KELLEY DRYE

Overview of Current Spam Law & Policy

by
Glenn B. Manishin
Stephanie A. Joyce
KELLEY DRYE & WARREN LLP

Although unsolicited commercial electronic mail — commonly known as "spam" — has been around for many years, in the past 24 months the incidence and volume of spam appears to have increased geometrically.[1] This, in turn, has led to an almost predictable response from politicians (both federal and state) seeking to latch on to an issue that resonates with voters. The culmination of these efforts was the passage by Congress in December 2003 of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,[2] *i.e.*, the "CAN-SPAM Act" for short.

The CAN-SPAM Act's approach to unsolicited commercial email (sometimes referred to as "UCE") and the legislation's potential effectiveness have been widely criticized for failing to reflect the fact that most senders of commercial email advertisements ("spammers") operate outside the United States — often using transitory, well-disguised facilities and techniques — in order to evade detection or prosecution. And there is little sign that in the six months since its enactment, the CAN-SPAM Act has made any appreciable inroad into either the volume or sexually graphic nature of most spam.[3]

Nonetheless, the CAN-SPAM Act will certainly have a pronounced impact on the email marketing activities of hundreds of thousands of companies. As the product of political compromise, the legislation exhibits the ambiguity so often typical of legislation in complex technology areas. Consequentially, understanding the origins and development of spam law and policy is essential to operating effectively and lawfully under the CAN-SPAM Act. It is not so much that those who ignore history are doomed to repeat it, but rather than complying with a new law like the CAN-SPAM Act requires at least some insight into its origins and purposes.

---

[1] *See*, *e.g.*, N. Vogel, "Bill Would Ban Spam E-Mail in California," *Los Angeles Times,* Feb. 18, 2003 at B1.

[2] Pub. L. No. 108-87 (108th Cong., 1st Sess. 2003). The CAN-SPAM Act passed the Senate (S.877) on October 22, 2003, passed the House on December 8, 2003, and was signed by President Bush on December 16, 2003.

[3] *See*, *e.g.*, E. Sinford, "Spam Runs Rampant Despite CAN-Spam Act," *USA Today,* March 25, 2004, available at <http://www.usatoday.com/tech/columnist/ericjsinrod/2004-03-25-sinrod_x.htm>.

A. Background and Prior FTC Enforcement Activities

While the CAN-SPAM Act is very new, governmental efforts to attack spam are not. Since 1998, the Federal Trade Commission ("FTC") has aggressively pursued fraudulent or misleading UCE as an unfair and deceptive trade practice under the Federal Trade Commission Act.[4] The FTC reports that it receives more than 110,000 examples of spam on a daily basis and maintains a database of over 42 million unsolicited commercial email messages. At the state level, more than 20 states have passed anti-spam statutes in the past fives years (a total of 34 states passed legislation affecting commercial email, in one way or another, prior to 2004). Most of these statutes adopted so-called "opt-out" and labeling requirements for commercial email, generally applying these mandates to unsolicited commercial email.[5] The CAN-SPAM Act follows this majority approach by applying an "opt-out" requirement to commercial email and banning fraudulent or deceptive email practices — including specifically the use of false or deceptive "From", "To" and "Subject" headers ("spoofed" email) — but also permits the FTC to expand the range of impermissible email practices by rulemaking.[6]

Acting under its general authority to proscribe unfair and deceptive trade practices, the FTC has brought more than 50 enforcement actions under the FTC Act against Internet marketers who used spam to promote get-rich quick scams and other misleading schemes. These include, for example:

(1) *Mega$Nets* (FTC 1998) — consent decree with supplier of pyramid software based on deceptive profit claims.[7]
(2) *Cyberpromoters* (FTC 1999) — consent decree with supplier of mailing list software based on misleading promotional claims.[8]
(3) *G.M. Funding* (C.D. Cal. 2002) — deceptive trade practice complaint against spammer based on "spoofing" email addresses.[9]

---

[4] 15 U.S.C. § 41 *et seq.* 15 U.S.C. § 45(a)(1) makes unlawful all "unfair or deceptive acts or practices in or affecting commerce" and gives the FTC the power to proscribe and penalize violations.

