

MINUTES OF THE SENATE COMMITTEE ON COMMERCE.

The meeting was called to order by Chairperson Senator Karin Brownlee at 8:30 a.m. on February 13, 2002 in Room 123-S of the Capitol.

All members were present except:

Committee staff present: April Holman, Legislative Research
Norman Furse, Revisor of Statues
Sherman Parks, Revisor of Statues
Lea Gerard, Committee Secretary

Conferees appearing before the committee: Steve Rarrick, Deputy Attorney General-
Consumer Protection
Doug Smith representing Direct Market Assoc.
Leo Vogel, Assistant Director Purchasing
Mike Murraray, Govt. Affairs, Sprint

Others attending: See attached list

Hearings on **SB 481**: On line procurement procedures pilot study.

In accordance with KSA 75-3715a, the fiscal note concerning **SB 481** was submitted to committee members.

Chairperson Brownlee gave a brief overview concerning **SB 481** stating that the Director of Purchases would be required to submit a report to the legislature once a year and a Post Audit would not be necessary.

Chairperson Brownlee recognized Leo Vogel, Assistant Director Purchasing who gave a few highlights of a report that was submitted to the legislature. Mr. Vogel stated the report explained the preparation the Purchasing Department went through to select vendors for the reverse auction procedure. The process turned out to be more complicated due to some vendors wanting to charge as much as \$30,000 for each auction. The Purchasing Department negotiated a contact and awarded it to "Materials Net" that paid them \$2,500. per auction regardless of the amount. The first auction will be held in the second or third week of March to purchase Highway Patrol cars.

Hearings closed on **SB 481**.

Senator Barone moved, seconded by Senator Emler, that **SB 481** be recommended favorably for passage. The voice vote was unanimous in favor of the motion.

Hearings on **SB 467**: Commercial electronic mail act; protection from deceptive and unwanted "spam".

In accordance with KSA 75-3715a, the fiscal note concerning **SB 467** was submitted to committee members.

Chairperson Brownlee recognized Steve Rarrick, Deputy Attorney General, Consumer Protection Division who testified in support of **SB 467** (Attachment 1). He stated **SB 467** would provide protection to Kansans from deceptive and unwanted commercial e-mail. **SB 467** is modeled primarily after statues in Washington and California (Attachment 2). Mr. Rarrick explained Section (b) of the bill that defines the definitions and Section (c) contains the prohibitions and requirements. The bill requires specific requirements on how a recipient can reply to get off the e-mail list and advise the company not to send anymore "spam".

The Committee discussed what constitutes an occurrence and would this law have an impact on charitable and non-profit organization. Chairperson Brownlee requested that Steve Rarrick double check the bill to prevent charitable and non-profit organizations from being in violation of this act.

CONTINUATION SHEET

MINUTES OF THE SENATE COMMITTEE ON COMMERCE at on February 13, 2002 in Room 123-S of the Capitol.

Doug Smith, representing Direct Marketing Association, testified in support of the concept of **SB 467** but would like the Committee to consider the State of Nevada statute (Attachment 3). The Nevada law creates four definitions for advertisement, electronic mail, network and a recipient. If a person transmits or causes to be transmitted an electronic message to a recipient that includes an advertisement, they are in violation of the act unless the person has an existing business or personal relationship.

The Committee asked Mr. Rarrick what his comments are regarding the Nevada law. Mr. Rarrick stated the problem he has with the Nevada law was it did not require the ADV label.

Mike Murraray, Sprint, testified they are neutral regarding **SB 467** in that they are still discussing the bill. Sprint is currently working with the Attorney General's office regarding some additional questions. Mike Murraray requested that the committee either hold the hearing open until some of their issues are resolved or be aware if Sprint has some difficulties, they may present some proposed amendments.

Emily Hackett, Internet Alliance, provided written testimony to committee members in support of **SB 467** (Attachment 4).

Senator Brungardt moved, seconded by Senator Steineger, that the Minutes of January 31, February 5, 6 and 7, 2002 be approved. The vote was unanimous in favor of the motion.

Meeting adjourned at 9:30 a.m.

The next meeting is scheduled February 14, 2002 at 8:15 a.m.

