTRODUCTION

As the Supreme Court stated in the 2020 case *Barr v. American Association of Political Consultants*, “Americans passionately disagree about many things. But they are largely united in their disdain for robocalls.”¹ Americans are similarly united in their disdain for spam emails.² However, Congress’s regulation of spam emails through the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) fails to protect vulnerable constituents in the same way the Telephone Consumer Protection Act (TCPA) protects from robocalls.³

Using the TCPA, *Barr*, and other commercial speech cases as illuminating precedent, this Note focuses on the future of spam email and spam social media message (“social spam”) regulation. In Part I, this Note discusses the text and background of the TCPA and CAN-SPAM, relevant litigation, spam-related consumer harms, and emerging social spam concerns.⁴

In Part II, this Note analyzes CAN-SPAM’s performance since its enactment. This Note argues CAN-SPAM has failed to protect consumers from spam emails and the emergence of social spam on several grounds.⁵ First, CAN-SPAM gives businesses too much leeway, which they have consistently abused. Second, CAN-SPAM lacks an expanded private right of action. Third, CAN-SPAM does not have a “do not email” registry. Fourth, CAN-SPAM allows non-commercial spam. Fifth, CAN-SPAM’s preemption provision prevents states from taking further steps in regulating spam emails. Sixth, CAN-SPAM is outdated and needs significant amendments to regulate social spam.

1. 140 S. Ct. 2335, 2343 (2020); see *infra* notes 36–40 and accompanying text.

2. See Geoffrey A. Fowler, *The Three Worst Things About Email, and How to Fix Them*, WASH. POST (July 21, 2020), <https://www.washingtonpost.com/technology/2020/07/21/gmail-alternative-hey/> [<https://perma.cc/C96L-7UG3>] (“Apologies if you’ve been waiting for an email from me. My Gmail has 17,539 unread messages. Raise your hand if you have even more. For many, Gmail accounts have become less communication space and more of an endless pile Google gets to snoop through.”).

3. See Vivek Arora, Note, *The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem*, 39 COLUM. J.L. & SOC. PROBS. 299, 300 (2006); Rebecca Bolin, Note, *Opting Out of Spam: A Domain Level Do-Not-Spam Registry*, 24 YALE L. & POL’Y REV. 399 (2006); Jasmine E. McNealy, *Spam and the First Amendment Redux: Free Speech Issues in State Regulation of Unsolicited Email*, 22 COMM. L. & POL’Y 351 (2017); David J. Rutenburg, Note, *Silence of the Spam: Improving the CAN-SPAM Act by Including an Expanded Private Cause of Action*, 14 VAND. J. ENT. & TECH. L. 225 (2011).

4. See *infra* Part I.

5. See *infra* Part II.

In Part III, this Note proposes that a new federal law needs to replace CAN-SPAM to effectively regulate spam emails and social spam.⁶ Utilizing the TCPA as a model, the new law should incorporate some current provisions of CAN-SPAM and add specialized regulations for social spam. The new law should include a provision which states that advertising emails, solicited and unsolicited alike, must include information on how the advertiser obtained the consumer's email address. This legislative solution must be content-neutral in accordance with the commercial speech regulation test in *Central Hudson Gas & Electric Corp. v. Public Service Commission*⁷ and abide by the ruling in *Barr*.

Finally, in Part IV, this Note concludes by reemphasizing the need for a new federal law regulating spam emails and social spam.⁸ If more media coverage and public interest arises, members of the Senate Commerce Subcommittee on Communications, Media, and Broadband should capitalize on the opportunity to ease this evolving burden on consumers.

I. BACKGROUND

Before delving into the compelling history of CAN-SPAM and spam regulation in the United States, it is crucial to understand the TCPA's legislative inception, impact, and interpretation. The parallels between the TCPA and CAN-SPAM go beyond the historical similarities, and the TCPA provides solid footing as model legislation for a new federal law replacing CAN-SPAM.

A. TCPA

In 1991, Congress passed the TCPA in response to "a torrent of vociferous consumer complaints about intrusive robocalls. A growing number of telemarketers were using equipment that could automatically dial a telephone number and deliver an artificial or prerecorded voice message."⁹ The TCPA was enacted to "prevent[] businesses from shifting their advertising costs to the recipients of unsolicited fax advertisements; discourag[e] and prevent[] unsolicited advertisements over the telephone

6. See *infra* Part III.

7. 447 U.S. 557 (1980).

8. See *infra* Part IV.

9. *Barr v. Am. Ass'n of Pol. Consultants*, 140 S. Ct. 2335, 2344 (2020); see also John C. Spiller, 35 FCC Rcd. 5948 (7) (2020) ("In enacting the Telephone Consumer Protection Act (TCPA), Congress determined that unwanted prerecorded voice message calls are a greater nuisance and invasion of privacy than live calls and that such calls delivered via wireless phones can be costly.").

lines; protect[] individual's privacy in their homes; and provid[e] a remedy to consumers for telemarketing abuses.”¹⁰

With the help of the Federal Communications Commission's (FCC's) power to create and implement rules, the TCPA prohibits robocalls to wireless telephone numbers unless the wireless consumer gives prior consent or the robocall is made for emergency purposes.¹¹ The TCPA also prohibits telemarketing calls to residential numbers listed on the National Do Not Call Registry and requires robocalls to identify “the entity responsible for initiating the prerecorded voice message call” at the beginning of the message.¹² The responsible entity must provide a telephone number so that the consumer who was called can make a do-not-call request either during or after the robocall.¹³ The TCPA also “restrict[s] the hours during which a telephone solicitor may call a consumer's residence (not prior to 8 a.m. or after 9 p.m.)”¹⁴

The TCPA has evolved through multiple legislative amendments. In 2015, Congress amended the TCPA to “allow[] robocalls that are made to collect debts owed to or guaranteed by the Federal Government, including robocalls made to collect many student loan and mortgage debts.”¹⁵ Essentially, this was a government-backed debts amendment. In 2019, Congress amended the TCPA again through the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED).¹⁶ TRACED “required the FCC to mandate the STIR/SHAKEN¹⁷ caller identification framework,” which “[r]equire[ed] voice service providers to

10. Eric C. Surette, Annotation, *Validity, Construction and Application of Telephone Consumer Protection Act* (47 U.S.C. § 227)—*State Cases*, 77 A.L.R.6th 1 § 2 (2012).

11. See 47 U.S.C. § 227(b)(1) (1991). In a declaratory ruling, the FCC held calls relating to the COVID-19 pandemic may qualify as made for emergency purposes. Rules and Regs. Implementing the Tel. Consumer Prot. Act of 1991, 35 FCC Rcd. 2840 (4) (2020). For a call to qualify:

First, the caller must be from a hospital, or be a health care provider, state or local health official, or other government official as well as a person under the express direction of such an organization and acting on its behalf. Second, the content of the call must be solely informational, made necessary because of the COVID-19 outbreak, and directly related to the imminent health or safety risk arising out of the COVID-19 outbreak.

Id. (emphasis in original).

