HOUSE OF REPRESENTATIVES STAFF ANALYSIS

BILL #: HB 45 CS False or Misleading Electronic Mail
SPONSOR(S): Porth
TIED BILLS: **IDEN./SIM. BILLS:** SB 80

REFERENCE	ACTION	ANALYST	STAFF DIRECTOR
1) Utilities & Telecommunications Committee	12 Y, 1 N, w/CS	Cater	Holt
2) Criminal Justice Committee	7 Y, 0 N	Ferguson	Kramer
3) Criminal Justice Appropriations Committee	6 Y, 0 N	Sneed	DeBeaugrine
4) Commerce Council			
5)			

SUMMARY ANALYSIS

HB 45 CS amends the Electronic Mail Communications Act and creates criminal penalties for sending unsolicited false or misleading commercial electronic mail messages. In addition, the bill creates the "Anti-Phishing Act," prohibiting the acquisition and fraudulent use of a Florida resident's personal identifying information through the use of a website or e-mail.

The bill requires that any state or local agency, as defined in s. 119.011, F.S., or legislative entity that operates a website and uses electronic mail to post the following statement in a conspicuous location on its website:

> *"Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing."*

In addition, the bill addresses the following:

False or Misleading Electronic Mail

- Provides that it is a misdemeanor of the first degree or a felony in the third degree under certain circumstances to send an unsolicited false or misleading commercial electronic mail.
- Provides immunity from criminal prosecution to an interactive computer service, customer premises equipment provider, communications services provider, or cable provider whose equipment is used to transport, handle, or retransmit a commercial electronic mail message.
- Provides that remedies and criminal penalties under the act are in addition to remedies and criminal penalties otherwise available under federal or state law.

Internet Phishing

- Creates a civil cause of action for internet access providers, financial institutions, web page or trademark owners harmed by a violation.
- Provides power to seek injunctive relief and damages and creates a three-year statute of limitations.
- Grants the Department of Legal Affairs rulemaking authority to implement the provisions of this act.

The Criminal Justice Impact Conference met on February 28, 2006 and determined that this bill would have an insignificant impact on the inmate population in the Department of Corrections. The Department of Legal Affairs has stated that the bill will have an indeterminate impact on the department's revenues and expenditures. See fiscal comments.

This bill takes effect July 1, 2006.

FULL ANALYSIS

I. SUBSTANTIVE ANALYSIS

A. HOUSE PRINCIPLES ANALYSIS:

Promote personal responsibility -- The bill creates criminal penalties for sending false or misleading electronic mail and creates a new civil cause of action to deter and punish identity theft.

Provide limited government -- The bill creates criminal penalties for sending false or misleading electronic mail and creates a new civil cause of action to deter and punish identity theft.

B. EFFECT OF PROPOSED CHANGES:

ELECTRONIC MAIL PUBLIC RECORDS NOTIFICATION

HB 45 CS requires that any state or local agency, as defined in s. 119.011, F.S.[1], or legislative entity that operates a website and uses electronic mail to post the following statement in a conspicuous location on its website:

"Under Florida law, e-mail addresses are public records. If you do not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing."

FALSE OR MISLEADING ELECTRONIC MAIL

Background

Federal Legislation

In 2003, Congress passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or the "CAN-SPAM Act of 2003."[2] The CAN-SPAM act provides that if the activity is in or affects interstate or foreign commerce, it is unlawful to knowingly:

- Access a protected computer, as defined in section 1030(e)(2)(B) of Title 18, without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from or through the computer.
- Use a protected computer, as defined in section 1030(e)(2)(B) of Title 18, 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.

[1] Section 119.011, F.S., states that an "agency" means any state, county, district, authority or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law including, for the purposes of this chapter, the Commission on Ethics, the Public Service Commission, and the Office of Public Counsel, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency.

[2] 15 U.S.C. ss. 7701-13.

- Falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of five or more Internet Protocol addresses, and intentionally initiate the transmission of multiple commercial electronic mail messages from such addresses.

The CAN-SPAM act specifies the penalties for a violation which may include a fine, imprisonment of up to five years, or both. Additionally, the court may 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.

