

NO. 69416-8

---

**SUPREME COURT OF THE STATE OF WASHINGTON**

---

STATE OF WASHINGTON,  
APPELLANT,

v.

JASON HECKEL,

Respondent.

ON APPEAL FROM KING COUNTY SUPERIOR COURT  
No. 98-2-25480-7 SEA

---

**AMICUS BRIEF  
OF THE WASHINGTON ASSOCIATION  
OF INTERNET SERVICE PROVIDERS**

---

Brian W. Esler  
Richard J. Busch  
Miller Nash LLP  
4400 Two Union Square  
601 Union Street  
Seattle Washington 98101-2352  
(206) 622-8484

Attorneys for Amicus  
Washington Association of  
Internet Service Providers

## I. AMICUS IDENTIFICATION AND INTEREST

The Washington Association of Internet Service Providers (WAISP) is a trade association formed in 1997 to represent the common interests of the Internet service provider ("ISP") industry in Washington.<sup>1</sup> WAISP is self-governing, with a Board of Directors elected from the membership. WAISP's specific goal is to represent the interests and concerns of commercial companies and non-profit organizations that provide access to the Internet. The 50 members of WAISP provide the bulk of Internet access services to Washington communities, serving as the first link in connecting most Washington consumers to the Internet.<sup>2</sup>

These companies are also the first to suffer the effects of unsolicited commercial e-mail, or spam,<sup>3</sup> bearing the literal burden of

---

<sup>1</sup> WAISP and its counsel would like to express their appreciation to the Center for Law, Commerce & Technology at the University of Washington School of Law, and especially to Ethan Ackerman and Aaron Perrine, for their excellent assistance with the research for and drafting of this Amicus Brief.

<sup>2</sup> Attached in Appendix A is a listing of the current WAISP members.

<sup>3</sup> Unsolicited commercial e-mail is commonly referred to as 'spam,' in reference to a Monty Python skit where the actors are drowned out by repetitive, annoying singers chanting the phrase "spam, spam, spam, spam." This reference likely originated because of the similar annoying, drowning-out effect the e-mails had on a recipient's in-box. *See* Gary S.

keeping the Internet running for consumers and businesses on a daily basis. WAISP advocates sensible, implementable, and effective legislative action that does not infringe on legitimate personal expression or business concerns, and strongly believes that the Commercial Electronic Mail Act (RCW 19.190.005 et seq.) is an excellent first step in that direction. WAISP's members, along with other ISPs and the Internet-using public, all stand to benefit from judicial resolution of the constitutionality of this legislation.

The parties have stipulated to WAISP's involvement in this case. Appendix 5. Rather than repeating the arguments advanced by the State, this brief will describe the finer points of the Internet technologies involved in this case in order to clarify the particularly damaging impact that spam has upon the Internet, ISPs, and Washington consumers.

## **II. STATEMENT OF THE CASE**

In light of RAP Rule 10.3(e) (requiring Amicus to avoid duplicity) this brief relies on the appellant's brief for a more extensive recitation of the proceedings below.

---

Moorefield, *SPAM - It's not Just for Breakfast Anymore* 5 B.U. J. SCI. & TECH. L. 10 (1997).

### **III. SUMMARY OF AMICUS ARGUMENT**

The Commercial Electronic Mail Act, RCW Ch. 19.190, ("Act") represents a lawful attempt by the State of Washington to prohibit the use of what amounts to forged license plates on the information superhighway. The Act affects only fraudulent or misleading spam to or from Washington users. While such deceptive spam is a small subset of all e-mail messages, this small subset causes a disproportionately large amount of technical problems and economic losses to ISPs and Internet users, as explained further below.

The Act is not preempted by any Federal regulation, and its analogue is even contemplated in proposed Federal consumer protection legislation. The Act passes the judicially-defined Dormant Commerce Clause tests for non-discriminatory state enactments that affect interstate commerce. The Act is non-discriminatory, facially and in effect. Also, the Act clearly passes the "burdens-benefits" test, the "inconsistent regulations that impede commerce" test, and the "wholly external regulation" exception that are routinely applied in Dormant Commerce Clause jurisprudence.