**SENATE COMMERCE COMMITTEE
GUEST LIST**

DATE: February 13, 2002

NAME	REPRESENTING
Ron CATES	CDA
Ernie Kutzley	AARP
Ernie Pogge	AARP
Freddie Gron	Am Inst of Architects/Ks
Doug McKinney	NC Reg. Planning Comm.
Curt Frasier	Leadership Mitchell County
PHIL ROBERTS	LEADERSHIP MITCHELL COUNTY
BOB JAYROE	CONNECT KANSAS
Bill Sneed	PSIU
Stephanie Buchanan	DOB
Zeo Vogel	Dept of Admin
D. KEITH MEYERS	Dept of Administration
Steve Rarrick	Attys Generals Office
David Harder	"
Larry Hansen	"
Hillary Hayes	Federico Consulting
LAIL GEXTON	WSU



CARLA J. STOVALL
ATTORNEY GENERAL

State of Kansas

Office of the Attorney General

CONSUMER PROTECTION / ANTITRUST DIVISION

120 S.W. 10TH AVENUE, 2ND FLOOR, TOPEKA, KANSAS 66612-1597

PHONE: (785) 296-3751 FAX: (785) 291-3699

CONSUMER HOTLINE
1-800-432-2310

Testimony of
Steve Rarrick, Deputy Attorney General
Consumer Protection Division
Office of Attorney General Carla J. Stovall
Before the Senate Commerce Committee
RE: Senate Bill 467
February 13, 2002

Chairperson Brownlee and Members of the Committee:

Thank you for the opportunity to appear on behalf of Attorney General Carla J. Stovall today to testify in support of Senate Bill 467. My name is Steve Rarrick and I am the Deputy Attorney General for Consumer Protection.

Senate Bill 467 would provide protections to Kansans from deceptive and unwanted commercial e-mail, or "spam." The term "spam" refers to unsolicited bulk e-mail, or "junk" e-mail, and the origin of the term arose out of a skit by the British comedy troupe Monty Python. The FTC reported on February 12, 2002, that consumers complaining about spam currently forward spam to the agency at a rate of approximately 15,000 a day. Our office regularly hears from consumers upset about receiving unwanted spam.

Senate Bill 467 is modeled primarily after statutes in Washington and California. Both laws have been challenged on Commerce Clause grounds, and both have been upheld. (*See, State v. Heckel*, 143 Wash.2d 824, 24 P.3d 404 (2001), and *Ferguson v. Friendfinders, Inc., et al.*, 94 Cal.App.4th 1255, 115 Cal.Rptr.2d 258 (2002), attached to my testimony).

Beyond being annoying and a waste of time, harm caused by unsolicited commercial e-mail to ISPs (internet service providers), actual owners of forged domain names, and e-mail users has been well documented by courts and commentators. (See discussion in attached cases). These problems have developed because unsolicited commercial e-mail is easy and inexpensive to create, but extremely difficult and expensive to eliminate.

ISPs incur significant business related costs accommodating bulk e-mail advertising and addressing the problems it creates. The costs of these efforts, like most business costs, are typically passed on to consumers. The use of deceptive tactics by spammers, including disguising the nature and origin of their messages to evade ISP attempts to filter out their messages, has caused even more expense to ISPs who must attempt to return messages to non-existent addresses or otherwise dispose of undeliverable messages. The use of fraudulent domain names and return e-mail addresses by spammers misdirect responses to innocent third parties who can suffer serious economic consequences. The *Heckel* court noted that the

Senate Commerce Committee
Feb. 13, 2002
Attachment 1-1

“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.” (*Heckel*, 24 P.3d at p. 410). As a result, the *Heckel* court concluded that the Washington Act served the “legitimate local purpose” of banning the cost-shifting inherent in the sending of deceptive spam.

The principle provisions of Senate Bill 467 are as follows:

- Section (b) defines specified terms of the act.
 - Section (b)(1) defines “assist the transmission” to mean action taken by a person to provide **substantial assistance or support** which enables any person to formulate, compose, send ...” This definition is intended to apply only to those service providers who are providing substantial assistance and support which enables companies to send spam in violation of the KCPA. We understand there are service providers who specifically market their services as internet advertising agencies for other businesses, in which the service provider provides aggregated e-mail addresses, techniques to send spam, and often actually transmits the spam for the client. This language is to provide liability for these type of service providers under section (d), not the typical service provider who simply routes the e-mail through to their customers.
 - Section (b)(2) defines “commercial electronic mail message” to mean an electronic mail message sent for the purpose of promoting property or services for sale or lease.
 - Section (b)(3) defines “initiate the transmission,” and clarifies again that action of an intervening interactive computer service, defined in section (b)(5), which handles or retransmits the message, is not covered unless the service provides substantial assistance or support when it knows or consciously avoids knowing, that the person initiating the transmission is engaging in violations of the KCPA.
- Section (c) contains the prohibitions and requirements of the bill, which:
 - Prohibits using third party domain names without the permission of the third party (deceptive spammers will give a third party domain name to make it look like it came from that source).
 - Prohibits misrepresenting or obscuring any information identifying the point of origin or the transmission path of a commercial electronic mail message (this is to keep the recipient from replying and directing the sender to cease sending spam).
 - Prohibits false or misleading information in the subject line (senders often use deceptive subject line statements to falsely suggest that an acquaintance of the recipient was trying to make contact or that the message contains some special or classified information for the recipient’s eyes only).
 - Requires the subject line contain “ADV:” as the first four characters to advise the recipient that it is advertising material. This requirement is present in spam laws in California, Colorado, and Tennessee. Nevada does not require the “ADV:” specifically, but does require labeling or identification that indicates the e-mail is an advertisement.
 - Requires the subject line contain “ADV:ADLT” as the first eight characters when the message contains advertising for adult material to advise the recipient of this material fact. California requires this, and Pennsylvania requires the e-mail to include “ADV-ADULT” to designate “explicit sexual materials.”

- Requires instructions on how to notify the sender not to send any subsequent spam via either (1) an electronic mail address or (2) the legal name and address for notice by mail and a toll-free number for notice by telephone.
- Prohibits sending spam or conspiring with another to send spam to the recipient after the recipient has notified the sender not to send any further spam.
- Prohibits giving, transferring, selling, or sharing e-mail addresses of any recipient who has notified the seller not to send further spam.
- Prohibits a person from assisting the transmission (defined in section (b)(1)) of spam when the person providing the assistance knows, or consciously avoids knowing, that the initiator of the spam is engaged in, or intends to engage, in acts or practices that violate the Kansas Consumer Protection Act (KCPA). As stated above, this will enable us to prosecute service providers who are providing substantial assistance and support which enables companies to send spam in violation of the KCPA.
- Section (d) of the bill provides that a person knows or has reason to know that the intended recipient of a commercial electronic mail message is a Kansas resident if that information is available, upon request, from the registrant of the internet domain name contained in the recipient's electronic mail address.
- Section (e) of the bill makes violations an unconscionable act and practice under the KCPA.
- Section (f) of the bill is intended to ensure a penalty is available to consumers who bring a private cause of action even though they may not be able to prove actual monetary loss. This is in response to a decision by the Kansas Supreme Court holding consumers may not recover a civil penalty if they are not able to prove actual monetary loss. This decision has also been applied in a slamming case, precluding a consumer from prevailing because the consumer could show no actual damages.
- Section (g) of the bill provides a private cause of action to non-consumer entities, such as corporations, partnerships, associations, churches, etc. A similar private cause of action was provided in our slamming law last session.
- Section (h) of the bill provides for a minimum \$500 and a maximum \$10,000 penalty for each violation.

You may hear that this bill will conflict with other state statutes regulating commercial electronic mail. This argument was rejected by the California Court of Appeals in the *Friendfinders* case, where the court recognized that 18 states have enacted laws regulating commercial electronic mail and the respondent was only able to identify one actual conflict pertaining to one requirement of the California law. (California required "ADV:ADLT" as the first eight characters for adult advertisements whereas Pennsylvania required "ADV-ADULT" as the first nine characters for advertisements containing explicit sexual materials). The *Friendfinders* court held the respondent had failed to show a spammer would ever face a situation where he/she would be required to comply with both laws at the same time. Additionally, the court noted that, "[a]ssuming that an originator of UCE [unsolicited commercial e-mail] faced a legal challenge because it complied with the subject line requirement of one state's law, but not the other's, we would expect that the doctrine of substantial compliance would be utilized to defend against a legal challenge to that usage." *Friendfinders*, 94 Cal.App.4th at 1266.

On behalf of Attorney General Stovall, I urge you to pass this bill out favorably. I would be happy to answer questions of the Chair or any member of the Committee.