[5] "Opt-out" refers to a negative-consent option, under which the recipient of a commercial email message has the option to reject future messages by affirmatively declining. The opposite approach, known as "opt-in," was applied by a small minority of states, most notably California in a piece of legislation (S.B. 186) that was to have taken effect on January 1, 2004. As discussed further below, is widely believed that a principal impetus for passage of the CAN-SPAM Act at the federal level was the inclusion of provisions that preempt such state laws.

California Senate Bill No. 186, codified at Cal Bus. & Prof. Code §§ 17.259 *et seq*., was approved on September 23, 2003. S.B.186 requires, among other things, that the recipient of an "unsolicited commercial e-mail advertisement" must either (a) provide "direct consent to receive advertisements from the advertiser," or (b) have a "preexisting or current business relationship … with the advertiser" in order to make the initiation of such e-mails to a "California electronic mail address" permissible. Cal Bus. & Prof. Code § 17.259.1(o). S.B. 186 bans unsolicited commercial e-mail advertisements unless *either* of these criteria are satisfied. "Direct consent" is defined as the "express consent" of the recipient in response to a "clear and conspicuous request" or at the recipient's own initiative. *Id.* § 17.259.1(d).

[6] An April 2003 report by FTC Staff concluded that more than 65% of spam contains fraudulent or deceptive header information. *False Claims in Spam,* Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission (April 29, 2003).

[7] *In re Kalvin P. Schmidt et al.,* File No. 9723308 (FTC July 14, 1998).

[8] *In re LS Enterprises LLC,* File No. 972-3149 (FTC April 21, 1999).

[9] *FTC v. G.M. Funding, Inc., et al*., SACV 02-1026 DOC (MLGx) (C.D. Cal. 2002). This action was settled with a permanent injunction entered by stipulation on November 20, 2003.

(4) *Dario Va* (S.D. Fl. 2002), etc. — series of seven unfair trade practice complaints against "chain letter" spammers peddling get rich quick scheme.[10]

(5) *FTC Spam "Crackdown"* (Feb. 2002) — 2,000 warning letters issued to other "chain letter" spammers.[11]

Since 2002, the FTC has also organized a dozen or more joint "sweeps" with state and local law enforcement agencies, resulting in more than 400 enforcement actions targeting what it calls "Internet scams and telemarketing fraud."[12]

Nonetheless, prior to passage of the CAN-SPAM Act, the FTC declined opportunities to take a more generalized approach to spam through promulgation of regulations directly proscribing unfair and deceptive commercial email practices. Indeed, in January 2003, the agency rejected a petition for rulemaking filed by the Telecommunications Research and Action Center in favor of continued case-by-case enforcement, concluding that "the possible benefits promised by such a rule do not justify the significant expenditure of time and resources a rulemaking would require."[13] To "address various issues surrounding spam and to explore potential solutions to the spam problem," the FTC instead held a three-day "public forum" on April 30 through May 2, 2003.[14]

B. Overview of the CAN-SPAM Act of 2003

1. Scope

Passed quickly at the end of the first session of the 108th Congress in December 2003, the CAN-SPAM Act of 2003 adopts an approach to spam that differs materially from the legislation as introduced and passed by the Senate (S.877) and from the many state laws on which it was modeled. Most significantly, the scope of the Act is not limited to "unsolicited" commercial electronic mail and is not confined to bulk email marketing campaigns.[15] Rather, the Act applies

---

[10] *E.g., FTC v. Daria Va* (S.D. Fla. Feb. 12, 2002). *See* Press Release, FTC Launches Crackdown on Deceptive Junk E-Mail, Feb. 12, 2002, available at < http://www.ftc.govopa/2002/02/eileenspam1.htm>.

