

Supreme Court of the State of Washington

Opinion Information Sheet

Docket Number: 69416-8  
Title of Case: State of Washington  
v.  
Jason Heckel Doing Business as  
Natural Instincts  
File Date: 06/07/2001  
Oral Argument Date: 03/20/2001

SOURCE OF APPEAL

-----

Appeal from Superior Court of King County  
Docket No: 98-2-25480-7  
Judgment or order under review  
Date filed: 03/10/2000  
Judge signing: Hon. Palmer Robinson

JUSTICES

-----

Authored by Susan J. Owens  
Concurring: Gerry L. Alexander  
Charles Z. Smith  
Charles W. Johnson  
Barbara A. Madsen  
Richard B. Sanders  
Faith E Ireland  
Tom Chambers  
Bobbe J. Bridge

COUNSEL OF RECORD

-----

Counsel for Appellant(s)  
Paula L. Selis  
Office of the Atty Gen.  
900 4th Ave., Ste 2000  
Seattle, WA 98164

Helen R. Cullen

Ste 2000  
900 4th Ave  
Seattle, WA 98164

W. S. Hirschfeld  
Wash St Atty General  
900-4th Ave, 23rd Floor  
Seattle, WA 98164

Jay D. Geck  
Assistant Attorney General  
Highways Licenses Bldg  
PO Box 40100  
Olympia, WA 98504-0100

Counsel for Respondent(s)

Robert C. Van Siclen  
Van Siclen & Stocks  
4508 Auburn Way N #a100  
Auburn, WA 98002-1381

Dale L. Crandall  
Attorney At Law  
280 Court Street NE  
Suite 14  
Salem, OR 97301

Charese Rhony  
698-12th Street SE  
Suite 200  
Salem, OR 97301

Amicus Curiae on behalf of Washington Association of  
Internet

Brian W. Esler  
Miller & Nash  
Two Union Sq  
601 Union St Ste 4400  
Seattle, WA 98101-2352

Richard J. Busch  
601 Union St #4400  
Seattle, WA 98101-2352

STATE OF WASHINGTON,	)
	)
Appellant,	) No.
69416-8	)
	)
v.	) En
Banc	)
	)
JASON HECKEL, doing business as	)
NATURAL INSTINCTS,	)
	)
Respondent.	)
Filed June 7, 2001	)
	)

OWENS, J. -- The State of Washington filed suit against Oregon resident Jason Heckel, alleging that his transmissions of electronic mail (e-mail) to Washington residents violated Washington's commercial electronic mail act, chapter 19.190 RCW (the Act). On cross-motions for summary judgment, the trial court dismissed the State's suit against Heckel, concluding that the Act violated the dormant Commerce Clause of the United States Constitution. This court granted the State's request for direct review. We hold that the Act does not unduly burden interstate commerce. We reverse the trial court's dismissal of the State's suit, vacate the order on attorney fees, and remand this matter for trial.

FACTS

As early as February 1996, defendant Jason Heckel, an Oregon resident doing business as Natural Instincts, began sending unsolicited commercial e-mail (UCE), or 'spam,' over the Internet.<sup>1</sup> In 1997, Heckel developed a 46-

page on-line booklet entitled 'How to Profit from the Internet.' The booklet described how to set up an on-line promotional business, acquire free e-mail accounts, and obtain software for sending bulk e-mail. From June 1998, Heckel marketed the booklet by sending between 100,000 and 1,000,000 UCE messages per week. To acquire the large volume of e-mail addresses,<sup>2</sup> Heckel used the Extractor Pro software program, which harvests e-mail addresses from various on-line sources and enables a spammer to direct a bulk-mail message to those addresses by entering a simple command. The Extractor Pro program requires the spammer to enter a return e-mail address, a subject line,<sup>3</sup> and the text of the message to be sent. The text of Heckel's UCE was a lengthy sales pitch that included testimonials from satisfied purchasers and culminated in an order form that the recipient could download and print. The order form included the Salem, Oregon, mailing address for Natural Instincts. Charging \$39.95 for the booklet, Heckel made 30 to 50 sales per month. In June 1998, the Consumer Protection Division of the Washington State Attorney General's Office received complaints from Washington recipients of Heckel's UCE messages. The complaints alleged that Heckel's messages contained misleading subject lines and false transmission paths.<sup>4</sup> Responding to the June complaints, David Hill, an inspector from the Consumer Protection Division, sent Heckel a letter advising him of the existence of the Act. The Act provides that anyone sending a commercial e-

mail message from a computer located in Washington or to an e-mail address held by a Washington resident may not use a third-party's domain name without permission,<sup>5</sup> misrepresent or disguise in any other way the message's point of origin or transmission path, or use a misleading subject line.<sup>6</sup> RCW 19.190.030 makes a violation of the Act a per se violation of the Consumer Protection Act, chapter 19.86 RCW (CPA).