State Legislation

In 2004, the Legislature passed the Electronic Mail Communications Act [3]. The act provides that a person may not:

- 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;
    - Contains false or misleading information in the subject line; or
    - Contains false or misleading information in the body of the message.
- 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.

Summarily, the Electronic Mail Communications Act (act) also:

- Authorizes the Department of Legal Affairs to bring an action for damages, or to seek declaratory or injunctive relief, or to impose a civil penalty for a violation of the prohibited activities outlined in the act;
- Creates a cause of action for a person who receives an unsolicited commercial electronic mail message in violation of the act's provisions;
- Provides that a violation of the act's prohibited activities is also a violation of the Florida Deceptive and Unfair Trade Practices Act within the meaning of part II of chapter 501;
- Provides an exemption from liability for certain commercial electronic mail providers and wireless providers who transmit commercial electronic mail, and allows an interactive computer service provider to block transmission of a commercial electronic message it believes may be sent in violation of the act's provisions;
- Provides that prevailing plaintiffs are entitled to:
    - An injunction to enjoin future violations for sending unsolicited false or misleading commercial electronic mail message.
    - Compensatory damages equal to actual damages to have resulted from the initiation of the unsolicited false or misleading commercial electronic mail message or liquidated damages of $500 for each unsolicited false or misleading commercial electronic mail message.
    - Plaintiff's attorney's fees and other reasonably incurred litigation costs.
- Provides that any person outside this state who initiates or assists in the transmission of a commercial electronic mail message received in this state and who knows, or should have

[3] Section 668.60, F.S.

known, that the commercial electronic mail message will be received in this state, submits to the jurisdiction of this state;
- Provides that the Act's provisions do not interfere with the confidential status of certain information relating to intelligence or investigative information; and
- Provides that an action must be commenced within 4 years following the date of any prohibited activity.

Section 668.6075, F.S., provides that sending an unsolicited false or misleading commercial electronic mail message shall be considered an unfair and deceptive trade practice within the meaning of part II of ch. 501, F.S., and that in addition to any remedies or penalties set forth in ch. 501, F.S., a violator is subject to the penalties and remedies provided in this part. The remedies in this part are in addition to the remedies otherwise available for the same conduct under federal or state law.

According to the Department of Legal Affairs, two cases under the current act were litigated in 2005, and at this time there are other active investigations. Other complaints have been filed, but the department has not been able to determine who sent the message; therefore, it has not been able to take further action.

Effect of bill

HB 45 CS amends section 668.606, F.S., to provide that the Act does not create a cause of action or provide for criminal charges against an interactive computer service, customer premises equipment provider, communications services provider, or cable provider whose equipment is used to transport, handle, or retransmit an unsolicited false or misleading commercial electronic mail message.

Currently, there are only civil remedies for sending an unsolicited false or misleading electronic mail message.[4] HB 45 CS creates section 668.608, F.S., which provides it is a misdemeanor in the first degree to send an unsolicited false or misleading commercial electronic mail message, which is punishable by a fine of up to $1,000[5] or imprisonment of up to one year.[6] It is a felony in the third degree punishable by a fine of up to $5,000,[7] or imprisonment up to five years[8], if:

- The volume of commercial electronic mail messages transmitted by the person exceeds 2,500 attempted recipients in any 24-hour period;
- The volume of commercial electronic mail messages transmitted by the person exceeds 25,000 attempted recipients in any 30-day period;
- The volume of commercial electronic messages transmitted by the person exceeds 250,000 attempted recipients in any 1-year period;
- The revenue generated from a specific commercial electronic mail message transmitted by the person exceeds $1,000;
- The total revenue generated from all commercial electronic mail messages transmitted by the person to any electronic mail message service provider or its subscribers exceed $50,000;
- The person knowingly hires, employs, uses, or permits any minor to assist in the transmission of a commercial electronic mail message in violation of section 668.603. F.S.;
- The person commits a violation within 5 years of a previous conviction under this section.

[3] Section 668.606(1), F.S.
[5] Section 775.083(1)(d), F.S.
[6] Section 775.082(4)(a), F.S.
[7] Section 775.083(1)(c), F.S.
[8] Section 775.082(3)(d), F.S.

Felony violations may also be punishable under the provisions for habitual felony offenders contained in section 775.084, F.S.