While this brief focuses primarily on the burdens to ISPs and Washington consumers arising from the fraudulent or misleading spam prohibited by the Act, WAISP agrees with the more detailed legal analysis submitted by the State of Washington. The Act was crafted with an eye to avoiding constitutional pitfalls, and the resulting legislation is entitled to a presumption of constitutionality, with a burden of reasonable doubt on the defendant to prove otherwise.

#### **IV. ARGUMENT**

##### **A. STANDARD OF REVIEW**

Review of a summary judgment is de novo. See Brief of Appellant, at 8.

##### **B. THE BENEFITS TO WASHINGTON ISPS AND CONSUMERS FROM ELIMINATING FRAUDULENT SPAM CLEARLY OUTWEIGHS WHATEVER INCIDENTAL BURDENS MAY BE PLACED ON INTERSTATE COMMERCE.**

At its core, the Act only prohibits commercial e-mail that has a misleading return address or subject line. The relevant provision reads as follows:

- (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 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 19.090.020.

WAISP agrees with the State's argument that fraudulent communications are not entitled to any protection under the U.S. Constitution's Dormant Commerce Clause. State's brief at 9. However, as explained below, even if the Court finds that defendant's conduct is legitimate commerce, the burden to defendant of sending "non-fraudulent spam" is minimal when compared to the Act's enormous benefits to Washington's businesses and residents.

1. [The Act places no real burden upon commerce.](#)

Essentially, the only 'burden' that the Act places upon commerce is the requirement that spam be truthful – that there be no deceptive header,

return address or subject line. In order to demonstrate that the Act places no burden on commerce, the Court needs to consider how e-mail works.

E-mail is sent from one e-mail user to other e-mail users through the Internet. The Internet is a giant "network of networks" for computers. It interconnects innumerable personal computers, computer networks and large computers, and allows them to share a wide variety of digital information including text, images, sound and video, among people, institutions, corporations and governments around the world. *Reno v. American Civil Liberties Union ("Reno")*, 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997), *aff'g American Civil Liberties Union ("ACLU") v. Reno*, 929 F. Supp. 824 (E.D. Pa. 1996); *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 164 (S.D. N.Y. 1997); *ACLU v. Johnson*, 4 F. Supp. 2d 1029, 1031 (D. N.M. 1998); *ACLU v. Reno ("Reno II")*, 31 F. Supp. 2d 473, 481 (E.D. Pa. 1999).

E-mail enables an individual to send an electronic message - generally akin to a note or letter - to another individual or to a group of addresses. *Reno I*, 117 S. Ct. at 2335; *Pataki*, 969 F. Supp. at 165. There are basically two parts to an e-mail message: the 'header' and the message itself. The header is the part of the e-mail message that contains address

and routing information, including the 'TO:' and 'FROM:' addresses, and the subject line of the e-mail. The 'FROM' address in the header includes sender's ISP's 'domain name' - the globally unique name for the sender's ISP's computer systems. *See* RCW 19.190.010(5).

The Act requires that spam contain truthful information in three areas: (1) the 'FROM' e-mail address (the point of origin of a message), (2) the domain name (the transmission path of a message), and (3) the subject line. RCW 19.190.020(1). E-mail programs, including the e-mail server programs run by WAISP's members and all other legitimate Internet computer systems, *automatically* generate a legitimate and correct address and domain name information.

Therefore, in order to comply with the Act, the only affirmative action a spammer needs to take is to send the e-mail messages using a truthful subject line. This requirement – using a truthful subject line – imposes absolutely no burden on legitimate commerce. Indeed, many commercial e-mail programs will include the first few words of the message as the subject if no subject is indicated, which would not be misleading under the Act. Literally, if the spammer does nothing out of the ordinary, he or she will always be in compliance with the Act.

Therefore, the Act is consistent with the Dormant Commerce Clause of the U.S. Constitution.

2. The defendant placed a burden upon himself when he sent deceptive spam.

In reality, it is easier to send spam that complies with the Act than it is to send deceptive spam that does not. Legitimate e-mail messages can be sent, in a single step, by pressing the "send" button. To send spam without a valid return address, spammers must take additional, affirmative actions to disguise the account sending the message. 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 message's address and domain name information. E.g., testimony of Dave Kramer, Gary Gardner, Jim Kendall, Ray Jones, Darwin Hill, Jay Stewart, and Ed McNichol, January 28, 1998, before Washington House Committee on Energy and Utilities (a partial transcript of which is attached as Appendix 2 and is available in full through TVW at <http://198.239.32.162/ramgen/199801/1998010112.ra> – (House testimony on HB2742)). Sending spam with a valid return address does not entail the deliberate act of on-line forgery. The defendant placed the additional burden upon himself when he violated the

Act by placing fraudulent 'license plates' on his messages over the information superhighway.