12. John C. Spiller, 35 FCC Rcd. 5948 (7), 5949 (2020); see also 47 U.S.C. § 227(d)(3)(A) (1991).

13. See 47 U.S.C. § 227(d)(3)(A) (1991).

14. Surette, *supra* note 10, at § 2; 47 U.S.C. § 227.

15. Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335, 2343 (2020).

16. Pallone-Thune TRACED Act, Pub. L. No. 116-105, 133 Stat. 3276 (2019) (codified as amended in scattered sections of 47 U.S.C.).

17. “STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards. This means that calls traveling through interconnected phone networks would have their caller ID ‘signed’ as legitimate by originating carriers and validated by other carriers before reaching consumers.” *Combating Spoofed Robocalls with Caller ID Authentication*, FCC, <https://www.fcc.gov/call-authentication> [<https://perma.cc/9XDY-VDFD>].

adopt call authentication technologies, enabling a telephone carrier to verify that incoming calls are legitimate before they reach consumers' phones."¹⁸ As a result, major carriers, including "AT&T, Sprint, T-Mobile, U.S. Cellular, and Verizon, have [implemented] services that alert [consumers] that an incoming robocall may be" spam.¹⁹ Also, TRACED "gives the FCC more time to take action against robocallers and fine them for up to \$10,000 per call."²⁰

Since its passage, the TCPA has been the subject of a considerable amount of litigation. In *Destination Ventures, Ltd. v. FCC*,²¹ the Ninth Circuit upheld the constitutionality of the TCPA.²² The Ninth Circuit applied the Supreme Court's commercial speech test from *Central Hudson*:

- (1) whether the speech is protected, that is, not false or deceptive; (2) if the speech is protected, whether the government has a substantial interest in regulating the kind of speech; (3) whether the regulation advances that government interest; and (4) whether the regulation is tailored to serve the government interest.²³

The test falls under the intermediate scrutiny standard.²⁴ In *Destination Ventures*, plaintiffs challenged the TCPA's provision "banning unsolicited

18. *TRACED Act Implementation*, FCC (Nov. 5, 2021), <https://www.fcc.gov/TRACEDAct> [<https://perma.cc/9JF3-3EV4>]; see also Press Release, Sen. John Thune, Thune, Markey Reintroduce Bill to Crack Down on Illegal Robocall Scams (Jan. 17, 2019), <https://www.thune.senate.gov/public/index.cfm/2019/1/thune-markey-reintroduce-bill-to-crack-down-on-illegal-robocall-scams> [<https://perma.cc/H8T9-XGJU>]; Paul C. Besozzi, *FCC To Review TCPA Regulatory Exemptions Per Traced Act*, NAT'L L. REV. (Oct. 5, 2020), <https://www.natlawreview.com/article/fcc-to-review-tcpa-regulatory-exemptions-traced-act> [<https://perma.cc/PE9C-P3H4>] ("More specifically, Section 8 requires that 'any such exemption contain requirements with respect to: '(i) the classes of parties that may make such calls; (ii) the classes of parties that may be called; and (iii) the number of such calls that a calling party may make to a particular called party.'").

19. Octavio Blanco, *Relief from Spoofed Robocalls Is on the Way: The Telecom Industry Says that New Technology to Manage Robocalls Will Start Rolling out Next Year*, CONSUMER REPS. (Nov. 7, 2018), <https://www.consumerreports.org/robocalls/spoofed-robocalls-relief-is-on-the-way/> [<https://perma.cc/QT5R-2T9D>] ("The technology, called 'SHAKEN/STIR,' wouldn't stop the calls but would ID them as potentially fraudulent so that you can decide whether to answer. The new system would work on both landline and cell phones.").

20. Mike Snider, *Robocalls Rang Up a New High in 2019. Two or More Daily Is Average in Some States*, USA TODAY (Jan. 15, 2020, 9:44 AM), <https://www.usatoday.com/story/tech/2020/01/15/robocalls-americans-got-58-5-billion-2019/4476018002/> [<https://perma.cc/4GPZ-2Y9J>].

21. 46 F.3d 54 (9th Cir. 1995).

22. *Id.* at 56–58.

23. McNealy, *supra* note 3, at 357 ("The Court revised the fourth prong of the *Central Hudson* test in *Board of Trustees v. Fox*, allowing a regulation of commercial speech that reasonably fit the government interest. Legislatures would be the best judge of what regulation best fit its interest."); see also *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n*, 447 U.S. 557, 565 (1980); Arora, *supra* note 3, at 304.

24. See Arora, *supra* note 3, at 304.

faxes that contain advertisements.”²⁵ The plaintiffs, Destination Ventures, did not dispute the first part of the *Central Hudson* test, that the speech is protected, or the second part of the test, that Congress had a substantial government interest in regulating robocalls and unsolicited faxes and “preventing the shifting of advertising costs to consumers.”²⁶ Destination Ventures challenged the third and fourth parts of the *Central Hudson* test—that a regulation advance a substantial government interest and be narrowly tailored—by arguing the TCPA was not a “reasonable fit” between the substantial government interest and the ban on unsolicited fax advertisements.²⁷ The Ninth Circuit disagreed, finding that because Congress’s goal in passing the TCPA was partially “to prevent the shifting of advertising costs, limiting its regulation to faxes containing advertising was justified,” and the TCPA was “evenhanded, in that it applies to commercial solicitation by any organization, be it a multinational corporation or the Girl Scouts.”²⁸

In *Moser v. FCC*, the Ninth Circuit again upheld the constitutionality of the TCPA, holding the statutory ban on prerecorded telemarketing calls was content-neutral and did not violate appellees’ free speech rights.²⁹ Under free speech analysis, Congress “may impose reasonable restrictions on the time, place, or manner of protected speech,” as long as the restrictions are (1) “justified without reference to the content of the restricted speech,” (2) “narrowly tailored to serve a significant governmental interest,” and (3) they “leave open ample alternative channels for communication of the information.”³⁰ Once again, the substantial interest in regulating robocalls and protecting “residential privacy” was not challenged.³¹ Instead, plaintiffs challenged whether the TCPA was narrowly tailored and whether it left open alternative channels.³² The Ninth Circuit concluded that the TCPA was narrowly tailored, holding that “Congress may reduce the volume of intrusive telemarketing calls without completely eliminating the calls.”³³ The court also found that Congress had considered adequately less

25. *Destination Ventures*, 46 F.3d at 55.

26. *Id.* at 56.

27. *Id.* “Specifically, [Destination Ventures] contends that the government has not shown that faxes containing advertising are any more costly to consumers than other unsolicited faxes such as those containing political or ‘prank’ messages.” *Id.* Destination Ventures’ viewpoint was that “Congress may not single out advertisements for regulation when other types of unsolicited faxes produce the same cost-shifting.” *Id.*

28. *Id.*

29. 46 F.3d 970 (9th Cir. 1995).

30. *Id.* at 973 (quoting *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984)).

31. *Id.* at 974.