[11] "In addition to the settlements, the FTC announced that today it will mail warning letters to more than 2,000 individuals who are still running this chain letter scheme. The addresses were culled from the FTC's unsolicited commercial e-mail (UCE) database. Consumers currently send spam to the agency at a rate of approximately 15,000 e-mails a day using the agency's database address, uce@ftc.gov. The FTC has collected more than eight million spam messages since 1998." *Id.*

[12] *See, e.g.,* Press Release, FTC Details Efforts to Halt Internet Scams, March 23, 2004, available at <http://www.ftc.gov/opa/2004/03/scamtestimony.htm>; Statement of Chairman Timothy J. Muris, Federal Trade Commission, Before the Subcommittee on Commerce, Trade, and Consumer Protection, Committee on Energy and Commerce, United States House of Representatives, June 11, 2003, available at <http://www.ftc.gov/os/2003/06/030611murishr.htm>.

[13] Letter from Donald S. Clark, Secretary, FTC, to Dirck Hargraves, Esq., Counsel, Telecommunications Research and Action Center, Jan. 28, 2003, available at <http://www.ftc.gov/os/2003/02/spamltr.htm>.

[14] Press Release, Commission Denial of Petition for Rulemaking, Feb. 3, 2003, available at <http://www.ftc.gov/opa/2003/02/fyi0310.htm>.

[15] Because the legislation as enacted applies to all commercial electronic mail messages, whether or not solicited, the CAN-SPAM Act eliminates the concept of "implied consent" that was included in S.877 as passed by the Senate as well as the definition of "unsolicited commercial email" from the Senate bill. *See, e.g.,* S. Rep. No. 108-102, 108th Cong., 1st Sess. 14-16 (2003). The rapidity of the Act's final revisions raises considerable ambiguity,

to all "commercial electronic mail messages," which are defined as emails for which the "primary purpose" is the "advertisement or promotion" of goods or services, including Web sites.[16] On the other hand, the Act largely exempts "transactional or relationship messages" (defined to include order fulfillment, warranty information, etc.) and the "routine conveyance" of electronic mail (defined essentially as the transmission of such messages by Internet Service Providers, or "ISPs") from its substantive mandates.[17]

The CAN-SPAM Act to all "senders" who "initiate" or "procure" the transmission of commercial email messages, unless such a sender operates through clearly identified "separate lines of business," in which case the Act's mandates apply separately to each such line of business.[18] It imposes civil and criminal penalties, including injunctive and damages relief for ISPs and states acting *parens patriae*, on a sliding scale based on the volume of messages transmitted, but rejects any private right of action for individual consumers.

2. Basic Mandates

The CAN-SPAM Act's basic substantive requirements fall into five general categories.

False/Misleading Messages. The Act prohibits both commercial *and* transactional email messages that contain "materially false or misleading" header information or deceptive subject lines.[19]

Functioning Return Address. The Act requires that all commercial email messages contain a functioning return address of other Internet-based reply "opt-out" mechanism, for at least 30 days after transmission of a message.[20]

10-Day Prohibition. The Act prohibits a sender from transmitting commercial email messages to any recipient after 10 business days following the exercise by the recipient of his or her right to opt-out of future commercial email messages.

Disclosure Requirements. In addition to its prohibition of false or misleading header information, the Act requires that all commercial email messages disclose three specific items of content: (a) a clear and conspicuous identification of the message as an "advertisement or solicitation," (b) a notice of the opt-out mechanism, and (c) a "valid physical postal address." The Act separately requires the FTC to prescribe, and senders to utilize, a so-called warning label (termed a "mark or notice") for all commercial email "that includes sexually oriented material."

---

however, because the structure of the Senate bill, which differentiated between unsolicited and impliedly consented commercial email messages, was retained even though the substantive legal difference was deleted.

[16] Act §§ 3(2)(A), 15. As noted below, the FTC has opened a rulemaking to define precisely what is a "primary commercial purpose."

[17] *Id*. § 3(2)(B).

[18] *Id*. §§ 3(9), 3(12).

[19] *Id.* §§ 5(a)(1)-(2).

[20] *Id.* § 5(a)(3).