Responding to Hill's letter, Heckel telephoned Hill on or around June 25, 1998. According to Hill, he discussed with Heckel the provisions of the Act and the procedures bulk e-mailers can follow to identify e-mail addressees who are Washington residents. Nevertheless, the Attorney General's Office continued to receive consumer complaints alleging that Heckel's bulk e-mailings from Natural Instincts appeared to contain misleading subject lines, false or unusable return e-mail addresses, and false or misleading transmission paths. Between June and September 1998, the Consumer Protection Division of the Attorney General's Office documented 20 complaints from 17 recipients of Heckel's UCE messages. On October 22, 1998, the State filed suit against Heckel, stating three causes of action. First, the State alleged that Heckel had violated RCW 19.190.020(1)(b) and, in turn, the CPA, by using false or misleading information in the subject line of his UCE messages. Heckel used one of two subject lines to introduce his solicitations: 'Did I get the right e-mail address?' and 'For your review--HANDS OFF!' Clerk's Papers (CP) at 6,

92, 113. In the State's view, the first subject line falsely suggested that an acquaintance of the recipient was trying to make contact, while the second subject line invited the misperception that the message contained classified information for the particular recipient's review.

As its second cause of action, the State alleged that Heckel had violated RCW 19.190.020(1)(a), and thus the CPA, by misrepresenting information defining the transmission paths of his UCE messages. Heckel routed his spam through at least a dozen different domain names without receiving permission to do so from the registered owners of those names. For example, of the 20 complaints the Attorney General's Office received concerning Heckel's spam, 9 of the messages showed '13.com' as the initial ISP to transmit his spam. CP at 44, 113. The 13.com domain name, however, was registered as early as November 1995 to another individual, from whom Heckel had not sought or received permission to use the registered name. In fact, because the owner of 13.com had not yet even activated that domain name, no messages could have been sent or received through 13.com.

Additionally, the State alleged that Heckel had violated the CPA by failing to provide a valid return e-mail address to which bulk-mail recipients could respond. When Heckel created his spam with the Extractor Pro software, he used at least a dozen different return e-mail addresses with the domain name 'juno.com' (Heckel used the Juno accounts in part because they were free). CP at 88-89. None of the Juno e-mail accounts was

readily identifiable as belonging to Heckel; the user names that he registered generally consisted of a name or a name plus a number (e.g., 'marlin1374,' 'cindy5667,' 'howardwesley13,' 'johnjacobson1374,' and 'sjtowns'). CP at 88-89. During August and September 1998, Heckel's Juno addresses were canceled within two days of his sending out a bulk e-mail message on the account. According to Heckel, when Juno canceled one e-mail account, he would simply open a new one and send out another bulk mailing. Because Heckel's accounts were canceled so rapidly, recipients who attempted to reply were unsuccessful. The State thus contended that Heckel's practice of cycling through e-mail addresses ensured that those addresses were useless to the recipients of his UCE messages.<sup>7</sup> During the months that Heckel was sending out bulk e-mail solicitations on the Juno accounts, he maintained a personal e-mail account from which he sent no spam, but that e-mail address was not included in any of his spam messages. The State asserted that Heckel's use of such ephemeral e-mail addresses in his UCE amounted to a deceptive practice in violation of RCW 19.86.020. The State sought a permanent injunction and, pursuant to RCW 19.86.140 and .080 of the CPA, requested civil penalties, as well as costs and a reasonable attorney fee. In early 2000, the parties cross-moved for summary judgment. On March 10, 2000, the trial court entered an order granting Heckel's motion and denying the State's cross motion. The court found that the Act violated the Commerce Clause (U.S. Const. art. I, sec.