32. *See id.*

33. *Id.* at 975.

restrictive alternatives.³⁴ The Ninth Circuit concluded the TCPA did leave open alternative channels, “including the use of taped messages introduced by live speakers or taped messages to which consumers have consented, as well as all live solicitation calls.”³⁵

In *Barr*, the Supreme Court held the 2015 government-backed debts amendment to the TCPA violated the First Amendment and was severable from the rest of the TCPA.³⁶ The legality of the 2015 amendment turned on whether a robocall “made solely to collect a debt owed to or guaranteed by the United States” is a content-neutral provision.³⁷ The government made three arguments to convince the court the provision was content-neutral: (1) the provision simply draws a distinction between speakers (authorized debt collectors versus others), (2) the provision depends on if a caller is engaged in certain economic activities (owing debt to the government), and (3) if the provision is invalidated it could mean other statutes that regulate government debt are invalid.³⁸ The Supreme Court was not persuaded by any of the government’s three arguments. The Court reasoned that (1) a speaker based distinction does not automatically make the distinction content-neutral, (2) the provision focuses on the caller speaking about a particular economic activity, not the economic activity itself, and (3) “courts have generally been able to distinguish impermissible content-based speech restrictions from traditional or ordinary economic regulation of commercial activity that imposes incidental burdens on speech.”³⁹ Ultimately, the Court held the provision unconstitutional “[b]ecause the law favors speech made for collecting government debt over political and other speech, [so] the law is a content-based restriction on speech.”⁴⁰

34. *Id.* (“Congress considered and rejected less restrictive forms of regulation, including a bill that would have required solicitors to give their names, addresses, and phone numbers in their messages and to use machines with certain disconnect features.”).

35. *Id.* (“That some companies prefer the cost and efficiency of automated telemarketing does not prevent Congress from restricting the practice.”).

36. See *Barr v. Am. Ass’n of Pol. Consultants*, 140 S. Ct. 2335, 2343 (2020) (“Applying traditional severability principles, seven Members of the Court conclude that the entire 1991 robocall restriction should not be invalidated, but rather that the 2015 government-debt exception must be invalidated and severed from the remainder of the statute.”).

37. *Id.* at 2346.

38. See *id.* at 2346–47.

39. *Id.* at 2347.

40. *Id.* at 2346 (“A robocall that says, ‘Please pay your government debt’ is legal. A robocall that says, ‘Please donate to our political campaign’ is illegal. That is about as content-based as it gets.”). A content-based law is subject to strict scrutiny, and the Government conceded that it could not satisfy that standard. “The Government’s stated justification for the government-debt exception is collecting government debt.” *Id.* at 2347. While maintaining that collecting government debt was a “worthy goal, the Government concede[d] that it ha[d] not sufficiently justified the differentiation between government-debt collection speech and other important categories of robocall speech, such as political speech, charitable fundraising, issue advocacy, commercial advertising, and the like.” *Id.*

Since the TCPA has been constitutionally upheld, the FCC has proposed and issued declaratory rulings imposing fines on violators. In June 2020, the FCC proposed a \$225 million dollar fine against Rising Eagle, a Texas-based telemarketer that apparently made over 1 billion health insurance sales robocalls to American consumers, including many on the Do Not Call registry.⁴¹ The uncontroverted factual background of the case exemplifies the continuing problem that robocalls pose to consumers. Rising Eagle made robocalls to sell “short-term, limited-duration health insurance plans” on behalf of its clients, like Health Advisors of America.⁴² “The prerecorded messages falsely implied that Rising Eagle and/or its clients were associated with well-known American health insurance companies like Blue Cross Blue Shield and Cigna.”⁴³ The company used spoofed numbers and took affirmative actions to direct the calls to consumers who put their names and numbers on the Do Not Call registry because those “consumers enhanced [the] business.”⁴⁴ Some calls included the following message:

Are you looking for affordable health insurance with benefits from a company you know? Policies have all been reduced nationwide such as Cigna, Blue Cross, Aetna, and United[,] just a quick phone call away. Press 3 to get connected to a licensed agent or press 7 to be added to the Do Not Call list.⁴⁵

If the consumer did press 3, the call would instead be transferred to a representative trying to sell them insurance from one of Rising Eagle’s clients.⁴⁶

These robocalls have the potential to drastically disrupt the lives of consumers. One victim commented, “I am disabled and elderly. I continue to receive repeated calls from this same caller. They call 2-3 times per day. I sometimes fall when trying to get to the phone. . . . Can’t hardly take it anymore. Can’t get my rest.”⁴⁷ Another victim described how they did the only thing they could do to stop the harassment by saying, “I took my phone off the hook for 3 days because I didn’t want to here [sic] their annoying calls anymore, otherwise I would have had twice this amount of disgusting numbers.”⁴⁸ Yet another victim described the helpless feeling they had by saying, “I have requested at least 15 times to be placed on a do not call list. I get relentless calls, maybe 15-20 a day from masked numbers. I’ve

41. See John C. Spiller, 35 FCC Rcd. 5948 (7), 5948 (2020).

42. *Id.* at 5956.

43. *Id.* at 5949.

44. *Id.* at 5950.

45. *Id.* at 5951 (alteration in original).

46. See *id.*

47. *Id.* at 5952.

48. *Id.* (alteration in original).

reported many of them to the DNC registry, but it hasn't even slowed down let alone stopped.”⁴⁹ Finally, these robocalls also disrupted the businesses who were spoofed, including Genworth North America Corporation, which was unable to use its network system because “it was inundated with so many callbacks from angry consumers.”⁵⁰

Despite the TCPA, its amendments, and its regulation from the FCC, robocalls have not been eradicated. Before it was enacted “more than 300,000 solicitors called more than 18 million Americans every day.”⁵¹ In 2019, “First Orion estimate[d] 50 percent of all mobile phone traffic [was] robocalls or spam” and consumers received “167.3 million robocalls a day, or 1,936 robocalls every second.”⁵² But as of June 30, 2021, when the TRACED Act's STIR/SHAKEN deadline took effect, the TCPA's structure and the FCC's implementation seem to be working well and robocalls are “actually on the decline.”⁵³

B. CAN-SPAM

Spam emails have a similar ability to disrupt the lives of consumers, but the TCPA offers no relief. In 2003, the FCC made clear that the TCPA does not apply to spam emails.⁵⁴ The order left open the possibility of allowing facsimile messages sent as emails; however, in a 2017 declaratory ruling,

49. *Id.*

50. *Id.* at 5953.

51. Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335, 2344 (2020).

52. Jake Swearingen, *The Beginning of the End of Robocalls*, INTELLIGENCER (Feb. 14, 2019), <https://nymag.com/intelligencer/2019/02/the-beginning-of-the-end-of-robocalls.html> [<https://perma.cc/KQT6-2GGV>]; see also Snider, *supra* note 20 (“Texas and California got the most robocalls in 2019, more than 6 billion. Seven other states (Florida, Georgia, New York, Ohio, Pennsylvania, North Carolina and Illinois) got more than 2 billion robocalls.”).

