



Sex in Spam: A Content Analysis

Szde Yu¹

Wichita State University, United States of America

Abstract

As previous research has indicated sex is the most prevalent theme in spam emails, the purpose of the current study is to explore how sex is presented and/or promoted in email spam. A content analysis was conducted on 2,291 spam emails featuring sexual content. The design of the message was analyzed. Moreover, as regulated by the CAN-SPAM Act of the United States, the illegality of these emails was also examined. The results indicate sex in spam is generally presented in a textual fashion rather than a graphic one. For the most part, the message is very direct and explicit. Unlike traditional advertisement, the message's readability is not the primary concern due to some technical maneuvers unique to email advertising. Although spammers have little intention to abide by the legal regulations, when they use spam to promote their sexual products there seems to be a line they are reluctant to cross.

Keywords: Email, Spam, CAN-SPAM Act, Sex.

Introduction

Email is one of the most pervasive forms of computer-mediated communication (Heisler & Crabill, 2006). It allows for instant and free communication between people at long distance. However, because email features convenience and low cost, it has been utilized as a cheap alternative to traditional advertising (Maggs, 2006). Sending unsolicited commercial emails in bulk is referred to as email spam. Spam has grown into such a serious problem that every email service provider has endeavored to stop spam emails from reaching the user's inbox before the inbox is inundated by junk emails on a daily basis (Weinstein, 2003; Gmail, 2010). Some attempts are more successful than the others. Hence, from time to time email users will still receive some commercial emails that they did not ask for, and spammers never stop trying even though most users probably simply delete those emails (Yeargain et al., 2004; Symantec, 2010; Wall, 2004).

In fact, email spam is more than just a nuisance awaiting deletion. It can be a criminal offense. In December 2003, the CAN-SPAM Act was enacted in the United States and took effect in January 2004 (Lee, 2005). Although this jurisdiction of this Act is limited to the United States, through international collaboration, such as Council of Europe's Convention on Cybercrime (Council of Europe, 2001), the Act might still be applicable to spammers of foreign nationalities in the future. The Federal Trade Commission (FTC)

¹Assistant Professor of Criminal Justice, School of Community Affairs, Wichita State University, 1845 Fairmount Box 135, Wichita KS 67260, USA. Email: szdeyu@gmail.com

was authorized to enforce provisions provided in the CAN-SPAM Act, and unsolicited commercial emails that fail to comply with its regulations would be declared criminal. The punishment could be a fine up to \$16,000 for each separate email in violation of the CAN-SPAM Act (FTC, 2009), or it could be imprisonment (Yeargain et al., 2004). In 2008, the so-called “Spam King” Robert Soloway was convicted under the CAN-SPAM Act for sending fraudulent emails along with two other charges and was sentenced to 47 months in federal prison (Rabinovitch, 2007). The Act also allows states and Internet service providers to file civil lawsuits against spammers (Ford, 2005; Yeargain et al., 2004).

The rationale of the CAN-SPAM Act can be seen as based on the expected utility theory in economics, which posits spammers would only choose to send spam when the expected gains exceed the expected cost (Lee, 2005). Since the Act was aimed to increase cost to spammers, it was expected spammers would be discouraged. However, this did not seem to be the result. According to Symantec’s monthly spam reports, the amount of spam is actually increasing (Symantec, 2010). More than 90% of emails sent in the world now are possibly spam (Symantec, 2010).

The CAN-SPAM Act of the United States defines spam as unsolicited commercial electronic mail that includes any commercial emails addressed to a recipient with whom the sender has no existing business or personal relationship and not sent with the consent of the recipient, and commercial electronic mail is defined as any electronic mail message the primary purpose of which is commercial advertisement or promotion of products or service (Rogers, 2006). Emails would be deemed as spam when they were sent in bulk without the recipient’s consent and the primary purpose must be commercial in nature (Rogers, 2006).