8, cl. 3) and was 'unduly restrictive and burdensome.' CP at 175. The order permitted Heckel to 'present a cost bill for recovery of his costs and statutory attorneys fees.' CP at 175. Heckel then moved the court for a fee award of \$49,897.50. Denying Heckel's request for fees under RCW 19.86.080 of the CPA, the court limited Heckel's award to statutory costs under RCW 4.84.030.

Challenging the trial court's finding that the Act violated the Commerce Clause, the State sought this court's direct review. Heckel cross-appealed, seeking reversal of the trial court's denial of his attorney fee request under the CPA. We granted direct review.

ISSUE

Does the Act, which prohibits misrepresentation in the subject line or transmission path of any commercial e-mail message sent to Washington residents or from a Washington computer, unconstitutionally burden interstate commerce?

#### ANALYSIS

Standard of Review. The State seeks review of the trial court's decision on summary judgment that the Act violated the dormant Commerce Clause. This court reviews de novo a trial court's grant of summary judgment and views all facts in the light most favorable to the party challenging the summary dismissal. *Lybbert v. Grant County*, 141 Wn.2d 29, 34, 1 P.3d 1124 (2000). A legislative act is presumptively constitutional, 'and the party challenging it bears the burden of proving it unconstitutional beyond a reasonable doubt.' *State v. Brayman*, 110 Wn.2d 183, 193, 751 P.2d 294

(1988); see also *Frach v. Schoettler*, 46 Wn.2d 281, 280 P.2d 1038, cert. denied, 350 U.S. 838 (1955). A party meets the standard 'if argument and research show that there is no reasonable doubt that the statute violates the constitution.' *Amalgamated Transit Union Local 587 v. State*, 142 Wn.2d 183, 205, 11 P.3d 762 (2000) (citing *Belas v. Kiga*, 135 Wn.2d 913, 920, 959 P.2d 1037 (1998)).

Heckel's Challenge under the Commerce Clause. The Commerce Clause grants Congress the 'power . . . {t}o regulate commerce with foreign nations, and among the several states.' U.S. Const. art. I, sec. 8, cl. 3. Implicit in this affirmative grant is the negative or 'dormant' Commerce Clause--the principle that the states impermissibly intrude on this federal power when they enact laws that unduly burden interstate commerce. See *Franks & Son, Inc. v. State*, 136 Wn.2d 737, 747, 966 P.2d 1232 (1998). Analysis of a state law under the dormant Commerce Clause generally follows a two-step process. We first determine whether the state law openly discriminates against interstate commerce in favor of intrastate economic interests. If the law is facially neutral, applying impartially to in-state and out-of-state businesses, the analysis moves to the second step, a balancing of the local benefits against the interstate burdens: Where the statute regulates evenhandedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. If a

legitimate local purpose is found, then the question becomes one of degree.

And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities . . . .

Id. at 754 (quoting *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142, 90 S. Ct. 844, 25 L. Ed. 2d 174 (1970)).

The Act is not facially discriminatory. The Act applies evenhandedly to in-state and out-of-state spammers: 'No person' may transmit the proscribed commercial e-mail messages 'from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident.' RCW 19.190.020(1) (emphasis added). Thus, just as the statute applied to Heckel, an Oregon resident, it is enforceable against a Washington business engaging in the same practices.

Because we conclude that the Act's local benefits surpass any alleged burden on interstate commerce, the statute likewise survives the Pike balancing test. The Act protects the interests of three groups--ISPs, actual owners of forged domain names, and e-mail users. The problems that spam causes have been discussed in prior cases and legislative hearings. A federal district court described the harms a mass e-mailer caused ISP CompuServe: In the present case, any value CompuServe realizes from its computer equipment is wholly derived from the extent to which that equipment can

serve its subscriber base. . . . {H}andling the enormous volume of mass mailings that CompuServe receives places a tremendous burden on its equipment. Defendants' more recent practice of evading CompuServe's filters by disguising the origin of their messages commandeers even more computer resources because CompuServe's computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (citations omitted) (granting preliminary injunction against bulk e-mailer on theory of trespass to chattels); see also Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998) ('rely{ing} on the reasoning of CompuServe' and finding that bulk e-mailer 'injured AOL's business goodwill and diminished the value of its possessory interest in its computer network'). To handle the increased e-mail traffic attributable to deceptive spam, ISPs must invest in more computer equipment.<sup>8</sup> Operational costs likewise increase as ISPs hire more customer service representatives to field spam complaints and more system

administrators to detect accounts being used to send spam.<sup>9</sup>

Along with ISPs, the owners of impermissibly used domain names and e-mail addresses suffer economic harm. For example, the registered owner of 'localhost.com' alleged that his computer system was shut down for three days by 7,000 responses to a bulk-mail message in which the spammer had forged the e-mail address 'nobody@localhost.com' into his spam's header.

