SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

BILL: SB 2574

SPONSOR: Senator Garcia

SUBJECT: Commercial Relations/Electronic Mail

DATE: March 12, 2004 REVISED: _____ _____ _____ _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	Wiehle	Caldwell	CU	Favorable
2.			CM	
3.			CJ	
4.			JU	
5.			ACJ	
6.			AP	

I. Summary:

The bill:

- makes specified actions relating to commercial electronic mail messages unlawful,
- authorizes the Department of Legal Affairs to bring an action for damages or for declaratory or injunctive relief or to impose a civil penalty,
- creates a cause of action for a person who receives an unsolicited commercial electronic mail message; and for an interactive computer service, telephone company, or cable provider that handles or retransmits the commercial electronic mail message, specifying the remedies and damages available in the action,
- provides that any person outside this state who initiates or assists in the transmission of a commercial electronic mail message received in this state which violates this law and who knows, or should have known, that the commercial electronic mail message will be received in this state submits to the jurisdiction of this state for purposes of this law,
- provides that an action must be commenced within 4 years following the date of any prohibited activity, and
- provides that an interactive computer service may, upon its own initiative, block the receipt or transmission through its service of any commercial electronic mail message that it reasonably believes is, or will be sent, in violation this law, shielding an interactive computer service from liability for any action voluntarily taken in good faith to block the receipt or transmission through its service of any commercial electronic mail message that it reasonably believes is, or will be sent, in violation of the law.

The bill creates the following sections of the Florida Statutes: 668.60, 668.601, 608.602, 668.603, 668.604, 668.605, 668.606, and 668.6075.

II. Present Situation:

Congress recently passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or the "CAN-SPAM Act of 2003." S.B. 877. 108th Cong., 1st Session (2003). It was signed by the President on December 16, 2003 and took effect January 1, 2004.

Unlawful acts

Section 4 of the act makes it unlawful, in or affecting interstate or foreign commerce, to knowingly do, or conspire to do, the following acts.

- Access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from or through the computer.
- Use a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages.
- Materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages.
- Register, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiate the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names.
- Falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiate the transmission of multiple commercial electronic mail messages from such addresses.

Violations of this section are punishable by a fine, imprisonment of up to five years, or both. Additionally, the court is to order forfeiture of any property constituting or traceable to gross proceeds obtained from the offense or any equipment used or intended to be used to commit the offense.

Section 5 makes it unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this provision:

- Header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading.
- A ''from'' line (the line identifying or purporting to identify a person initiating the message) that accurately identifies any person who initiated the message shall not be considered materially false or materially misleading.
- Header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

Section 5 also makes it unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message if such person has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that a subject heading of the message would be likely to mislead a recipient, acting reasonably under the circumstances, about a material fact regarding the contents or subject matter of the message.

Section 5 also makes it unlawful for any person to initiate the transmission to a protected computer of a commercial electronic mail message that does not contain a functioning return electronic mail address or other Internet-based mechanism, clearly and conspicuously displayed, that:

- a recipient may use to submit, in a manner specified in the message, a reply electronic mail message or other form of Internet-based communication requesting not to receive future commercial electronic mail messages from that sender at the electronic mail address where the message was received; and
- remains capable of receiving such messages or communications for no less than 30 days after the transmission of the original message.

If a recipient makes a request not to receive some or any commercial electronic mail messages from such sender, then it is unlawful:

- for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request;
- for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request;
- for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate these provisions; or
- for the sender, or any other person who knows that the recipient has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

These prohibitions do not apply if there is affirmative consent by the recipient subsequent to the request.

Section 5 also makes it unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides:

- clear and conspicuous identification that the message is an advertisement or solicitation;
- clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender; and
- a valid physical postal address of the sender.