Commercial emails actually could be considered legitimate unless they violate certain provisions, including 1. using authentic header information; 2. no deceptive subject lines; 3. identifying the message as an advertisement; 4. providing real physical location of the business; 5. offering an opt-out choice; 6. honoring opt-out requests within 10 business days (FTC, 2009). It is punishable if the emails were knowingly sent through a third party without authorization, or if the emails were sent randomly to an email list that was obtained illegally (e.g. stealing from other online proprietary service or automated collection from websites) (Spammer X, 2004; Yeargain et al., 2004; Ford, 2005). The sender cannot sell or lease the opt-out email addresses and should specify in the subject line any sexually explicit content (Yeargain et al., 2004). As sexually explicit content is rampant on the Internet, email spam is no exception.

Research has found that among spam emails, sex is a predominant theme and some people indeed respond to these spam emails instead of just deleting them (Yu, 2011; Ting, 2004). Research has found that teenagers, especially males, tend to actively seek sexual content in the media, including the Internet (Bleakley, Hennessy, & Fishbein, 2011), and people tend to remember sexual advertisement contents better than nonsexual ones (Furnham & Mainaud, 2011). Although no literature has looked into sex hiding in email spam, it is reasonable to assume people would be more likely to pay attention to the sexual content in email the same way they do in other forms of media. As an exploratory effort, the present study was intended to examine these sexually explicit spam emails and shed light on how sex is presented and promoted in email spam.

Adopting the framework of previous research (Yu, 2011; Kigerl, 2009), selected spam emails were examined with regard to purpose, design, and legal compliance (i.e., The CAN-SPAM Act regulations).

Methods

Sampling

In the present study, 2,291 spam emails collected between July 2009 and April 2012 were analyzed. The spam emails were intentionally collected by disseminating a number of email addresses on the Internet, such as registering for online forums or posting on open discussion boards. Doing so increases the chance for spammers to collect such addresses. To be comparable, only the emails that have sex-related content were chosen in the present study.

Analysis

The analysis involves the extraction, analysis and presentation of digital evidence obtained from electronic mails. Each spam email in the sample was analyzed in terms of content and format. Moreover, the illegality of these emails was tested based on the following criteria as regulated by the CAN-SPAM Act.

1. Opt-out choice: The recipient should be provided an option to opt out so that they will not receive any emails from the sender again. This was verified by examining the body of the email message. Moreover, if an option is provided, an attempt was made to actually opt out so as to see what the response is.
2. Non-deceptive subject: The subject needs to clearly indicate its advertising nature and sexually explicit content needs to be marked as such. This was verified by inspecting the subject line of each email.
3. Honest header: The sender's information should not be deceiving and the recipient should be consistent with what is shown in the header. To verify this, the header information was examined and the sender's email address underwent a DNS validation. A DNS validation determines whether the sender's email address is a real one, but it does not guarantee it is the email address used by the sender. Hence, the sender's IP address was traced to compare the IP's domain name and the email address' domain name.
4. Physical address: The Act requires a valid physical address of the business to be included in the email. This was verified by examining the body of the message.
5. SPF: Sender Policy Framework validation was used to verify the email was sent from a real host responsible for sending messages for the particular domain. This is automatically done by the email service provider when receiving the message. The email header typically reveals the result of SPF validation in the header information. If it shows pass, it means the sender did not use a third party server to send emails.

Results

Purpose

According to the content analysis, when spam emails feature sex there are generally three main purposes. First, they are aimed to sell drugs that allegedly can enhance a person's sexual performance or increase sexual gratification. Of the 2,291 spam emails in the sample, 1,373 of them were aimed to sell drugs related to sexual performance (e.g. Viagra). These drugs usually target males but occasionally they might be targeting females in terms of their respective reproductive functions. Figure 1 and Figure 2 show examples of this type of spam email.

Figure 1. Spam example 1

From: **Testosterone Booster** <offer@goxd211ofiling.com>
Date: Wed, Aug 29, 2012 at 10:30 AM
Subject: Increase your sex drive, boost your energy, fight fatigue.
To:
ATTENTION MEN: Save 60% NOW on GNC's New Clinically Proven Testosterone Booster!

[Click Here](#)



Figure 2. Spam example 2

Get.Vigara
Now 6345B8C26@progressivefinancial.com
to me.

