Copyright © 2009 International Journal of Cyber Criminology (IJCC) ISSN: 0974 – 2891
July - December 2009, Vol 3 (2): 566–589

CAN SPAM Act: An Empirical analysis

Alex Conrad Kigerl[1]
Portland State University, USA

Abstract

In January 2004, the United States Congress passed and put into effect the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN SPAM). The Act was set forth to regulate bulk commercial email (spam) and set the limits for what was acceptable. Various sources have since investigated and speculated on the efficacy of the CAN SPAM Act, few of which report a desirable outcome for users of electronic mail. Despite the apparent consensus of anti-spam firms and the community of email users that the Act was less than effective, there is little to no research on the efficacy of the Act that utilizes any significant statistical rigor or accepted scientific practices. The present study seeks to determine what, if any, impact the CAN SPAM Act had on spam messages and to identify areas of improvement to help fight spam that is both fraudulent and dangerous. The data consisted of 2,071,965 spam emails sent between February 1, 1998 and December 31, 2008. The data were aggregated by month and an interrupted time series design was chosen to assess the impact the CAN SPAM Act had on spam. Analyses revealed that the CAN SPAM Act had no observable impact on the amount of spam sent. The Act was found to have no effect on spammer compliance with two out of three spam laws in the CAN SPAM Act. The one law out of the three where there was a noticeable effect resulted in a decrease in compliance following the Act's passing. Lastly, the Act had no impact on the number of spam emails with IP addresses assumed to be within the United States. Implications of these findings and suggestions for policy are discussed.

Keywords: CAN SPAM Act, Spam, IP Address, Cyber Crime.

Introduction

The advancement of computing today has allowed human beings to automate many tasks that together make life easier. As technology continues to improve, more and more of our everyday activities are similarly improved, with better speed, ease, and functionality. Yet technology is a tool, the functionality of which can be given many different meanings. Technology together with information in this age is power, and power can be used for both good and ill.

With new ways to exploit technology, the law has always been there to reign in the means by which criminals take advantage of changing tools. The law, like technology, is not static. But in this age science and technology have known an exponential improvement of accelerating returns, where newer inventions emerge faster than they did before. The legal system does not seem to have matched this speed.

[1] Department of Criminology and Criminal Justice, Portland State University, 725 Southwest Harrison Street, Portland, Oregon 97201, USA Email: kigerl.alex@gmail.com

In the information age, knowledge is power. So too is the fraudulent representation of knowledge similarly powerful. Computers have given fraud new meaning, and new avenues to locate victims in the millions. The abuse of information to mislead is likely as old as language itself.

The information technology highly suited to abuse by fraud is email, or spam, as email is the most efficient way to send literally billions of messages at the press of a button, without so much as a dime being spent to produce so many transmissions. And the high degree of anonymity of the sender of such messages makes getting away with perpetrating fraud by such means all the easier. The most common purpose of malware today is to send spam from millions of infected computers controlled by the cyber criminal (Schiller, Binkley, Harley, Evron, Bradley, & Willems, 2007).

Spam is the sending of unsolicited electronic mail messages to multiple recipients, usually for commercial purposes. The sending of spam started small since its emergence in the 1990's (Kleiner, 2008), but like any technology, it has since grown. Spam is a multibillion dollar industry today (Kleiner, 2008) and is responsible for slowed internet traffic, wasted time and costly effort separating junk email from legitimate email, malware infections and spyware proliferation, stolen credit card and online account credentials, stolen identities, fraudulently sold commercial products and duped victims who are tricked into committing crimes for the cyber criminal (Smith, Holmes, & Kaufmann, 1999).

According to a Microsoft security report in 2009, spam makes up 97% of all emails sent over the internet (Waters, 2009). In 2003, only 45% of email was spam (McCain, 2003), but has risen as professional spammers grow in skill and reach further and further to make more money. An average of 120 billion spam messages are sent every day (Kleiner, 2008).

The foremost purpose of spam messages are to make money for the spammer (Schiller et al., 2007), and the primary means to do this is through fraudulent offers and deals. Among the most costly fraud includes phishing and advance fee scams. Phishing is the sending of email messages that masquerade as a source the user trusts, such as their online bank or EBay account (Brody, Mulig, & Kimball, 2007). The purpose of this tactic is to trick the target into revealing sensitive personal credential information, such as account logins, passwords, credit card numbers, or any piece of information that can be converted into stolen cash. This specific type of identity theft costs the United States 52.6 billion dollars a year (Brody et al., 2007).

When spammers don't have the technical ability to spoof a victim's familiar website, such as their Bank account, they can always resort to relying exclusively on persuasion. Advance fee fraud does just this, where the spammer sends email solicitations pretending to be a potential business partner or foreign character with an opportune offering. A fanciful story is described in which the victim stands to make millions of dollars, by laundering money, collecting lottery earnings, or making a business deal. The catch is that the victim must pay an advance sum of money before they can collect their reward. Of course, the reward never arrives and the victim is left empty handed (Smith et al., 1999).

Such frauds are dangerous only because they reach so many people's inboxes. In the case of one spam operation, it has been observed that only 1 in 12.5 million spam messages receive a buyer (Larkin, 2008). Only a rare few recipients are fooled by these messages. However, this is enough for spam to cost billions in damages. But such damages can only be dealt if the spammer is able to send bulk email in millions of messages per day. The best means the spammer has to do such a thing is through malware infections.

Computers infected with malware and networked together in what is called a botnet are responsible for the majority of spam (Schiller et al., 2007). This is malware installed on a victim computer through trojans, viruses, or worms that can scan a host computer for user contacts, web browser data, and anything where email addresses might be stored. The botnet subsequently automates the sending of spam messages to these addresses, from the victim's own computer, and not the spammer's, sometimes posing as the victim. Spammers can control these computers remotely, sometimes owning botnet clients installed on millions of unsuspecting victims' PCs. It is estimated that between 16 and 25% of computers are infected by a botnet (Weber, 2007).

Cyber criminals seem just as professional and organized as a legitimate industry, with a strict division of labor, investments, traded goods and hired consultants. Spammers contract botnet herders, who allow the spammer to rent botspace to send bulk email, and the spammer is hired by a malware writer, who writes phishing websites and scripts to install malicious code on victim computers (Anderson, Bohme, Clayton, & Moore, 2008). Identities stolen from such operations can be bought and sold online, with a credit card selling for as little as $0.50 each (Brody et al., 2007).

This lucrative and booming business is not going away anytime soon. Most of the fight against spam is technological, with new filters, authentication software, antivirus, and antispyware being developed and improved to limit the amount of spam users receive or that can fool recipients. Aside from building these technological defenses, there are also offensive measures to combat spam, which involve criminalizing certain spamming techniques and enforcing such laws.

Deleting and blocking spam messages makes it harder for the spammers, if only a little. But arresting the spammers themselves ends their operations entirely. Unfortunately, spam crosses international borders, and no country has jurisdiction over all the spam that it receives. Anti-spam laws exist in many countries, but they are unequipped to target spammers not in their jurisdiction. In America, Federal anti-spam legislation went into effect in January 1, 2004, called the CAN SPAM Act. The act supersedes any state laws in existence regulating the sending of spam, replacing them with some basic requirements if businesses so choose to send commercial email messages (CAN SPAM Act of 2003).

The major laws outlined in the CAN SPAM Act include requirements for honesty and accuracy of the content of email messages, genuine identifying information about the sender of the email messages such as address and contact information, and an opt-out method that allows recipients to choose to no longer receive messages from a given sender. Harsher sentences exist for those who send spam from an unauthorized location, such as from a botnet on an unwilling person's computer.

Since the CAN SPAM Act went into effect in early 2004, efforts have been made to determine its efficacy in limiting spam. The CAN SPAM Act is enforced by the Federal Trade Commission, which subsequently produced a report on the success on its Act to Congress in 2005 (Majoras, Leary, Harbour, & Leibowitz, 2005). Contained in the report was the conclusion that spam has stabilized since the creation of the CAN SPAM Act, whereas before spam displayed a steady increase over time. The data used were the number of spam emails received per day by the FTC.

Other authorities have similarly analyzed spam volume to determine whether spam rates or content differed after the passing of the Act. According to MessageLabs, an anti-spam and security company, after one year following the CAN SPAM Act, email that was considered spam went up from 60% of all global email the year before to 80% by the end of the year (Zeller, 2005). When the FTC measured spam in absolute terms (amount received per day), spam seemed to have slowed. But when measured in relation to the amount of legitimate email sent, spam seemed to have increased.

It should be mentioned however that neither the Federal Trade Commission nor MessageLabs report the statistical significance of their findings. Although overwhelming consensus seems to be that spam has not decreased significantly since the creation of the CAN SPAM Act (Lee, 2005; Arora, 2006), such conclusions should be finalized with a little more statistical rigor.