24 P.3d 404

(Cite as: 143 Wash.2d 824, 24 P.3d 404)

HSupreme Court of Washington,
En Banc.

STATE of Washington, Appellant,

v.

Jason HECKEL, doing business as Natural Instincts,
Respondent.

No. 69416-8.


Argued March 20, 2001.


Decided June 7, 2001.

State sued Oregon resident, alleging that his transmissions of electronic mail to Washington residents violated commercial electronic mail act, and sought a permanent injunction and civil penalties. The Superior Court, King County, Palmer Robinson, J., granted Oregon resident's motion for summary judgment, finding that act violated dormant Commerce Clause. The state appealed. After granting direct review, the Supreme Court, Owens, J., held that commercial electronic mail act, which prohibited misrepresentation in subject line or transmission path of commercial e-mail messages, did not unconstitutionally burden interstate commerce.


Reversed and remanded.

West Headnotes

[1] Appeal and Error  893(1)
30k893(1) Most Cited Cases


[1] Appeal and Error  895(2)
30k895(2) Most Cited Cases

Appellate 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.


[2] Constitutional Law  48(1)
92k48(1) Most Cited Cases

[2] Constitutional Law  48(3)
92k48(3) Most Cited Cases

A legislative act is presumptively constitutional, and the party challenging it bears the burden of proving it unconstitutional beyond a reasonable doubt; a party meets the standard if argument and research show that there is no reasonable doubt that the statute violates the constitution.


[3] Commerce  12
83k12 Most Cited Cases

Implicit in the Commerce Clause's affirmative grant of power to regulate interstate commerce is the negative or "dormant" Commerce Clause, which is the principle that the states impermissibly intrude on this federal power when they enact laws that unduly burden interstate commerce. U.S.C.A. Const. Art. 1, § 8, cl. 3.


[4] Commerce  12
83k12 Most Cited Cases

[4] Commerce  13.5
83k13.5 Most Cited Cases

Analysis of a state law under the dormant Commerce Clause generally follows a two-step process, with the court first determining whether the state law openly discriminates against interstate commerce in favor of intrastate economic interests, and 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. U.S.C.A. Const. Art. 1, § 8, cl. 3.

[5] Commerce  13.5
83k13.5 Most Cited Cases


Where a 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. U.S.C.A. Const. Art. 1, § 8, cl. 3.


[6] Commerce  13.5
83k13.5 Most Cited Cases

Extent of the burden on interstate commerce that will be tolerated will depend on the nature of the local interest

Senate Commerce Committee
Feb. 13, 2002
Attachment 2-1

involved, and on whether it could be promoted as well with a lesser impact on interstate activities. U.S.C.A. Const. Art. 1, § 8, cl. 3.


[7] Commerce  **59**
83k59 Most Cited Cases

[7] Telecommunications  **262**
372k262 Most Cited Cases

Commercial electronic mail act, which prohibited misrepresentation in subject line or transmission path of any commercial e-mail message sent to Washington residents or from a Washington computer, did not unconstitutionally burden interstate commerce, and thus did not violate the dormant Commerce Clause of the United States Constitution; act was not facially discriminatory, act served legitimate local purpose of banning cost-shifting inherent in sending of deceptive spam, or unsolicited bulk e-mail, only burden act placed on spammers was requirement of truthfulness, and truthfulness requirements did not conflict with any requirements in other states' statutes. U.S.C.A. Const. Art. 1, § 8, cl. 3; West's RCWA 19.190.010 et seq.

[8] Commerce  **13.5**
83k13.5 Most Cited Cases

Inconsistent-regulations test and extraterritoriality analysis are facets of *Pike* balancing test in dormant Commerce Clause analysis to determine whether burden imposed on interstate commerce is clearly excessive in relation to putative local benefits. U.S.C.A. Const. Art. 1, § 8, cl. 3.

[9] Commerce  **59**
83k59 Most Cited Cases

[9] Telecommunications  **262**
372k262 Most Cited Cases

Other states' statutes regulating electronic solicitations merely created additional, but not irreconcilable, obligations, such that they were not inconsistent for purposes of dormant Commerce Clause analysis of Washington's commercial electronic mail act; inquiry under dormant Commerce Clause was not whether states had enacted different anti-spam statutes but whether those differences created compliance costs that were clearly excessive in relation to putative local benefits. U.S.C.A. Const. Art. 1, § 8, cl. 3; West's RCWA 19.190.010 et seq.