HB 45 CS provides that the remedies and criminal penalties are in addition to the remedies and criminal penalties otherwise available under federal or state law.

INTERNET PHISHING

Background

Identity theft is a substantial problem in the United States and "phishing" represents the cutting edge of this practice.

"Phishing" refers to obtaining personal identifying information from individuals via the Internet with the intent to possess or use such information fraudulently. Typically, a person attempting to obtain information sends an e-mail that appears to come from a bank or other trusted business requesting an individual to verify their account by typing personal identifying information, such as credit card information, social security numbers, account usernames, passwords, etc. A person may also use a phony web site to trick citizens into revealing sensitive personal information.

The Federal Trade Commission (FTC) reported that 27.3 million Americans have been victims of identity theft in the last five years, including 9.9 million people in 2003 alone.[11] According to the FTC, last year's identity theft losses to businesses and financial institutions totaled nearly $48 billion and consumer victims reported $5 billion in out-of-pocket expenses.[12]

Moreover, according to the Anti-Phishing Working Group, the volume of fraudulent phishing e-mail is growing at a rate in excess of 30 percent each month.[13]

Federal Legislation

The Subcommittee on Crime, Terrorism, and Homeland Security of the U.S. House of Representatives is currently reviewing H.R. 1099, which criminalizes internet scams involving the fraudulent obtaining of information, commonly known as "phishing".[14]

H.R. 1099 imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in an activity constituting fraud or identity theft under federal or state law: (1) creates or procures the creation of a website or domain name that represents itself as a legitimate online business without the authority or approval of the registered owner of such business; and (2) uses that website or domain name to solicit means of identification from any person.

---

[11] See article issued by Federal Trade Commission, dated September 3, 2003 "FTC Releases Survey of Identity Theft in U.S. 27.3 Million Victims in Past 5 Years, Billions in Losses for Businesses and Consumers". See also http://www.ftc.gov/opa/2003/idtheft.htm.
[12] Id.
[13] The Anti-Phishing Working Group (APWG) is a global pan-industrial and law enforcement association that focuses on eliminating fraud and identity theft that results from phishing and e-mail spoofing of all types.
[14] The Senate companion, S.472 is before the Judiciary Committee.

In addition, H.R. 1099 imposes a fine or imprisonment for up to five years, or both, for a person who knowingly and with the intent to engage in activity constituting fraud or identity theft under federal or state law sends an electronic mail message that: (1) falsely represents itself as being sent by a legitimate online business; (2) includes an Internet location tool referring or linking users to an online location on the World Wide Web that falsely purports to belong to or be associated with a legitimate online business; and (3) solicits means of identification from the recipient.

Effect of bill

This bill creates the "Anti-Phishing Act".

Prohibited Acts

This bill prohibits obtaining identifying information from individuals through certain means via the internet with the intent to possess or use such information fraudulently. This bill prohibits:

- representing oneself, either directly or by implication to be another person, without the authority or approval of such other person, through the use of a web page or internet domain name; and
- using that web page, a link to the web page, or another site on the Internet to induce, request, or solicit another person to provide identifying information.

This bill also prohibits sending or causing to be sent an e-mail to a resident of this state that:

- is falsely represented as being sent by another person, without the authority or approval of such person;
- refers or links the recipient to a falsely represented web site; and
- directly or indirectly solicits from the recipient identifying information for a purpose that the recipient believed to be legitimate.

This bill defines or incorporates by reference definitions of terms as follows:

- "Department" means the Department of Legal Affairs.
- "Electronic mail message" means an electronic message or computer file that is transmitted between two or more telecommunications devices; computers; computer networks, regardless of whether the network is a local, regional, or global network; or electronic devices capable of receiving electronic messages, regardless of whether the message is converted to hard copy format after receipt, viewed upon transmission, or stored for later retrieval.[15]
- "Electronic mail address" means a destination, commonly expressed as a string of characters, to which electronic mail may be sent or delivered.[16]
- "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any:
    - name, postal or electronic mail address, telephone number, social security number, date of birth, mother's maiden name, official state-issued or United States-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, Medicaid or food stamp account number, bank account number, credit or debit card number, or personal identification number or code assigned to the holder of a debit card by the issuer to permit authorized electronic use of such card;

[15] s. 668.602(7), F.S.
[16] s. 668.602(6), F.S.

    - unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
    - unique electronic identification number, address, or routing code;
    - medical records;
    - telecommunication identifying information or access device; or
    - other number or information that can be used to access a person's financial resources.[17]
- "Internet domain name" means a globally unique, hierarchical reference to an internet host or service, which is assigned through centralized Internet naming authorities and which is comprised of a series of character strings separated by periods, with the right-most string specifying the top of the hierarchy.[18]
- "Web page" means a location that has a single uniform resource locator (URL) with respect to the world wide web or another location that can be accessed on the internet.

Remedies

This bill gives standing to bring a civil action under this part to:

- a person engaged in the business of providing internet access to the public who was adversely affected by the violation;
- a financial institution as defined by s. 655.005(1)(h), F.S., adversely affected by the violation.
- an owner of a web page or trademark who was harmed by a violation under this bill; and
- the Attorney General.

A person bringing an action may seek injunctive relief to halt a violation under this bill, recover damages in the greater amount of the actual damages arising from the violation, or $5,000 for each violation of the same nature, or seek both injunctive relief and damages. Violations are considered of the same nature if they consisted of the same action or course of conduct regardless of how many times the act occurred. A court may increase damages to three times the actual damages sustained if violations constitute a pattern or practice. This bill also provides for an award of attorney's fees and costs to a prevailing plaintiff.

HB 45 CS provides that the violator submits personally to the jurisdiction of the courts of the State of Florida by committing a violation of this act. In addition, the bill establishes a 3-year statute of limitations to bring a suit under the act. This bill also provides that venue lies in any county in which the plaintiff resides or in which any part of the violation occurred. This bill does not preclude the award of damages otherwise available for the same conduct pursuant to federal or state law.

This bill requires that any moneys received by the Attorney General for attorney's fees and costs, or not utilized to reimburse persons harmed under this act, shall be deposited in the Legal Affairs Revolving Trust Fund. This bill grants the Department of Legal Affairs rulemaking authority to implement the provisions of this act.

Exemptions

This bill exempts from liability a telecommunication provider's or an Internet service provider's good faith transmission or intermediate temporary storing of identifying information. The bill also exempts providers of an interactive computer service when removing or disabling access to content that resides on an internet website or other online location controlled or operated by

[17] s. 817.568(1)(f), F.S.
[18] s. 668.602(10), F.S.

such provider if such provider believes in good faith that the content is used to engage in a violation of the provisions of this bill.

C. SECTION DIRECTORY:

Section 1: Requires any state, county, district, authority, or municipal officer, department, division, board, bureau, commission, or other separate unit of government created or established by law, and any other public or private agency, person, partnership, corporation, or business entity acting on behalf of any public agency, or legislative entity that operates a website and uses electronic mail to post the following statement in a conspicuous location on its website:

"*Under Florida law, e-mail addresses are public records. If you don not want your e-mail address released in response to a public-records request, do not send electronic mail to this entity. Instead, contact this office by phone or in writing."*

Section 2: Amends s. 668.606 (2), F.S., providing an exemption from criminal liability for certain carriers and equipment providers whose equipment transmits commercial electronic mail messages.

Section 3: Amends s. 668.6075, relating to unfair and deceptive trade practices and renumbers s. 668.6075 (2), F.S., as s. 668.610, F.S., relating to cumulative remedies.

Section 4: Creates s. 668.608, F.S., relating to criminal penalties.

Section 5: Creates ss. 668.701, 668.702, 668.703, 668.704, and 668.705., F.S., providing a title, definitions; prohibited acts; remedies and standing; and exemptions.

Section 6: Provides an effective date of July 1, 2006 and pertains to violations committed on or after that date.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT

A. FISCAL IMPACT ON STATE GOVERNMENT:

1. Revenues:

Indeterminate. HB 45 CS provides for fines and civil penalties that would accrue to the state as penalties for violations of the act. It is not known how many cases may be brought under the bill; thus, the revenue impact cannot be determined at this time.