Despite this, the actual volume of spam sent is not the only measure of the success of the CAN SPAM Act. Questions as to whether compliance with the specific requirements detailed in the act may have increased since the passing of the law have been investigated. In one such case, 1,100 unsolicited commercial emails were randomly selected from 5 email accounts, once six months after the passing of the CAN SPAM Act and another sampling two years after the act went into effect (Grimes, 2007). Each email message was rated as either complying with the CAN SPAM Act, or not complying with the act.

Unfortunately, 14.3% of spam complied with legal requirements the first six months following the act, whereas a mere 5.7% of emails complied with it two years later (Grimes, 2007). However, a sample size of 1,100 might not be large enough for something done on as massive a scale as spam. Additionally, no baseline of compliance was established in spam messages before the CAN SPAM Act was instated.

Another possible measure that seems lacking in the literature includes the location from which spam is sent. If spam has not been affected by existing laws, it could be that spammers have moved their operations across borders, outside of the United States, where the CAN SPAM Act has no jurisdiction. CAN SPAM may not have decreased spam rates, but rather moved spam sending botnets to where the Act has no reach.

Considering the enormity of the problem spam poses to the 1.6 billion people online (Internet World Stats, 2009), and some of the seeming impunity spammers enjoy since the majority of anti-spam practices have been defensive rather than offensive, existing spam law warrants extensive investigation. Anti-spam law has been given less emphasis than anti-spam technology, and it should be improved just as much as spam filters and intrusion detection systems. With the rigor of scientific analysis of existing laws, such as the CAN SPAM Act, we can hope to piece together what laws might work, and which ones could stand to see some improvement.

Methods

Sample

The sample for the present study consisted of 2,071,965 email messages sent and received between February, 1998 and December, 2008. The sample was acquired from Untroubled Software, a software security and optimization website that also provides downloadable spam archives for researchers. The data were retrieved on January 3, 2009 from http://untroubled.org/spam, and consists of millions of email files.

According to the author of Untroubled Software (http://untroubled.org/spam/), the spam archives were gathered via multiple bait email addresses, which are email accounts created with the sole purpose of baiting spammers to add the baited address to their spam lists.

Since the date each message was received was important for the purposes of this research, some cases had to be eliminated due to false or missing received dates. There were 4,959 cases that were found to have no date contained in the email headers, and 2 more messages that had clearly incorrect dates ("12/95/2005"). This was likely due to falsifying headers and general tampering by spammers. The data were further aggregated by month for the purposes of time series analysis. Grouping the eleven years (1998-2008) of data by month resulted in a series of 131 months total.

There was an additional dataset acquired for this research from the Federal Trade Commission (FTC). The FTC had conducted their own analysis on the state of spam, and a subsequent Freedom of Information Act request allowed a portion of the FTC's data to be used in this study. The data consisted of a summary of 479,701,868 emails collected by the FTC between the beginning of 2000 and the end of 2007.

Procedures

The sample of spam email messages was measured by a program written in PERL (Practical Extraction and Report Language). The script written for this research subsequently scanned all email messages until all messages were parsed in chronological order one by one. While scanning each message, the script recorded eight variables for that given message in a comma separated values file as a single row.

The script also used a database of world IP addresses to create a variable representing the country the spam message was sent from. The database contained IP address codes and a lookup of global information about each address type, including the country of origin for a given computer's IP address. The database was downloaded from WebNet77 (http://software77.net/cgi-bin/ip-country/geo-ip.pl) on March 20, 2009.

Measures and Variables

Date Received: The script was set to record the first date it could identify when scanning each message, starting its scan from the top of the message headers. Email headers have a timestamp for each hop, or each time a message is routed through a network on its way to its destination. Information for each hop is appended to the top of the email headers. Thus, the most recent time a message was transmitted can be assumed to be the topmost date and time recorded in an email's headers. The topmost date was assumed to be the date the message was received. All other dates below the first were ignored by the script.

IP Address: This variable was only recorded just in case there was a need to further inspect the country of origin variable. The IP address was used to look up the country from which the message was sent from. The IP address the script was set to record was the lowermost IP address found in the message's headers. Each hop of a message records the IP address of the server which handled that transmission. Newer hops are appended to the top of the message. Therefore, the last IP address found in a message's headers can be assumed to be the originating mail server from which the email was sent from assuming there was no tampering of the headers. These IP addresses were identified and recorded in the CSV file by the software.

Country of Origin: After the recording of an email message's originating IP address, the address is looked up in a database containing geographic information about world IP addresses. Details about the database can be found in the Procedures section above. If an address can be successfully identified in the database, the name of the country associated with that IP address can be identified. The full name of the country is then read from the database and saved to the CSV file.

Opt-Out Compliance: Opt-out compliance is a measure of whether the email in question complies with the CAN SPAM Act regulation of providing a suitable opt out option for recipients. Opt-out allows recipients to notify the sender that they no longer wish to continue receiving spam messages, followed by a ten business day requirement of the spammer to discontinue sending to that recipient. The message was assumed to have a valid opt-out option if any of the following keywords were found in the body of the email message: "opt-out", "opt out", or "unsubscribe". The keywords to identify were not case sensitive. The opt-out variable was represented as a dichotomous measure of compliance, zero for no compliance, and a one if any of the three strings above were identified.

The opt-out compliance variable was tested for interrater reliability from a random sample of fifty emails. An independent coder rated each of the fifty emails in terms of whether each complied with the CAN SPAM opt-out requirement. The reliability of this measure was high (Cohen's kappa = .9, p< .001), suggesting that the software's judgment was consistent with that of the human coder's.

Valid Mailing Address Compliance: A second CAN SPAM Act compliance measure attempted to determine the emails compliance with the requirement that the sender provide his own valid physical mailing address in the body of the email. The script used a regular expression that could identify any string with the following pattern: a number of any length, followed by one or more spaces, then any valid acronym for an addresses direction ("NE", "SW", etc.), followed by another series of spaces of any length, followed by any number of any characters so long as there was no line break, followed by one or more spaces, and ending with a street suffix of some sort ("ave", "st", "apt", etc.) all without any line breaks found within the string. If a string was found in the body of the email message that matched this description, the address variable was recorded as "1". Otherwise it would be "0".

A sample of fifty emails was used to test the address compliance variable for interrater reliability. The interrater reliability of this measure was relatively high (Cohen's kappa = .73, p< .001), indicating that the software and an independent human coder agreed on most of the items.

Accurate Subject Heading Compliance: The CAN SPAM Act requires all commercial email to have a subject heading that is related to the actual content of the email message. The script identified this level of compliance by checking to see if any word in the subject line was also found in the body of the email message. First the subject line was recorded by the software. Then the subject line was stripped of any common words (e.g. "the", "from", "and", "for"). The remaining words were then exploded into an array (a list). This list was then compared with each and every word contained within the body of the email. If one subject word matched any word in the body, compliance was assumed. Compliance was a true or false variable ("1" being compliance found, "0" being noncompliance assumed).

The accurate subject heading measure was tested for interrater reliability. The reliability for this variable was very low (Cohen's kappa = .29, p = .003), suggesting the software was not consistently successful at identifying compliance with this particular law. However, given that the reliability was still significantly different from zero, this variable was kept in the dataset for use in subsequent analysis.

Notice of Advertisement Compliance: CAN SPAM require commercial emails to identify themselves as advertisements. An email was assumed to have complied with this regulation if any of the following strings were found in either the body of the email message or the subject line: “advertisement”, “ad” surrounded by at least one space, comma, or colon on each side, and “adv” surrounded by at least one space, comma, or colon on each side. The last two strings had to have been surrounded by spaces or similar characters to avoid false positives of words that contain those letters (“add”, “adverture”, etc.). If any of these three expressions were matched, “1” for compliance assumed was recorded. Otherwise a record of “0” for noncompliance was written to file.

The notice of advertisement measure was tested for interrater reliability. It was found that the reliability of this measure was not significant (Cohen’s kappa = .16, *p* = .241). This suggests that the ability of the software and the human rater to agree were on average no better than chance. Because of the lack of reliability, the advertisement compliance variable was excluded from further use in any subsequent analysis.

Aggregated Percent Compliance per Month: The three compliance variables (opt-out, valid address, and accurate subject) were aggregated by month. Each of the three variables represents the percent of emails which complied with the CAN SPAM Act each month. Each of these three variables was to be used as a separate time series for impact assessment.

Number of Messages per Month: Number of messages per month is the total number of spam emails received for each month. This measure will be used as a spam rate to test whether spam appears to change in frequency following the introduction of the CAN SPAM Act.

After inspection of the spam rate time series, however, there appeared to be an inordinately large spike in spam rates for three months between August and October 2006 (see Figure 1). The author who collected the spam data and provided it online for research purposes (http://untroubled.org/spam), makes note that the unusual spike was due to the use of a wildcard email address enabled in 2006. Wildcard addresses allow misspelling of an email address username (user@domain.com), to be successfully routed to the owner of the domain, regardless of the misspelling. This accounted for the inordinate increase in spam (mostly duplicates) in 2006. In 2007, the wildcard addressing was disabled, which was followed by a subsequent decrease in spam rates.