****405 *826** Honorable Christine Gregoire, Attorney

General, Paula Lillian Selis, Helen Regina Cullen, W. Stuart Hirshfeld, Assts., Seattle, Jay Douglas Geck, Asst., Olympia, for Appellant.

Van Siclen & Stocks, Robert Craig Van Siclen, Auburn, Dale L. Crandall, Charese Rhony, Salem, for Respondent.

Miller, Nash, Brian William Esler, Richard J. Busch, Seattle, Amicus Curiae on Behalf of Washington Association of Internet Service Providers.

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. ****406** 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. [FN1] In 1997, Heckel developed a 46 page on-line booklet entitled "How to Profit from the Internet." ***827** 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, [FN2] 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, [FN3] 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.

FN1. " '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). 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."

FN2. " '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).

FN3. 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.

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. *828 The complaints alleged that Heckel's messages contained misleading subject lines and false transmission paths. [FN4] Responding **407 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, [FN5] misrepresent or disguise in any other way the message's point of origin or transmission path, or use a misleading subject line. [FN6] RCW 19.190.030 makes a violation of the Act a per se violation of the Consumer Protection Act, chapter 19.86 RCW (CPA).

FN4. 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 "spoof") 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.

FN5. See RCW 19.190.010(6) (defining "Internet domain name").

FN6. "(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.

*829 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 *830 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**408 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. [FN7] 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 *831 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.

[FN7]. 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.

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, § 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

[1][2] *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 *832 views all facts in the light most favorable to the party challenging the summary dismissal. Lybbert v. Grant County, 141 Wash.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 Wash.2d 183, 193, 751 P.2d 294 (1988); *see also* Frach v. Schoettler, 46 Wash.2d 281, 280 P.2d 1038, *cert. denied*, 350 U.S. 838, 76 S.Ct. 75, 100 L.Ed. 747 (1955). A party meets the standard "if argument and research show that there is no reasonable doubt that the statute violates the constitution." **409 Amalgamated Transit Union Local 587 v. State, 142 Wash.2d 183, 205, 11 P.3d 762 (2000) (citing Belas v. Kiga, 135 Wash.2d 913, 920, 959 P.2d 1037 (1998)).

[3][4][5][6] *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, § 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 Wash.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 *833 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, 966 P.2d 1232 (quoting Pike v. Bruce Church, Inc., 397 U.S. 137, 142, 90 S.Ct. 844, 25 L.Ed.2d 174 (1970)).

[7] 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 *834 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.**410 [FN8] 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. [FN9]

FN8. "[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.

FN9. *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).

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, *835 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/106query.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. [FN10] 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.

FN10. 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>).

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. [FN11] 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." *836 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. § 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.

FN11. 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).

Under the *Pike* balancing test, "[i]f a legitimate local purpose is found, then the question **411 becomes one of degree." 397 U.S. at 142, 90 S.Ct. 844. 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, *837 because they must take steps to introduce forged information into the header of their message. [FN12] 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. [FN13] 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, 90 S.Ct. 844. 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, 90 S.Ct. 844 (emphasis added).

[FN12]. "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.

[FN13]. 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).

[8][9] 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. [FN14] The inconsistent-regulations test and the extraterritoriality analysis are appropriately regarded as facets of the *Pike* balancing test. [FN15] The Act survives both inquiries. At present, 17 other states have passed legislation *838 regulating**412 electronic solicitations. [FN16] 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, 90 S.Ct. 844. 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. [FN17]

[FN14]. Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L.J. 785, 789 (2001).

[FN15]. 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 "[t]he 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").

FN16. See David E. Sorkin, *Spam Laws*, at [http:// www.spamlaws.com/state/index.html](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>.

FN17. 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.

Nor does the Act violate the extraterritoriality principle *839 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. [FN18] 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 *840 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 **413 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.

FN18. 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).

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.

ALEXANDER, C.J., SMITH, JOHNSON, MADSEN,
SANDERS, IRELAND, CHAMBERS and BRIDGE,
JJ., concur.

