F I S C A L I M P A C T R E P O R T

SPONSOR Culbert **ORIGINAL DATE** 2/25/2007 **LAST UPDATED** **HB** 1258

SHORT TITLE Anti-Spam Act **SB**

ANALYST Moser

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Non-Rec	Fund Affected
FY07	**FY08**		
	NFI		

(Parenthesis ( ) Indicate Expenditure Decreases)

Conflicts with: NMSA 57.12.23 and .24 (Unfair Practices Act)

Relates to and possibly conflicts with: Federal Title 47 Section 33(c)(1) of the US Code of Federal Regulations

Relates to and possibly conflicts with: "CAN-SPAM Act of 2003" (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003)

SOURCES OF INFORMATION
LFC Files

Responses Received From
NM Attorney General' Office(AGO)
Administrative Office of the Courts (AOC)
Corrections Department (CD)
Department of Environment (DOE)

SUMMARY

Synopsis of Bill

House Bill1258 requires all unsolicited email advertisements containing explicit sexual materials to be labeled as such, requiring the term "ADV-ADULT" to be included in the subject line.

More broadly, HB 1258 also prohibits the transmittal of unsolicited commercial email advertisements to any New Mexico email address or to be sent from New Mexico, except those email advertisements sent in the context of a current or pre-existing business relationship. For those commercial email advertisements sent within the context of a current or pre-existing

business relationship, the sender must provide recipients of such messages the opportunity to opt-out.

In addition, HB1258 prohibits the use of misleading or deceptive subject lines and false, forged or misleading headers in unsolicited commercial email advertisements. HB 1258 would also make it illegal to collect email addresses from the Internet if the purpose is to send unsolicited commercial email advertisements to those addresses.

HB 1258 would create a variety of new civil and criminal penalties. The Attorney General, email service providers or recipients of unsolicited commercial email advertisements may bring suit to enforce the provisions of the Anti-Spam Act.

SIGNIFICANT ISSUES

The AGO and the AOC point out that this Bill is in apparent conflict with at least in part federal law, specifically, the CAN-SPAM Act of 2003, 15 U.S.C. 7701, which went into effect on January 1, 2004. State laws that require labels on unsolicited commercial email or prohibit such messages entirely **are pre-empted** by the CAN-SPAM Act, except to the extent that those provisions which merely address falsity and deception would remain in place. Thus, HB 1258 is largely pre-empted by the CAN-SPAM Act.

Additionally, to the extent that those provisions of HB 1258 which address falsity and deception, appear to be in conflict with New Mexico's Unfair Practices Act, unless they are deemed to be more specific as to this SPAM subject matter and thereby not preempted.

- Section 57-12-23 of the Unfair Practices Act pertains to the transmission of unsolicited faxed and emailed advertisements.
- Section 57-12-24 provides private remedies for email service providers or recipients of unsolicited commercial email advertisements who have been harmed or to bring suit to enforce the provisions of the Act.

The Environment Department additionally points out that the federal government and 37 other states[1] have adopted anti-SPAM laws. Although this bill states that nothing in Section 7 of HB 1258 would limit or restrict the rights of an e-mail service provider under Section 330(c)(1) of Title 47 of the United States Code.

The AOC indicates that:

- it appears that the only criminal portions of the Act are for transmissions pertaining to sexually explicit materials when such transmissions are not labeled as such in the transmission subject line; violation of paragraphs 2 and 3 of subsection A (misrepresented domain name and/or misleading header (return address) information) when the volume of sent emails exceeds 10,000 attempts in 24 hours, one hundred thousand attempts in thirty days, or one million attempts in one year. It also criminalizes using minors to falsify transmission header information for the purpose of misleading

[1] Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Michigan, Minnesota, Missouri, Nevada, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, S. Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming.

recipients and avoiding prosecution. Specific criminal penalties are only listed for violations of the "sexually explicit" provisions when the return address is falsified.

- The Act requires that those sending unsolicited emails of a commercial nature provide an "opt-out" mechanism. According to Symantec, the largest manufacturer of anti-virus/anti-spam software, most opt-out links in commercial emails or on Websites do nothing except create an expectation on the part of the email recipient that his or her email address will be removed from the list, even though in most instances it will not be removed from a list but will be retained and perhaps even resold to other spammers.
- Opt-out features are also used in unsolicited emails to allow the entity sending the email to confirm that they have actually hit a live person, which means that the amount of spam going to that person will increase if they "opt-out." Many, perhaps most, spammers send far more unsolicited email than they expect will actually reach a live person, thus a person who exercises the option only confirms the validity of their email address.
- The Act could actually require that the opt-out lead to the outcome of having the email address permanently removed from the particular list used to generate the unsolicited email and also dropped from any other list maintained by the entity that originally sent the email. It could also levy fines and other penalties against those who fail to actually remove recipients from lists when they opt-out.
- The Act applies both to entities whose spam originates in New Mexico and to entities who send spam to those in New Mexico. Estimates are that the vast majority of spam is from off-shore sources and that the small amount of spam that originates in the U.S. is so effectively masked that it is impossible to determine origin. Moreover, many spammers use address information harvested from completely uninvolved individuals as return addresses on their spam. As such, it is likely that any spam that appears to be from a New Mexico source did not actually originate in New Mexico. The Act could have the unintended consequence of leading to prosecution of perfectly innocent New Mexicans whose information was hijacked by spammers and then used for spam return addressing/email header purposes.
- In most instances there are no way that the sender of unsolicited, commercial email can distinguish between New Mexico and non-New Mexico email addresses. Most email providers don't provide email addresses that are state-specific, except for government email providers who provide email domains such as "state.nm.us" or "nmcourts.gov." This means that any spammer trying to work within appropriate legal constraints will find it impossible to obey provisions of the Act related to a "New Mexico email address."
- The area of spam interdiction and prosecution is extremely technical and very few people are truly expert in this complex area. All federal attempts to constrain spam and criminalize spammers have been completely ineffective due to inability to enforce. A consultant that is thoroughly experienced in this area could be of enormous benefit in constructing legislation, but regardless of the quality of the law, it is unlikely that spam will be lessened as a result of a state law. This is because spam is an international problem. Any state that succeeds in controlling spammers (which is extremely unlikely) will find that the spammers simply move their operations beyond that state's jurisdiction. Most spam now violates a combination of various state and federal laws, yet the increase in the amounts of total spam, just over the past year, has been astonishing.
- It appears that the only criminal portions of the Act are for transmissions pertaining to sexually explicit materials when such transmissions are not labeled as such in the transmission subject line; violation of paragraphs 2 and 3 of subsection A

(misrepresented domain name and/or misleading header (return address) information) when the volume of sent emails exceeds 10,000 attempts in 24 hours, one hundred thousand attempts in thirty days, or one million attempts in one year. It also criminalizes using minors to falsify transmission header information for the purpose of misleading recipients and avoiding prosecution. Specific criminal penalties are only listed for violations of the "sexually explicit" provisions when the return address is falsified.

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

Conflicts with NMSA 1978, Sections 57.12.23 and .24 (Unfair Practices Act)

Relates to and possibly conflicts with Federal Title 47 Section 33(c)(1) of the US Code of Federal Regulations, which regulates interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet.

ALTERNATIVES

Criminal penalties should be associated with all criminalized sections of the Act, and it would improve readability if all criminal provisions and penalties were carefully listed in one section of the Act to avoid confusion with civil remedies specified in the Act.

GM/nt