3. [The benefits of the Act are enormous for Washington state's ISPs and Internet users.](#)

In order to better understand the benefits of the Act for Washington state's ISPs and Internet users, the Court should understand how ISPs send, receive and manage e-mail messages that are sent through the Internet.

Individual Internet users gain access to the Internet through a personal computer that is connected to a telephone or other data line. The personal computer may use the telephone line to connect to one of the many ISPs who provide account numbers and passwords enabling users to gain access to their networks. *Reno I*, 117 S. Ct. at 2334; *Pataki*, 969 F. Supp. at 164-165. ISPs offer their subscribers dial-up or dedicated telephone access to the ISPs' computers or networks, which are in turn linked directly to the Internet. *ACLU v. Reno*, 929 F. Supp. at 832-33; *Reno I*, 117 S. Ct. at 2334. ISPs who charge a fee to provide Internet access services may charge either a flat monthly fee for unlimited usage, or a usage-based fee based upon the amount of time that the user spends 'on-line'. In addition, the dial-up telephone connection may be a local

telephone call, or might be a toll call where the user pays their telephone company a fee for each minute that they spend connected to the ISPs' computer networks.

When an Internet user connects - or 'logs-on' - to their ISP and sends an e-mail message, the ISPs who transmit the message also make computer log entries to record the event.

If a spammer complies with the Act, then (1) these ISPs make only one computer log entry and (2) the Internet user may decide whether to spend the time (and money if they are using any usage-based services) to download and read the messages based upon truthful information in the e-mail header. If a spammer sends deceptive spam, then the following occurs:

- a. **ISPs must buy additional computer equipment, hire additional personnel, and charge higher Internet usage fees to manage deceptive spam while maintaining quality service levels for their customers.**

Deceptive spam imposes significant burdens on ISPs' computer hardware, computer software, personnel and Internet usage costs; banning deceptive spam would significantly and concretely ameliorate these burdens. Increased e-mail traffic on the ISP's e-mail computers (called

'servers') requires expensive infrastructure upgrades, the costs of which are born entirely by the ISP and never by the spammer. *See* Statement of Rep. Gary Miller, *House Hearing before the Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce*, 106<sup>th</sup> Congress, 1<sup>st</sup> Session, November 3, 1999, *citing ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition*, Gartner Consulting Report, June 1999 (attached as Appendix 3).

As the Legislature knew when it passed the Act, deceptive spam burdens ISPs by forcing them to purchase additional computer equipment to handle the increased e-mail traffic that it generates. For example, when Internet users attempt to reply to deceptive spam that has a fraudulent return address or domain name, one e-mail message (and the ISPs' 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. Appendix 2.

In March 1998, Pacific Bell was required to invest \$500,000 in extra e-mail gateways due to a sudden surge in bulk spam that disrupted e-mail service at its Pacific Bell Internet Services for several days. *See: Postage due on junk e-mail – Spam costs Internet millions every month*, InternetWeek, May 4, 1998 (found on the World Wide Web at: <http://www.techweb.com/se/directlink.cgi?INW19980504S0003>). This is precisely the type of economic cost that the Act is designed to avoid through the prohibition of deceptive spam.

Spam also imposes increased personnel costs on ISPs in two ways. First, ISPs must hire additional customer service staff to handle the tidal wave of complaints from consumers who blame their ISP for spam. Over half of users who complain about spam complain to their ISP. *See ISPs and Spam: The Impact of Spam on Customer Retention and Acquisition*, Gartner Consulting Report, June 1999 (attached as Appendix 3). The *Gartner* study found that 3-5 additional customer support staff would be needed by each one-million user ISP, at a total cost of up to \$250,000 per

year. The cost of not hiring additional customer service staff would be additional "churn", described below, and/or the breakdown of any meaningful customer service effort, especially on the part of small to mid-sized ISPs. Second, ISPs must hire additional system administrators to ferret out accounts being used to send spam. Nearly all ISPs require new users to agree to a use-policy that prohibits the sending of spam; spammers are always in violation of this policy, and ISPs expend significant administrative resources attempting to police their users. As noted by the *Gartner* study, this cost - tied to one additional full-time system administrator - has been estimated at over \$75,000. *Id.*