53. Octavio Blanco, *The Best Ways to Block Robocalls: Unwanted Calls Declined Further in August as Carriers Roll Out Blocking Technology*, CONSUMER REPS. (Feb. 25, 2021), <https://www.consumerreports.org/robocalls/the-best-ways-to-block-robocalls-a1048700708/> [<https://perma.cc/LA6G-7K7P>] (“In August the number of robocalls received in the U.S. dropped by 4.4 percent from the previous month . . . By June 30, a deadline imposed by the TRACED Act, all carriers had to certify in a Federal Communications Commission database that they had begun implementing the technology across their networks.”); YouMail Inc., *U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index*, PRNEWswire (Jan. 6, 2022, 9:00 AM), <https://www.prnewswire.com/news-releases/us-phones-were-hit-by-more-than-50-billion-robocalls-in-2021-says-youmail-robocall-index-301455319.html> [<https://perma.cc/WW2B-7G8P>] (“The good news is that monthly robocalls continue to be on a lower plateau since the STIR/SHAKEN rollout on June 30th,” said YouMail CEO Alex Quilici. “The bad news is that total robocalls still exceeded 50 billion for the year, which is roughly 200 robocalls this year for every adult with a phone.”).

54. See Rules and Regs. Implementing the Tel. Consumer Prot. Act (TCPA) of 1991, 68 Fed. Reg. 44143, 44170 (July 25, 2003), (codified at 47 C.F.R. pt. 64, 68) (“We conclude that faxes sent to personal computers equipped with, or attached to, modems and to computerized fax servers are subject to the TCPA's prohibition on unsolicited faxes. However, we clarify that the prohibition does not extend to facsimile messages sent as email over the Internet.”).

the FCC reaffirmed the 2003 order and closed the door on the possibility of allowing facsimile messages to be regulated by the TCPA.⁵⁵ The petitioner in the declaratory ruling, Amerifactors, argued that facsimile messages sent as emails should not be regulated by the TCPA because for the four following reasons:

(1) [O]nline fax services do not fit within the plain meaning of the TCPA's prohibition on conventional faxes; (2) online faxes do not result in the type of harm the Congress sought to avoid in the TCPA; (3) a declaratory ruling here would be a first step toward curbing abusive litigation practices; and (4) applying the TCPA to faxes received on a device other than a telephone facsimile machine would be an impermissible restriction on commercial speech in violation of the First Amendment.⁵⁶

The FCC agreed with Amerifactors' arguments and added that "[c]onsumers can manage those [facsimile] messages" sent as emails "by blocking senders or deleting incoming messages without printing them."⁵⁷

In 2001, Congress passed CAN-SPAM in response to "a substantial government interest in regulation of commercial electronic mail on a nationwide basis."⁵⁸ CAN-SPAM was enacted partially because "[t]he receipt of a large number of unwanted messages . . . decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost . . . thus reducing the reliability and usefulness of electronic mail to the recipient."⁵⁹ Legislators were also concerned that "[s]ome commercial electronic mail contains material that many recipients may consider vulgar or pornographic in nature."⁶⁰

55. See Amerifactors Fin. Grp., 34 FCC Rcd. 11950 (15) (2019).

56. *Id.* at 2.

57. *Id.* at 4.

58. 15 U.S.C. § 7701(b) (2003).

59. *Id.* § 7701(a)(4).

60. *Id.* § 7701(a)(5); Legislators also found:

The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic, up from an estimated 7 percent in 2001, and the volume continues to rise. Most of these messages are fraudulent or deceptive in one or more respects. The receipt of unsolicited commercial electronic mail may result in costs to recipients who cannot refuse to accept such mail and who incur costs for the storage of such mail, or for the time spent accessing, reviewing, and discarding such mail, or for both. . . . Many senders of unsolicited commercial electronic mail purposefully disguise the source of such mail. Many senders of unsolicited commercial electronic mail purposefully include misleading information in the messages' subject lines in order to induce the recipients to view the messages.

Id. § 7701(a)(2)–(3), (7)–(8).

CAN-SPAM has three main requirements:

- (1) it prohibits commercial advertisement e-mail senders from deceiving recipients about the 'source or subject matter of their e-mail';
- (2) it requires that all senders provide and comply with an opt-out mechanism in their e-mails that allows recipients to choose to stop receiving e-mail from a particular sender; and
- (3) it requires all senders of unsolicited commercial e-mail to provide 'a valid physical address' and proper notification that the message is an advertisement.⁶¹

It also requires that spammers place warning labels on commercial electronic mail containing sexually oriented material.⁶²

CAN-SPAM is constitutional under the *Central Hudson* test. First, the speech to be regulated is protected.⁶³ Second, there is a substantial government interest for CAN-SPAM because there is broad consumer concern and "interest in trying to reduce the costs and burdens spam imposes on the e-mail system."⁶⁴ Third, CAN-SPAM advances the government's interest "because it regulates only commercial spam" and it directly tries to "eliminate the problems" that spam emails impose on consumers.⁶⁵ Fourth, CAN-SPAM is narrowly tailored "because it does not create any blanket prohibition of speech."⁶⁶

While less often than the TCPA, CAN-SPAM has also been the subject of litigation since its passage. Some of the litigation focuses on how CAN-SPAM expressly preempted state attempts at regulating the spam problem. The Fourth and the Ninth Circuit Courts of Appeals have held that if a state

61. Arora, *supra* note 3, at 300; 15 U.S.C. §§ 7701–7713 (2003).

62. See 15 U.S.C. § 7704(d).

63. See Arora, *supra* note 3, at 303, 305.

64. *Id.* at 305 ("When enacting the CAN-SPAM Act, Congress listed specific costs and burdens that spam creates. Such burdens include the costs for storing such mail, the chance that 'wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages,' and significant monetary costs on ISPs and businesses.").

65. *Id.* at 305–06. "Because most of these problems result from commercial spam, a regulation focused solely on commercial spam still satisfies this requirement." *Id.* at 306. As the Tenth Circuit has stated, "'First Amendment challenges based on underinclusiveness face an uphill battle in the commercial speech context. As a general rule, the First Amendment does not require that the government regulate all aspects of a problem before it can make progress on any front.'" *Id.* at 306 (quoting *Mainstream Mktg. v. FTC*, 358 F.3d 1228, 1238 (10th Cir. 2004)).

66. *Id.* ("Rather, it allows recipients to protect themselves from receiving unwanted e-mails. Courts have upheld similar restrictions with respect to do-not-mail regulations and the do-not-call registry.").

regulation causes confusion about the state of the law, then CAN-SPAM preempts the anti-spam statute.⁶⁷ In *Jaynes v. Commonwealth of Virginia*, the Virginia Supreme Court held that the state legislature's unsolicited email provision was unconstitutional.⁶⁸ Complicating the state preemption issue further, the Fifth Circuit upheld the constitutionality of a university's spam regulation in *White Buffalo Ventures, LLC v. University of Texas*,⁶⁹ ruling that "although the university's spam regulation could be considered a state regulation, Texas could be considered an Internet Service Provider and, therefore, exempt from preemption under CAN-SPAM."⁷⁰

One of the more famous CAN-SPAM perpetrators, Sandford Wallace, also known as "Spamford Wallace" and the "Spam King," "was sentenced to two and a half years in federal prison after pleading guilty to one count of fraud" in June 2016.⁷¹

Wallace was notorious for sending more than twenty-seven million unsolicited Facebook messages between 2008 and 2009 and gaining access to more than 500,000 Facebook accounts through an external URL included in the direct messages that, when accessed, collected personal login information. He would then spam the users and those on their friends list, earning money from traffic directed to the URLs embedded in the messages.⁷²

Spam emails, like those sent out by Wallace, have potential to cause substantial damage to consumers. Spam "wastes bandwidth and storage, delays valid emails, and hurts human productivity."⁷³ Other concerns include "privacy, false email identities, questionable message content, enticement, and fraud."⁷⁴ Location-based advertisers direct spam based on location and personal characteristics of the consumer, especially when

67. See McNealy, *supra* note 3, at 353–54 ("Both the Fourth and Ninth Circuit Courts of Appeal, however, have found that the federal statute preempts anti-spam statutes with provisions different from CAN-SPAM that would cause confusion about the law.").