Aggravated Violations. In a special attack on what Congress viewed as particularly pernicious commercial email practices, the CAN-SPAM Act prescribes as "aggravated violations," warranting additional civil and commercial penalties, (a) e-mail "harvesting" or the knowing use of harvested addresses, (b) the automated creation of multiple e-mail accounts used for commercial e-mail, and (c) the use of unauthorized relays for commercial e-mail messages.

3. Third-Party Liability

Originating in an amendment sponsored by Sen. John McCain, the CAN-SPAM Act includes provisions that restrict the liability of third parties (despite the Act's application to parties that "procure" transmission of commercial email by third-party senders) for violation of the Act's prohibition on false and misleading commercial email messages.[21] Thus, an entity that has commercial email sent by a third party is nonetheless liable for unlawful message if it (1) reasonably knew that the third party sent emails on its behalf, (2) received or expected to receive an economic benefit from those messages, and (3) took no action to "prevent" or "detect the transmission and report it to the" FTC.[22] The third-party sender may also be liable, in addition to the sender, if the third party (1) owns greater than 50% of the sender, *or* (2) reasonably knew its products were being promoted by third-party, and (3) received or expected to receive an economic benefit.[23] According to Senate Report, this section is intended as "follow the money" hook for FTC enforcement if actual sender(s) cannot be located.[24]

4. Enforcement

The Act authorizes enforcement of its provisions by the FTC, including injunctive relief awardable without a showing of *scienter* ("actual knowledge") on the part of a defendant. Additionally, the CAN-SPAM Act authorizes *parens patriae* actions by state attorneys general for either injunctive or damages relief and creates a civil right of action by ISPs to recover actual or statutory damages or injunctive relief. In a significant concession, however, one at odds with prior legislation such as the "junk fax" law of 1991,[25] the Act does not provide a private right of action for consumers. As penalties, the Act specifies damages of $250 per message up to a $2 million cap.[26]

5. Preemption of State Laws

One of the more significant achievements of the CAN-SPAM Act is its establishment of a uniform, nationwide regime governing commercial email practices. In support thereof, the Act

---

[21] Act § 6.

[22] *Id*. § 6(a).

[23] *Id*. § 6(b).

[24] S. Rep. No. 108-102, 108th Cong., 1st Sess. 19 (2003).

[25] Telephone Consumer Protection Act of 1991 ("TCPA"), 47 U.S.C. § 227. TCPA authorizes private civil actions and establishes statutory liquidated damages. Consumers can bring private suits to enjoin the unlawful conduct and either recover the actual monetary loss stemming from the TCPA violation or receive up to $500 in damages for each violation, whichever is greater. The court may increase damages to $1,500 per violation if it finds that the defendant willingly or knowingly committed the violation.

[26] Act § 7(f)(3).

expressly preempts, in large part, the many state statutes affecting UCE that had been enacted in the five years preceding passage of the federal legislation.

The scope of federal preemption under the Act is both wide-ranging and somewhat unclear. On the one hand, the CAN-SPAM Act expressly supercedes "supersedes "any" state or local "statute, regulation, or rule" that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute . . . prohibits falsity or deception in any portion of a commercial electronic mail message[.]"[27] On the other hand, the Act provides that it does not affect "State laws that are not specific to electronic mail, including State trespass, contract, or tort law," or "other State laws to the extent that those laws relate to acts of fraud or computer crime."[28] The Senate Report explains that a state law "requiring some or all commercial e-mail to carry specific types of labels, or to follow a certain format or contain specified content, would be preempted."[29]

Although some aspects of the Act's preemption provisions are quite clear — most notably in that the Act overrules the California opt-in approach that would otherwise have become effective on January 1, 2004[30] — the practical impact of the Act's preemptive scope in detail will need to await judicial interpretation of state laws in specific enforcement proceedings and civil lawsuits. For instance, although the federal legislation does not permit consumer suits, many state laws do. It is unclear, therefore, whether the CAN-SPAM Act's preservation of state laws that prohibit deception in "any portion" of a commercial email message will also support state-law actions for damages by consumers based on false header information.