Finally, section 5 makes it unlawful for any person to initiate, in or affecting interstate commerce, the transmission, to a protected computer, of any commercial electronic mail message that includes sexually oriented material and to:

- fail to include in the subject heading for the electronic mail message marks or notices prescribed by the Federal Trade Commission as a warning of the content; or
- fail to provide that the matter in the message that is initially viewable to the recipient, when the message is opened by any recipient and absent any further actions by the recipient, includes only
    - the prescribed warning marks or notices;
    - the information required to be included in the message relating to the ability to send a notice to a physical address requesting not to receive any further such electronic mail messages; and
    - instructions on how to access, or a mechanism to access, the sexually oriented material.

This prohibition does not apply to the transmission of an electronic mail message if the recipient has given prior affirmative consent to receipt of the message.

Any person who knowingly violates these prohibitions is to be fined or imprisoned not more than 5 years, or both.

Section 6 of the act makes it unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation of the prohibition on false or misleading transmission information if that person:

- knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;
- received or expected to receive an economic benefit from such promotion; and
- took no reasonable action:
    - to prevent the transmission; or
    - to detect the transmission and report it to the Federal Trade Commission.

The states are excluded from enforcing this section.

Enforcement

Section 7 provides that a violation of the act is an unfair and deceptive act or practice and may be enforced by the Federal Trade Commission. Additionally, a state attorney general may bring an action on behalf of the residents of the state in a federal district court in any case in which the attorney general has reason to believe that an interest of the residents of the state has been, or is threatened to be, adversely affected by any person who violates specified sections of the act. The attorney general may seek an injunction against further violations or to obtain damages in an amount equal to the greater of actual monetary losses suffered by residents or statutory damages consisting of up to $250 per violation. For a violation of section 5 other than section 5(a)(1), damages cannot exceed $2,000,000. The court may increase a damage award to not more than three times the amount otherwise available if the court determines that the defendant committed

the violation willfully and knowingly, or the defendant's unlawful activity included "address harvesting" or "dictionary attacks" or automated creation of multiple electronic mail accounts or the relay or retransmission of a commercial electronic mail message through unauthorized access. Address harvesting involves using automated means to obtain electronic mail addresses from an Internet website or proprietary online service whose operator has posted a notice that addresses maintained by the site or service will not be given, sold, or otherwise transferred to any other party. Dictionary attacks involve obtaining an electronic mail address by using an automated means that generates possible electronic mail addresses by combining names, letters, or numbers into numerous permutations. In a successful action, the court may award attorney fees and costs to the state.

Preemption

Section 8 of the act expressly supersedes any state statute, regulation, or rule that expressly regulates the use of electronic mail to send commercial messages, except to the extent that such law prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto. The act does not preempt state laws that are not specific to electronic mail or other state laws to the extent that those laws relate to acts of fraud or computer crime.

Additionally, the act is not to be construed to have any effect on the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

III. Effect of Proposed Changes:

The bill creates s. 668.60, F.S., to provide a short title; s. 668.601, F.S., to provide legislative intent; and s. 608.602, F.S., to provide definitions.

Unlawful acts

The bill creates s. 668.603, F.S., to make it unlawful to:

- initiate the transmission of an unsolicited commercial electronic mail message from a computer located in this state or to an electronic mail address that is held by a resident of this state which:
  - Uses a third party's Internet domain name without permission of the third party;
  - Contains falsified or missing routing information or otherwise misrepresents, falsifies, or obscures any information in identifying the point of origin or the transmission path of the unsolicited commercial electronic mail message; or
  - Contains false or misleading information in the subject line.
- Assist in the transmission of an unsolicited commercial electronic mail message when the person providing the assistance knows, or has reason to know, that the initiator of the commercial electronic mail message is engaged in or intends to engage in a practice that violates this section.
- Distribute software or any other system designed to falsify missing routing information identifying the point of origin or the transmission path of the commercial electronic mail message.