Hi XXXX, discount prices:

[Cilais](#) - 1.62\$

[Levtira](#) - 1.86\$

[Vigara](#) - 0.68\$

[Femela Vigara](#) - 1.13\$

Professional Pack - 3.55\$

[Famyli Pakc](#) - 2.18\$

<http://fkVC.ivesdoctor.ru/>

Personal discount coupon: [DSC-8B3FDE]

Second, some spam emails are aimed to promote either an adult website or the sales of pornographic videos. In the present study, 848 emails were found to serve this purpose. Figure 3 shows an example of this type of spam email. Third, in the present study, 70 spam emails were identified as solicitation, meaning these emails appear to solicit a personal response from the recipient, rather than simply commercial advertising. This type of spam emails is usually much more implicit about the intent. Unlike those selling drugs or promoting pornography, solicitous emails rarely use provocative phrases to disclose the sex component in the message. Sex is usually hidden in the connotation by emphasizing gender, age, and the desire to establish a relationship. Such messages could be a precursor of an online scam or another way of promoting erotic services. Figure 4 shows an example.

Figure 3. Spam Example 3



to [ingenuity_black](#)

Is a **man you can not miss**.

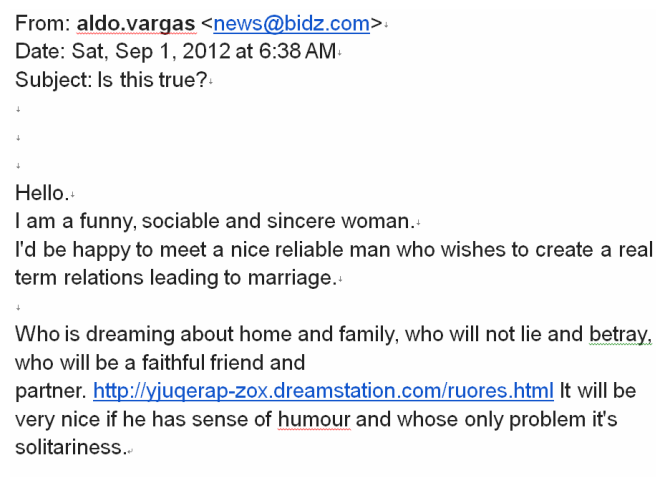
Classic Japanese film! Vast amount! 2012 Summer
Popular file.
And.

**With the point to see the discs to not
have to wait.**

You want to when it all lines.
Still journeying disc era has passed.
[Speed adult online cinema](#) / under the
age of 18 do not enter /.

This week the new [Kitahara](#)
[multi-vanilla](#), [Yoshizaki](#) [straight thread](#) [Hazuki](#)
[Chennai spike](#) ... support teams [Jiangdang](#) [Thecus](#)
new film.

Figure 4. Spam Example 4



From: [aldo.vargas](#) <news@bidz.com>

Date: Sat, Sep 1, 2012 at 6:38 AM

Subject: Is this true?

↓

↓

↓

Hello.

I am a funny, sociable and sincere woman.

I'd be happy to meet a nice reliable man who wishes to create a real term relations leading to marriage.

↓

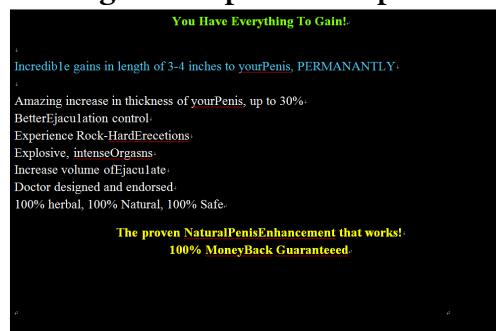
Who is dreaming about home and family, who will not lie and [betray](#), who will be a faithful friend and partner. <http://yjuqerap-zox.dreamstation.com/ruores.html> It will be very nice if he has sense of [humour](#) and whose only problem it's solitariness.