Percent from within the United States per Month: The measure of whether a message was sent from the United States was computed as a percentage of messages assumed to have been sent from within the United States for each month. Percent US was calculated by dividing the number of IP addresses identified as coming from within the United States by the sum of this number plus the number of countries not of the United States. If a country could not be identified by the software (invalid IP address, no IP address found, etc.), then those cases were not computed in the percentage. There were a total of 107,971 email messages that could not be geolocated to a specific country. Of those that could be identified, 904,974 were found to be from within the United States, and 1,054,059 were determined to be from countries other than the United States.

Design

An interrupted time series design was used to test the data. There were five time series to conduct, one for spam rates, three for each of the individual compliance variables, and a final model for percent of US IP addresses.

The intervention point for each of the five models was January 1, 2004. On this day, the CAN SPAM Act first went into effect. The questions of this research are whether the

CAN SPAM Act affected (1) spam rates, (2) spam legality compliance, and (3) assumed spam originating IP addresses

Results

Monthly Spam Rates

A time series model was developed to examine the effect the introduction of the CAN SPAM Act of 2004 had on the amount of spam received per month. To test the validity of the spam rate time series itself, a Spearman's correlation was conducted between the monthly spam data and the Federal Trade Commission's own monthly spam data. The two samples included the spam archives of spam collected between 1998 and 2008, and the Federal Trade Commission data collected between 2000 and 2007. The two datasets were found to be strongly related ($r(96) = .81$, $p < .001$). High correlation can be taken to mean that the two datasets measure the same spam activity within the United States.

However, after inspection of the spam rate time series, there appeared to be a large spike in spam rates between the months of August and October 2006 (see Figure B.1 of the appendix). This indicated a non-constant variance, and so a logarithmic transformation of the time series was necessary. The logarithmically transformed series can be seen in Figure B.2 of the appendix. An Augmented Dickey-Fuller test revealed that the spam rate series was not trend stationary (t = -2.63, p = .089), meaning that there was high serial dependency in the time series data. After regular differencing, the data were identified to be sufficiently stationary (t = -10.75, $p < .001$).

With the parameters for the model estimated, an ARIMA(0, 1, 0) model was identified. Diagnostic checks of the residuals were conducted to test for the presence of autocorrelation. A Ljung-Box test was not found to be significant (p = .922), indicating no autocorrelation between the residuals. Refer to Appendix A.1.

A dummy variable for the intervention component of the model was created, with the intervention point starting in January 1, 2004, when the CAN SPAM Act first went into effect. The impact parameter was tested on the logarithmically transformed spam rate time series. Referring to Table 1, the intervention coefficient (-.132) was found to be nonsignificant (t = -.395, p = .694, R^2 = .001), suggesting that there was no change in the underlying trend for spam rates in January 1, 2004. Thus the CAN SPAM Act had no influence over the volume of spam sent after the passing of the Act.

Table 1 Linear regression model for log transformed spam rates, 1998-2008

Variable	Coefficient	Standard error	*t*	*p*-value
Intercept	.069	.029	2.36	.02
Intervention	-.132	.335	-.395	.694
R^2 = .001				

Percent Compliance with Unsubscribe Option in Spam per Month

A second time series model was developed to determine the effect the CAN SPAM Act of 2004 had on the percent of spam that provided an opt-out choice for recipients. An Augmented Dickey-Fuller test revealed that the percent of compliance with an opt-out method series was trend stationary (t = -3, p = .038), and therefore met the underlying assumptions of the model.

With the parameters for the model estimated, an ARIMA(1, 0, 0) model was identified. Diagnostic checks of the residuals were conducted to test for the presence of autocorrelation. A Ljung-Box test was not found to be significant (*p* = .845), indicating no autocorrelation between the residuals. Refer to Appendix A.2.

A dummy variable for the intervention component of the model was created, with the intervention point starting in January 1, 2004, when the CAN SPAM Act first went into effect. The impact parameter was tested with CAN SPAM compliance with an opt-out requirement as the dependant variable. The autoregressive parameter (.81) was significant (*t* = 15.21, *p*< .001).

The intervention parameter (-.05) was not found to be a significant predictor (*t* = -1.8, *p* = .075, R^2 = .77), indicating that patterns of spammers providing an unsubscribe option in emails were not affected by the CAN SPAM Act. See Table 2.

Table 2 Linear regression model for unsubscribe compliance percentage, 1998-2008

Variable	Coefficient	Standard error	*t*	*p*-value
Intercept	.127	.024	5.373	< .001
AR(1)	.809	.053	15.207	< .001
Intervention	-.054	.03	-1.8	.075
R^2 = .77				

Percent Compliance with Providing Physical Mailing Address in Spam per Month

A third time series model was created to test the impact the CAN SPAM Act of 2004 had on the percentage of emails that provided a physical mailing address in the body of the message. An Augmented Dickey-Fuller test revealed that the percent of address compliance series was sufficiently trend stationary (*t* = -5.52, *p*< .001).

With the parameters for the model estimated, an ARIMA(3, 0, 0) model was identified, with one autoregressive parameter at lag 4 and another at lag 36. Diagnostic checks of the residuals were conducted to test for the presence of autocorrelation. A Ljung-Box test was not found to be significant (*p* = .81), indicating no autocorrelation between the residuals. Refer to Appendix A.3. The estimated constant parameter (< .001) was found to be nonsignificant (*t* = .08, *p* = .936), and therefore had to be eliminated from the model.

An intervention point for the model was created starting in January 1, 2004, when the CAN SPAM Act first went into effect. The impact parameter was tested with percent of compliance with an address requirement set as the dependent variable. The autoregressive parameter at lag 1 (.33) was significant (*t* = 3.98, *p*< .001), the parameter at lag 4 (.32) was significant (*t* = 4.34, *p*< .001), and the final autoregressive parameter at lag 36 (.13) was also significant (*t* = 2.83, *p* = .006). Refer to Table 3.

The intervention parameter (.002) was not significant (*t* = .94, *p* = .35, R^2 = .56), suggesting that the intervention of the CAN SPAM Act had no noticeable impact on compliance with the Act's address requirement.

Table 3 Linear regression model for physical address compliance percentage, 1998-2008

Variable	Coefficient	Standard error	*t*	*p*-value
AR(1)	.326	.082	3.983	< .001
AR(4)	.318	.073	4.343	< .001
AR(36)	.125	.044	2.833	.006
Intervention	.002	.002	.94	.35
R^2 = .56				

Percent Compliance with a Descriptive Subject Heading in Spam per Month

A fourth time series model was created to test the effect the CAN SPAM Act of 2004 had on whether spam used descriptive wording in their subject lines. An Augmented Dickey-Fuller test revealed that the average compliance per month series was not trend stationary (t = -1.35, p = .605). After regular differencing, the data were identified to be sufficiently stationary (t = -14.17, p< .001).

With the parameters for the model estimated, an ARIMA(0, 1, 1) model was identified. Diagnostic checks of the residuals were conducted to test for the presence of autocorrelation. A Ljung-Box test was not found to be significant (p = .806), indicating no autocorrelation between the residuals. Refer to Appendix A.4. The estimated constant parameter (-.003) was found to be nonsignificant (t = -1.41, p = .162), and therefore had to be eliminated from the model.

The intervention component of the model was created, with the intervention point starting in January 1, 2004, when the CAN SPAM Act was first instated. The impact parameter was tested with compliance with a descriptive subject per month as the dependent variable. The local moving average parameter (-.31) was significant (t = -3.77, p< .001).

Looking at Table 4, the intervention parameter (-.09) was found to be a significant predictor (t = -2.32, p = .022, R^2 = .09), indicating that the intervention parameter had a negative impact on average compliance with CAN SPAM requirements for a meaningful subject heading in emails. The average percentage of compliance before the CAN SPAM Act was about 81.34% of emails that had accurate subjects. After the intervention, compliance appeared to have dropped by 9%.

Table 4 Linear regression model for accurate subject compliance percentage, 1998-2008

Variable	Coefficient	Standard error	t	p-value
MA(1)	-.312	.083	-3.77	< .001
Intervention	-.087	.038	-2.325	.022
R^2 = .09				

Percent of Spam from Within the United States

A fifth and final time series model was developed to examine the effect the CAN SPAM Act had on the amount of spam with IP addresses that appear to be from within the United States. An Augmented Dickey-Fuller test found the percentage of United States spam to be stationary (t = -3.27, p = .018), suggesting no significant serial dependency of the time series data.

The parameters for the model were estimated and an ARIMA(1, 0, 0) model was chosen. Diagnostic checks of the residuals were conducted to test for the presence of autocorrelation. A Ljung-Box test was not found to be significant, indicating no autocorrelation between the residuals. Refer to Appendix A.5.

The interval chosen was the point starting in January 1, 2004, when the CAN SPAM Act first went into effect. The autoregressive parameter (.895) was found to be significant (t = 26.69, p< .001). The intervention parameter (.026), however, was not found to be significant (t = .43, p = .667, R^2 = .85). See Table 5. The results indicate that the CAN SPAM Act had no impact on which country spam appears to be originating from.