68. 666 S.E.2d 303 (Va. 2008).

69. 420 F.3d 366 (5th Cir. 2005).

70. McNealy, *supra* note 3, at 353 fn.17. In *White Buffalo Ventures*, the plaintiff, White Buffalo Ventures "operate[d] several online dating services, including longhornsingels.com, which target[ed] students at the University of Texas at Austin." *White Buffalo Ventures*, 420 F.3d at 368. The Fifth Circuit held that the university could continue using its anti-solicitation policy to block White Buffalo's attempts to send unsolicited bulk commercial email to students. See *id.* at 369.

71. McNealy, *supra* note 3, at 351.

72. *Id.* at 351–52.

73. Craig A. Shue, Minaxi Gupta, Chin Hua Kong, John T. Lubia & Asim S. Yuksel, *Spamology: A Study of Spam Origins*, in THE 6TH CONFERENCE ON EMAIL AND ANTI-SPAM 1 (CEAS) (2009), <http://web.cs.wpi.edu/~cshue/research/ceas09.pdf> [<https://perma.cc/A99P-AYMG>].

74. Janice C. Sipior, Burke T. Ward & P. Gregory Bonner, *Should Spam Be on the Menu?*, 47 COMM'NS ACM 59, 60 (2004), <https://doi.org/10.1145/990680.990681> [<https://perma.cc/JRF6-RUFP>].

location services can be traced to a mobile device.⁷⁵ “Some spammers routinely spoof, or misrepresent return addresses and headers, to conceal their identities.”⁷⁶ An estimated eighteen percent of spam includes messages “surprising recipients with pornographic, violent, hateful, or otherwise offensive content,” according to the Federal Trade Commission (FTC).⁷⁷

Researchers and Ph.D. candidates at Indiana University conducted a study by exposing 22,230 emails and monitoring how much spam was received over nearly five months.⁷⁸ The study concluded that “[s]pamming crawlers exist and can be tracked” and that “[t]op spammers use multiple email-harvesting strategies.”⁷⁹ “To obtain the email addresses . . . spammers [can] use web crawlers to access the web pages and then extract the email addresses on each page.”⁸⁰

Even when committing enticement, fraud, and theft, “[c]osts to spammers are minimal while unwilling recipients bear the burden.”⁸¹ “Spam email transmission has formed its own economy with a business model,” where spammers are “capable of stealing millions of dollars from victims in less than a year.”⁸² Meanwhile, the U.S. Chamber of Commerce estimated in 2003 that spam costs corporations ten billion dollars annually “for personnel time spent perusing unwanted messages, implementing better blocking software, or recovering from spam overload.”⁸³

In recent years, spam has spread to social media platforms, like Facebook, Twitter, and Instagram, becoming what is known as “social spam.”⁸⁴ “A substantial amount of research has been directed to combat

75. See *id.* (“One of the most objectionable aspects of spam is the intrusion on privacy. The degree to which privacy can be violated is illustrated by the scenario in which location-based marketers direct mobile spam to the recipient . . . with a precise message based on location and personal characteristics.”).

76. *Id.* “False identities can be obtained through one-time use of an email service, unauthorized use of an email account, or utilization of an ISP’s connection points.” *Id.* “Outrage toward spammers has prompted spam vigilantes to hack into spammers’ computers, to blacklist spam advertisers, and to publish names and contact information to encourage spamming of the spammers.” *Id.*

77. *Id.* (“Further, inappropriate content may be seen by underage recipients or in the workplace.”).

78. See Shue et al., *supra* note 73.

79. *Id.* (finding that “[u]sers must exercise caution when divulging their email addresses,” “[s]pam arrives instantly,” and “[c]ommonly-used email obfuscation techniques are offering protection (for now)”).

80. *Id.* (“Spammers can harvest email addresses from multiple sources on the Internet, including web pages, blogs, newsgroups, social networking sites, and mailing lists.”).

81. Sipior et al., *supra* note 74, at 60.

82. Shue et al., *supra* note 73.

83. Sipior et al., *supra* note 74, at 60.

84. Manajit Chakraborty, Sukomal Pal, Rahul Pramanik & C. Ravindranath Chowdary, *Recent Developments in Social Spam Detection and Combating Techniques: A Survey*, 52 INFO. PROCESSING & MGMT. 1053, 1053 (2016) (“The increase in user base for social platforms like Facebook, Twitter, YouTube, etc., has opened new avenues for spammers. The liberty to contribute content freely has

spam on” email servers and social media platforms.⁸⁵ “Social networks[,] being quite different in nature from the earlier two, have different kinds of spam and spam-fighting techniques from these domains seldom work. Moreover, due to the continuous and rapid evolution of social media, spam[mers] themselves evolve very fast[,] posing a great challenge to the community.”⁸⁶

Social spamming scams are rampant now more than ever, with many spammers using COVID-19 to defraud consumers on Facebook and other social media platforms.⁸⁷ The Better Business Bureau issued a warning to protect consumers.⁸⁸ Without action and adequate protection from the federal government, social media platforms have had to deal with social spam largely by themselves.⁸⁹ It is possible that social media companies have the potential to provide consumers relief similar to the relief major phone carriers are now providing. “Recently-adopted tech standards are meant to help providers identify spam calls and ‘spoofed’ call numbers to prevent them from even going to consumers.”⁹⁰

Some select district courts have concluded that CAN-SPAM can apply to social spam on social media platforms. In *Facebook, Inc. v. MaxBounty, Inc.*, Facebook alleged that MaxBounty, an advertising and marketing company, engaged “in impermissible advertising and commercial activity

encouraged the spammers to exploit the social platforms for their benefits. E-mail and web search engine being the early victims of spam have attracted serious attention from the information scientists for quite some time.”).

85. *Id.*

86. *Id.*

87. See *BBB Scam Alert: Don't Be Fooled into Thinking That's Your Friend on Facebook*, BETTER BUS. BUREAU (Sep. 16, 2021), <https://www.bbb.org/article/news-releases/22110-bbb-scam-alert-dont-let-boredom-fool-you-into-thinking-thats-your-friend-on-facebook> [<https://perma.cc/Q6B8-4QTR>].