↓

Design

The incorporation of HTML allows the email to contain more than just plain text. Most email service providers or email programs have enabled HTML designs by default, so many people can utilize it even without knowing what HTML is. In this analysis, spammers for the most part used HTML to add visual appeal. Spam emails need a response from the recipient to accomplish their purpose, be it selling drugs, promoting pornography, or soliciting personal contact. To this end, spammers have to find a way to catch attention. In Figure 1, a well-designed image can be seen being used to convey the message. Even without an image, colorful text is often used supposedly in an attempt to attract attention. Figure 5 shows an illustration.

Figure 5. Spam Example 5



Another tactic to attract attention from potential consumers is to use a tempting subject for the email. For instance, in Figure 1, the subject is rather explicit. In contrast, in Figure 4, the subject is ambiguous but intended to be intriguing. Although the design of spam emails varies, but there is almost always a link provided in the message. After attracting the recipient to read the message, spammers need to further lead the reader to click on the link. Spammers seem to take different approaches in this regard. When an image like Figure 1 is used, usually a hyperlink is embedded in the photo so that when clicking anywhere on the photo the reader would be redirected to the website that sells the products. Without an image, typically an address would be specified in the content. Some are somewhat elaborate on what they sell as illustrated in Figure 2, while others might be more casual as shown in Figure 6.

Figure 6. Spam Example 6

```
Message 1:-
.
Subject: website"WorldPharmacy".
Sender: Nola@dfgbifedji.abvgdejka.com.

http://fvaxitumen.mindnmagick.com/hilymig.html

Hate not at the first harm.

=====

Message 2:-

Subject: RE:SiteWorldPharmacy.
Sender: Eloy@cbhaahggbj.pilluliradosti.com.
website, which you asked:http://xesuveryj.o-f.com/amixine.html.
A clean hand wants no washing.
.
```

Examining the content of these emails revealed that with a few exceptions, most of these messages are not well-organized in terms of layout and writing, despite the use of HTML. It is almost as if spammers did not deem it worthy to spend much time creating persuasive sales pitch, or they simply believed their products sell themselves without the need for extra polish. It is noteworthy that most spam emails are fraught with typos and misspellings. Aside from the fact that spammers might not be the most educated people, most of these mistakes are actually by design (Spammer X, 2004; Yu, 2011). Spammers have been known for trying to deceive spam filters. Spam filters, if effective, would prevent spam emails from reaching the recipient's inbox and hence probably never being read. Intentionally misspelling some sensitive words, such as "Viagra" or "penis" could potentially defeat machine-based filters. They also sometimes insert random textual strings or numbers to make each message look unique (SpammerX, 2004; Goodman et al., 2007; Yu, 2011). This way they could trick the spam filter to believe this email is not sent in bulk. For example, in Figure 6, there are two messages that contain slightly different subjects, different senders, and seemingly different content, but the hyperlinks embedded in both messages were actually linked to the same website. By doing so, the readability of the message is inevitably impaired, but to spammers the recipient cannot read anything if the message never passes spam filters. All in all, the design of spam emails is rarely elegant, unlike traditional advertising. Spammers have to be concerned about bypassing spam filters before employing effective marketing strategies to make the message personal, relevant, artistically appealing, rewarding, interesting, or helpful (Phelps et al., 2004; Jenkins, 2009).

When the design of the advertisement is not overtly attractive, the only thing left to appeal to the customers is the underlying component of the message, sex.

CAN-SPAM Violations

Whether the email serves the advertising purpose is one thing, but whether it violates the law is a different issue. In the present study, all 2,291 spam emails violated the regulations in the CAN-SPAM Act. The most violated regulation was of not providing a physical address. In the sample of the present study, only two spam emails provided an address, which is probably bogus. In light of another regulation, only 23 emails provided an opt-out option. Only 5 of them resulted in a response that informs the recipients they have been removed from the mail list. Whether the recipient is really removed is uncertain, however.