Table 5 Linear regression model for percentage of spam sent from the US, 1998-2008

Variable	Coefficient	Standard error	*t*	*p*-value
Intercept	.46	.064	7.158	< .001
AR(1)	.895	.034	26.691	< .001
Intervention	.026	.059	.431	.667
R^2 = .849				

Discussion and Conclusion

The current study attempted to determine whether the CAN SPAM Act had any kind of significant impact on the behavior of spammers. Five interrupted time series models were constructed to assess the potential effect CAN SPAM had on spam rates, spam's legality, or spam's apparent originating IP address. This research found that no impact could be discerned on the spam rate or the IP address time series. Nor were two of the three spam law compliance series significantly predicted by CAN SPAM. It was found that CAN SPAM may have been followed by a drop in spam complying with a specific CAN SPAM requirement, that being that emails must have descriptive subject headings in emails.

Spam is a relatively new form of crime, and is also a relatively new form of communication technology. Inspecting the visual change in spam rates over time on a line graph, both on the spam rates collected for this research and that collected by the Federal Trade Commission (see Figure B.1 and Figure B.3 of the appendix), spam clearly started out small in the early preintervention period of both spam rate time series datasets. Perhaps a baseline for something as early as before 2004 might have been during a time when there was too little spam to begin with to properly contrast with what spam is like today. Looking at both figures of spam rates over time, spam clearly starts out small and unnoticeable and then expands considerably over the decade. This increase in spam was likely inevitable, as the beginning of both time series are near a time when spam was new. Like any new form of crime or technology, it takes some time before it can grow into more stable levels. Perhaps if the CAN SPAM Act was released later, we might have witnessed some sort of noticeable change in spam trends following the Act. Fortunately, the CAN SPAM Act has since been amended in 2008, called the CAN SPAM Act of 2008. If a preintervention prior to 2004 truly is not a time we'd consider to be a proper baseline measurement of spam rates, then maybe future research could assess the impact of the CAN SPAM Act of 2008.

Considering that spam rates remained unaffected by the CAN SPAM Act of 2004, this could be evidence that the CAN SPAM Act was not a sufficient deterrent to sending bulk commercial emails illegally. Profitability for a spammer requires quantity over quality. Most recipients ignore spam, and so the solution to this is to send so many messages that by chance alone at least some recipients will take the bait. A spammer must send millions of emails per month, and to have to make those emails comply with spam law would make profitability nearly impossible. Decreasing the volume of spam would not be in the spammer's best interest.

But the CAN SPAM Act did not make spam illegal, it only regulated what kinds of spam is allowable. Certainly a spammer could send just as much spam as he/she did before, with only some substantial adjustments to make his electronic messages comply with the United States Code. If spammers sent just as much spam as before the Act, only making their messages comply with its regulations, then perhaps Congress would be wise to make all spam, regardless of how compliant it is, illegal.

As the present study revealed, noncompliance with spam law was similarly not deterred by the passing of the CAN SPAM Act. The first step towards mitigating the spam problem would be to actually affect spammers in some way, the result of which would hopefully be combined with both compliance and a decrease in mass produced spam. Criminalizing all spam, regardless of compliance, would likely have produced a result little different than that observed already. Most spam already is illegal anyway, not because of how much is sent, but because of the numerous violations present in the messages and headers themselves.

Compliance with the accurate subject requirement was significantly decreased after CAN SPAM. Inspecting the line graph for this measure depicted in AppendixB.4, compliance looks to begin dropping at around early 2002, well before the CAN SPAM Act was passed. Compliance plummets and evens off at the beginning of 2005. It could be that the CAN SPAM Act came at a bad time in history when commercial emails were becoming more fraudulent and less considerate of recipients.

While the meaningful subject requirement of spam was the most common item spammers complied with, it is still likely a useful trick in the spammer's book. If someone cannot tell an email is spam just by reading the title of the subject, then maybe they will open the message and read it before deciding to delete it. Certainly more spammers might adopt this trick as time progresses and spammers become savvier to turning a profit through spam. As spammers share more ideas online and learn from each other, certain spam techniques will be adopted, and the more successful ones will likely persist over time. Perhaps around 2002, when compliance drops off for the meaningful subject law, spammers were just starting to learn the utility of this technique. If it is found to be a successful means of influencing recipients to open an email, then surely that technique will continue to increase in prevalence among spam messages over time.

Spammers might think twice about installing a spam bot or sending spam from within the United States considering the penalties set forth in the CAN SPAM Act. No research prior has addressed this possibility, although it might be considered that there would be fewer spammers in the US, or even less spam sent from the US, after the Act went into effect. It is difficult to determine what proportion of spam originated in the United States by examining the headers alone. It is even more difficult to determine this proportion merely by geolocating the first IP address found in spam, as this present research did. The findings in this research that relate to this question are still inconclusive. Determining the originating IP address of an email message that is considered to be spam requires a careful inspection of the headers to identify and eliminate obviously false routing insertions or invalid IP addresses. The software used to gather the present data was not equipped to inspect the headers with such precision.

If there had been a noticeable trend in the percentage of US IP addresses per month, then perhaps the time series might be considered to be meaningful of some underlying force, perhaps representative of spammer or cyber criminal behavior. Inspecting the time series of US spam contributions in Figure B.8 of the appendix, there does not seem to be a consistent direction to which US spam percentage takes. It may be that the United States CAN SPAM Act was not a sufficient deterrent for local spammers, or also likely is that the originating IP address of spam has little to nothing to do with the actual IP address of the spammer. Given the lack of significant findings with this data, it is difficult to say anything substantive about the underlying reasons for the results of the data.

Whatever the case, this research has concluded that the CAN SPAM Act has not significantly deterred spam. It could be that such legislation was too early to have an impact in the nascent and growing spam volume over time. Not only has spam grown, but technology and especially the internet and everything in it has grown as well. As more people start using the internet, more computers that can be infected with spam bots are connected, more potential victims of the spammer arise, and more people with the motive and the means to send spam exist. Growth in spam might have been inevitable, as the internet itself has grown, potentially confounding this article's findings. If that is the case, the CAN SPAM Act of 2008 should be considered for a follow up, assuming growth in 2008 was not as strong as it was in 2004. However, that seems unlikely.

The risks associated with committing any form of cyber crime, spam or otherwise, are clearly not high enough, especially if only 5% of malware writers and other cyber criminals are ever caught (Paul, 2006).But actually catching such criminals can be a difficult endeavor given the high degree of anonymity provided by the internet. Compound this with cyber crime crossing international borders, and there are problems of enforcement with the mix of jurisdictions involved.

The United States ought not just create and enforce local cyber crime laws; there must be some protocol in place to allow the collaboration with the governments of other countries to help bring offenders across borders to justice. There are already some rudimentary measures put in place to accomplish just this, such as the Tripartite Memorandum of Understanding on Spam Enforcement Cooperation. This is an agreement between the United Kingdom, the United States, and Australia to enforce laws against cyber crime violators (Mustakas, Ranganathan & Duquenoy, 2005).

It will take more than the cooperation of just these three countries before anti-spam laws can pose a significant deterrent to offenders everywhere in the world. Since there are almost no borders on the internet, enforcing laws such as CAN SPAM will have to be done under greater agreement about the illegality of spam of all nations. While cyber criminals have made their operations more effective by collaborating and becoming more organized, with other like minded groups and individuals, so too must law enforcement be similarly organized. If two jurisdictions from more than one country do not agree on the illegality of spam, then spam will surely continue.

Considering the profitability of spam, the negative findings of this research, and the low risks involved in sending spam, spam is a sound business strategy, with a low risk to reward ratio. In order to sufficiently deter spammers, punishments may have to be more probable for each cyber criminal that sends spam. However, in order to do such a thing, law enforcement may need more than just new laws. They may simply need better law enforcement, staffed with security experts or even former cyber criminals that are better able to track and apprehend other cyber criminals. Spammers evolve and adopt new technology to boost their business with alacrity and eager readiness. Government agencies and other bodies granted the authority to pursue spammers legally may not be so adept at utilizing the internet and technology to make sure those in cyberspace comply with their laws. It may be necessary, in order to catch spammers, that government agencies begin to think like spammers themselves.

References

Anderson, R., Bohme, R., Clayton, R., & Moore, T. (2008). Security economics and the internet market. Retrieved July 30, 2008, from http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf.

Arora, V. (2005). The CAN-SPAM Act: An inadequate attempt to deal with a growing problem. *Columbia Journal of Law and Social Problems*, 300-330.

Brody R. G., Mulig, E., & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, *11*, 43-56.

CAN SPAM Act: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. Sec 7701 (2005).

Computer Fraud and Abuse Act, 18 U.S.C. Sec 1030 (2006).

Dredze, M, Gevaryahu, R., & Elias-Bachrac. (2007). *Learning fast classifiers for image spam.* Proceedings of the Conference on Email and Anti-Spam (CEAS).