*Seidl v. Greentree Mortgage Co.*, 30 F. Supp. 2d 1292, 1297-98 (D. Colo.

1998); see also *Spamming: The E-Mail You Want to Can: Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the Comm.*

on Commerce, 106th Cong. 9 (1999) (statement of Rep. Gary G. Miller)

(attached as App. 4, Br. of Amicus WAISP); 146 Cong. Rec. H6373 (daily ed.

July 18, 2000) (statement of Rep. Miller), available at <http://thomas.loc.gov/home/c106query.html> (recounting similar experience of

California constituent).

Deceptive spam harms individual Internet users as well. When a spammer

distorts the point of origin or transmission path of the message, e-mail

recipients cannot promptly and effectively respond to the message (and

thereby opt out of future mailings); their efforts to respond take time,

cause frustration, and compound the problems that ISPs face in delivering

and storing the bulk messages. And the use of false or misleading subject

lines further hampers an individual's ability to use computer time most

efficiently. When spammers use subject lines 'such as 'Hi There!,'

'Information Request,' and 'Your Business Records,' it becomes 'virtually

impossible' to distinguish spam from legitimate personal or business messages.<sup>10</sup> Individuals who do not have flat-rate plans for Internet access but pay instead by the minute or hour are harmed more directly, but all Internet users (along with their ISPs) bear the cost of deceptive spam.

This cost-shifting--from deceptive spammers to businesses and e-mail users--has been likened to sending junk mail with postage due or making

telemarketing calls to someone's pay-per-minute cellular phone.<sup>11</sup> In a case

involving the analogous practice of junk faxing (sending unsolicited faxes

that contain advertisements), the Ninth Circuit acknowledged 'the

government's substantial interest in preventing the shifting of advertising

costs to consumers.' *Destination Ventures, Ltd. v. F.C.C.*, 46 F.3d 54, 56

(9th Cir. 1995) (holding that the Telephone Consumer Protection Act's (47

U.S.C. sec. 227) limitations on commercial speech did not violate the First

Amendment). We thus recognize that the Act serves the 'legitimate local

purpose' of banning the cost-shifting inherent in the sending of deceptive

spam.

Under the Pike balancing test, '{i}f a legitimate local purpose is found,

then the question becomes one of degree.' 397 U.S. at 142. In the present

case, the trial court questioned whether the Act's requirement of

truthfulness (in the subject lines and header information) would redress

the costs associated with bulk e-mailings. As legal commentators have

observed, however, 'the truthfulness requirements (such as the requirement

not to misrepresent the message's Internet origin) make spamming unattractive to the many fraudulent spammers, thereby reducing the volume of spam.' Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 *Yale L.J.* 785, 819 (2001). Calling 'simply wrong' the trial court's view 'that truthful identification in the subject header would do little to relieve the annoyance of spam,' the commentators assert that '{t}his identification alone would allow many people to delete the message without opening it (which takes time) and perhaps being offended by the content.' *Id.* The Act's truthfulness requirements thus appear to advance the Act's aim of protecting ISPs and consumers from the problems associated with commercial bulk e-mail.

To be weighed against the Act's local benefits, the only burden the Act places on spammers is the requirement of truthfulness, a requirement that does not burden commerce at all but actually 'facilitates it by eliminating fraud and deception.' *Id.* Spammers must use an accurate, nonmisleading subject line, and they must not manipulate the transmission path to disguise the origin of their commercial messages. While spammers incur no costs in complying with the Act, they do incur costs for noncompliance, because they must take steps to introduce forged information into the header of their message.<sup>12</sup> In finding the Act 'unduly burdensome,' CP at 175, the trial court apparently focused not on what spammers must do to comply with the Act but on what they must do if they choose to use

deceptive subject lines or to falsify elements in the transmission path. To initiate deceptive spam without violating the Act, a spammer must weed out Washington residents by contacting the registrant of the domain name contained in the recipient's e-mail address.<sup>13</sup> This focus on the burden of noncompliance is contrary to the approach in the Pike balancing test, where the United States Supreme Court assessed the cost of compliance with a challenged statute. Pike, 397 U.S. at 143. Indeed, the trial court could have appropriately considered the filtering requirement a burden only if Washington's statute had banned outright the sending of UCE messages to Washington residents. We therefore conclude that Heckel has failed to prove that 'the burden imposed on . . . commerce {by the Act} is clearly excessive in relation to the putative local benefits.' Id. at 142 (emphasis added).

