The CAN-SPAM Act of 2003: A False Hope

Jay Reyero
The CAN-SPAM Act of 2003: A False Hope

Jay Reyero*

If Legislation was created to protect "an extremely important and popular means of communication" from the threatening "rapid growth in the volume of unsolicited commercial electronic mail," one would think that the threat would be controlled within a short time of the legislation being implemented. Congress created the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act") to aid consumers in the fight against unsolicited commercial electronic mail. But despite going into effect on January 1, 2004, we are no closer to eliminating or controlling spam now than we were three years ago. Why does this inability to control spam still exist even with the creation of Congressional legislation? While the CAN-SPAM Act was initially designed to fight spam, it actually does very little in the fight against spam. Instead of protecting consumers, it protects commercial marketers; instead of focusing on "unsolicited" email, it focuses on "deceptive" email; instead of tackling the problem, it shifts the burden to others; instead of creating a strong legal foundation when preemption occurs, it creates a weak national standard that usurps stronger state initiatives.

Considering that even after the enactment of the CAN-SPAM Act there is a continued inundation of unsolicited emails into our mailboxes, this comment argues that the CAN-SPAM Act of 2003 was a false hope—the enactment of the Act presented an apparent promise to consumers to prevent the continued invasion by unsolicited emails, but the Act’s intentions and effect were never meant to meet consumers’ expectations. This comment begins in Part I laying a foundation defining the exact nature of spam by detailing the birth of spam, describing how it works, and highlighting the problems associated with it. Part II focuses on Congress’s response to the spam problem by describing the policy determinations supporting the CAN-SPAM Act of 2003, and briefly discussing the sections contained within the Act. Part III’s focus is on the particularly important preemption Section 7707. Included is a brief look into preemption precedents, followed by an analysis of the statutory text of the section, and lastly, an examination of two cases that focused

* Jay Reyero is a May 2008 candidate for Juris Doctor at Southern Methodist University Dedman School of Law. He graduated from the University of Texas at Austin with a Bachelor of Business Administration in Management Information Systems, with a minor in Economics.

2. Id. § 7701(a)(2).
on Section 7707. Finally, Part IV presents four issues with the CAN-SPAM Act, relying on the statutory text and subsequent case decisions that support the notion that it is a false hope.

I. What Is Spam?

How many times have you accessed your email, excited about the prospect of receiving personal emails, and instead found emails for pornographic websites, creative new diet plans, or, my personal favorite, the opportunity to work from home and make six figures? These unwanted and annoying emails exemplify a kind of email message that is known as “spam.”

A. The Birth of Spam

“Spam” is defined as “unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups.”4 Spam has also been referred to as “junk email.”5 The most common types of spam are pyramid schemes, chain letters, get-rich-quick schemes, and advertisements for pornographic websites.6 While spam typically evokes a negative connotation, it also refers to the commercial marketing efforts of legitimate businesses.7 The term’s origin results from a British skit about Spam, the meat product, where a group of Vikings sing a chorus of “spam, spam, spam...” increasing in volume to the point of drowning out all other conversation taking place.8 The analogy was applied to spam email because it “was drowning out normal discourse on the Internet.”9 Spam’s first occurrence is attributed to two immigration lawyers, who in 1994 used Usenet newsgroups10 to send an advertising message about their law firm’s services.

5. Id.
10. Usenet is a world-wide discussion system consisting of newsgroups. Information is posted to the newsgroups which then distribute it to all other intercon-
to thousands of people. This one act "opened a Pandora’s box" as copycats began using the Internet to promote unwanted commercial solicitations. Eventually the wave of spam resulted in the destruction of the usefulness of newsgroups and, as a result, spammers shifted their techniques to targeting individual email addresses. However, this evolution was initially limited due to the difficulty of obtaining enough email addresses to justify the costs, but as the Internet became a mass medium and more email addresses became more accessible, the limitation was no longer an issue.

B. How Does it Work?

One method employed by spammers to obtain email addresses is called a "dictionary attack." Using special software, email addresses are automatically generated and short bursts of communications are then sent to Internet Service Providers ("ISPs") indicating a desire to contact the email addresses. If the ISP responds with a willingness to accept email for a certain address, the software includes it in a list knowing it has generated a valid address. The spammer can then generate emails to be sent to this list of valid addresses. Another method used is a "web bug," or other tiny computer code, which is activated when an email is opened by the recipient alerting the sender that the address is valid. Additionally, this notifies the sender about the recipient’s propensity to open unsolicited email. The final method, "Email harvesting," is the most common technique spammers use to obtain email addresses. Spammers utilize automated computer programs to search certain areas on the Internet and then compile lists of discovered email connected computer systems. What is Usenet?, http://www.faqs.org/faqs/usenet/what-is/part1/ (last visited Dec. 1, 2007).


13. Netcraft, supra note 11.

14. Id.


16. Id.

17. Id. at 3-4.

18. Id. at 4.

19. Id.

20. Id.

addresses. These areas include webpages, newsgroups, chat rooms, message boards, online directories, and many other online sources. While email harvesting continues to be a source of information gathering, spammers are using new and improved techniques to "breach the Internet's defenses" and capture information. Spam harvesters often use "Botnets," which are small programs that secretly install themselves on thousands of computers and then together utilize the collective power of this network to harvest information. Today more than eighty percent of all spam originates from botnets.

C. What Are the Problems With Spam?

Spam presents a number of problems, some of which are not readily apparent to an individual receiving it. The most obvious problem spam creates is reflected in its definition: the emails are unwanted, annoying solicitations. This "annoyance factor" presents itself as Internet users must sift through the multitude of spam emails just to locate legitimate personal emails. This process also creates other smaller problems such as the loss of productivity (cleaning out spam takes time) and the risk of deleting legitimate emails. Also, even though broadband adoption is significant now, users who still use dial-up internet access at home or on business trips some-
times pay per minute. The time it takes these people to individually delete each piece of spam then translates from a time cost to a financial cost. Another problem with spam is that it wastes and strains network resources in two different places. First, spam creates problems during its journey from the sender to the recipient as numerous systems in between are forced to carry these unwanted messages. As other systems are forced to handle these emails, their resources are not being used to process other legitimate (“wanted”) information. Recently, a single Internet service provider generated more than one billion spam email messages in twenty-four hours. Imagine the resources needed to process those and the amount of information queued as a result. Second, spam creates a problem once it reaches its destination. As spam passes through multiple points prior to arriving at the Exchange Server where email is stored—i.e. the internet connection, firewall, etc.—it consumes system resources such as bandwidth, processing power, and memory. While the amount of resources consumed by one spam email is not significant, problems arise when that number increases. In addition, once the spam reaches the Exchange Server, it must be stored and, as a result, disk space on the server becomes an issue. The final problem created by spam is that it shifts costs from the sender to the recipient. While it is relatively inexpensive to send spam, it is costly for those that receive it. Costs include both performance and financial costs. Performance costs are represented in terms of time and are exhibited when spam is being processed and the processing time for legitimate email is slowed. Processing resources are also used when filtering schemes are implemented, decreasing the number of available resources. Additionally, as spam arrives at the destination,

32. Id.
35. Id.
37. Posey, supra note 29.
38. Id.
39. Id.
41. Id.
42. Id.
it consumes the destination’s bandwidth,\textsuperscript{43} decreasing the relative transfer rate available for other information.\textsuperscript{44} "Massive volumes of spam can clog a computer network, slowing Internet service for those that share the network."\textsuperscript{45} These performance costs lead directly to financial costs as the choice must be made between coping with slower resources and investing in a technology upgrade simply to receive the same results that would be available without spam.\textsuperscript{46} New equipment with larger capacity, implementing and maintaining filtering systems, and additional customer service personnel are a few of the high monetary costs.\textsuperscript{47} Despite the solution adopted, there are always costs.

II. CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003

In 2003, the growing problems that spam created and the large costs associated with fighting spam\textsuperscript{48} compelled Congress to enact the Controlling the Assault of Non-Solicited Pornography and Marketing Act ("CAN-SPAM Act").

A. Policy Behind the Act

In 2003, Congress understood the significance of email in the daily lives of Americans.\textsuperscript{49} At the time, nearly half (140 million) of all Americans regularly used email.\textsuperscript{50} Given this unrestricted passage, marketers quickly identified it as an optimal way to cheaply and quickly reach millions of people.\textsuperscript{51} As a result, Congress identified spam as "one of the most pervasive intrusions in the lives of Americans."\textsuperscript{52} The volume of spam was rapidly increas-


\textsuperscript{45} Id.

\textsuperscript{46} Id; see also CAN-SPAM Act, 15 U.S.C.S. § 7701(6).

\textsuperscript{47} S. REP. NO. 108-102 at 6.

\textsuperscript{48} Eighty percent of email received by AOL was spam and fighting spam would cost U.S. companies more than $10 billion. Optinrealbig.com v. Ironport Sys., Inc., 323 F. Supp. 2d 1037, 1039-40 (N.D. Cal. 2004).

\textsuperscript{49} S. REP. NO. 108-102 at 2.

\textsuperscript{50} Id.

\textsuperscript{51} Id.

\textsuperscript{52} Id.
The CAN-SPAM Act of 2003

Spam was also flooding network systems of ISPs like AOL and Microsoft, as they were blocking 2.4 million spam messages a day. Congress recognized the “significant economic burden” spam was placing on ISPs and consumers.55

While some spam messages were the product of marketing efforts by legitimate businesses, Congress’ primary concern focused on those who intended to defraud consumers and to “prey on unsuspecting email users.”56 Many times spammers would falsify or use misleading information in order to disguise the content of their emails.57 By placing false information in the email’s “from”, “reply-to”, and “subject” lines, spammers could confuse consumers as to the content contained in the email, the identity of the sender, and the reply address.58 Consumers were forced to go through each individual email just to understand the content of the message.59 Still, even after understanding the content, the fraudulent sender and reply information provided no usable information allowing a consumer to contact the spammer to request they stop sending emails.60 Given the increasing amount of spam received by consumer’s mailboxes, and their fraudulent nature, consumers were becoming overwhelmed because of their inability to manage their email.61 Congress identified additional problems resulting from fraudulent emails.62 Many fraudulent schemes created risks to unsuspecting email users in that they would be asked to provide sensitive information—this is commonly referred to as phishing.64 Credit card and social security numbers would be obtained, resulting in identity theft.65 In addition, spam would direct consumers to websites where their computers would be infected with viruses, spyware, Trojan horses, or other harmful computer codes.66 Pornographers would provide innocent subject lines such as “Hi, it’s me” or “Your order has been filled” only to have the emails contain objectionable

53. Id.
54. Id. at 2-3.
55. Id. at 6-7; see supra Part I.C.
57. Id. at 3.
58. Id.
59. Id.
60. Id.
61. Id.
62. Id.
63. Id. at 5.
66. Id. at 6.
images or automatically load pornographic websites. All fraudulent emails made the already-difficult task of tracking down spammers even more expensive and therefore improbable.

Because of the problems spam produced, Congress recognized a "substantial government interest in the regulation of commercial electronic mail on a nationwide basis." Many states had already enacted their own legislation to regulate and reduce spam. However, due to the different standards and requirements of each of the states, Congress feared the legislation was inadequate. Congress reasoned that the lack of geographic information in email addresses created a setback for those honest businesses that could not identify the state law to follow. So, in drafting federal legislation, Congress kept two things in mind: (1) "senders of commercial [email] should not mislead recipients as to the source or content of such mail," and (2) "recipients of commercial [email] have a right to decline to receive additional commercial [email] from the same source." Ultimately, Congress aimed to create a "Federal statutory regime that would give consumers the right to demand that a spammer cease sending them messages, while creating civil and criminal sanctions for the sending of spam meant to deceive recipients as to its source or content."

B. Specific Sections of the Act

In creating the CAN-SPAM Act, there were four underlying purposes: (1) to prohibit deception by the sender of both recipients and ISPs as to the source and content of an email, (2) to require senders to provide a method for recipients to request the abolition of future emails and to compel senders to honor those requests, (3) to require the inclusion of a physical address and the indication that the email is an advertisement or solicitation, and (4) to prohibit businesses from "knowingly promoting or permitting" spam to be sent of their behalf. Below are discussions of each section of the Act.

67. Id. at 4, 6.
68. Id. at 4-5.
72. Id.
73. Id. §§ 7701(b)(2)-(3).
75. Id. at 1.
1. Sections 7701 - 7703

Section 7701 is an important administrative inclusion because it provides a summary of the findings and policies Congress considered in drafting the Act. Congress understood the importance of email in the lives of Americans, the threat posed by the rapidly rising volume of spam, and the inability of state legislation to effectively deal with the problem. In Section 7701(b), Congress affirms their determinations of public policy implications, offering a foundation that can be used to assist in the interpretation of the Act.

Section 7702 is also an important, but not uncommon, administrative inclusion, which defines key terms used throughout the Act. In total seventeen terms are defined, including important terms such as "commercial electronic message," "initiate," "internet access service," "recipient," and "sender." Section 7703 simply directs the United States Sentencing Commission to review and possibly amend the sentencing guidelines for violations of Section 1037 of Title 18, United States Code in light of the new CAN-SPAM Act.

2. Section 7704

Section 7704 is the core clause of the CAN-SPAM Act. It specifies the requirements that must be followed when attempting to initiate commercial email messages. In general, this section prohibits false or misleading header information, prohibits deceptive subject lines, requires the email to provide recipients an opt-out option, and requires a clear and conspicuous identifier.

---

77. Id.; see also supra Part II.A.
79. See generally id. § 7702.
80. Id. § 7702 (2).
81. Id. § 7702 (9).
82. Id. § 7702 (11).
83. Id. § 7702 (14).
84. Id. § 7702 (16).
87. "[T]he source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." CAN-SPAM Act, 15. U.S.C.S. § 7702(8).
that the email is an advertisement or solicitation. The purpose of Section 7704(a)(1) is "to eliminate the use of inaccurate originating email addresses that disguise the identities of the senders."

Section 7704(a)(1) makes it unlawful for any person to "initiate" the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. Materially misleading header information would include instances where the originating email address, domain name, or IP address are technically correct, but they were obtained under "false or fraudulent pretenses or representations." It also includes a person knowingly using a different computer to relay or transmit a commercial message and then failing to accurately identify the original computer used for the transmission. In all other instances, violations of Section 7704(a)(1) require that the alteration or concealment of header information prevent recipients from responding to the sender of the commercial message or prevent third parties (i.e. those enforcing the Act) from identifying, locating, investigating, or responding to the sender of the commercial email. It is important to note that the mere existence of falsities in the header information is not sufficient, as they must "prevent" identification, investigation, etc.