Dyrud, M. (2005). "I brought you a good news": An analysis of Nigerian 419 letters. Proceedings of the 2005 Association for Business Communication Annual Convention.

Federal Trade Commission Act, 15 U.S.C. Sec 41 (2007).

Grimes, G. A. (2007, February). Compliance with the CAN-SPAM Act of 2003: Studying the application of the of the CAN-SPAM Act and its effect on controlling unsolicited email messages. *Communications of the ACM*, 50(2), 56-62.

Internet World Stats: Usage and Population Statistics (2009). Retrieved July 20, 2009 from http://www.internetworldstats.com/stats.htm

Kleiner, K. (2008). *Happy spamiversary! Spam reaches 30.* Retrieved July 15, 2009, from New Scientist Web site: http://www.newscientist.com/article/dn13777-happy-spamiversary-spam-reaches-30.html?full=true

Larkin, E. (2009, February). Economies of scale in the spam business. *PC World*, 47-48.

Lee, Y. (2005, June). The CAN-SPAM Act: A silver bullet solution? *Communications of the ACM*, 48(6), 131-132.

Majoras, D. P., Leary, T.B., Harbour, P.J., & Leibowitz, J. (2005, December). Effectiveness and enforcement of the CAN-SPAM Act: A report to Congress. *Federal Trade Commission.*

McCain, Sen. (2003, October 22). CAN SPAM Act of 2003. In Congressional Record 149, S13020.

McDowall, D., McCleary, R., Meidinger, E. E., & Hay, R. A. (1980). *Interrupted time series analysis.* Iowa City, IA: Sage Publications, Inc.

Moustakas, E., Ranganathan, C., & Duquenoy, P. (2005). Combating spam through legislation: a comparative analysis of US and European approaches. *Proceedings of Second Conference on Email and Anti-Spam, CEAS.*

Paul, H. (2006). It's time to arrest cyber crime. *Business Week Online*, 17-17.

Schiller, C. A., Binkley, J., Harley, D., Evron, G., Bradley, T., Willems, C. & Cross, M. (2007). *Botnets: The killer web app. Rockland, MA:* Syngress Publishing.

Smith, R. G., Holmes, M. N., & Kaufmann, P. (1999). Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice*, *121*, 1-6.

Sophos. (2006, April). *Sophos report reveals 'dirty dozen' spam relaying countries for January-March 2006: Asia named worst spam relaying continent.* Retrieved September 1, 2009, from http://www.sophos.com/pressoffice/news/articles/2006/04/dirtydozapr06.html

Waters, D. (2009, April 8). *Spam overwhelms e-mail messages.* Retrieved August 7, 2010, from http://news.bbc.co.uk/2/hi/technology/7988579.stm

Weber, T. (2007). *Criminals may overwhelm the web.* Retrieved May 31, 2009 from http://news.bbc.co.uk/2/hi/business/6298641.stm.

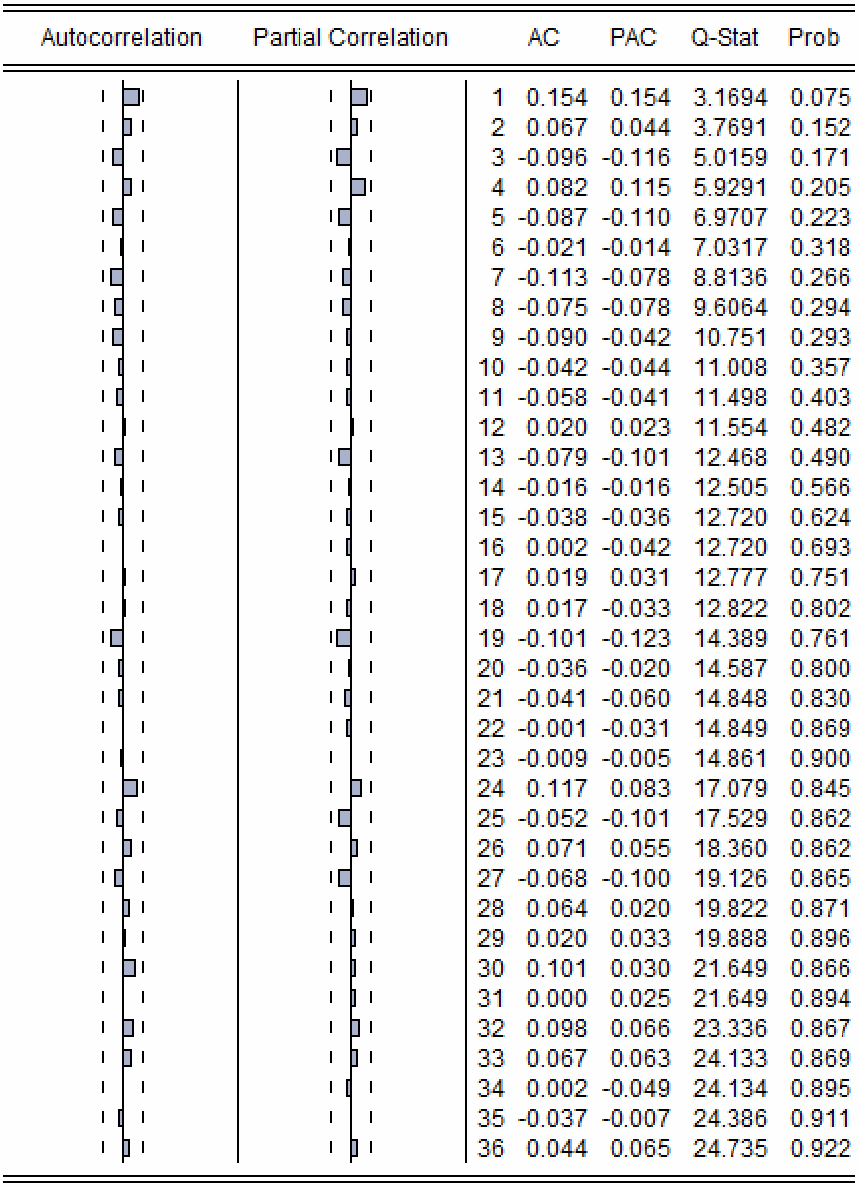
Weston, L. P. (Feb 5, 2010). *Four reasons we get ripped off.* Retrieved February 25, 2010, from http://articles.moneycentral.msn.com/SavingandDebt/ConsumerActionGuide/weston-4-reasons-we-get-ripped-off.aspx?page=1

Why Am I Getting All This Spam? Unsolicited Commerical E-mail Research Six Month Report. (2003). Retrieved September 11, 2009 from http://www.cdt.org/speech/spam/030319spamreport.shtml

Zeller, T. (Feb. 1, 2005). Law barring junk email allows a flood instead. *New York Times*, A1.