Drawing on two 'unsettled and poorly understood' aspects of the dormant Commerce Clause analysis, Heckel contended that the Act (1) created inconsistency among the states and (2) regulated conduct occurring wholly outside of Washington.<sup>14</sup> The inconsistent-regulations test and the extraterritoriality analysis are appropriately regarded as facets of the Pike balancing test.<sup>15</sup> The Act survives both inquiries. At present, 17 other states have passed legislation regulating electronic solicitations.<sup>16</sup> The truthfulness requirements of the Act do not conflict with any of the requirements in the other states' statutes, and it is inconceivable that

any state would ever pass a law requiring spammers to use misleading subject lines or transmission paths. Some states' statutes do include additional requirements; for example, some statutes require spammers to provide contact information (for opt-out purposes) or to introduce subject lines with such labels as 'ADV' or 'ADV-ADLT.' But because such statutes 'merely create additional, but not irreconcilable, obligations,' they 'are not considered to be 'inconsistent'' for purposes of the dormant Commerce Clause analysis. *Instructional Sys., Inc. v. Computer Curriculum Corp.*, 35 F.3d 813, 826 (3d Cir. 1994). The inquiry under the dormant Commerce Clause is not whether the states have enacted different anti-spam statutes but whether those differences create compliance costs that are 'clearly excessive in relation to the putative local benefits.' *Pike*, 397 U.S. at 142. We do not believe that the differences between the Act and the anti-spam laws of other states impose extraordinary costs on businesses deploying spam.<sup>17</sup> Nor does the Act violate the extraterritoriality principle in the dormant Commerce Clause analysis. Here, there is no 'sweeping extraterritorial effect' that would outweigh the local benefits of the Act. *Edgar v. MITE Corp.*, 457 U.S. 624, 642, 102 S. Ct. 2629, 73 L. Ed. 2d 269 (1982). Heckel offers the hypothetical of a Washington resident who downloads and reads the deceptive spam while in Portland or Denver. He contends that the dormant Commerce Clause is offended because the Act would regulate the

recipient's conduct while out of state. However, the Act does not burden interstate commerce by regulating when or where recipients may open the proscribed UCE messages. Rather, the Act addresses the conduct of spammers in targeting Washington consumers. Moreover, the hypothetical mistakenly presumes that the Act must be construed to apply to Washington residents when they are out of state, a construction that creates a jurisdictional question not at issue in this case. In sum, we reject the trial court's conclusion that the Act violates the dormant Commerce Clause. Although the trial court found particularly persuasive *American Libraries Association v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997), that decision--the first to apply the dormant Commerce Clause to a state law on Internet use--is distinguishable in a key respect.<sup>18</sup> At issue in *American Libraries* was a New York statute that made it a crime to use a computer to distribute harmful, sexually explicit content to minors. The statute applied not just to initiation of e-mail messages but to all Internet activity, including the creation of websites. Thus, under the New York statute, a website creator in California could inadvertently violate the law simply because the site could be viewed in New York. Concerned with the statute's 'chilling effect,' *id.* at 179, the court observed that, if an artist 'were located in California and wanted to display his work to a prospective purchaser in Oregon, he could not employ his virtual {Internet} studio to do so without risking prosecution under the New York law.'

Id. at 174. In contrast to the New York statute, which could reach all content posted on the Internet and therefore subject individuals to liability based on unintended access, the Act reaches only those deceptive UCE messages directed to a Washington resident or initiated from a computer located in Washington; in other words, the Act does not impose liability for messages that are merely routed through Washington or that are read by a Washington resident who was not the actual addressee.

CONCLUSION

The Act limits the harm that deceptive commercial e-mail causes Washington businesses and citizens. The Act prohibits e-mail solicitors from using misleading information in the subject line or transmission path of any commercial e-mail message sent to Washington residents or from a computer located in Washington. We find that the local benefits of the Act outweigh any conceivable burdens the Act places on those sending commercial e-mail messages. Consequently, we hold that the Act does not violate the dormant Commerce Clause of the United States Constitution. We reverse the trial court and remand the matter for trial. The trial court's order on attorney fees is vacated.