The Fourth Circuit reinforced this notion when it held that the incorrect identification of an originating server and the use of a non-functional address in the "from" line did not meet the "materially false or materially misleading" requirement. The Court de-

---


90. The term "initiate" is defined in the Act so that liability exists under two different circumstances. See CAN-SPAM Act, 15 U.S.C.S. § 7702(9). First, under normal circumstances, a person can be liable if they originate or transmit the commercial message themselves. Id. Second, a person can also be liable if they "procure" the origination or transmission of the commercial message. Id. This is the "procure" clause. To "procure" means to "intentionally pay or provide other consideration to, or induce, another person to initiate" a commercial message on one's behalf. CAN-SPAM Act, 15 U.S.C.S. § 7702(12).


92. Id. § 7704(a)(1)(A).

93. Id. § 7704(a)(1)(C).

94. Id. § 7704(a)(6) (providing the definition of "materially").

95. See Omega World Travel v. Mummagraphics, Inc., 469 F.3d 348, 357-58 (4th Cir. 2006).

96. Id.
The CAN-SPAM Act of 2003
termined that despite these two inaccuracies, the headers of the emails sent by a cruise traveling website were “replete with accurate identifiers of the sender” providing plenty of methods to “identify, locate, or respond to the sender or to investigate an alleged violation of the CAN-SPAM Act.”97 The messages contained links for removal from future mailing lists, links to the main website, toll-free telephone numbers, a mailing address, a local telephone number, and several references to the domain name.98 The Court posited about the needless inclusion of the materiality requirement if they were to adopt the interpretation that “inaccuracies in a message containing so many valid identifiers could be described as ‘materially false or materially misleading.’”99

Section 7704(a)(2) prohibits the use of deceptive subject headings and requires that the person who initiates the commercial message know or should know—“implied on the basis of objective circumstances”—that the subject headings would likely mislead a recipient “about a material fact regarding the contents or subject matter of the message.”100 Congress did not intend for minor typographical errors or “truly accidental mislabeling” to create liability.101

Section 7704(a)(3) requires all commercial e-mail to contain “a functioning return electronic mail address or other Internet-based mechanism” that allows the recipient to opt-out of future messages.102 The return e-mail address must be able to receive recipients’ messages for no less than thirty days after the original commercial email was sent,103 but temporary unavailability due to technical problems beyond the sender’s control are exempt.104 Congress recognized the potential volume of responses a sender could receive after sending unwanted commercial e-mail and therefore, it included protections for those who act in good faith.105 However, this exemption does not protect those that craft systems unequipped to handle responses, nor those that do not remedy the situation in a reasonable amount of time.106

Section 7704(a)(4) continues by prohibiting the transmission of commercial

97. Id.
98. Id.
99. Id. at 358.
103. Id. § 7704(a)(3)(A)(ii).
104. Id. § 7704(a)(3)(C).
106. Id.
e-mail to a recipient within ten business days\textsuperscript{107} of receiving an opt-out request.\textsuperscript{108} This applies to a single sender of commercial email, one who sends commercial email on behalf of a sender, and one who provides or selects emails for the sender; though the last two require actual or implied knowledge that the recipient made an opt-out request.\textsuperscript{109} Congress added the additional knowledge requirement to ensure that persons providing email marketing services will be responsible for making a good faith inquiry of their clients... to determine whether there are recipients who should not be emailed.\textsuperscript{110} Also prohibited is the sale, lease, exchange or transfer of an email address.\textsuperscript{111} Congress wanted to prevent an opt-out request from being treated as a “confirmation of a ‘live’ email address,” generating information then sold to other spammers.\textsuperscript{112}

Section 7704(a)(5) requires that all commercial emails\textsuperscript{113} contain “clear and conspicuous identification that the message is an advertisement or solicitation,” “clear and conspicuous notice” of the ability to opt-out of future emails, and “a valid physical postal address of the sender.”\textsuperscript{114}Section 7704(b) classifies several spammer techniques, such as address harvesting, dictionary attacks, automated creation of multiple email accounts, and unauthorized relays or retransmissions, as “aggravated violations.”\textsuperscript{115} People using these techniques in violation of Section 7704(b) would be subject to “sharply increased liability.”\textsuperscript{116} Finally, Section 7704(d) imposes a “requirement to place warning labels on commercial [emails] containing sexually oriented material.”\textsuperscript{117}

\textsuperscript{107} The Federal Trade Commission, through regulation, can modify the ten business day requirement to a more reasonable period of time depending on factors including the burdens imposed on senders of lawful commercial email. CAN-SPAM Act, 15 U.S.C.S. § 7704(c).


\textsuperscript{109} Id.


\textsuperscript{113} This section does not apply to commercial emails sent to recipients who have given prior affirmative consent. CAN-SPAM Act, 15 U.S.C.S. § 7704(a)(5)(B).


\textsuperscript{115} Id. § 7704(b).


\textsuperscript{117} CAN-SPAM Act, 15 U.S.C.S. § 7704(d).
3. Section 7705

Offered as an Amendment,118 Congress added Section 7705 to hold people liable if they promote their business, or allow it to be promoted, in spam emails which violate Section 7704(a)(1).119 This section does not rely on the Federal Trade Commission's ("FTC") ability to find out who "initiated" the spam emails.120 Instead, the purpose of this section was "to give the FTC a tool to more effectively 'follow the money' and enforce the law against businesses that hire spammers to send email to consumers in large volumes with deliberately falsified header information."121 Section 7705 also provides an alternative to the more difficult standard necessary in Section 7704 requiring proof that the business "procured" the spammer to send email on its behalf.122 However, there are important limitations included in the section.

First, section 7705(a) only applies to emails that contain false header information.123 This limitation protects legitimate marketers and retailers from violating this section given that they would not falsify the heading information in legitimate commercial emails.124 Second, promoted businesses are held liable only if: 1) they knew or should have known that their business was being promoted in falsified spam emails; 2) they received or are expected to receive an economic benefit; and 3) they took no reasonable action to stop the spam or report it to the FTC.125 The purpose of the last criterion is to shield legitimate marketers from prosecution in the event their business is promoted using "spoof emails."126 Third, section 7705 provides a safe harbor to third-parties who supply goods or services to persons in violation of section 7705(a). But this section does not protect third-parties who own more than fifty-percent of the business in question or those who benefited from their knowledge of the falsified spam.127 Section 7705(a) offers protection to


120. S. REP. NO. 108-102 at 19.

121. Id.

122. Id.


126. Spoof emails are a popular tactic used by spammers: they send unauthorized emails to consumers using the corporate name or an employee's email address. The email looks legitimate and tricks the consumer into believing the company sent the email. See S. REP. NO. 108-102, at 20.

third-parties such as web hosts, landlords, and equipment lessors. Finally, this section is limited to enforcement by the FTC.