The header information in most spam emails showed signs of alteration. Only 233 spam emails did not appear to have misleading header information. This means the sender's email address and IP address can be verified, and the recipient's information is not disguised. As shown in Figure 1 and Figure 6, most spammers use a forged sender address which does not really exist, and most spammers do not disclose who is actually receiving the message. In contrast to the dishonest header information, SPF validation was mostly passed although 901 of them did not pass. This means most spammers are comfortable enough to use their own Internet domains and machines to disseminate spam emails without hiding behind a third party. Although 602 emails were sent from an IP address overseas, most spam emails originated in the USA. The significance of this finding is it showed that although it is not necessarily easy, it is not impossible to trace the spammer's physical location. If they had used a fake IP address in the email, they would not have passed the SPF test. However, it should be noted that what can be traced is the machine, not necessarily the person.

There is one more CAN-SPAM regulation examined in this study, that is, commercial emails are required to use a non-deceptive subject. None of these spam emails in this study indicated themselves as advertisement on the subject. However, most of them were fairly explicit in their intent so it is not difficult to infer. The exception was those emails purported for solicitation as discussed earlier. Mostly the subject line was informative enough to let the recipient know what is being promoted such as the example in Figure 1. In a sense, they are not deceptive but they simply have no desire to abide by the Act by providing warning against sexually explicit content, because for the most part the subject is already sexually explicit.

In a nutshell, this analysis revealed that spammers show little, if any, intention to follow the CAN-SPAM Act. This is especially ironic considering how the Act was criticized for providing guidance for spammers to send more spam emails legally. The reality is spammers are sending more spam emails, but they do not need the guidance as they have no interest in following it.

Discussion

Although the sample of the study by no means is representative of all spam emails in the cyberspace, it is rather evident that the law does not have much impact on how spammers operate in spite of the fairly harsh penalties. In this study of the 2,291 emails, none met the legal requirements. Perhaps it is because what they are selling is already deviant and therefore it bears little meaning to obey the law when advertising it.

However, in the present analysis there was one somewhat surprising finding. None of those sexually explicit emails contained obscene images. This is especially counterintuitive considering the purpose of those emails was to promote sex. Even when they were promoting pornography, spammers never used any pornographic photos in their spam emails. Recipients usually had to click on a link to see pornography on the promoted website. It seemed there is a line spammers are reluctant to cross. Perhaps it is a concern about law enforcement. Sending pornography via email to unsolicited recipients could violate some federal laws, especially when it is suspected to be child pornography. However, spammers show no interest in complying with the CAN-SPAM Act, so it seems they are aware of the police priority. In other words, without obscene photos, a spam email albeit illegal is just an annoying advertisement that calls for merely deletion, while with obscene photos inserted the spam email itself becomes pornography and thus more likely attracts attention from the authorities. Conceivably there are people who send pornography in the email, but according to this analysis it does not seem to be the typical strategy most spammers adopted.

Without pornographic photos, promoting sex in spam emails relies on a quick message that clearly conveys or unobtusly implies the sex component. As discussed, the message is rarely elegant or elaborate. Although the message is not necessarily vulgar, the lack of censorship on email allows it to be direct and explicit. Keywords like “enlargement” or “ejaculation” are very commonly used. Hence, sex in email spam is fearless as it generally reveals its intent obviously and it is so primitive that it does not require well-phrased sales pitch or embellishment.

Unfortunately, very little if any literature exists to examine sex in email spam. Consequently, it limits the inference that can be drawn from the findings. Although this type of spam emails could be tempting to many recipients because sex has always been appealing in its own right (Fogel & Shlviko, 2009; Fogel & Shlviki, 2010; Bleakley et al.,