2. Expenditures:

This bill creates an unranked third degree felony offense. The Criminal Justice Impact Conference met on February 28, 2006 and determined that this bill would have an insignificant impact on the prison bed population in the Department of Corrections. The Department of Legal Affairs has stated that the bill will have an indeterminate impact on the department's revenues and expenditures. See fiscal comments.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS:

1. Revenues:

Indeterminate. HB 45 CS provides for fines as a penalty for criminal violations. It is not known how many cases may be brought under the bill; thus, the revenue impact cannot be determined at this time.

2. Expenditures:

The bill could result in increased demand for jail beds. Data are unavailable to estimate the impact. Based on data regarding civil actions under current law, the likely impact is insignificant.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

None.

D. FISCAL COMMENTS:

The bill provides that the Attorney General may bring a civil action against a person that violates the Act, and would be able to collect the greater of the actual damages or $5,000, which is to be deposited into the Legal Affairs Revolving Trust Fund.

The bill grants the Attorney General authority to enforce violations under this bill. Therefore, the Attorney General will incur costs in order to prosecute persons that violate this bill. The costs, however, are indeterminate.

According to the Department of Legal Affairs, it prosecuted only two cases under the 2004 Electronic Mail Communications Act, which creates criminal penalties for sending unsolicited false or misleading commercial electronic mail messages to an electronic mail address that is held by a resident of Florida. A number of persons filed additional complaints; however the Department of Legal Affairs has not been able to determine who sent the messages, preventing further action under the statute.

III. COMMENTS

A. CONSTITUTIONAL ISSUES:

1. Applicability of Municipality/County Mandates Provision:

The bill appears to be exempt from the requirements of Article VII, Section 18 of the Florida Constitution because it is a criminal law. Other than the criminal provisions, the bill does not appear to require counties or municipalities to take an action requiring the expenditure of funds, reduce the authority that counties or municipalities have to raise revenue in the aggregate, nor reduce the percentage of state tax shared with counties or municipalities.

3. Other:

FALSE OR MISLEADING ELECTRONIC MAIL

HB 45 CS creates section 668.608, F.S., to provide criminal penalties for sending unsolicited false or misleading commercial mail messages from a computer located in Florida or to an electronic mail address that is held by a resident of Florida. Constitutional challenges could be made based on the dormant commerce clause or the first amendment.

Dormant Commerce Clause

The commerce clause empowers Congress to regulate commerce among the several states.[19] "This affirmative grant of authority to Congress also encompasses an implicit or dormant limitation on the authority of the states to enact legislation affecting interstate commerce."[20] The aspect of the

[19] *See* U.S. Const., art. I, § 8, cl. 3.

[20] Healy v. The Beer Insitiute, 491 U.S. 324 (1989).

commerce clause which operates as an implied limitation upon state and local government authority is often referred to as the dormant commerce clause.[21]

In Pike v. Bruce Church Inc.,[22] a two prong test was announced to determine if a state statute violates the dormant commerce clause:

> Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

The Supreme Court held that the critical consideration is the overall effect of the statute on both local and interstate activity with respect to both parts of the Pike test.[23] The Supreme Court has invalidated statutes under the Pike test on the grounds that their extraterritorial effect renders them unconstitutional.

> [T]he extraterritorial effects of state economic regulation stand at a minimum for the following proposition:
>
> > First, the "commerce clause . . . preludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State" . . . . Second, a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State. Third, the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other Sates and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the commerce clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another state.[24]

"The Healy Court explained that the extraterritoriality principles detailed above are not a separated or distinct commerce clause analysis. Rather, they are simply a more detailed way of explaining the two-part test established in Pike and clarified in Brown-Forman."[25]

Under the first prong of Pike , section 668.603, F.S., appears to apply evenhandedly to in-state and out-of-state transmitters of unsolicited false or misleading commercial electronic mail. "A *person* may not . . . transmi[t] . . . 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. . . ."[26] Thus, section 668.603 applies to residents of Florida as well as residents of other states.

Under the second prong of Pike, the local benefit of section 668.603 is balanced against the alleged burden on interstate commerce.

---

[21] MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); citing Bd. of Trs. of the Employees' Ret. Sys. of Baltimore City v. Mayor and City Council of Baltimore, 317 Md. 72 at 131 (1989).

[22] 397 U.S. 137 (1970).

[23] *See* Brown-Forman Distillers Corp. v. N.Y. State Liquor Authority, 476 U.S. 573 at 579 (1986).