6. "Affirmative Consent" Exceptions

Although it rejects the notion of "implied consent" included within the bill passed by the Senate,[31] the CAN-SPAM Act nonetheless includes a definition of "affirmative consent," which is used to limit the scope of some of the Act's content mandates. Defined as "express" consent either by a recipient in response to a "clear and conspicuous" request or at the recipient's initiative,[32] affirmative consent operates under the Act to exempt commercial email messages from the 10-day opt-out requirement, the mandate that commercial email messages be identified as advertising, and the requirement that sexually explicit messages include the FTC-prescribed warning label.

Together with the "transactional or relationship message" exclusion, these provisions appear to establish a safe harbor in which business providing emails as a service (newsletters, periodical content, etc.) can operate, based on prior consent obtained from customers, without complying fully with all content mandates imposed by the Act. On the other hand, no affirmative consent suffices to override the Act's prohibitions on false and deceptive commercial email

---

[27] *Id*. § 8(b)(1).
[28] Act § 8(b)(2).
[29] S. Rep. No. 108-102, 108th Cong., 1st Sess. 21-22 (2003).
[30] *See* note 5 *supra.*
[31] *See* note 15 *supra.*
[32] Act § 3(1).

header information or the requirement that all commercial email messages include a functioning "opt-out" capability for recipients.

7. FTC Rulemakings

As noted, the CAN-SPAM Act delegates federal enforcement to the FTC, and also requires the FTC to further elucidate some of the Act's provisions via regulations. The Act required the FTC, within 120 days of enactment, to prescribe a warning label for commercial emails including sexually explicit materials. In addition, it requires the agency, within 12 months, to implement the Act's general "primary purpose" definition of commercial email messages via a rulemaking in which the agency is directed to "define[e] the relevant criteria to facilitate the determination of the primary purpose of an electronic mail message."[33] Finally, the Act gives the FTC the power (but not a duty) to modify the statute's 10-day opt-out requirement and to outlaw additional practices that are "contributing substantially to the proliferation of [unlawful] commercial electronic mail messages."

a. Sexually Explicit Email

On April 13, 2004, the FTC released Final Rule 316.1, 16 C.F.R. § 316.1, governing commercial email messages carrying sexually explicit content. The rule was published April 19, 2004 at 69 Fed. Reg. 21024 and became effective May 19.

This rule includes several disclosure requirements and content restrictions for messages containing "sexually oriented material" as that term is defined in 18 U.S.C. § 2256, which is a criminal statute prohibiting child pornography. That definition, entitled "sexually explicit conduct," covers "actual or simulated" sexual acts and "lascivious exhibition" of body parts. 18 U.S.C. § 2256(2). Where such content is included in an email, the initial message, termed "the initially viewable area" must be clear of sexually oriented content, requiring the recipient to "take further deliberate action" — a click-through — to view the content.

Thus, the initially viewable area must include *only* the following:

(1) "SEXUALLY-EXPLICIT:" must appear as the first 19 characters of the subject line;
(2) Sexually oriented content must not appear in the subject line;
(3) The message must provide "clear and conspicuous" notice that it is an advertisement;
(4) There must be "clear and conspicuous" opportunity to opt out;
(5) A functioning email address or URL must be provided;
(6) A "valid physical postal address" must be displayed; and
(7) Instructions or means of accessing the explicit content should be in the body of the message.

[33] Act § 3(2)(C).

16 C.F.R. § 316.1(a), 69 Fed. Reg. at 21033-34. None of these requirements apply to a message sent to a recipient that has already "given prior affirmative consent to the receipt of the message. *Id*. § 316.1(b), 69 Fed. Reg. at 21034.

The FTC terms these content requirements an "electronic brown paper wrapper," akin to how explicit magazines are sent through the mail in opaque wrapping. The purpose of the "wrapper" is to ensure that "the recipient is not bombarded with graphic sexual materials" in the body of the initial email. 69 Fed. Reg. at 21030. Accordingly, the FTC requires that "these materials cannot be located in the subject line or the area of the email that is initially viewable to an email recipient." *Id*.