2011), it is not known how prevalent it is for people to actually respond to this type of spam emails or what kind of people is more likely to be attracted to this type of spam emails. It remains unknown what action people take after they respond to these spam emails. Are they merely curious or are they seriously pursuing what is offered? The further action that the recipient might take after reading these emails calls for concern for there are potential ramifications. Any responses from the recipient may incite the production of more counterfeit drugs and deviant pornography (e.g. child pornography or bestiality) (US FDA, 2012). Some spam emails as shown in this analysis are aimed to solicit personal information and it could result in financial or personal harm (e.g. identity theft). Moreover, sex in spam can easily reach teenagers and younger children. As described, sex is usually explicit in spam emails. When youngsters who are most curious about sex are prematurely exposed to this kind of messages, the negative effect is not hard to imagine. Early exposure to sexual content could lead to unhealthy sexual socialization (Brown & L'Engle, 2009; Stulhofer, Busko, & Landripet, 2010) and even sexual addiction (ElHage, 2004). Many parents are only concerned about the adult websites and overlook sex in spam. Email spam brings sex to children without them searching for it. Further, there is some information conveyed via email spam that may not be easily found on the Internet even if you search for it. For instance, some drugs that allegedly can improve sexual performance are not available on any websites, but would be sold on spam emails. Some illegal pornography is unlikely to be openly promoted on the Internet but could be introduced via email spam (Lueg, 2003; Yu, 2011).

Conclusion

In sum, the main findings are as follows. First, in email spam, sex is generally promoted with explicit languages rather than explicit images even though it is not difficult to insert images in emails. Second, due to the concern about spam filters, the design of the spam email is more aimed to defeat the filter so as to successfully deliver the message rather than aimed to promote the product. This tradeoff is one aspect traditional advertising does not need to worry about. Third, the sexual component becomes more implicit when the purpose of the email is to solicit personal connections. Otherwise, sex is usually clearly indicated in email spam. Fourth, although email spam can be used to promote legitimate businesses, for the most part it implicates criminality, either in the products being promoted or in the methods used to send these advertisements. To say the least almost all spam emails violate the CAN-SAPM Act. Fifth, to some extent these spammers are not entirely untraceable. The machines sending spam emails can be traced as discussed. Moreover, the sexual products they are selling generally require subsequent transactions, such as mailing the drugs or meeting for sexual service. Their businesses cannot completely hide on the Internet and this makes them vulnerable from a law enforcement point of view.

Although sex in email spam is still sex but the avenue through which it is being conveyed is worth exploring. Email spam is already a deviant act. Therefore hiding deviant sex in a deviant act makes a sensible solution. Although in the present study the focus is on the illegality of the emails rather than the illegality of the sexual products being promoted, it is not too arbitrary to assume most of the sexual products are not perfectly legal, such as prescription drugs and some deviant pornographic websites or services. The policy implication is obvious. Should law enforcement pay more attention to email spam when criminals practically provide information to you voluntarily? Additionally, this

analysis suggested the design of spam email does not follow traditional standards of advertising. Does this reduce (or somehow enhance) the appeal of its sexual content? To what extent is it affected? Future research should address these issues so as to fully understand the impact of sex in spam.

References

- Bleakley, A., Hennessy, M., & Fishbein, M. (2011). A model of adolescents' seeking of sexual content in their media choices. *Journal of Sex Research*, 48(4), 309-315.
- Brown, J. D., & L'Engle, K. L. (2009). X-rated: Sexual attitudes and behaviors associated with U.S. early adolescents' exposure to sexually explicit media. *Communication Research*, 36, 129.
- Council of Europe. (2001). Convention on Cybercrime. Retrieved April 18, 2014 from <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>
- ElHage, A.M. (2004). Sexual degradation: How pornography destroys the family. Retrieved September 23, 2013 from <https://ncfpc.org/PolicyPapers/Findings%200407-SexualDegrad.pdf>
- Federal Trade Commission. (2009). The Can-SPAM Act: A Compliance Guide for Business. Retrieved September 7, 2012 from <http://www.ftc.gov/bcp/edu/pubs/business/e-commerce/bus61.shtm>
- Fogel, J., & Shlivko, S. (2009). Consumers with sexual performance problems and spam e-mail for sexual performance products. *Journal of Internet Banking and Commerce*, 14(1). Retrieved Oct 18, 2012 from <http://www.arraydev.com/commerce/jibc/2009-04/Fogel.doc.pdf>
- Fogel, J. & Shlivko, S. (2010). Consumers with sexual performance problems and spam email for pornography. *Journal of Internet Banking and Commerce*, 15(1). Retrieved Oct 18, 2010 from <http://www.arraydev.com/commerce/jibc/201004/Fogel%20pornography%20sexual%20health.pdf>
- Ford, R.A. (2005). Preemption of state spam laws by the federal CAN-SPAM Act. *The University of Chicago Review*, 72(1), 355-384.
- Furnham, A. & Mainaud, L. (2011). The effect of French television sexual program content on the recall of sexual and nonsexual advertisements. *Journal of Sex Research*, 48(6), 590-598.
- Gmail. (2010). Gmail uses Google's innovative technology to keep spam out of your inbox. Retrieved September 22, 2010 from <http://www.google.com/mail/help/fightspam/spamexplained.html>
- Goodman, J., Cormack, G. V., & Heckerman, D. (2007). Spam and the ongoing battle for the inbox. *Communications of the ACM*, 50(2), 25-33.
- Heisler, J., & Crabill, S. (2006). Who are "stinkybug" and "packerfan4"? Email pseudonyms and participants' perceptions of demography, productivity, and personality. *Journal of Computer-Mediated Communication*, 12(1).
- Jenkins, S. (2009). *The truth about email marketing*. Upper Saddle River, NJ: Pearson Education.
- Kigerl, A. C. (2009). CAN SPAM Act: An empirical analysis. *International Journal of Cyber Criminology*, 3(2), 566-589.
- Lee, Y. (2005). The CAN-SPAM Act: A silver bullet solution? *Communications of the ACM*, 48(6), 131-132.