Enforcement

The bill creates s. 668.606, F.S., to provide remedies. The Department of Legal Affairs is authorized to bring an action for damages or for declaratory or injunctive relief or to impose a civil penalty as provided in this section. The bill creates a cause of action, without regard to any other remedy or relief to which a person is entitled, including the right to seek declaratory and injunctive relief against a person who initiates or assists in the transmission of a commercial electronic mail message that violates, has violated, or is otherwise likely to violate s. 668.603, F.S., for:

- A person who receives an unsolicited commercial electronic mail message; and
- An interactive computer service, telephone company, or cable provider that handles or retransmits the commercial electronic mail message.

A prevailing plaintiff in an action filed under the bill is entitled to:

- An injunction to enjoin future violations of s. 668.603, F.S.
- Compensatory damages equal to any actual damage proven by the plaintiff to have resulted from the initiation of the unsolicited commercial electronic mail message or liquidated damages of $500 for each unsolicited commercial electronic mail message that violates s. 668.603, F.S., when that message is sent by the defendant:
  - To the plaintiff;
  - Through the plaintiff's interactive computer service; or
  - To any consumer in this state, if the department is the plaintiff.
- The plaintiff's attorney's fees and other litigation costs reasonably incurred in connection with the action.

The section expressly provides that it does not create a cause of action against an interactive computer service, telephone company, or cable provider whose equipment is used to transport, handle, or retransmit a commercial electronic mail message that violates s. 668.603, F.S.

The section creates a long-arm jurisdiction statute, providing that any person outside this state who initiates or assists in the transmission of a commercial electronic mail message received in this state which violates s. 668.603, F.S., and who knows, or should have known, that the commercial electronic mail message will be received in this state submits to the jurisdiction of this state for purposes of this part.

The section creates a statute of limitations, providing that an action under this section must be commenced within 4 years following the date of any activity prohibited by s. 668.603 F.S.

The bill creates s. 668.6075, F.S., to provide that a violation of s. 668.603, F.S., is deemed an unfair and deceptive trade practice within the meaning of part II of chapter 501. In addition to any remedies or penalties set forth in that part, a violator shall be subject to the penalties and remedies provided for in this act. Also, the remedies of this act are in addition to remedies otherwise available for the same conduct under federal or state law.

The bill creates s. 668.605, F.S., to provide that its provisions do not contravene the provisions of s. 501.2065, F.S., which provides for maintaining the confidential status of certain information

relating to intelligence or investigative information on alleged violations of the unfair and deceptive trade practices act.. This relates to newly created s. 668.6075, F.S., discussed above.

Service provider blocking of messages

The bill creates s. 668.604, F.S., to provide that an interactive computer service may, upon its own initiative, block the receipt or transmission through its service of any commercial electronic mail message that it reasonably believes is, or will be sent, in violation of newly created s. 668.603, F.S. It also shields an interactive computer service from liability for any action voluntarily taken in good faith to block the receipt or transmission through its service of any commercial electronic mail message that it reasonably believes is, or will be sent, in violation of newly created s. 668.603, F.S.

Section 2 of the bill is a severability clause, providing that if any provision of this act or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this act which can be given effect without the invalid provision or application, and to this end the provisions of this act are severable.

Section 3 provides that the bill takes effect July 1, 2004.

IV. Constitutional Issues:

A. Municipality/County Mandates Restrictions:

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

V. Economic Impact and Fiscal Note:

A. Tax/Fee Issues:

None.

B. Private Sector Impact:

Persons and businesses injured by unlawful commercial e-mail activity may be able to recover damages. They maybe able to better use computers and e-mail without the hindrance of prohibited commercial e-mails.

C. Government Sector Impact:

The Office of the Attorney General states that it can enforce the bill with existing resources.

VI. Technical Deficiencies:

None.

VII. Related Issues:

The federal act provides that it "supersedes any statute, regulation, or rule of a State . . . that expressly regulates the use of electronic mail to send commercial messages, except to the extent that such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto."