Deceptive spam causes customer defections, or "churn," from ISPs. The *Gartner* study commissioned by the FTC shows that 83% of online users dislike spam. That study found that 7% of users who switch ISPs did so to avoid spam, and an additional 38% would switch if the spam they received doubled. Whether or not spam doubles is currently not a question of "if," but "when", with e-mail accounts receiving proportionally more and more spam the longer a user maintains the account. When users leave, ISPs lose their subscription revenue and must spend additional funds attempting to acquire new subscribers. Deceptive

spam generates bad public relations for ISPs, which in turn generates churn. Assuming a churn rate of 4.5% for a one-million user ISP, the *Gartner* study estimates the total cost of spam to a 1-million customer ISP at nearly \$7 million per year.

b. [Internet end users pay higher costs for Internet usage fees and communications charges.](#)

Some Internet customers subscribe to usage-based Internet service plans because of the plans provide economical access to the Internet, thereby making the Internet accessible to a wider variety users. If the Internet users are misled into downloading fraudulent spam, their bill for Internet access services will increase, since they are downloading messages they might otherwise ignore or delete except for the misleading subject line.

In addition, many persons in rural Washington do not have toll-free access to Internet access services and are required to pay toll charges to use the Internet. Any time these users spend downloading spam because they were misled about the subject or the point of origin of the message is a second cost of deceptive spam.

c. Deceptive spam shifts the economic cost of 'electronic junk mail' to ISPs and Internet end users.

As discussed above, deceptive spam imposes significant economic costs on Internet end users and ISPs. The spammer could send their messages through U.S. postal mail, but the cost of sending such messages through the mail is significantly higher than the cost of sending spam. Essentially, spammers are shifting the economic cost of their messages from themselves to the ISPs and the Internet end users.

The spammers' shifting of costs to ISPs and Internet end users is identical to the shifting of costs involved in unsolicited "junk faxing." In both cases the recipients and their service providers bear the cost of the advertising. Here, the cost is multiplied exponentially as frustrated users attempt to respond to the spammers' fraudulent return address. The 9<sup>th</sup> Circuit recognized that it is a legitimate government interest to ban such cost-shifting from the sender of the message to the recipient of the message. *Destination Ventures, Ltd. v. FCC*, 46 F.3d 54 (9th Cir. 1995). Likewise, it is a legitimate exercise of Washington state's interest for Washington state to prohibit the shifting of costs to Internet end users and ISPs.

**C. THE ACT DOES NOT CONFLICT WITH ANY OTHER STATE'S REGULATIONS**

As the State's brief indicates, the Dormant Commerce Clause generally discourages inconsistent regulations among the several states where the practical effect of those inconsistent obligations would be to stunt or paralyze interstate commerce. To clarify what constitutes 'inconsistent,' the 3<sup>rd</sup> Circuit has held that "state laws which merely create additional, but not irreconcilable obligations are not considered to be 'inconsistent'" for purposes of a dormant commerce clause analysis. *Instructional Systems, Inc. v. Computer Curriculum Corp.*, 35 F.3d 813, 826 (3d Cir. 1994).

Federal legislators have acknowledged that "There are multiple players involved in resolving these problems in the telecommunications industry, the Federal Government as well as at the State level." *Statement of Rep. Edward Markey, Mass. before House Hearing, Subcommittee on Telecommunications, Trade, and Consumer Protection of the Committee on Commerce*, 106<sup>th</sup> Congress, 1<sup>st</sup> Session, November 3, 1999. *See also Statement of Rep. Gene Green* (specifically recognizing and commending Washington Unsolicited E-mail Act, also recognizing need for "...more than one solution") (both attached as Appendix 4). Indeed, as a testing

ground, or 'laboratory of democracy,' Washington's Act is affirmatively searching for a solution, apparently one that has caught federal notice and acceptance. *E.g.*, *New State Ice Co. v. Liebmann*, 285 U.S. 262, 311 (1931) (Brandeis, dissenting) ("It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory . . .")