- Lueg, C. (2003). Spam and anti-spam measures: A look at potential impacts. Retrieved Aug 18, 2012 from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.4.6385&rep=rep1&type=pdf>
- Maggs, P.B. (2006). Abusive advertising on the Internet (SPAM) under United States law. *The American Journal of Comparative Law*, 54, 385-394.
- Phelps, J. E., Lewis R., Mobilio, L., Perry, D., & Raman, N. (2004). Viral marketing or electronic word-of-mouth advertising: Examining consumer responses and motivations to pass along email. *Journal of Advertising Research*, 44(4), 333-348.
- Rabinovitch, E. (2007). Staying protected from “social engineering”. *Communications Magazine, IEEE*, 45(9), 20-21.
- Rogers, K.M. (2006). Viagra, viruses and virgins: A pan-Atlantic comparative analysis on the vanquishing of spam. *Computer Law & Security Report*, 22, 228-240.
- Spammer X. (2004). *Inside the SPAM cartel: Trade secrets from the dark side*. Rockland, MA: Syngress Publishing.
- Stulhofer, A., Busko, V., & Landripet, I. (2010). Pornography, sexual socialization, and satisfaction among young men. *Archives of Sexual Behavior*, 39, 168-178.
- Symantec. (2010). Global spam categories. State of Spam & Phishing: A Monthly Report. Retrieved on Oct 6, 2010 from http://www.symantec.com/content/en/us/enterprise/other_resources/b_state_of_spam_and_phishing_report_09-2010.en-us.pdf
- Ting, A.S.H. (2004). Penis enlargement, cheap Viagra, and noni juice: Evaluating and winning the war against health product spam. Retrieved Oct 18, 2012 from <http://leda.law.harvard.edu/leda/data/665/Ting.html>
- US Food and Drug Administration. (2012). Buying medicines over the Internet. Retrieved Feb 4, 2013 from <http://www.fda.gov/Drugs/ResourcesForYou/Consumers/BuyingUsingMedicSafely/BuyingMedicinesOvertheInternet/default.htm>
- Wall, D. S. (2004). Digital realism and the governance of spam at cybercrime. *European Journal on Criminal Policy and Research*, 10, 309-335.
- Weinstein, L. (2003). Spam wars. *Communications of the ACM*, 46(8), 136.
- Yeargain, J.W., Settoon, R.P., & McKay, S.E. (2004). Can-Spam Act of 2003: How to spam legally. *Journal of Strategic E-Commerce*, 2(1), 15-30.
- Yu, S. (2011). Email spam and the CAN-SPAM Act: A forensic analysis. *International Journal of Cyber Criminology*, 5(1), 715-735.