88. *Id.*

89. See Rebecca Heilweil, *Facebook Messenger Will Now Try to Fight Scammers Without Reading Your Messages*, VOX (May 21, 2020, 9:00 AM), <https://www.vox.com/recode/2020/5/21/21265828/facebook-messenger-scams-fake-accounts-artificial-intelligence> [<https://perma.cc/F4F4-27LB>] (“The company will use artificial intelligence to help identify these potential bad actors and provide safety notices to users about messages from shady accounts. . . . Facebook is trying to limit how much its AI actually reads the content of user messages in order to identify scams.”); David Murphy, *How Facebook's 'Forwarding Limit' Can Control Chain-Spam*, LIFEHACKER (Sept. 9, 2020, 8:03 AM), <https://www.lifehacker.com.au/2020/09/how-facebooks-forwarding-limit-can-limit-chain-spam/> [<https://perma.cc/7QVM-DCRH>] (“I know, I know. Facebook trying to do the right thing and limit spam on its network is kind of like saying I’m going to use this masking tape to seal the hole in this nearby dam, but every little bit helps, right?”); Sarah Perez, *Twitter to Test a New Filter for Spam and Abuse in the Direct Message Inbox*, TECHCRUNCH (Aug. 16, 2019, 10:35 AM), <https://techcrunch.com/2019/08/16/twitter-to-test-a-new-filter-for-spam-and-abuse-in-the-direct-message-inbox/> [<https://perma.cc/7QVM-DCRH>] (“While one solution is to adjust your settings so only those you follow can send you private messages, that doesn’t work for everyone. Some people—like reporters, for example—want to have an open inbox in order to have private conversations and receive tips.”).

90. Snider, *supra* note 20.

on Facebook[],” tricked affiliates “‘into believing that its campaigns are approved by Facebook,’” and promoted “‘traffic to its contracting advertiser websites by ‘provid[ing] technical support to its affiliates on how to create fake Facebook campaigns, and [by] provid[ing] substantial advance payments to its affiliates that agree to participate in [MaxBounty’s] Facebook campaigns.’”⁹¹

The United States District Court for the Northern District of California held that Facebook’s CAN-SPAM claim was sufficiently pled.⁹² The court’s holding that the claim was sufficiently pled gives credence to an argument that CAN-SPAM applies to social spam.

II. ANALYSIS

CAN-SPAM has failed to protect consumers from spam emails and the emergence of social spam. First, CAN-SPAM gives businesses too much leeway, which they have consistently abused. The Act “does not effectively reduce the amount of commercial spam”⁹³ and the New York Times reported that junk e-mail has actually increased in the years following CAN-SPAM becoming law.⁹⁴ Anti-spam laws, like CAN-SPAM are often “totally ignored” by spammers.⁹⁵ Some experts have estimated that “63% of the [time, the] opt-out option does not work,” and that “[w]hen recipients click on the ‘unsubscribe/remove me’ button on the spam e-mails, often they merely end up confirming to the spammers that they (the spammers) reached valid e-mail addresses, and so [they] end up receiving a lot more spam e-mails later.”⁹⁶

Second, CAN-SPAM lacks an expanded private right of action, which is one reason why spammers “totally ignore” the law.⁹⁷ Only the Federal Trade Commission, state attorneys general, and Internet Service Providers can bring an action under CAN-SPAM’s provisions.⁹⁸ “Each of these authorized entities either lacks the incentive or the resources to adequately enforce the

91. 274 F.R.D. 279, 281 (N.D. Cal. 2011).

92. *See id.* at 284.

93. Arora, *supra* note 3, at 302 (“Commentators complained about the inadequacy of opt-out regulations even before the *New York Times* article. One pointed out that ‘[i]ndividual recipients are forced to take an affirmative step against each piece of unwanted mail; such [a] step wastes more time and money than the problem itself.’”) (alterations in original).

94. *See* Tom Zeller, Jr., *Law Barring Junk E-Mail Allows a Flood Instead*, N.Y. TIMES, Feb. 1, 2005, at A1.

95. Won Kim, Ok-Ran Jeong, Chulyun Kim & Jungmin So, *The Dark Side of the Internet: Attacks, Costs and Responses*, 36 INFO. SYS. 675, 698 (2011).

96. *Id.*

97. *Id.*; *see* Rutenburg, *supra* note 3, at 232–33.

98. *See* Rutenburg, *supra* note 3, at 225.

Act, resulting in little to no reduction of spam. As a result, email recipients—not spammers—bear the cost of spam.”⁹⁹ Consumers themselves need to have the opportunity to pursue legal recourse when they have been wronged by spam.

Third, CAN-SPAM does not have a “do not email” registry list. Unlike the TCPA and the Do Not Call Registry, CAN-SPAM fails to provide consumers with a simple way to opt out of all uncalled-for solicitation. “[CAN-SPAM] has also created an entitlement to send spam—one free message—before a recipient’s wish to avoid spam must be honored. This reverses the entitlement set in other media and ignores consumer demand for privacy and a Do-Not-Call Registry for email.”¹⁰⁰ The lack of a “do not email” registry list creates an unbalanced and inconsistent reality for advertisers who are given an incentive to spam instead of making a robocall.

Fourth, CAN-SPAM allows noncommercial spam. Critics of the Act have pointed out that while commercial spam is regulated, CAN-SPAM “allows political spam to invade recipients’ right to privacy.”¹⁰¹

There is an invasion of privacy caused by all kinds of spam because there is a recognized right to privacy in one’s home. The intrusive nature of spam results from the fact that spam, as one commentator describes, “more closely resembles television, radio advertisements, or telemarketing calls, in which an individual must view or hear the objectionable content before she has an opportunity to avoid it.” The public considers spam to be “as intrusive as telemarketing calls and much more intrusive than door-to-door solicitation or junk ‘snail’ mail.” Attempts to regulate political spam, however, must acknowledge the protection extended to political speech.¹⁰²

Fifth, CAN-SPAM’s preemption provision prevents states from taking further steps in regulating spam emails.¹⁰³ “The challenge to a state spam

99. *Id.* “The burden is further increased on the final spam filter—the spam recipient—who uses sixteen seconds on average to determine if a given message is spam.” *Id.* at 229. “[C]oncerns linger about ‘false positives,’ email that filtering software incorrectly identifies as spam. This contributes to additional lost time and lowered productivity resulting from the search for legitimate emails that, unbeknown to the intended recipient, the server did not deliver.” *Id.* (quoting Saul Hansell, *The High, Really High or Incredibly High Cost of Spam*, N.Y. TIMES (July 29, 2003), <http://www.lexisone.com/balancing/articles/n080003d.html> [<https://perma.cc/3KNJ-PQDL>]).

100. Bolin, *supra* note 3, at 399. “[A] Do-Not-Spam registry would clearly find public support. Certainly, the Do-Not-Call Registry is wildly popular. In one poll, eighty-three percent of respondents thought the registry was a good idea, and even sixty-six percent of those who did *not* plan to sign up considered it a good idea.” *Id.* at 426.

101. Arora, *supra* note 3, at 308.

102. *Id.* at 308–09.