WE CONCUR:

1 'Commercial electronic mail message' means an electronic mail message sent for the purpose of promoting real property, goods, or services for sale or lease.' RCW 19.190.010(2). The term 'spam' refers broadly to unsolicited bulk e-mail (or 'junk' e-mail), which 'can be either

commercial (such as an advertisement) or noncommercial (such as a joke or chain letter).' Sabra-Anne Kelin, State Regulation of Unsolicited Commercial E-Mail, 16 Berkeley Tech. L.J. 435, 436 & n.10 (2001). Use of the term 'spam' as Internet jargon for this seemingly ubiquitous junk e-mail arose out of a skit by the British comedy troupe Monty Python, in which a waitress can offer a patron no single menu item that does not include spam: 'Well, there's spam, egg, sausage and spam. That's not got much spam in it.' 2 Graham Chapman et al., The Complete Monty Python's Flying Circus: All the Words 27 (Pantheon Books 1989); see also Kadow's Internet Dictionary, at <http://www.msg.net/kadow/answers/s.html> (last visited May 7, 2001). Hormel Foods Corporation, which debuted its SPAM luncheon meat in 1937, has dropped any defensiveness about this use of the term and now celebrates its product with a website ([www.spam.com](http://www.spam.com)). See Hormel Objects to Cyber Promotions' Use of 'SPAM' Mark, 4 No. 1 Andrews Intell. Prop. Litig. Rep. 19 (1997); Laurie J. Flynn, Gracious Concession on Internet 'Spam,' N.Y. Times, Aug. 17, 1998, at D3. Because the term has been widely adopted by Internet users, legislators, and legal commentators, we use the term herein, along with its useful derivatives 'spammer' and 'spamming.'

2 "'Electronic mail address' means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.'  
RCW 19.190.010(3).

3 The subject line, similar to the 'RE' line of a letter or memorandum, is

generally displayed (at least in part) alongside the sender's name in the recipient's e-mail inbox.

4 Each e-mail message, which is simply a computer data file, contains so-called 'header' information in the 'To,' 'From,' and 'Received' fields.

When an e-mail message is transmitted from one e-mail address to another, the message generally passes through at least four computers: from the sender's computer, the message travels to the mail server computer of the sender's Internet Service Provider (ISP); that computer delivers the message to the mail server computer of the recipient's ISP, where it remains until the recipient retrieves it onto his or her own computer.

Every computer on the Internet has a unique numerical address (an Internet Protocol or IP address), which is associated with a more readily recognizable domain name (such as 'mysite.com'). As the e-mail message travels from sender to recipient, each computer transmitting the message attaches identifying data to the 'Received' field in the header. The information serves as a kind of electronic postmark for the handling of the message. See Clerk's Papers (CP) at 130-34. It is possible for a sender to alter (or 'spooof') the header information by misidentifying either the computer from which the message originated or other computers along the transmission path. See Kelin, *supra* note 1, at 445.

5 See RCW 19.190.010(6) (defining 'Internet domain name').

6 '(1) No person may initiate the transmission, conspire with another to initiate the transmission, or assist the transmission, of a commercial

electronic mail message from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident that:

'(a) Uses a third party's internet domain name without permission of the third party, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or

'(b) Contains false or misleading information in the subject line.

'(2) For purposes of this section, a person knows that the intended recipient of a commercial electronic mail message is a Washington resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address.'

RCW 19.190.020.

7 The experience of 1 of the 17 complainants to the Attorney General's Office is illustrative. Nancy Smith received Heckel's spam on September 1, 1998; the message was sent from a Juno account with the user name 'apollo1113,' and the subject line read 'For your review--HANDS OFF.' CP at 140. On or about September 1, 1998, Smith sent a copy of the Natural Instincts order form with a check for \$39.95 by U.S. Mail to the Salem, Oregon, address provided on the order form. Hearing nothing for some weeks, Smith sent a message by return e-mail on September 30, 1998, but within a minute she received a return e-mail from Juno stating that the attempt had failed due to termination of the account. Unable to find any

information about Natural Instincts on the Internet, Smith contacted her bank and learned that the check had cleared two weeks earlier. Smith then contacted the Attorney General's Office. CP at 140-41, 149-50.