While fifteen states have enacted alternate, usually more restrictive, regulations for spam, it is vital to note that it is not possible for a spammer to violate another state's law in attempting to comply with Washington state's law. WAISP is not aware of any state law or regulation which prohibits spammers from utilizing truthful return addresses and subject lines. Examples of other state requirements include prohibitions of forged headers, opt-out clauses, and requirements that spam be labeled "advertisement" in the subject line. These fall well within the Third Circuit's observation that additional, but not irreconcilable, obligations are not 'inconsistent.' *Instructional Systems*, 35 F.3d at 826. For a comprehensive coverage and timeline of all sixteen state enactments, see Max P. Ochoa, *Recent State Laws Regulating Unsolicited Electronic Mail*, 16 Computer & High Tech. L.J. 459 (May 2000).

**D. THE ACT IS PRESUMED CONSTITUTIONAL AND DEFENDANT BEARS THE BURDEN TO PROVE OTHERWISE.**

As Appellant points out, legislatively enacted statute is presumed to be constitutional and the challenger bears the burden of establishing the unconstitutionality of the legislation beyond a reasonable doubt. (Brief for Appellant at 8.) WAISP urges the court to maintain this high bar, as the Act clearly serves a beneficial role by safeguarding citizens and corporations, and is clearly compatible with the Constitution.

**V. CONCLUSION**

The Washington Unsolicited Commercial Electronic Mail Act represents a legitimate attempt to protect the interests of Washington citizens at no expense to any legitimate interstate commerce. WAISP urges the court to recognize that this case amounts to little more than a question of the constitutionality of a ban on using forged license plates on the Information Superhighway.

DATED this 2<sup>nd</sup> day of October, 2000.

MILLER NASH LLP

---

Brian W. Esler  
WSB No. 22168

Richard J. Busch  
WSB No. 16739

Attorneys for Appellant

## TABLE OF AUTHORITIES

### Page

#### CASES

<i>ACLU v. Johnson</i> , 4 F. Supp. 2d 1029 (D. N.M. 1998) .....	7
<i>ACLU v. Reno</i> , 929 F. Supp. at 832-33 .....	10
<i>ACLU v. Reno ("Reno II")</i> , 31 F. Supp. 2d 473 (E.D. Pa. 1999) .....	7
<i>American Libraries Association v. Pataki</i> , 969 F. Supp. 160 (S.D. N.Y. 1997) .....	7, 10
<i>Destination Ventures, Ltd. v. FCC</i> , 46 F.3d 54 (9th Cir. 1995) .....	16
<i>Instructional Systems, Inc. v. Computer Curriculum Corp.</i> , 35 F.3d 813 (3d Cir. 1994) .....	17, 18
<i>New State Ice Co. v. Liebmann</i> , 285 U.S. 262 (1931) .....	17
<i>Reno v. American Civil Liberties Union ("Reno")</i> , 521 U.S. 844, 117 S. Ct. 2329, 138 L. Ed. 2d 874 (1997), aff'g <i>American Civil Liberties Union ("ACLU") v. Reno</i> , 929 F. Supp. 824 (E.D. Pa. 1996) .....	6, 7, 10

#### MISCELLANEOUS

Gary S. Moorefield, <i>SPAM - It's not Just for Breakfast Anymore</i> 5 B.U. J. SCI. & TECH .....	1
Max P. Ochoa, <i>Recent State Laws Regulating Unsolicited Electronic Mail</i> , 16 Computer & High Tech. L.J. 459 (May 2000) .....	18

An extra section break has been inserted above this paragraph. Do not delete this section break if you plan to add text after the Table of Contents/Authorities. Deleting this break will cause Table of Contents/Authorities headers and footers to appear on any pages following the Table of Contents/Authorities.

I hereby certify that I served the foregoing AMICUS BRIEF on:

H. Regina Cullen  
Attorney General's Office  
900 Fourth Ave., #2000  
Seattle, WA 98164-1012

Dale L. Crandall  
280 Court St. NE, #14  
Salem, OR 97301

by the following indicated method or methods:

- by **mailing** full, true, and correct copies thereof in sealed, first-class postage-prepaid envelopes, addressed to the attorneys as shown above, the last-known office addresses of the attorneys, and deposited with the United States Postal Service at Seattle, Washington, on the date set forth below.

DATED this 2<sup>nd</sup> day of October, 2000.

---

Carol Munnerlyn

Certificate of Service