[24] Healy at 336-37; *see also* MaryCle, at 15.

[25] Id.

[26] Section 668.603 (1), F.S.

Virtually identical statutes to section 668.608, F.S., pertaining to unsolicited false or misleading commercial electronic mail, have been examined by other courts under the dormant commerce clause and found to be constitutional.[27]

In Heckel, the court held that there was no sweeping extraterritorial effect that would outweigh the local benefits of the Act because the statute regulates only those emails directed to a Washington resident or sent from a computer located within Washington.[28]

In MaryCle, the court held that a Maryland statute was facially neutral because it applies to all email advertisers, regardless of their geographic location. It does not discriminate against out-of-state senders.[29]

In Ferguson, the court held that a California statute did not violate the commerce clause because the only burden on interstate commerce is that the email be truthful and non-deceptive email.[30]

Similarly, the local benefit of section 668.603 is to protect the public and legitimate business from deceptive and unsolicited commercial electronic mail[31], and the only burden imposed is sending truthful and non-deceptive email.

First Amendment

In Central Hudson Gas & Electric Corp. v. Public Service Comm. of New York,[32] the Supreme Court articulated a four part test for evaluating the constitutionality of a content-neutral regulation of commercial speech:

> First, the court must determine whether the speech is lawful and not misleading, otherwise it is outside the First Amendment's protection. If the speech is neither misleading or unlawful, then the court must ascertain whether the government has asserted a substantial interest. If the government has asserted a substantial interest, then a court must evaluate whether the regulation directly advances the asserted governmental interest and whether it is more extensive than necessary to serve that interest.[33]

Here, if the content of the electronic mail communication is unlawful or misleading, then under Central Hudson it is outside the protection of the first amendment. However, if the content of the electronic mail communication is not unlawful or misleading, then the state could assert its substantial interest is protecting the public from deceptive and unsolicited commercial electronic mail.[34] A court would then evaluate whether section 668.608, F.S., is the least restrictive means in advancing Florida's interest in protecting its citizens.

INTERNET PHISHING

This Act creates sections 668.701 – 668.705, F.S., to provide civil penalties for the acquisition of personal identifying information from a resident of this State with the intent to possess or use such information fraudulently. Under certain circumstances, it is possible that this bill could assert Florida's

---

[27] *See* State v. Heckel, 24 P.3d 404 (Wash 2001); MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); Ferguson v. Friendfinders, Inc., 94 Cal.App.4th 1255 (1st Dist. 2002).

[28] Heckel ,at 412-13.

[29] MaryCle, at 19.

[30] Feruson, at 1265.

[31] *See* section 668.601, F.S.

[32] 447 U.S. 557 (1980).

[33] White Buffalo Ventures, LLC. v. The University of Texas, 2004 WL 1854168 (W.D. Tex. 2004).

[34] *See* section 668.601, F.S.

police power over non-residents of Florida, and therefore this bill could possibly violate the Commerce Clause of the U.S. Constitution.

The Commerce Clause empowers Congress to regulate commerce among the several states.[35] "This affirmative grant of authority to Congress also encompasses an implicit or dormant limitation on the authority of the States to enact legislation affecting interstate commerce."[36] The aspect of the Commerce Clause, which operates as an implied limitation upon state and local government authority is often referred to as the dormant Commerce Clause.[37]

In Pike v. Bruce Church Inc.,[38] the court devised a two prong test to determine if a state statute violates the dormant Commerce Clause:

> Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. If a legitimate local purpose is found, then the question becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.

The Supreme Court explained that the critical consideration is the overall effect of the statute on both local and interstate activity with respect to both parts of the Pike test.[39] The Supreme Court has invalidated statutes under the Pike test on the grounds that their extraterritorial effect renders them unconstitutional.