8 '{W}hen Internet users attempt to reply to deceptive spam that has a fraudulent return address or domain name, one e-mail message (and the ISP{'s} related computer log entry) instantly becomes three separate e-mail messages (and additional computer log entries) because: (1) the ISP server that is the victim of the fraudulent return address or domain name sends an error message back to the Internet user and their ISP announcing that the return path was invalid, (2) a message is sent to the server administrator requesting an investigation of the return address for potential problems, and (3) a message is sent to the server log in case the ISP wishes to track down the problem later. With bulk spam, these messages snowball to clog ISP resources, and ISPs have little choice but to purchase additional equipment at a significant cost.' Br. of Amicus Washington Association of Internet Service Providers (WAISP) at 11-12.

9 See Br. of Amicus WAISP at 12-13; see also Spamming: The E-Mail You Want to Can: Hearing Before the Subcomm. on Telecommunications, Trade, and Consumer Protection of the Comm. on Commerce, 106th Cong. 41-42 (1999) (statement of Michael Russina, Director of Systems Operations, SBC Internet Services) (attached as App. 4, Br. of Amicus WAISP).

10 Testimony of Ed McNichol at Hearing on H.B. 2752 Before the Washington House Comm. on Energy and Utilities (Jan. 28, 1998) (partial transcript

attached as App. 2, Br. of Amicus WAISP; audio also available at <http://198.239.32.162/ramgen/199801/1998010112.ra>).

11 See *Spamming: The E-Mail You Want to Can*, supra note 9, at 1 (statement of Rep. W.J. Tauzin, Chairman, Subcomm. on Telecommunications, Trade, and Consumer Protection) (attached as App. 4, Br. of Amicus WAISP).

12 'This generally involves paying a bulk re-mailing service to forge e-mail headers and send out the spammer's message, or at least running additional software programs to alter the e-mail messages' address and domain name information.' Br. of Amicus WAISP at 8.

13 See RCW 19.190.020(2). The Washington Association of Internet Service Providers (WAISP) and the Washington Attorney General co-sponsor a registry of Washington residents who do not want to receive spam. See WAISP Registry Page, at <http://registry.waisp.org> (last visited May 7, 2001).

14 Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 *Yale L.J.* 785, 789 (2001).

15 See Goldsmith & Sykes, supra note 14, at 808 (concluding that 'inconsistent-regulations cases, like extraterritoriality cases, should be viewed as just another variant of balancing analysis'); see also William Lee Biddle, *State Regulation of the Internet: Where Does the Balance of Federalist Power Lie?* 37 *Cal. W. L. Rev.* 161, 167 (2000) (suggesting that 'the burden placed on interstate commerce through inconsistent local regulation is more appropriately placed as part of the Pike balancing test, rather than its own, separate line of inquiry').

16 See David E. Sorkin, *Spam Laws*, at

<http://www.spamlaws.com/state/index.html>; see also Max P. Ochoa,  
Legislative Note: Recent State Laws Regulating Unsolicited Electronic Mail,  
16 Santa Clara Computer & High Tech. L.J. 459 (2000); Br. of Appellant at  
23 and App. A, B. Proposed federal legislation, the Unsolicited Commercial  
Electronic Mail Act of 2000, H.R. 3113, 106th Cong. (2000), was passed by  
the House on July 18, 2000, and has been referred to the Senate Committee  
on Commerce, Science, and Transportation. The text of the bill may be  
accessed through <http://thomas.loc.gov/home/c106query.html>.  
17 As the State notes, '{p}resently, mail and phone solicitors are expected  
to abide by different states' telemarketing laws and other consumer  
protection laws. E-mail solicitors should not be excused from the burden  
of complying with a state's law simply because of the ease of sending bulk  
e-mail solicitations in relation to other forms of commercial  
solicitation.' CP at 53.  
18 See CP at 216. At least 10 other cases have distinguished American  
Libraries. See, e.g., Hatch v. Super. Ct., 80 Cal. App. 4th 170, 94 Cal.  
Rptr. 2d 453 (2000); People v. Hsu, 82 Cal. App. 4th 976, 99 Cal. Rptr. 2d  
184 (2000); Ford Motor Co. v. Tex. Dep't of Transp., 106 F. Supp. 2d 905,  
909 (W.D. Tex. 2000).