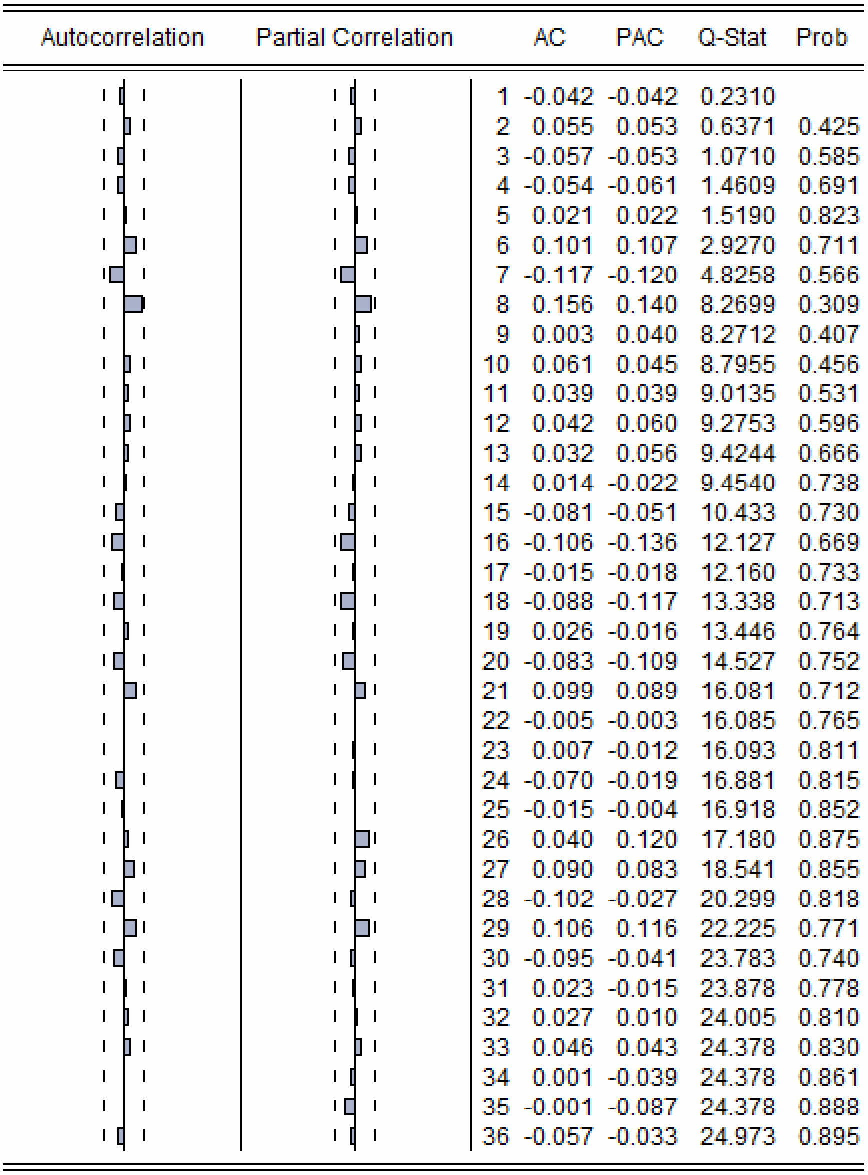
APPENDIX A: RESIDUAL CORRELOGRAMS

Figure A.1 Correlogram of residuals for log transformed spam rate model



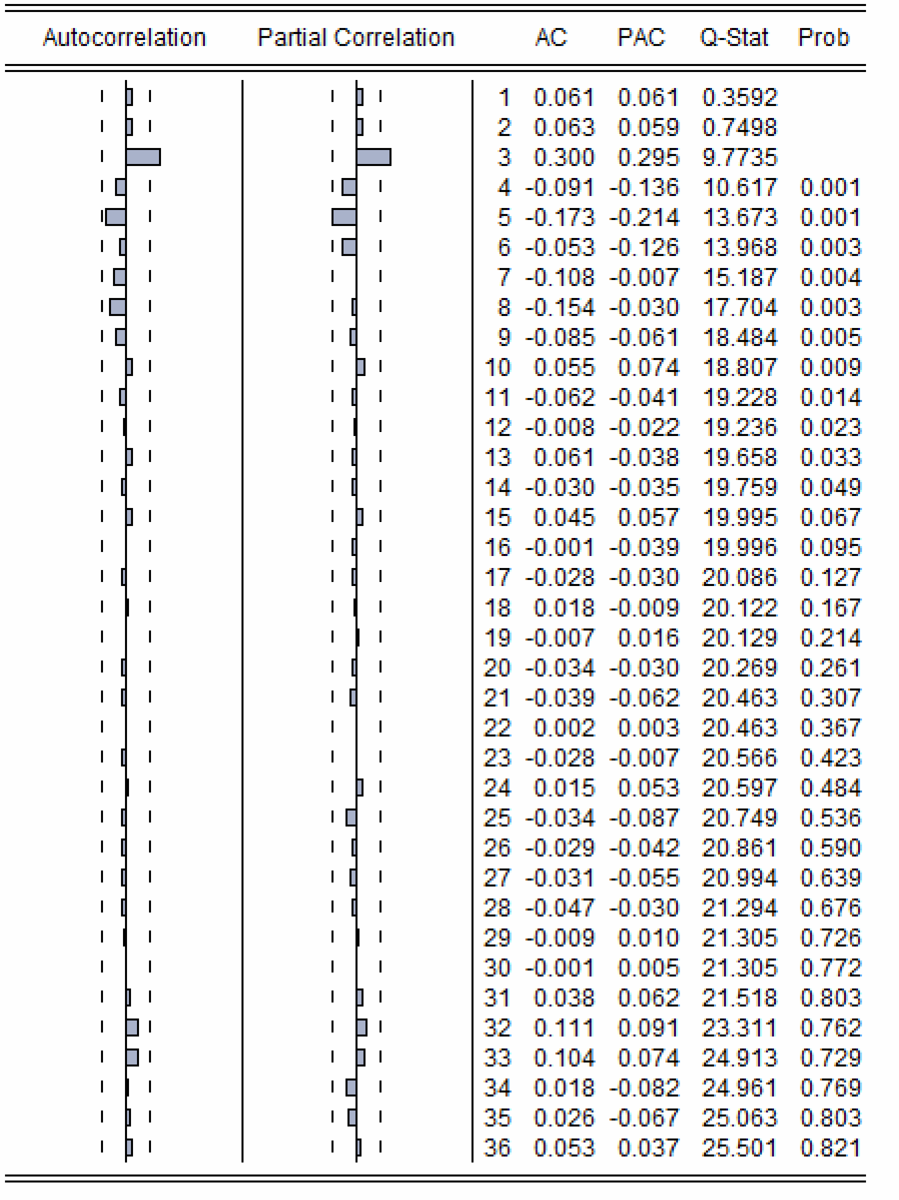
Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	0.154	0.154	3.1694	0.075
		2	0.067	0.044	3.7691	0.152
		3	-0.096	-0.116	5.0159	0.171
		4	0.082	0.115	5.9291	0.205
		5	-0.087	-0.110	6.9707	0.223
		6	-0.021	-0.014	7.0317	0.318
		7	-0.113	-0.078	8.8136	0.266
		8	-0.075	-0.078	9.6064	0.294
		9	-0.090	-0.042	10.751	0.293
		10	-0.042	-0.044	11.008	0.357
		11	-0.058	-0.041	11.498	0.403
		12	0.020	0.023	11.554	0.482
		13	-0.079	-0.101	12.468	0.490
		14	-0.016	-0.016	12.505	0.566
		15	-0.038	-0.036	12.720	0.624
		16	0.002	-0.042	12.720	0.693
		17	0.019	0.031	12.777	0.751
		18	0.017	-0.033	12.822	0.802
		19	-0.101	-0.123	14.389	0.761
		20	-0.036	-0.020	14.587	0.800
		21	-0.041	-0.060	14.848	0.830
		22	-0.001	-0.031	14.849	0.869
		23	-0.009	-0.005	14.861	0.900
		24	0.117	0.083	17.079	0.845
		25	-0.052	-0.101	17.529	0.862
		26	0.071	0.055	18.360	0.862
		27	-0.068	-0.100	19.126	0.865
		28	0.064	0.020	19.822	0.871
		29	0.020	0.033	19.888	0.896
		30	0.101	0.030	21.649	0.866
		31	0.000	0.025	21.649	0.894
		32	0.098	0.066	23.336	0.867
		33	0.067	0.063	24.133	0.869
		34	0.002	-0.049	24.134	0.895
		35	-0.037	-0.007	24.386	0.911
		36	0.044	0.065	24.735	0.922