4. Section 7706

Section 7706 is the enforcement clause, specifying those who have rights to enforce the provisions of the CAN-SPAM Act. While consumers do have statutory rights under the Act, the Act does not give consumers a private right of action. Instead, the Act provides standing to four different groups. First, section 7706 provides authority to the Federal Trade Commission ("FTC") to enforce the Act. The FTC regulates violations of the CAN-SPAM Act under the guise of Section 18(a)(1)(B) of the Federal Trade Commission Act ("FTC Act"), treating violations as if they were unfair or deceptive acts. The FTC is afforded all of the "jurisdictional, remedial, and civil enforcement provisions of the FTC Act." Second, section 7706 provides enforcement authority to certain other enumerated agencies. These agencies include the Office of the Comptroller of the Currency, the Securities and Exchange Commission, the Secretary of Transportation, and the Federal Communications Commission. Section 7706 also permits these agencies to exercise any authority granted to them by other laws. Third, section 7706 grants authority to an "attorney general of a State, or an official or agency of a State" to bring "a civil action on behalf of the re-

130. See id. § 7701(b)(3).
137. Id. § 7706(b)(1)(A).
138. Id. §§ 7706(b)(3)-(5).
139. Id. § 7706(b)(7).
140. Id. § 7706(b)(10).
141. Id. § 7706(c).
sidents of the State in a district court of the United States of appropriate jurisdiction."\textsuperscript{142}

The Act allows injunctive relief as well as actual or statutory damages.\textsuperscript{143} For injunctive relief, section 7706 does not require that the plaintiff allege or prove the state of mind required in sections 7704(a)(1)(C), (a)(2), (a)(4)(A)(ii)-(iv), (b)(1)(A), or (b)(3).\textsuperscript{144} However, except as provided in sections 7704(a)(1)(C), (a)(2), (a)(4)(A)(ii)-(iv), (b)(1)(A), or (b)(3), the Act requires the plaintiff to show that the defendant had actual or implied knowledge of the action violating the CAN-SPAM Act in order to recover monetary damages.\textsuperscript{145} Finally, section 7706 allows internet service providers (ISPs) to bring civil actions "in any district court of the United States with jurisdiction over the defendant."\textsuperscript{146} Civil actions may be sought for violations of Section 7704(a)(1), 7704(b), 7704(d), and 7704(a)(2)-(5).\textsuperscript{147} However, Section 7706 imposes two additional hurdles that ISPs must meet in order to prove violations within Section 7704. First, for violations of Section 7704(a)(2)-(5), it must be additionally established that there was a pattern or practice of violations.\textsuperscript{148} For example, the Fourth Circuit held that the mere allegation by an ISP of a failure to remove a single email address, particularly in the absence of any allegation of a failure to comply with other requests could not establish "a pattern or practice" of violations.\textsuperscript{149} Second, there is a special definition for "procure" that holds that to be liable under the "procure" clause,\textsuperscript{150} the defendant must have actual knowledge, or have consciously avoided the knowledge, that the person sending the emails was violating the CAN-SPAM Act.\textsuperscript{151} If the ISP can overcome either of these two hurdles, they can request injunctive relief, actual damages or statutory damages.\textsuperscript{152}

\textsuperscript{142} Id. § 7706(f)(1).
\textsuperscript{143} Id. § 7706(f)(1), (3).
\textsuperscript{144} Id. § 7706(f)(2).
\textsuperscript{145} Id. § 7706(f)(9).
\textsuperscript{146} Id. § 7706(g).
\textsuperscript{147} Id. § 7706(g)(1).
\textsuperscript{148} Id.; see also Omega World Travel v. Mummagraphics, Inc., 469 F.3d 348, 358 (4th Cir. 2006).
\textsuperscript{149} Omega World Travel, 469 F.3d at 358.
\textsuperscript{150} See Federal Trade Commission, supra note 88.
\textsuperscript{151} CAN-SPAM Act, 15 U.S.C.S. § 7706(g)(2); see also Hypertouch, Inc. v. Kennedy-Western Univ., 2006 U.S. Dist. LEXIS 14673 at 15-16 (N.D. Cal. 2006) (finding no evidence that an online university knew or avoided knowing that their marketing agents would violate the CAN-SPAM Act).
\textsuperscript{152} CAN-SPAM Act, 15 U.S.C.S. § 7706(g)(1).
5. Section 7707

This section is known as the preemption clause of the CAN-SPAM Act. It will be discussed in more detail below.\textsuperscript{153}

6. Section 7708, 7709 & 7710

Sections 7708-7710 called for reports to be created soon after the CAN-SPAM Act was enacted. One report was to be submitted to both the Senate and House of Representatives within six months detailing a plan and timetable for establishing a Do-Not-Email registry.\textsuperscript{154} The second report called for a "detailed analysis of the effectiveness and enforcement" of, as well as suggestions for modifications to, the CAN-SPAM Act and was to be submitted within 24 months.\textsuperscript{155} A third report, to be submitted within nine months, called for the creation of a system that would reward those who supplied information concerning violations of the CAN-SPAM Act.\textsuperscript{156} The final report, to be submitted within eighteen months, required the detailing of a plan that would require commercial electronic mail (spam) to be identifiable from its subject line.\textsuperscript{157}

7. Section 7711, 7712 & 7713

Section 7711 gives the FTC the ability to issue regulations in order to implement the provisions of the CAN-SPAM Act;\textsuperscript{158} however, the regulations cannot require the insertion into any particular part of an email of "specific words, characters, marks, or labels" or those requirements set forth in Section 7704(a)(5)(A).\textsuperscript{159} The CAN-SPAM Act specifies its application to

---

\textsuperscript{153} See infra Part III.B.


\textsuperscript{158} CAN-SPAM Act, 15 U.S.C.S. § 7711(a).

\textsuperscript{159} \textit{Id.} § 7711(b).
the wireless realm by expressly stating its inability to "preclude or override" sections of the Communications Act of 1934\textsuperscript{160} and the Telemarketing and Consumer Fraud and Abuse Prevention Act.\textsuperscript{161,162} The CAN-SPAM Act also calls on the Federal Communications Commission to publicize rules aimed at protecting consumers from unwanted "mobile" service messages.\textsuperscript{163} Finally, the last section, Section 7713, is a separability clause allowing the portions of the Act not at issue to remain effective in the event that a provision or an application of the Act is held invalid.\textsuperscript{164}

III. THE CAN-SPAM ACT § 7707

An important section in the CAN-SPAM Act that requires a separate analysis is the preemption clause. A brief discussion of Federal preemption is followed by an extensive look at what is contained in the preemption clause of the CAN-SPAM Act. Following this analysis is a look at White Buffalo, a case that wrestled with two conflicting interpretations inherent in the preemption doctrine and Omega World Travel, a case that further defined an exception to the preemption clause.

A. Preemption Precedence

Federal preemption stems from the Supremacy Clause of the United States Constitution. This clause provides that "[t]his Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land . . . any Thing in the Constitution or Laws of any State to the Contrary notwithstanding."\textsuperscript{165} From this clause our jurisprudence has established three circumstances in which a federal law preempts a state law.\textsuperscript{166} First, and easiest to apply, is referred to as express preemption and arises when Congress has explicitly defined the extent to which the Federal law preempts state laws.\textsuperscript{167} Under this circumstance, Congress has made its intent known through the statutory language.\textsuperscript{168} The second circumstance, field preemption, occurs when state laws attempt to regulate conduct in a field that Congress intended federal law to regulate exclusively.\textsuperscript{169} This intention manifests itself when the "scheme of federal regulation [is] so perva-

\begin{footnotes}
\item[162.] CAN-SPAM Act, 15 U.S.C.S. § 7712(a).
\item[163.] Id. § 7712(b).
\item[164.] Id. § 7713.
\item[165.] U.S. Const. art. VI, cl. 2.
\item[167.] Id; see e.g., Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 95-100 (1983).
\item[168.] English, 496 U.S. at 79.
\item[169.] Id; see e.g., Rice v. Santa Fe Elevator Corp., 331 U.S. 218 (1947).
\end{footnotes}
sive as to make reasonable the inference that Congress left no room for the States to supplement it” or when federal interest in a field is “so dominant that the federal system will be assumed to preclude enforcement of state laws on the same subject.” Finally, the last circumstance in which federal law preempts state law is conflict preemption. Under conflict preemption, a federal law preempts a state law when it becomes impossible for one to simultaneously comply with both the federal and state laws, or when a state law “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.”