The FTC's analysis creates a discrepancy with the text of Rule 316.1. May there be content in the initially viewable area other than what is required in Rule 316.1(a), so long as it is not sexually oriented? The question may be one of degree. That is, if the content is plainly innocuous, and does not approach the bounds of the definition in 18 U.S.C. § 2256, then its inclusion would not seem to run afoul of Rule 316.1. A strict interpretation, however, requires that no extraneous content appear at all. This discrepancy will most likely be clarified through actual FTC enforcement actions.

b. "Primary Purpose" Rulemaking

The FTC received more than 6,200 comments regarding its forthcoming definition of what constitutes a "primary commercial purpose." A great portion of these comments were one-paragraph form comments that "applaud the Commission" for its anti-spam efforts but express concern about "suppression lists" (a "Do-Not-Email Registry") that emailers must maintain to prevent transmissions to those who have opted out. Such lists, argues the form comment, "could easily fall into the hands of spammers, leading to more spam instead of less." The danger of suppression lists, particularly their costs, was the leading issue among the comments we have reviewed.

The FTC must adopt a final definition of "primary purpose" by December 16, 2004. Act, § 3(2)(c). In addition, the FTC must report to Congress by June 16, 2004, with "a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry," *id*. § 9(a), for which the FTC also ought comment in this rulemaking. (That report recently concluded that a Do-Not-Email registry was unnecessary and technically risky, especially as most spam violators exhibit little inclination to comply with legal requirements in the first place.)[34] Other issues presented for comment in the prinmary purpose rulemaking were the concept of a rewards program for reporting spam violations and the proper definition of a "sender" for purposes of the Act. Most likely, these questions will be resolved together with the mandatory "primary purpose" decision later this year.

[34] Act § 9(a). *See FTC Won't Create Do-Not-Spam List,* ComputerWorld, June 15, 2004, available at <http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,93844,00.html> To avoid the congressional authorization issues addressed by the federal courts in connection with the FTC's earlier Do-Not-Call registry,, the CAN-SPAM Act expressly authorizes the FTC to "establish and implement" a Do-Not-Email registry, but "no earlier" than nine months after enactment (Sept. 16, 2004). Act § 9(b).

C. State and Private Party Spam-Related Enforcement Actions

As should be obvious from the proliferation of state spam statutes preceding enactment of the CAN-SPAM Act, legal doctrine related to unsolicited commercial email also includes a developing body of law arising from both private and state-initiated lawsuits against spammers. Indeed, Private litigation against spammers, based on fraud, trespass, etc., dates to AOL's efforts in 1996 to block email from Cyber Promotions, Inc. (Sanford Wallace), a notorious bulk emailer.[35] In other significant actions:

- *April 2003* — AOL filed five civil lawsuits in Virginia (E.D. Va.) against spammers based on VA, WA and federal computer crime statutes.
- *May 2003* — EarthLink was awarded a $16 million default judgment and injunction against Howard Carmark for sending 825 million pieces of spam using EarthLink e-mail accounts.
- *June 2003* — Microsoft and Washington State Attorney General Christine Gregoire filed 15 parallel lawsuits against spammers under the Washington State anti-spam statute for forged addresses and deceptive headers.
- *December 2003* — Microsoft and New York Attorney General Elliot Spitzer filed parallel suits against Synergy6 Inc. and Scott Richter for sending illegal spam through 514 compromised IP addresses in 35 countries spanning six continents.
- *March 2004* — EarthLink, AOL, Microsoft and Yahoo! initiated a series of coordinated civil lawsuits under CAN-SPAM Act.

The vast majority of private and state civil actions against senders of UCE, nonetheless, have to date not resulted in a significant number of reported judicial decisions defining either common law tort theories applicable to spam (trespass, breach of "acceptable use" agreements and the like) or interpretation of state spam-specific laws. Many of them assert an array of different legal theories and frequently have resulted either in default judgments or decisions limited to *in personam* jurisdictional issues. As a consequence, while there has been much discussion and debate over how general tort and contract law should apply to the complex domain of Internet-based commercial email, there is little pre-CAN-SPAM Act decisional law on which to draw. It is also likely, as the March 2004 initiative by major ISPs suggests, that future private party lawsuits will proceeding directly under the CAN-SPAM Act itself. As the Act provides for state enforcement as well, it is also likely that state law enforcement actions will proceed, at least in part, under the federal regime.