Generally, when a federal law expressly preempts state law, the states may not enact any law on the specific subject matter of the federal law. Here, however, the bulk of the federal law regulates falsity or deception in commercial electronic mail messages; the law expressly preempts state law regulating commercial electronic mail messages; but yet it also expressly exempts from this preemption state law that prohibits falsity or deception in any portion of the email or an attachment. In this context, the plain meaning of the words expressing the preemption and those expressing the exemption appear to be at odds, and it appears difficult to give effect to both the preemption and the exemption.

There are at least two possible interpretations to reconcile these potentially conflicting provisions. The first focuses on giving meaning and effect to the preemption; the second on giving meaning and effect to the exemption.

Under the first possible interpretation (focusing on giving meaning and effect to the preemption), the states are prohibited from regulating deception or falsity in routing, addressing, and so forth (as the federal law does this), and the exemption is to be interpreted to allow state law only prohibiting falsity or deception in text of the email or attachments. Under such an interpretation, SB 2574 may be subject to challenge as being preempted by federal law.

Under the second possible interpretation, (focusing on giving meaning and effect to the exemption), the exemption language means exactly what appears to say, even though arguably this would negate the meaning and effect of the bulk of the preemption. Under this interpretation, the states could enact laws prohibiting falsity or deception in *any portion of* the email or an attachment, including information relating to routing, addressing, and so forth. All that would be preempted are requirements such as those relating to labeling and notice and to notice to the sender not to send any more emails. Under this interpretation, SB 2574 would not appear to be subject to challenge of federal preemption.

There is some indication that this second interpretation is the one intended. In discussing the bill on the House floor on January 28, 2004, (to add to the statements made in the November 21, 2003 and December 16, 2003, floor debate on S. 877) Representative John Dingell said:

> Mr. Speaker, this statement represents my views as well as the views of W.J. ``BILLY'' TAUZIN, Chairman of the Committee on Energy and Commerce, on S. 877 the Can-Spam Act of 2003 (``the Act''). Our views on Sections one through five of the Act are contained in a separate statement submitted today by Chairman TAUZIN.
>
> . . .
>
> Section (b) provides for preemption of state laws that expressly regulate the use of e-mail to send commercial messages, including laws that regulate the form or manner of sending commercial e-mail (e.g. labeling requirements). It does not preempt statutes dealing with fraud, falsity, or deception in any portion of a commercial e-mail message or attachment thereto. Thus, State opt-in spam laws, such California S.B. 186 enacted in the fall of 2003, state opt-out spam laws, and state ADV labeling requirements for commercial e-mail *would be entirely preempted, except to the limited extent that those laws also prohibited use of falsification techniques or deception such as those prohibited in 18 U.S.C.1037, Section 5(a)(1) and Section 5(a)(2) of this Act. Similarly, State anti-spam laws, such as Virginia's, that expressly regulate or criminalize e-mail falsification techniques would not be preempted.* In addition, Section 8(b) is not intended to preempt general purpose State deceptive trade practice laws, or State common law rules, such as State trespass to chattels theories, that have been used in anti-spam litigation. Nor does Section 8(b) preempt State laws relating to acts of fraud or computer crime. However, to the extent any State or local law regulates the manner of sending commercial e-mail, the mere titling of the law as an ``anti-fraud statute'' or the combination of commercial e-mail regulation provisions with actual falsification or computer crime provisions in the same statute is not sufficient to avoid preemption of those regulatory provisions by this Act.

Under either interpretation, the provisions of newly created s. 608.604, F.S., authorizing a service provider to block messages it reasonably believes violates the prohibited activity section and exempting the provider from liability for such blocking, should be allowed under the federal act. The federal act's preemption provisions expressly state that it is not to be construed to have any effect on the lawfulness or unlawfulness, under any other provision of law, of the adoption, implementation, or enforcement by a provider of Internet access service of a policy of declining to transmit, route, relay, handle, or store certain types of electronic mail messages.

VIII. Amendments:

None.