Fundamental to all of these situations is the question of Congressional intent to preempt state law. When evaluating circumstances under the Supremacy Clause, the underlying assumption as to federal preemption is that Congress does not intend to displace state law. However, if preemption was Congress’s “clear and manifest purpose[,]” a federal act will supersede state laws or regulations.

B. Section 7707

Referred to as the preemption clause, section 7707 expresses the CAN-SPAM Act’s effect on other federal and state laws. As for federal laws, section 7707 provides that nothing in the Act interferes with the enforcement of Sections 223 and 231 of the Communications Act of 1934, or federal criminal statutes, including United States Code chapter 71 of title 18 relating to obscenity and chapter 110 of title 18 relating to the sexual exploitation of children. The Act also does not interfere with the FTC’s ability to enforce actions under the Federal Trade Commission Act for “materially false or deceptive representations or unfair practices in commercial electronic mail messages.”

171. Indus. Truck Ass’n v. Henry, 125 F.3d 1305, 1309 (9th Cir. 1997).
172. English, 496 U.S. at 78-79.
173. Id.
174. Id.
178. Id. § 231.
180. 18 U.S.C. §§ 2251-2260A.
182. Id. § 7707(a)(2).
The preemption clause does provide for displacement of state laws, however, by stating:

This Act 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.183

The state laws that the Act preempts are those that require specific labels on some or all commercial emails, require specific content to be contained in commercial emails, or define specified formats that commercial emails must follow.184 Congress’s goal behind section 7707(b)(1) was to create a national standard to eliminate the difficulty legitimate businesses had in determining which State laws to adhere to in their business dealings.185 Congress included an exemption for state laws that prohibit falsity or deception because Congress understood that legitimate businesses would not be using deception in their emails, and therefore would be unaffected by the exemption. In addition, Congress exempted state laws that can apply to electronic mail, but are not specific to it, like contract or tort law.186 Finally, the Act does not affect the “adoption, implementation, or enforcement by a provider of Internet access service of a policy declining to transmit, route, relay, handle, or store certain types of electronic mail messages.” Congress did not want to impede an ISP’s “efforts to filter or block emails traversing their systems.”188

C. White Buffalo Ventures v. University of Texas at Austin

While the preemption clause’s statutory language appears to be clear, two important cases have sought to further explain its application. The first case involved the University of Texas’s (UT) regulation of unsolicited commercial emails from White Buffalo Ventures, LLC (White Buffalo).189 At

183. Id. § 7707 (b)(1).
185. Id.
187. Id. § 7707(c).
189. White Buffalo Ventures, LLC v. University of Texas at Austin, 420 F.3d 366, 368 (5th Cir. 2005).
issue, with regards to the CAN-SPAM Act, was whether federal law preempted UT's internal anti-spam policy. This represented the first case in which a court evaluated the preemption clause of the CAN-SPAM Act. The court likened the case to a Venn diagram, where one circle represents state action that is expressly preempted by federal law, the other circle represents Internet Access Providers (IAP, aka ISP) that are expressly exempted from preemption, and the common middle section that represents state entities that are themselves considered IAPs. It was up to the Fifth Circuit to decide which circle controlled the middle section.

UT provided free Internet access along with email addresses at the domain “utexas.edu” for their faculty, staff, and students. The email accounts were stored on one of UT’s 178 servers and were accessible either: 1) on school property through wired, authenticated ports or through wireless connectivity, or 2) by logging in remotely using an individual’s own IAP. Through their general policy against solicitation, UT instituted procedures that combat unsolicited emails sent to the domain “utexas.edu.” Specifically, whenever complaints, system monitors, or other devices indicated the existence of unsolicited emails, the technology department (“ITC”) worked to block or stop the transmission of these emails, sometimes providing notice to the sender.

White Buffalo operated an online dating service at “longhornsingles.com” that targeted University of Texas students. In February 2003, utilizing a Public Information Act, White Buffalo sought “all non-confidential, non-exempt email addresses” from UT. UT complied and turned over all qualifying email addresses to White Buffalo. A couple of months later,
White Buffalo started sending legal202 commercial spam to numerous people in the UT community.203 After receiving several complaints about the emails, UT's investigation revealed that White Buffalo had sent tens of thousands of unsolicited emails to UT email-account holders.204 Thereupon, UT sent a cease and desist letter, but White Buffalo refused to comply.205 They then blocked all emails from White Buffalo's IP address sent to addresses containing "@utexas.edu."206

White Buffalo responded by obtaining a temporary restraining order in state court.207 However, UT removed the cause to federal court for a preliminary injunction hearing, and the district court denied the injunction.208 Subsequently both parties conducted discovery and both moved for summary judgment.209 At the center of the case was the CAN-SPAM Act's preemption clause which once again states:

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 message or information attached thereto.210

White Buffalo's position was that UT was a state actor and the emails were not false or fraudulent,211 so the CAN-SPAM Act preempted UT's internal anti-spam regulations and prevented UT from blocking longhorningles.com emails to utexas.edu users.212 Given that no court had ever considered the preemption clause,213 White Buffalo relied solely on the text

202. The court presumed the emails to be legal "based on the record, the parties' agreement, and the absence of any challenge." Id. at 369 n.5.
203. Id. at 369.
204. Id.
205. Id.
206. Id.
207. Id. at 370.
208. Id.
209. Id.
211. See supra note 204.
212. White Buffalo Ventures, 420 F.3d at 371.
213. Id; Even though the Fifth Circuit had no knowledge of another court considering the preemption clause, the Eastern District of Washington had in fact applied the clause a month earlier. See Gordon v. Impulse Marketing Group, Inc., 375 F. Supp. 2d 1040, 1044-46 (E.D. Wash. 2005).
of the clause to support their position. The district court disagreed and granted summary judgment to UT on the basis of four determinations. The court held that: 1) Congress did not intend, in passing the CAN-SPAM Act, to “preempt technological approaches to combating spam,” 2) Section 7707(c) specifically exempts UT from preemption, 3) UT’s anti-spam policy is a part of the larger anti-solicitation policy and under Section 7707(b)(2) is exempt from preemption, and 4) Section 7707(b)(1) does not apply because UT’s anti-spam policy is not a “statute, regulation, or rule of a State or political subdivision of a state.” In the Fifth Circuit’s analysis, they did not specifically address all of these determinations in their affirmation of the district court’s summary judgment, instead taking a different approach and discussing them when appropriate.

Two meager attempts by UT to claim an exemption from the preemption clause were quickly disposed of by the Fifth Circuit. First, UT argued that Section 7707(b)(1) applied to state political subdivisions and that ITS was not a political subdivision of the state. The Fifth Circuit found the argument meritless, as UT is a public school. Second, UT attempted to convince the court that the CAN-SPAM Act’s preemption clause pertained to state rules relating to the “sending” of unsolicited commercial emails. UT pointed to Congress’s use of the word “send” in the Act and contended that the CAN-SPAM Act only regulated the sending of spam, and not the receipt; ITS’s anti-spam policy regulated only the “receipt” of spam. The Fifth Circuit “decline[d] to imbue the word ‘send’ with the particular significance UT urge[d].” Instead, the court recognized that all email is both “sent” and “received,” and an emphasis on a distinction between the two should not be made under this particular provision.