D. Current Spam Law Issues

Although there remains a wide array of unsettled legal issues involving spam, this article focuses on three of the most significant issues of current importance.

[35] *See* <http://legal.web.aol.com/ decisions/dljunk/aolarchive.html>.

1. Constitutionality of the CAN-SPAM Act

While trade associations representing the direct mail industry aggressively (and eventually unsuccessfully) challenged the FTC's "Do Not Call" list in 2003,[36] no reported case or complaint to date has mounted a constitutional challenge to the CAN-SPAM Act. We believe that a constitutional challenge to the CAN-SPAM Act is unlikely to succeed if brought, however, based on prior decisions regarding the 1991 Telephone Consumer Protection Act.[37] Facing similar challenges to the prohibition on unsolicited facsimile advertisements under that statute, the federal courts had little difficulty holding that there was a sufficiently strong governmental interest in protecting consumers against unwanted and potentially misleading fax intrusions to meet the *Central Hudson* test applicable to restraints on commercial speech.[38]

2. Scope of State Law Preemption

As noted above, while state spam statutes imposing an opt-in regime (*e.g.*, California) are clearly preempted by the CAN-SPAM Act, the scope of preemption of prior state statutes specifically addressing fraud and deception in Internet e-mail not yet addressed by courts. Additionally, the status of pre-CAN-SPAM litigation filed by New York and Washington State authorities is unclear, although such state law cases arising from anti-deception requirements and tort law on stronger ground because such causes of action are expressly preserved by Section 8(b)(2) of the Act.

3. Extraterritorial Jurisdiction

The issue of judicial jurisdiction over entities operating via the Internet is both complex and newsworthy.[39] While decisions to date (especially at the state level) have generally, albeit with some sharp disagreements, tended to permit the exercise of *in personam* jurisdiction based on operation of Web sites accessible from within a form state, many of those early decisions are being reconsidered in the context of non-gambling prosecutions, and in any event raise complex due process issues under *Internatonal Shoe* that are beyond the scope of this article.[40] But it is manifestly clear that jurisdictional issues will remain central to enforcement of the CAN-SPAM Act, both because ISPs and other plaintiffs assert a right to choice-of-forum, without any physical presence by the defendants, and because the larger issue of conflict-of-laws — for instance between European Union and other foreign statutes, which generally adopt the more

---

[36] *U.S. Security, Inc., et al. v. FTC*, No. Civ-03-122-W (W.D. Okl. Sept. 22, 2003), available at <http://news.findlaw.com/wp/docs/ftc/donotcall92303ord.pdf>.

[37] 47 U.S.C. § 227.

[38] *Missouri ex rel. Nixon v. American Blast Fax*, 323 F.3d 649 (8th Cir. 2003) (prohibition on unsolicited facsimiles does not violate the First Amendment); *Texas v. American BlastFax, Inc.*, 121 F. Supp. 2d (W.D. Tex. 2000). *See Central Hudson Gas & Elec. Corp. v. Pub. Svc. Comm'n*, 447 U.S. 557 (1980).

[39] For instance, in late March the World Trade Organization ("WTO") preliminarily announced that it intends to find United States efforts to assert jurisdiction pursuant domestic wire fraud statutes over casino and sports wagering operations conducted via the Internet from offshore Caribbean locations unlawful as a matter of international trade law. *See* M. Crutsinger, "U.S. Loses Early Internet Gaming Ruling," *Los Angeles Times*, March 23, 2004, available at <http://www.latimes.com/news/nationworld/politics/wire/sns-ap-internet-gambling,1,6602353.story?coll=sns-ap-politics-headlines>.

[40] *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

protective opt-in approach to spam, and the CAN-SPAM Act — are inherent in the globally networked environment for electronic commerce enabled by the Internet.