Figure A.2 Correllogram of residuals for unsubscribe compliance percentage model



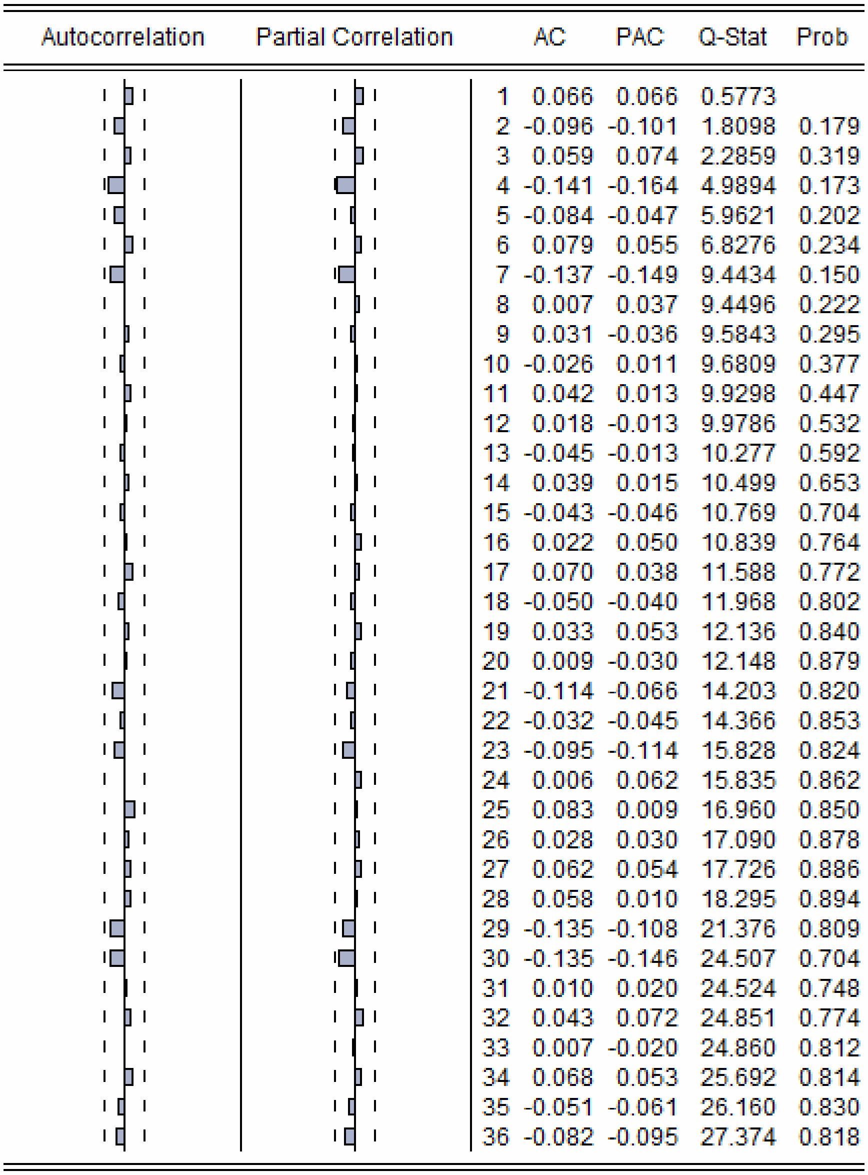
Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	-0.042	-0.042	0.2310	
		2	0.055	0.053	0.6371	0.425
		3	-0.057	-0.053	1.0710	0.585
		4	-0.054	-0.061	1.4609	0.691
		5	0.021	0.022	1.5190	0.823
		6	0.101	0.107	2.9270	0.711
		7	-0.117	-0.120	4.8258	0.566
		8	0.156	0.140	8.2699	0.309
		9	0.003	0.040	8.2712	0.407
		10	0.061	0.045	8.7955	0.456
		11	0.039	0.039	9.0135	0.531
		12	0.042	0.060	9.2753	0.596
		13	0.032	0.056	9.4244	0.666
		14	0.014	-0.022	9.4540	0.738
		15	-0.081	-0.051	10.433	0.730
		16	-0.106	-0.136	12.127	0.669
		17	-0.015	-0.018	12.160	0.733
		18	-0.088	-0.117	13.338	0.713
		19	0.026	-0.016	13.446	0.764
		20	-0.083	-0.109	14.527	0.752
		21	0.099	0.089	16.081	0.712
		22	-0.005	-0.003	16.085	0.765
		23	0.007	-0.012	16.093	0.811
		24	-0.070	-0.019	16.881	0.815
		25	-0.015	-0.004	16.918	0.852
		26	0.040	0.120	17.180	0.875
		27	0.090	0.083	18.541	0.855
		28	-0.102	-0.027	20.299	0.818
		29	0.106	0.116	22.225	0.771
		30	-0.095	-0.041	23.783	0.740
		31	0.023	-0.015	23.878	0.778
		32	0.027	0.010	24.005	0.810
		33	0.046	0.043	24.378	0.830
		34	0.001	-0.039	24.378	0.861
		35	-0.001	-0.087	24.378	0.888
		36	-0.057	-0.033	24.973	0.895

Figure A.3 Correllogram of residuals for physical address compliance percentage model



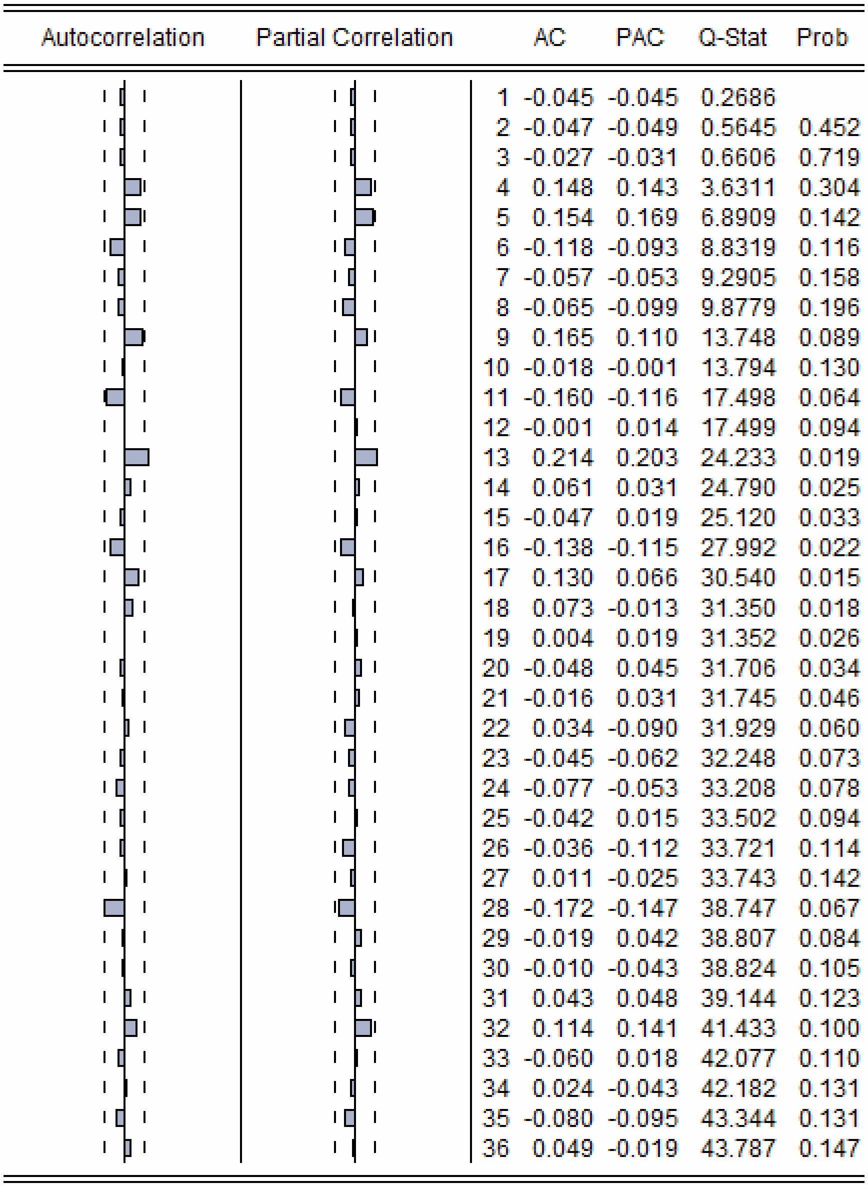
Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	0.061	0.061	0.3592	
		2	0.063	0.059	0.7498	
		3	0.300	0.295	9.7735	
		4	-0.091	-0.136	10.617	0.001
		5	-0.173	-0.214	13.673	0.001
		6	-0.053	-0.126	13.968	0.003
		7	-0.108	-0.007	15.187	0.004
		8	-0.154	-0.030	17.704	0.003
		9	-0.085	-0.061	18.484	0.005
		10	0.055	0.074	18.807	0.009
		11	-0.062	-0.041	19.228	0.014
		12	-0.008	-0.022	19.236	0.023
		13	0.061	-0.038	19.658	0.033
		14	-0.030	-0.035	19.759	0.049
		15	0.045	0.057	19.995	0.067
		16	-0.001	-0.039	19.996	0.095
		17	-0.028	-0.030	20.086	0.127
		18	0.018	-0.009	20.122	0.167
		19	-0.007	0.016	20.129	0.214
		20	-0.034	-0.030	20.269	0.261
		21	-0.039	-0.062	20.463	0.307
		22	0.002	0.003	20.463	0.367
		23	-0.028	-0.007	20.566	0.423
		24	0.015	0.053	20.597	0.484
		25	-0.034	-0.087	20.749	0.536
		26	-0.029	-0.042	20.861	0.590
		27	-0.031	-0.055	20.994	0.639
		28	-0.047	-0.030	21.294	0.676
		29	-0.009	0.010	21.305	0.726
		30	-0.001	0.005	21.305	0.772
		31	0.038	0.062	21.518	0.803
		32	0.111	0.091	23.311	0.762
		33	0.104	0.074	24.913	0.729
		34	0.018	-0.082	24.961	0.769
		35	0.026	-0.067	25.063	0.803
		36	0.053	0.037	25.501	0.821

Figure A.4 Correllogram of residuals for accurate subject compliance percentage model



Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	0.066	0.066	0.5773	
		2	-0.096	-0.101	1.8098	0.179
		3	0.059	0.074	2.2859	0.319
		4	-0.141	-0.164	4.9894	0.173
		5	-0.084	-0.047	5.9621	0.202
		6	0.079	0.055	6.8276	0.234
		7	-0.137	-0.149	9.4434	0.150
		8	0.007	0.037	9.4496	0.222
		9	0.031	-0.036	9.5843	0.295
		10	-0.026	0.011	9.6809	0.377
		11	0.042	0.013	9.9298	0.447
		12	0.018	-0.013	9.9786	0.532
		13	-0.045	-0.013	10.277	0.592
		14	0.039	0.015	10.499	0.653
		15	-0.043	-0.046	10.769	0.704
		16	0.022	0.050	10.839	0.764
		17	0.070	0.038	11.588	0.772
		18	-0.050	-0.040	11.968	0.802
		19	0.033	0.053	12.136	0.840
		20	0.009	-0.030	12.148	0.879
		21	-0.114	-0.066	14.203	0.820
		22	-0.032	-0.045	14.366	0.853
		23	-0.095	-0.114	15.828	0.824
		24	0.006	0.062	15.835	0.862
		25	0.083	0.009	16.960	0.850
		26	0.028	0.030	17.090	0.878
		27	0.062	0.054	17.726	0.886
		28	0.058	0.010	18.295	0.894
		29	-0.135	-0.108	21.376	0.809
		30	-0.135	-0.146	24.507	0.704
		31	0.010	0.020	24.524	0.748
		32	0.043	0.072	24.851	0.774
		33	0.007	-0.020	24.860	0.812
		34	0.068	0.053	25.692	0.814
		35	-0.051	-0.061	26.160	0.830
		36	-0.082	-0.095	27.374	0.818