With respect to the CAN-SPAM Act, the Fifth Circuit devoted a majority of its discussion to White Buffalo’s argument that Section 7707(b)(1) expressly preempts UT’s internal regulations. The court recognized and created the Venn diagram idea by pointing out that Section 7707, in addition to

214. White Buffalo Ventures, 420 F.3d at 371.
215. Id. at 370-71.
216. Id. at 371.
217. Id.
218. Id. at 372 n.10.
219. Id.
220. Id.
221. Id. at 372 n.11.
222. Id. at 372.
223. Id. at 372 n.11.
creating preemption, also identifies a set of entities that are exempt from any preemptive effect. Specifically,

Nothing in this Act shall be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

In the creation of Section 7707, Congress failed to contemplate, as this case presented, the instance when the state actor also acts as an IAP. As a result of the two competing subsections, the court identified two potential interpretations of the Act: 1) "state entities may not regulate commercial speech except where that regulation relates to the authenticity of the speech's source and content," and 2) "state entities may implement a variety of non-authenticity related commercial speech restrictions, provided the state entity implementing them is an Internet access provider." The Fifth Circuit began with the understanding that preemption jurisprudence has established an assumption against preemption of state law. Given the jurisprudence of a "strong" presumption against preemption and the "textual ambiguity" of Section 7707, the court determined that the clause exempting IAPs should prevail over the preemption clause. The court next examined whether UT qualified as an IAP, falling within the exception granted in Section 7707. The district court found that UT "is certainly a provider of Internet access service to its students, if not to its employees and faculty, so it is expressly authorized under the statute to implement policies declining to transmit, route, relay, handle, or store spam." While the district court felt "certain" that UT qualified as an IAP, the Fifth Circuit pointed out that the district court made its determination without any reference to the definition provided in the statute. Therefore, the court focused its attention on the statutory definition, which defines IAPs as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access

224. Id. at 371; see also CAN-SPAM Act, 15 U.S.C.S. § 7707(c).
226. White Buffalo Ventures, 420 F.3d at 372.
227. Id.
228. Id. at 370.
229. Id.
230. The court actually declared twice that UT's internal anti-spam policy was not preempted by the CAN-SPAM Act before determining whether UT qualified as an IAP. See id. at 372-73.
231. Id. at 373.
232. Id.
to proprietary content, information, and other services as part of a package of services offered to consumers.”" Under this definition, UT did provide Internet access service anytime an individual sat down at a computer terminal on campus. However, the court carefully pointed out that even though individuals can access their email remotely, this did not affect the status of being an IAP. The court held that UT qualified under the Section 7707(c) exception because they were “hard-pressed to find that providing email accounts and email access [did] not bring UT within the statutory definition” of an IAP. The Fifth Circuit concluded with an interesting public policy argument that it would be an “unusual policy” to find UT’s anti-spam regulations preempted, but allow a private educational institution, under the same facts, to protect the interests of its online community. However, the court was quick to point out that the “prudence of the policy” did not predetermine their decision that UT should be considered an IAP under the Act.

D. Omega World Travel, Inc. v. Mummagraphics, Inc.

The second case involved Mummagraphics' receipt of email advertisements about cruise vacations from Omega World Travel (Omega) through Cruise.com, a wholly owned subsidiary. Mummagraphics sought statutory damages, alleging that Omega's emails violated both the CAN-SPAM Act and Oklahoma law regulating emails. The court's interpretation and application of the CAN-SPAM Act's preemption clause is the focus of this section.

Mummagraphics was an Oklahoma company that provided online services such as hosting webpages, registering domain names, and setting up computer servers. Their domain name was webguy.net and they used the

233. CAN-SPAM Act, 15 U.S.C.S § 7702(11) (importing the definition from the Communication Act of 1934, 47 U.S.C. § 231(e)(4)). The court actually referred to the use of the Internet Tax Freedom Act for the definition; however, the language in both acts is identical.

234. White Buffalo Ventures, 420 F.3d at 373.

235. Id.

236. Id.

237. Id. at 373 n.13.

238. Id.

239. Omega World Travel v. Mummagraphics, Inc., 469 F.3d 348, 350 (4th Cir. 2006). There were three named appellees in the suit: Omega World Travel, Inc., Gloria Bohan, Omega's president and founder, and Cruise.com, the wholly owned subsidiary of Omega. For purposes of this comment, Omega will be used to collectively refer to all three appellees.

240. Id.

241. Id. at 350-51.
email account "inbox@webguy.net" for company purposes.\textsuperscript{242} Cruise.com, operating online, sold cruise vacations and advertised by sending emails called "E-deals."\textsuperscript{243} Between December 29, 2004, and February 9, 2005, Omega sent eleven "E-deals" to Mummagraphics’s "inbox@webguy.net."\textsuperscript{244} Also during this period, Mummagraphics expressed to Omega through telephone conversations and letter correspondence their desire not to receive any more "E-deal" messages and their intention to file suit if the emails continued.\textsuperscript{245} When they continued to receive "E-deals" emails after this plea and Omega refused their settlement offer, Mummagraphics posted information pertaining to Omega on their "anti-spam" website, labeling Omega as a "spammer" who violated state and federal law.\textsuperscript{246} This action resulted in the commencement of a defamation suit against Mummagraphics, who responded with counterclaims against Omega for violating federal and Oklahoma law.\textsuperscript{247} On appeal, only the counterclaims came before the Fourth Circuit.\textsuperscript{248} With respect to the counterclaims, Mummagraphics alleged that the "E-deals" emails "contained actionable inaccuracies and that [Omega] failed to comply with federal and state requirements that they stop sending messages to [Mummagraphics]."\textsuperscript{249} After both parties requested summary judgment, the district court granted summary judgment for Omega, holding that (1) the CAN-SPAM Act preempted Mummagraphics’ Oklahoma state law claims, and (2) Omega did not violate the CAN-SPAM Act.\textsuperscript{250} The district court held that the Oklahoma state law claims were preempted "insofar as they applied to immaterial representations."\textsuperscript{251} Mummagraphics chal-

242. Id. at 351.
243. Id.
244. Id.
245. Id.
246. Id. at 351-52.
247. Id. at 352; The primary Oklahoma provision Mummagraphics relied on provides:

   It shall be unlawful for a person to initiate an electronic mail message that the sender knows, or has reason to know:
   (1) Misrepresents any information in identifying the point of origin or the transmission path of the electronic mail message;
   (2) Does not contain information identifying the point of origin or the transmission path of the electronic mail message; or
   (3) Contains false, malicious, or misleading information which purposely or negligently injures a person.


248. \textit{Omega World Travel}, 469 F.3d at 352.
249. Id.
250. Id.
251. Id. at 353.
lenged this determination relying on the CAN-SPAM Act’s exclusion from preemption for state laws that “prohibit falsity or deception.” In other words, the Fourth Circuit needed to decide if the exception for state laws prohibiting “falsity” or “deception” gave power to the states to prohibit immaterial or bare errors in emails.