END OF DOCUMENT

Copr. © West 2001 No Claim to Orig. U.S. Govt.
Works

2.10

Direct Marketing Association

TESTIMONY
SENATE COMMERCE COMMITTEE
SENATE BILL NO. 467

February 13, 2002

Senator Brownlee and Members of the Senate Commerce Committee:

Thank you for the opportunity to present the remarks of the Direct Marketing Association (DMA) on Senate Bill No. 467. The Direct Marketing Association serves as a professional trade association for direct marketers, with over 4,700 members. The DMA is the oldest and largest national trade association, serving the direct marketing industry since 1917.

We understand that unsolicited email (or "spam") has become an increasing problem for both consumers and the industry alike. These unwanted messages have contributed to server and router failures undermining network reliability and added to additional infrastructure development costs. Yet how do you counterbalance the issues of free speech and providing only band-aid fixes for consumers with the technical aspects of regulation without being burdensome on legitimate businesses?

The DMA supports the concept of Senate Bill No. 467 but we feel that the State of Nevada adopted straightforward statutory language that this Committee may want to consider. (I have attached a copy to my testimony.)

We would encourage the committee to focus on the Nevada statute as a format for protecting consumers in Kansas from unwanted electronic mail messages.

As a side note the DMA offers a free service to consumers who wish to reduce the amount of unsolicited email they receive. This service is called the E-Mail Preference Service and operates in a fashion similar to our direct mail and telephone preference services. I must remind you that this new service will only affect messages from DMA members and not fraudulent or deceptive marketers.

Thank you for your time today and consideration

Presented by Doug Smith on behalf of the Direct Marketing Association

Senate Commerce Committee
Feb. 13, 2002
Attachment 3.1

2001 Nevada Revised Statutes

Current as of 12/3/01

41 - ACTIONS AND PROCEEDINGS IN PARTICULAR CASES CONCERNING PERSONS

LIABILITY OF PERSONS WHO TRANSMIT ITEMS OF ELECTRONIC MAIL THAT INCLUDE ADVERTISEMENTS

NRS 41.705 Definitions. As used in NRS 41.705 to 41.735, inclusive, unless the context otherwise requires, the words and terms defined in NRS 41.710 to 41.725, inclusive, have the meanings ascribed to them in those sections.

(Added to NRS by 1997, 1255)

NRS 41.710 “Advertisement” defined. “Advertisement” means material that:

1. Advertises for commercial purposes the availability or the quality of real property, goods or services; or
2. Is otherwise designed or intended to solicit a person to purchase real property, goods or services.

(Added to NRS by 1997, 1256)

NRS 41.715 “Electronic mail” defined. “Electronic mail” means a message, a file or other information that is transmitted through a local, regional or global network, regardless of whether the message, file or other information is:

1. Viewed;
2. Stored for retrieval at a later time;
3. Printed onto paper or other similar material; or
4. Filtered or screened by a computer program that is designed or intended to filter or screen items of electronic mail.

(Added to NRS by 1997, 1256)

NRS 41.720 “Network” defined. “Network” means a network comprised of one or more computers that may be accessed by a modem, electronic or optical technology, or other similar means.

(Added to NRS by 1997, 1256)

NRS 41.725 “Recipient” defined. “Recipient” means a person who receives an item of electronic mail.

(Added to NRS by 1997, 1256)

NRS 41.730 Action for damages; exceptions; injunctive relief.

1. Except as otherwise provided in NRS 41.735, if a person transmits or causes to be transmitted to a recipient an item of electronic mail that includes an advertisement, the person is liable to the recipient for civil damages unless:
 - (a) The person has a preexisting business or personal relationship with the recipient;

- (b) The recipient has expressly consented to receive the item of electronic mail from the person; or
 - (c) The advertisement is readily identifiable as promotional, or contains a statement providing that it is an advertisement, and clearly and conspicuously provides:
 - (1) The legal name, complete street address and electronic mail address of the person transmitting the electronic mail; and
 - (2) A notice that the recipient may decline to receive additional electronic mail that includes an advertisement from the person transmitting the electronic mail and the procedures for declining such electronic mail.
2. If a person is liable to a recipient pursuant to subsection 1, the recipient may recover from the person:
 - (a) Actual damages or damages of \$10 per item of electronic mail received, whichever is greater; and
 - (b) Attorney's fees and costs.
 3. In addition to any other recovery that is allowed pursuant to subsection 2, the recipient may apply to the district court of the county in which the recipient resides for an order enjoining the person from transmitting to the recipient any other item of electronic mail that includes an advertisement.