103. See Bolin, *supra* note 3, at 421–22 (“For its part, Congress assessed the preemption as ‘minimal’ since CAN-SPAM does not preempt most of the laws previously used against spammers. In

law is unsurprising. After the passage of CAN-SPAM, state spam laws were supposed to be obsolete. Passed, in part, to rectify the uncertainty that state spam laws created, the federal law expressly preempted state attempts at regulating the spam problem.”¹⁰⁴

Sixth, CAN-SPAM is outdated and would need significant amendments to regulate spam social media messages. Direct messages that consumers receive on social media platforms do not contain the typical “envelope features” that CAN-SPAM regulates, like the subject line, header, and routing information that emails contain.¹⁰⁵ The only analogous feature would be CAN-SPAM’s regulation of the body of emails and the body of the direct messages received on social media platforms.¹⁰⁶ “With this in mind, prosecution or civil suits against social media spammers could only be based on false commercial information included in the body of the message or deception by connecting a message falsely to a profile, which would amount to a fraud.”¹⁰⁷

III. PROPOSAL

Successfully regulating spam emails will take a concerted effort from Congress. The first necessary decision is whether to amend CAN-SPAM or replace it. “For both contracts and public laws, the drafting process begins with researching the existing legal context. In the public arena, the drafter’s research may even reveal that a legal framework already exists relevant to the client’s objective, but for some reason the current law is not working effectively.”¹⁰⁸ Because of the number of significant amendments that are needed to make CAN-SPAM successful, Congress should replace the Act and start anew or, in the alternative, pass the significant amendments and attach a sunset provision.¹⁰⁹

If Congress decides a new federal law needs to replace CAN-SPAM to effectively regulate spam emails and social spam, the new law should use

particular, its preemption excludes laws related to ‘fraud or computer crime,’ which many states now have. In other words, most state spam laws are still in effect.”).

104. McNealy, *supra* note 3, at 353; *see supra* notes 67–70 and accompanying text; *infra* note 117 and accompanying text.

105. McNealy, *supra* note 3, at 373.

106. *See id.*

107. *Id.*

108. J. Lyn Entrikin & Richard K. Neumann Jr., *Teaching the Art and Craft of Drafting Public Law: Statutes, Rules, and More*, 55 DUQ. L. REV. 9, 49–50 (2017) (“Whether drafting private or public law, the drafter must always take existing law into account, including relevant case law interpreting current statutes and regulations.”).

109. *See id.* at 50 (“[T]he drafter might consider adding a ‘sunset provision’ that would terminate the program after a set time unless the legislature amends the statute to extend the program or make it permanent. Or the drafter might consider establishing a pilot program in an appropriation bill . . .”).

the TCPA as a model. “[L]egal drafting is the most difficult thing a lawyer is called upon to do, and legislative drafting is the most difficult form of legal drafting.”¹¹⁰ “Familiarity and habit” are main factors in traditional legal drafting because of “the security that comes from adopting forms and words that have been used before and seen to be effective.”¹¹¹ Some scholars argue this factor “operate[s] as a hindrance to ‘innovative legal drafting,’”¹¹² but those scholars would sacrifice clarity for innovation. Ambiguity is “‘the most serious disease of language’, and nowhere is the absence of this disease more important than in legislation. The avoidance of ambiguity is aided in a very significant way by the drafter’s reliance on words which have a well-established meaning.”¹¹³ Modeling the law that replaces CAN-SPAM after the TCPA follows one of the main factors of traditional legislative drafting and avoids ambiguity.

Following the TCPA as a model, the new law should not allow any unsolicited emails, commercial or otherwise, without consumers’ prior consent, unless the email was made for an emergency purpose. It should include a “do not email” registry list and restrict the hours during which a solicitor may email a consumer to provide more consumer privacy and be consistent with the Do Not Call Registry. It should not preempt any more restrictive state spam email laws, allowing states to take further steps in regulating unsolicited emails sent to constituents. It should include a private right of action for consumers so that those with an incentive to reduce spam, consumers themselves, may bring suit, possibly in the form of class action.

The new law should include some current or similar provisions to those in CAN-SPAM. For example, it should require that all senders provide and comply with an opt-out mechanism in their emails that allows recipients to choose to stop receiving email from a particular sender.¹¹⁴ It should require all senders of unsolicited commercial email to provide “a valid physical

110. *Id.* at 17 (quoting Reed Dickerson, *How to Write a Law*, 31 NOTRE DAME L. REV. 14, 15 (1955)).

111. Brian Hunt, *Plain Language in Legislative Drafting: An Achievable Objective or a Laudable Ideal?*, 24(2) STATUTE L. REV. 112, 113 (2003); see also Grace E. Hart, *State Legislative Drafting Manuals and Statutory Interpretation*, 126 YALE L.J. 438, 443 (2016) (discussing “normative justifications for using drafting manuals in statutory interpretation as well as principles to guide state courts in considering drafting manuals in their jurisprudence” that can be paralleled to using one piece of legislation as a model for another).

112. PETER BUTT & RICHARD CASTLE, *MODERN LEGAL DRAFTING: A GUIDE TO USING CLEARER LANGUAGE* 5 (Cambridge 2001).

113. Hunt, *supra* note 111, at 114. “Clear language is that which is unambiguous and is capable of only bearing the meaning intended by its author. Plain language is not necessarily clear language. A concept expressed in plain language, will not always carry a clear and unambiguous meaning.” *Id.* at 116. See also Entrikin & Neumann Jr., *supra* note 108, at 12, 46–47 (describing how Professor Reed Dickerson, “a national hero for his leadership in improving the art and craft of drafting” and an “internationally renowned [scholar] for his leadership in professionalizing legal drafting,” emphasizes drafting legal rules “clearly and effectively”).

114. See 15 U.S.C. § 7704(a)(5).

postal address” and proper notification that the message is an advertisement.¹¹⁵ Also, it should require that spammers place warning labels on emails containing sexually oriented material.¹¹⁶

Similar to including provisions from CAN-SPAM, the new law should also include ideas from states that proposed taking stronger steps to regulate spam. For example, the New Mexico legislature considered a bill that would have made it unlawful for “any person or entity to collect email addresses posted on the internet” whether automated or otherwise for the purpose of sending unsolicited commercial emails.¹¹⁷ The new law should attempt to stop spam before it is sent by adding a similar provision that would prevent spammers from harvesting emails. How the FCC or another federal agency should enforce a provision preventing spammers from harvesting emails is beyond the purview of this Note, but the study from Indiana University concluded that spam harvesting can be tracked and identified multiple plausible anti-spam techniques.¹¹⁸ While adding this provision into the new law would not prevent each and every technique spammers use, it would curb a substantial amount.¹¹⁹

The new law should include not only current CAN-SPAM provisions and proposed provisions from states, but also provisions from outside sources. A provision in the Rules Governing the Missouri Bar and the Judiciary states that “any written solicitation prompted by a specific occurrence involving or affecting the intended recipient of the solicitation or family member shall disclose how the lawyer obtained the information prompting the solicitation.”¹²⁰ The new law should include a provision that states advertising emails, solicited and unsolicited alike, must include information on how the advertiser obtained the consumer’s email address. This will help consumers who did somehow consent to receiving the email understand why they received an advertisement. Consumers who did not consent will also benefit because they will know what they need to rebut in any contact with the advertiser or private suit they may pursue.