The Fourth Circuit began their analysis of the CAN-SPAM Act’s preemption clause by underscoring their respect for the basic principles of preemption and a presumption against federal preemption, but in the end they agreed with the district court that preemption prevails. In their interpretation of the preemption clause, the Fourth Circuit did not believe the exception provided for states was straightforward and their analysis involved an attempt to define “falsity” and “deception.” The Court quickly determined, without analysis, that “deception” requires more than bare error and proceeded to devote the majority of their time defining “falsity.”

To determine the expansiveness of “falsity” the Fourth Circuit first considered the word in isolation. Using dictionary definitions, the Court was unable to unambiguously define the intended scope of “falsity” because it recognized that “falsity” can be defined as simply “untrue,” but it could also “convey an element of tortiousness or wrongfulness.” Next, the Court proceeded to consider the word in relation to the whole clause, using the maxim “noscitur a sociis” (“a word is generally known by the company that it keeps”). It was here that the Court began to find support that “falsity” did not refer to bare errors. “Deception” is one of the several tort actions based upon misrepresentations and the pairing of “falsity” with it suggests that Congress intended for “falsity” to refer to torts involving misrepresentation, and not to other errors. Additionally, in Section 7704(a)(1), Congress uses the title “[p]rohibition of false or misleading transmission information,” to expressly “prohibit[] only header information that is ‘materially’ false or ‘materially’ misleading.” Utilizing the “normal rule of statutory construction” where “identical words used in different parts of the same act are in-

253. Omega World Travel, 469 F.3d at 353.
254. Id. at 352-53.
255. Id. at 354.
256. Id.
257. Id.
258. Id.
259. Id.
260. Id.
261. Id. (emphasis added by court); see also CAN-SPAM Act, 15 U.S.C.S. § 7704(a)(1).
tended to have the same meaning,"262 this link to materiality suggests once again that Congress did not intend "falsity" to include bare errors.263 Regardless of whether the link is to deception or materiality, the Fourth Circuit found support that bare errors were not intended to be covered by Congress’s use of the word "falsity" in the preemption exception.264

The Fourth Circuit strengthened their conclusion by discussing the policy elements behind the creation of the CAN-SPAM Act.265 The Court identified, through the enacted findings in Section 7701, Congress’s balancing between "preserving a potentially useful commercial tool and preventing its abuse."266 Congress struck this balance by targeting "only emails containing something more than an isolated error."267 The court expressed concern that this balance would be undermined if "falsity" were to encompass bare errors.268 Also, the national standard Congress intended to create with the Act would be reduced to irrelevancy; "the strict liability standard imposed by a state such as Oklahoma would become a de facto national standard."269 The exception to preemption would thus be "a loophole so broad that it would virtually swallow the preemption clause itself."270 States could effectively make all errors in emails actionable, impeding "unique opportunities for the development and growth of frictionless commerce."271 In light of the policies behind the Act, the Fourth Circuit concluded that defining "falsity" as including bare errors was "not compatible with the structure of the CAN-SPAM Act as a whole."272

IV. IS THE CAN-SPAM ACT A FALSE HOPE?

When the CAN-SPAM Act was first announced, it was likely that many people hoped the days spent ("wasted") sorting through unsolicited commercial emails would soon be over. After all, is that not what the "Controlling the Assault of "Non-Solicited" Pornography and "Marketing" Act was supposed to do? While this optimism might have been carried by some, others

262. Omega World Travel, 469 F.3d at 354 (citing Gustafson v. Alloy Co., 513 U.S. 561, 570 (1995)).
263. Id.
264. Id.
265. Id. at 354-55.
266. Id.; see also CAN-SPAM Act, 15 U.S.C.S. § 7701.
267. Omega World Travel, 469 F.3d at 355.
268. Id.
269. Id. at 355-56.
270. Id. at 355.
271. Id. (citing CAN-SPAM Act, 15 U.S.C.S. § 7701(a)(1)).
272. Id. at 356.
quickly realized\textsuperscript{273} that in fact the CAN-SPAM Act would have other consequences. Four issues arising from the text of the Act and subsequent decisions by the courts support this view that the CAN-SPAM Act was nothing but a false hope.

The first issue with the CAN-SPAM Act is the allowance of legitimate commercial marketers to continue sending unwanted commercial emails as long as they comply with the specified guidelines in the Act. How does this help consumers whose inboxes are flooded with spam, or the networks whose resources are strained by the large influx of spam emails? Remember the problems associated with spam discussed earlier in the comment\textsuperscript{274} - annoyance, costs, etc. Those problems never indicated they were singularly attributed to fraudulent spam and in no way occurred when originating from legitimate sources; a distinction was not made. As defined in the beginning, spam is "unsolicited email," meaning unwanted, not that it is wanted if it comes from legitimate sources and meets detailed requirements. While it is nice to have opt-out options available, consumers want to save time, not spend extra time opting-out of all their spam emails. Consumers want their inboxes free of emails that they were not looking forward to, or did not request. Some business consumers might be too busy with higher corporate priorities to deal with spam, or might lack sufficient resources to process it. Congress even recognized that email has become extremely important and relied on by millions of Americans for commercial purposes.\textsuperscript{275} So why would Congress allow commercial marketers to continue invading this vital business communication tool? Why would Congress want to allow marketers to plague and interrupt an important, evolving area of commerce? It is not as if commercial marketers don't have ample opportunities in other areas to bombard us with advertisements during our personal time. Billboards, signs on buses, banners on websites, and even the five commercial breaks during our favorite one-hour television show\textsuperscript{276} provide plenty of opportunities for legitimate marketers to shower consumers with unwanted solicitations. It is apparent that Congress made the choice to focus on email as a marketing opportunity and assist in its development, instead of protecting consumers from all "unwanted" solicitations. The statutory text of the CAN-SPAM Act simply provides guidelines for legitimate marketers to effectively create "legal" spam. A stricter law addressing consumers' concerns about the receipt of "unsolicited" email could have prohibited all unsolicited email.


\textsuperscript{274} See supra Part I.C.


A stricter law would not place responsibility on the consumer to actively participate in an opt-out program to force the cessation of unsolicited email. In the end, while consumers were optimistic Congress would fight spam in an attempt to protect consumers and vital resources, Congress simply legalized spam in an attempt to protect the unique opportunity in the "development and growth of frictionless commerce."  

A second issue with the CAN-SPAM Act is that it unproductively focuses on illegitimate marketers responsible for sending fraudulent emails. Section 7704 strives to prohibit a false or misleading transmission of information, prohibit deceptive subject lines, including return email addresses—all techniques employed by malicious spammers. In essence, this legislation is aimed at those spammers who have been content obtaining email addresses and menacing consumers with their deceptive emails in the face of applicable FTC laws. But did Congress really believe that focusing on those committed to deceiving consumers through fraudulent emails would suddenly force them to conform to societal rules? Some could point out Congress’ inclusion of Section 7705 as being productive. It could be seen as an attempt to hold businesses accountable for employing spammers who promote their business through spam emails. But the Act requires a standard of knowing or should have known in the ordinary course of business, both of which create problems. First, if the business knows that the person they are utilizing is promoting the business through fraudulent or deceptive means, are they not in the same category as the spammers who are unlikely to be deterred by new legislation? Isn’t it more likely that these shady businesses will increase their efforts to help spammers remain untraceable as opposed to suddenly promoting their business in legitimate ways? Second, how do you define “ordinary course of business” in relation to email when it is an emerging and developing marketing tool? Do the businesses need to be aware of the deception before the emails are sent, or do they meet the “should have known” standard only after consumers complain to them directly about being deceived? Also, who should define this—judges, the technology industry, both? Finally, some could argue that the CAN-SPAM Act’s classification of spamming techniques as aggravating and the ability of the FTC to specify additional activities as aggravating is productive in the fight against malicious spammers. Even if the CAN-SPAM Act was productive in fighting malicious spam, this section is simply reactive, rather than proactive toward spammers. New techniques, such as botnets, are constantly being discovered and used by malicious spammers. The FTC would be reacting to the old techniques, while spammers were moving on to their new inventive methods.