(Added to NRS by 1997, 1256)

NRS 41.735 Immunity for persons who provide users with access to network; applicability to items of electronic mail obtained voluntarily.

1. If a person provides users with access to a network and, as part of that service, transmits items of electronic mail on behalf of those users, the person is immune from liability for civil damages pursuant to NRS 41.705 to 41.735, inclusive, unless the person transmits an item of electronic mail that includes an advertisement he prepared or caused to be prepared.
2. The provisions of NRS 41.705 to 41.735, inclusive, do not apply to an item of electronic mail that is obtained by a recipient voluntarily. This subsection includes, but is not limited to, an item of electronic mail that is obtained by a recipient voluntarily from an electronic bulletin board.

(Added to NRS by 1997, 1256)

1111 19th Street, NW, Suite 1180
Washington, D.C. 20036
Tel: 202-955-8091
Cell: 202-422-8092
Email: emilyh@internetalliance.org
Web: www.internetalliance.org

February 12, 2002

Senator Karin Brownlee, Chair
Senate Commerce Committee
Room Number: 123-S
State House
Topeka, KS 66612

Dear Senator Brownlee:

I am unable to attend the Commerce Committee hearing today to discuss SB 467. However, I would like to take this opportunity to express my support for most sections of the bill and ask that it be amended to eliminate the labeling requirement, as better ways exist to control spam and bulk email.

The Internet Alliance and its' members share the legitimate concerns your committee has about the annoying spam consumers find in their email inbox. We believe that labeling does little to protect consumers and that more meaningful technological solutions exist that can keep spam and bulk mail from ever reaching a consumers inbox.

The "ADV" and "ADV:ADLT" labeling requirements contained in Section One (c) (1) (C) and Section One (c) (1) (E) will do little to stem the flow of objectionable email. In fact, we believe labeling laws undermine consumer confidence and trust in the Internet because it promises a solution that does not work. Labeling laws have been adopted in California, Colorado and Tennessee and there is no evidence these laws have reduced spam or bulk mail or that they are being enforced. In fact, they are not enforced.

The best way to control spam is to educate consumers to use the technology that exists to divert or block it. Email services like Yahoo Mail and Hotmail offer free institutional screens that automatically divert spam and bulk mail away from your inbox and place it in a bulk mailbox. You never need to see or open this unwanted email. If you ignore it, it remains in your bulk email box and is automatically deleted.

Other email services like Microsoft Outlook will automatically highlight spam and bulk mail in a different color so you can delete it without even looking at the subject line. This is easier than searching for an ADV label that a marketer may or may not know is required. Additionally, all services including AOL allow you to install personal screens built into your email browser that lets you automatically delete spam and bulk mail by keywords, by sender or by address. These systems give the consumer a foolproof way to banish spam and bulk mail from their inbox with NO cost to the state or any consumer.

Senate Commerce Committee
Feb. 13, 2002
Attachment 4-1

I applaud your efforts elsewhere in this bill to go after the real cyber criminals. We support Section One (c) (1) (A), which makes it illegal to fraudulently identify or forge headers and return addresses. We support Section One (c) (1) (B), the prohibition against false or misleading information in the subject line.

Additionally, it should be illegal to sell or distribute software that is designed to falsify electronic mail transmissions or other routing information.

Internet service providers (ISPs) should be given the ability to sue and recover attorney's fees from businesses that break the laws that make offensive or fraudulent email illegal. The ISP needs legal tools to help keep commercial email traffic free of these objectionable materials.

Additionally, police and prosecutors need additional tools, training and funding to investigate, identify and prosecute cyber criminals. The Internet industry is available to help train law enforcement on the technology and help consumers protect themselves from illegal email operators. The Internet Alliance's Law Enforcement and Security Council launched an innovative program in New York in early 2001 to bring industry leaders and police and prosecutors together to discuss Internet crime issues and search for common solutions.

Finally, the Internet is in its infancy. We urge you not to legislate stagnant solutions to evolving problems when effective technological solutions are available, that can stretch and adapt, as the Internet and the issues it raises change. Again, I ask you to remove the labeling requirements before you advance this bill from your committee.

Thank you for taking time to review our position. Please let me know if I can be of any further assistance to you or other members.

Sincerely,

Emily Hackett