115. *Id.*

116. 15 U.S.C. § 7704(d).

117. Anti-Spam Act, H.R. 1258, 48th Leg., 1st Sess. (N.M. 2007).

118. See Shue et al., *supra* note 73. One technique is to “use[] cryptographic primitives to make it easier for a destination to confirm that only the indicated source sent the message” and “prioritize legitimate senders while blocking spamming organizations.” *Id.* A second technique is “hiding one’s email address using a [sic] ephemeral email addresses. If spams begin to arrive via the ephemeral email address, the address is retired. This type of service is offered commercially to end users.” *Id.*

119. See *id.* Spammers can also use a dictionary-based campaign or relay spamming to attempt to send emails to people with common first and last names (e.g., richevans@example.com). *Id.*

120. MO. SUP. CT. RULES, RULE 4-7.3(B)(6) (2010), <https://www.courts.mo.gov/courts/ClerkHandbooksP2RulesOnly.nsf/c0c6ffa99df4993f86256ba50057dcb8/3a8366293969e46486256ca6005211ed?OpenDocument>.

To resolve current problems and anticipate future ones,¹²¹ the new law should include regulations of social spam that differ from the regulation of emails. Beyond the differences in spam emails and social spam, there are different methods that spammers can use to reach consumers on social media, including through direct social media messages and through a social tagging system, which all need to be addressed.¹²² Some scholars have argued that there are “six distinct features that address various properties of social spam, finding that each of these features provides for a helpful signal to discriminate spammers from legitimate users.”¹²³ Scholars have been able to compute these features “in various machine learning algorithms for classification, achieving over 98% accuracy in detecting social spammers with 2% false positives.”¹²⁴ Analyzing these features closely could provide a baseline for legislation that would combat social spam.

This new law would need to pass the Supreme Court’s commercial speech test from *Central Hudson*, be content-neutral and not violate free speech rights, and abide by the ruling in *Barr*. To satisfy the commercial speech test from *Central Hudson*, the government needs to have a substantial interest in regulating spam emails; the new law needs to advance that government interest; and the new law needs to be narrowly tailored.¹²⁵

121. See Entrikin & Neumann Jr., *supra* note 108, at 23 (“[L]egal drafting is a deliberative process lawyers use to create generally applicable rules by identifying current problems, anticipating future problems, and resolving those problems without resorting to litigation. The specific individuals to whom a public rule will apply in the future are unknowable at the time the rule is drafted.”).

122. Benjamin Markines, Ciro Cattuto & Filippo Menczer, *Social Spam Detection*, in AIRWEB ’09: PROC. OF THE 5TH INT’L WORKSHOP ON ADVERSARIAL INFO. RETRIEVAL ON THE WEB 41, 42 (2009) (“Long before social tagging became popular, spam was a problem in other domains, first in email then in Web search. Unfortunately, the countermeasures that were developed for email and Web spam do not directly apply to social systems.”).

123. *Id.* at 41. The six distinct features include: TagSpam, TagBlur, DomFP, NumAds, Plagiarism and ValidLinks. *Id.* at 43–45. TagSpam is a feature “built upon the notion” that “[s]pammers . . . use tags and tag combinations that are statistically unlikely to appear in legitimate posts.” *Id.* TagBlur is a feature based on “[t]he underlying assumption . . . that spam posts tend to lack semantic focus.” *Id.* at 44. DomFP focuses on the content of social spam, “observing that Web pages in social spam often tend to have a similar document structure, possibly due to the fact that many of them are automatically generated by tools that craft web sites from predefined templates.” *Id.* NumAds “draws upon the idea that spammers often create pages for the sole purpose of serving ads.” *Id.* Plagiarism analyzes how “[s]pammers can easily copy original content from all over the Web.” *Id.* “To estimate the odds that a page’s content is not genuine, we look for authoritative pages that are likely sources of plagiarized content,” and “[w]e . . . extract a random sequence of 10 words from the page’s content.” *Id.* ValidLinks “focuses on the detection of user profiles created for spam purposes.” *Id.* at 45. “Malicious users may temporarily set up a page to obtain sensitive information, and then post the malicious resource to a social site.” *Id.*

124. *Id.* at 41.

125. See *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm’n*, 447 U.S. 557, 564–65 (1980) (“[T]he restriction must directly advance the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government’s purpose. . . . [I]f the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.”); see also *Bates v. State Bar*, 433 U.S. 350 (1977); *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748 (1976).

The new law proposed above should satisfy the test. To be content-neutral and not violate free speech rights, the new law would need to be a reasonable restriction on the time, place, or manner of the protected speech, without reference to the content of the restricted speech; narrowly tailored to serve a significant governmental interest; and leave open ample alternative channels for communication of the information.¹²⁶ Like the TCPA and CAN-SPAM, the new law should be deemed content-neutral and not a violation of free speech rights, if challenged. Finally, to abide by the ruling in *Barr*, the new law could only impose incidental burdens on speech because of the ordinary economic regulation of commercial activity, not an impermissible content-based speech restriction.¹²⁷ Because the proposed new law would regulate any unsolicited emails, commercial or otherwise, it is especially important that the law is carefully written and implemented in a way that abides by the ruling in *Barr*.

CONCLUSION

Americans are largely united in their disdain for spam. It breaches consumer privacy, hurts human productivity, and imposes the cost of either protecting oneself from fraud or becoming a victim of it.¹²⁸ CAN-SPAM has allowed exactly what its acronym spells out—advertisers and spammers are making millions of dollars by spamming unwilling consumers.¹²⁹ A new federal law is necessary to effectively regulate spam emails and social spam. Legislators in the Senate Commerce Subcommittee on Communications, Media, and Broadband should follow up their great work curbing robocalls through the TRACED Act by curbing spam emails and social spam. There will likely need to be more media coverage and public outcry about the issue before legislators will be motivated to tell businesses they CAN'T SPAM any more.

*Drew Smith**

126. See *Moser v. FCC*, 46 F.3d 970, 973 (9th Cir. 1995).

127. See *Barr v. Am. Ass'n of Pol. Consultants*, 140 S. Ct. 2335, 2346–47 (2020); *supra* notes 36–40 and accompanying text.

128. See Shue et al., *supra* note 73; Sipior et al., *supra* note 74, at 60.

129. See Shue et al., *supra* note 73.

* J.D., Washington University in St. Louis (2022). B.A., University of Arkansas (2019). Thank you to Siobhan O'Carroll for helping me craft this Note, and to Frankie Cascone, Bob Neel, Alida Babcock, Jake Keester, and Maya Kieffer for their wonderful edits. Thank you to Daniel Harawa and Andrea Katz for being amazing professors and mentors. Thank you to Dan Le Batard, Jon "Stugotz" Weiner, Guillermo "Billy" Gil, Mike Stoklasa, Jay Bauman, Rich Evans, and Jason and Leah Gastrow for helping me make it through the worst stretch of the pandemic. Thank you to my parents, my siblings (Will, Montana, and Sierra), and to other family and friends for their motivation and inspiration. Finally, thank you to my wife, Andrea, for her unwavering support, encouragement, and love.