280. Id. § 7704(c)(2).
281. See MessageLabs, supra note 3.
of gathering emails and deceiving consumers. Legislation would become a patchwork exercise as the FTC would just continue adding on techniques to be classified as aggravating violations. Ask Microsoft Windows users or other software consumers how they appreciate patches as solutions to problems created by spiteful technological exploiters. While the CAN-SPAM Act’s attention on dishonest marketers supplies consumers with the anticipatory hope that they will no longer be subjected to malicious emails, the circumstances suggest that it is ultimately a futile endeavor.

Both of the aforementioned issues lead directly to the third issue with the CAN-SPAM Act—Congress has simply shifted the burden of protecting consumers from spam to providers of internet access or email. As discussed above, Congress allows legitimate marketers to send spam (assuming it meets the requirements), while hopelessly attempting to control illegal spam; consumers despise both forms of spam. Congress has essentially appropriated the responsibility to internet access and email providers to discover and implement technological solutions that eliminate all “unsolicited” commercial email. The problems associated with spam will only be avoided if “all” of the unsolicited commercial email is eliminated. The current approach to accomplish this is not relying on and enforcing the CAN-SPAM Act, but through the evolution of filtering technology created and paid for by those affected most—internet access or email providers. When a consumer gets inundated with spam, even if all are legal commercial emails, they will not stop to think to blame Congress for their inadequate legislation. Instead, they will look to the top of the webpage and identify the name of their email or internet service provider. This is most evident in the White Buffalo case, where it was agreed that White Buffalo legally obtained addresses and sent legal commercial spam to thousands of members of the University of Texas community. However, those members complained to the University of Texas, who was forced for consumer satisfaction purposes to institute a filter blocking all of White Buffalo’s emails. Consumer satisfaction was achieved as a result of the University using resources to implement a filter technology adequate enough to block all of White Buffalo’s emails, not as a result of the enforcement of the CAN-SPAM Act. In fact, it was the Fifth Circuit’s interpretation of the preemption clause of the CAN-SPAM Act as applied to internet providing state actors that allowed the University to regu-

282. While we continue to search for solutions addressing the spam problem in relation to email, spammers are quickly moving to exploit new areas, such as cell phones. See CNNMoney.com, Get outta my phone!, Feb. 9, 2007, http://money.cnn.com/magazines/fortune/fortune_archive/2007/02/19/8400173/index.htm?postversion=2007020906 (last visited Dec. 1, 2007). Even though the CAN-SPAM Act addresses this issue in Section 7712, this is another example of the reluctant search for new methods to deceive consumers by spammers.


284. White Buffalo Ventures, 420 F.3d at 369 n.5.

285. Id. at 369-70.
late its email system. Otherwise, had the CAN-SPAM Act preempted the University of Texas's regulations, White Buffalo's emails would have had to be received, forcing complaining members to go through the hassle of opting-out. The decision in effect encourages state actors to use resources to provide email accounts and email access in order to be exempt from preemption; only then will state actors be able to implement their own regulations to satisfy their consumers. What kind of legislation encourages the investment into resources in order to be exempt from the legislation in order to provide total consumer satisfaction? The CAN-SPAM Act and the interpretation of the preemption clause in White Buffalo signify Congress's failure to actively solve consumer concerns about spam and their willingness to burden others with the responsibility.

A final issue with the CAN-SPAM Act is apparent in the preemption doctrine's text and in Omega World Travel—states are unable to protect their citizens from spam. Instead, they are forced to rely on an inadequate federal statute. The preemption doctrine was included in the Act in order to supersede differing state and local statutes and create a national standard to govern commercial emails. While I agree that creating a national standard for fighting spam is the correct move, it must be a strict standard providing consumers the protection that they seek. The Fourth Circuit's interpretation of the preemption clause in Omega World Travel highlights the conclusion that the CAN-SPAM Act is a weak national standard. The decision in Omega World Travel is not at issue, as I believe it was rightly decided within the terms of the CAN-SPAM Act. If the CAN-SPAM Act supported a "bare-error reading of falsity," the exception to the preemption provision would categorically be turned into a loophole "so broad that it would virtually swallow the preemption clause itself." Because the Oklahoma statutes are preempted insofar as they apply to immaterial misrepresentations, the problem arises in the fact that Mummagraphics was forced to rely on the national standard encompassed in the CAN-SPAM Act. While the receipt of numerous unsolicited "E-deals" is a good example of the problem consumers face and want eliminated, under the national standard, Mummagraphics was left powerless against this form of legal spam. The inability of a national


287. I specify "within the terms of the CAN-SPAM Act" because I disagree with Congress' desire to protect law-abiding senders of unsolicited commercial spam. I would opt for legislation that prohibited all forms of unsolicited commercial email; but I agree with the Fourth Circuit's interpretation of the text of the preemption clause as it is.

288. Omega World Travel, 469 F.3d at 355.

289. Id. at 351-356.

290. Id. at 357-58.
standard to provide protection under those circumstances to a consumer such as Mummagraphics indicates its futility. While the CAN-SPAM Act is believed to be a consumer-friendly statute, it instead cuts the knees off of states in their attempt to protect their citizens as consumers, and forces consumers to rely on a national standard that provides less protection.\footnote{See Spamhaus, supra note 273.} In fact, a national standard exists that legalizes spam.

In the end, the CAN-SPAM Act simply created a false hope. While it seemed that Congress was proactively attempting to protect the consumer from unwanted commercial solicitations, they instead invite spam by legalizing it, fruitlessly fight fraudulent spam from illegitimate spammers, shift the burden and costs of meeting consumers’ expectations (those that were supposed to be met by the CAN-SPAM Act), and usurp states in their attempt to protect their citizens as consumers.

V. CONCLUSION

It has been three years since the CAN-SPAM Act went into effect. Since that time, the war on spam has continued to escalate as spammers produce inventive new methods to skirt the law and technology, while email providers scramble to update filtering technologies to successfully eliminate spam. It is unclear if there will ever be a complete solution; it is unquestioned that corrupt individuals determined to overcome obstacles and defy laws in order to maliciously trick people will always exist. Maybe the solution lies in the form of stricter legislation; maybe the answer lies in the form of advanced technology and software processes; or maybe a combination of both is required. Maybe the problem needs to be addressed by privacy laws, in terms of the right to be left alone, or some other form of tort laws. Regardless, the first question that must be answered is whether we should treat email as a private personal item or as a commercial advertising medium. Only after that decision is made can we begin moving toward a unified standard in how to treat spam—a standard that can be trusted by consumers and correctly defines their expectations. The first attempt by Congress with the CAN-SPAM Act failed miserably at this. The CAN-SPAM Act appeared to promise a lot, but ultimately delivered nothing . . . except more spam.