For instance, in Healy, the court held:

> [T]he extraterritorial effects of state economic regulation stand at a minimum for the following proposition:
>
> First, the "commerce clause . . . preludes the application of a state statute to commerce that takes place wholly outside of the State's borders, whether or not the commerce has effects within the State" . . . . Second, a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State. Third, the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other Sates and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another state.[40]

In American Libraries Ass'n v. Pataki[41], the first case to apply the dormant Commerce Clause to a state law on Internet use[42], a federal trial court granted an injunction preventing the State of New York

---

35 *See* U.S. Const., art. I, § 8, cl. 3.
36 Healy v. The Beer Insitiute, 491 U.S. 324 (1989).
37 MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); citing Bd. of Trs. of the Employees' Ret. Sys. of Baltimore City v. Mayor and City Council of Baltimore, 317 Md. 72 at 131 (1989).
38 397 U.S. 137 (1970).
39 *See* Brown-Forman Distillers Corp. v. N.Y. State Liquor Authority, 476 U.S. 573 at 579 (1986).
40 Healy at 336-37; *see also* MaryCle, at 15.
41 Am. Libraries Ass'n, 969 F. Supp. 160 (S.D.N.Y. 1997).
42 *See* State v. Heckel, 24 P.3d 404 (Wash 2001).

from enforcing a statute that criminalized intentional communications via the internet for the purpose of engaging in harmful sexual conduct with a minor. The court held that the New York Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons:

> First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area, subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require.[43]

"Many courts have followed the logic of American Libraries Ass'n."[44]

Moreover, courts have examined "spam" statutes, which prohibit unsolicited false or misleading commercial electronic mail under the dormant Commerce Clause and found those statutes to be constitutional.[45]

In Heckel, the court held that there was no sweeping extraterritorial effect that would outweigh the local benefits of the Act because the statute regulates only those emails directed to a Washington resident or sent from a computer located within Washington.[46] The Act specifically prohibited 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.[47] The court distinguished the case from American Libraries Ass'n stating that the Washington Act did 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.[48]

In MaryCle, the court held that a Maryland statute was facially neutral because it applies to all email advertisers, regardless of their geographic location. It does not discriminate against out-of-state senders.[49]

In Ferguson, the court held that a California statute did not violate the commerce clause because the only burden on interstate commerce is that the email be truthful and non-deceptive email.[50]

Similarly, in Cashatt, a Florida court, using the Pike test, upheld a statute that criminalized the use of a computer on-line service or Internet service to seduce, lure or entice, a child to commit any illegal act.[51]

The Anti-Phishing Act, appears to apply evenhandedly to in-state and out-of-state transmitters. The local benefit of this Act is to protect the public and businesses from misleading and deceptive practices involving fraudulent use of personal information, a legitimate local public interest, and the

---

[43] Am. Libraries Ass'n, 969 F. Supp. at 169 (S.D.N.Y. 1997)
[44] *See* The Internet and the Dormant Commerce Clause, 110 The Yale Law Journal 787 (2001).
[45] *See* State v. Heckel, 24 P.3d 404 (Wash 2001); MaryCle, LLC. v. First Choice Internet, Inc., 2006 WL 173659 (Md. App. 2006); Ferguson v. Friendfinders, Inc., 94 Cal.App.4th 1255 (1st Dist. 2002).
[46] Heckel ,at 412-13.
[47] Id at 413.
[48] Id.
[49] MaryCle, at 19.
[50] Feruson, at 1265.
[51] *See* Cashatt v. State, 873 So.2d 430 (1st DCA 2004).

only burden imposed is not using the Internet for the purpose of obtaining another's personal information for a fraudulent purpose.

B. RULE-MAKING AUTHORITY:

None.

C. DRAFTING ISSUES OR OTHER COMMENTS:

None.

IV. AMENDMENTS/COMMITTEE SUBSTITUTE & COMBINED BILL CHANGES

On January 10, 2006, the Utilities & Telecommunications passed HB 45 with one amendment. The amendment provides that a customer premise equipment provider is immune from criminal penalties. Additionally, the amendment changed "telephone company" to "communications services provider" to ensure consistency.

On April 17, 2006, the Criminal Justice Appropriations Committee adopted a strike-all amendment to the bill and reported the bill favorably with committee substitute. The strike-all amendment adds a provision requiring all state and local agencies and legislative entities that operate a website and use electronic mail to post a public records disclaimer notification in a conspicuous location on its website. The amendment also creates the "Anti-Phishing Act," prohibiting the acquisition of personal identifying information from a Florida resident through the use of a website or e-mail with the intent to possess or use such information fraudulently.