Figure A.5 Correlogram of residuals for percentage of spam within the US model



Autocorrelation	Partial Correlation		AC	PAC	Q-Stat	Prob
		1	-0.045	-0.045	0.2686	
		2	-0.047	-0.049	0.5645	0.452
		3	-0.027	-0.031	0.6606	0.719
		4	0.148	0.143	3.6311	0.304
		5	0.154	0.169	6.8909	0.142
		6	-0.118	-0.093	8.8319	0.116
		7	-0.057	-0.053	9.2905	0.158
		8	-0.065	-0.099	9.8779	0.196
		9	0.165	0.110	13.748	0.089
		10	-0.018	-0.001	13.794	0.130
		11	-0.160	-0.116	17.498	0.064
		12	-0.001	0.014	17.499	0.094
		13	0.214	0.203	24.233	0.019
		14	0.061	0.031	24.790	0.025
		15	-0.047	0.019	25.120	0.033
		16	-0.138	-0.115	27.992	0.022
		17	0.130	0.066	30.540	0.015
		18	0.073	-0.013	31.350	0.018
		19	0.004	0.019	31.352	0.026
		20	-0.048	0.045	31.706	0.034
		21	-0.016	0.031	31.745	0.046
		22	0.034	-0.090	31.929	0.060
		23	-0.045	-0.062	32.248	0.073
		24	-0.077	-0.053	33.208	0.078
		25	-0.042	0.015	33.502	0.094
		26	-0.036	-0.112	33.721	0.114
		27	0.011	-0.025	33.743	0.142
		28	-0.172	-0.147	38.747	0.067
		29	-0.019	0.042	38.807	0.084
		30	-0.010	-0.043	38.824	0.105
		31	0.043	0.048	39.144	0.123
		32	0.114	0.141	41.433	0.100
		33	-0.060	0.018	42.077	0.110
		34	0.024	-0.043	42.182	0.131
		35	-0.080	-0.095	43.344	0.131
		36	0.049	-0.019	43.787	0.147

APPENDIX B: SPAM LINE CHARTS

Figure B.1 Line chart for spam messages received per month, 1998-2008

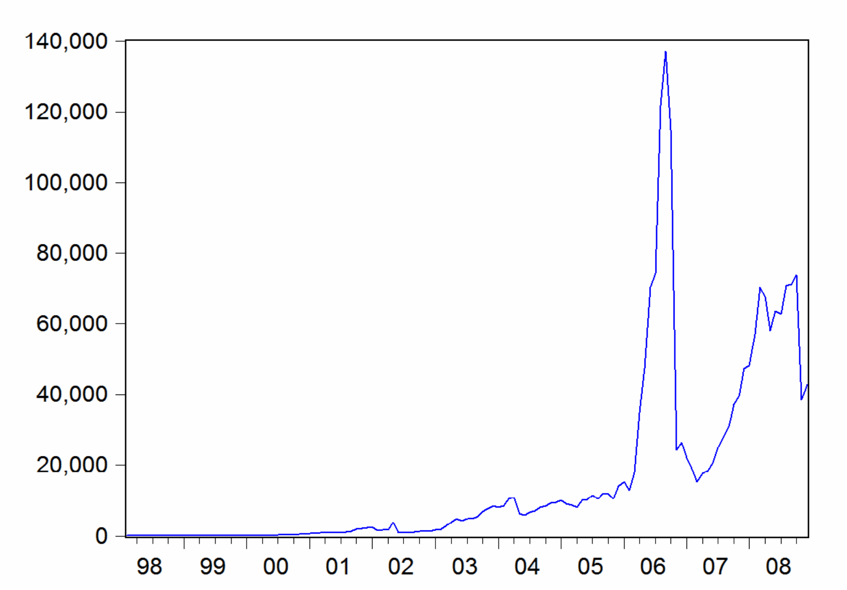


Figure B.2 Line chart for log transformed spam messages received per month, 1998-2008

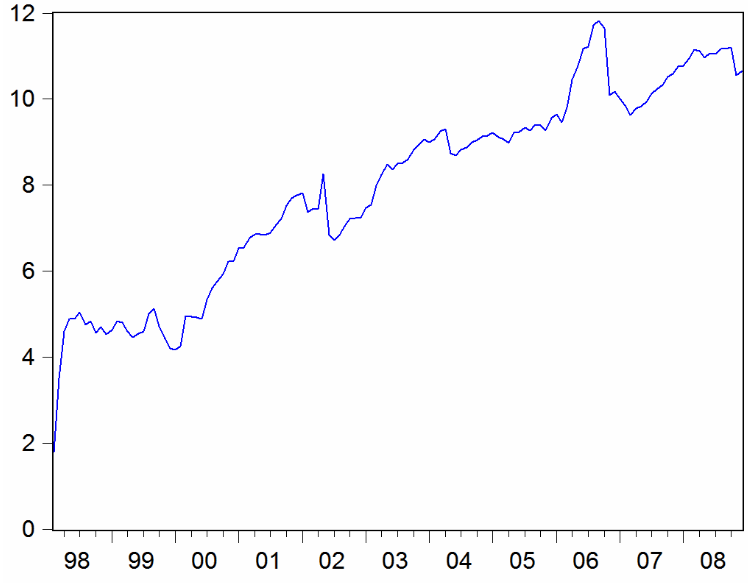


Figure B.3 Line chart for spam messages received per month collected by the FTC, 2000-2007

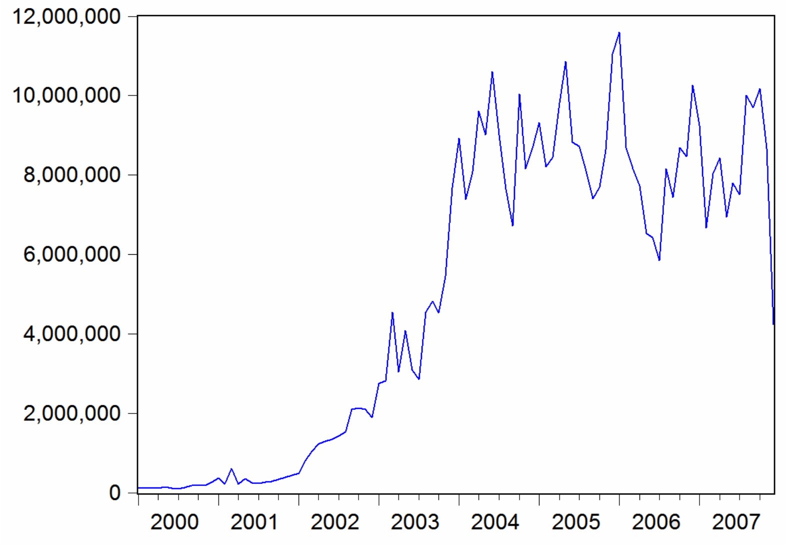


Figure B.4 Line chart of percentage compliance with accurate subject headings per month, 1998-2008

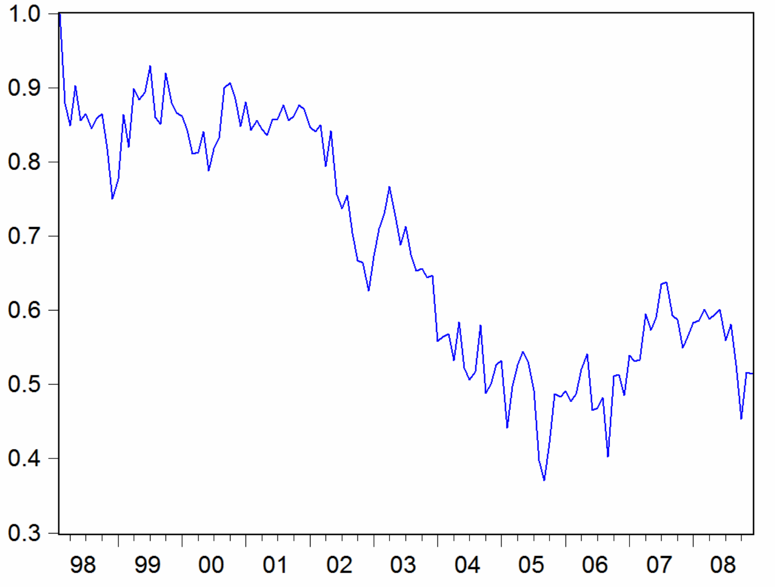


Figure B.5 Line chart of percentage compliance with physical address per month, 1998-2008

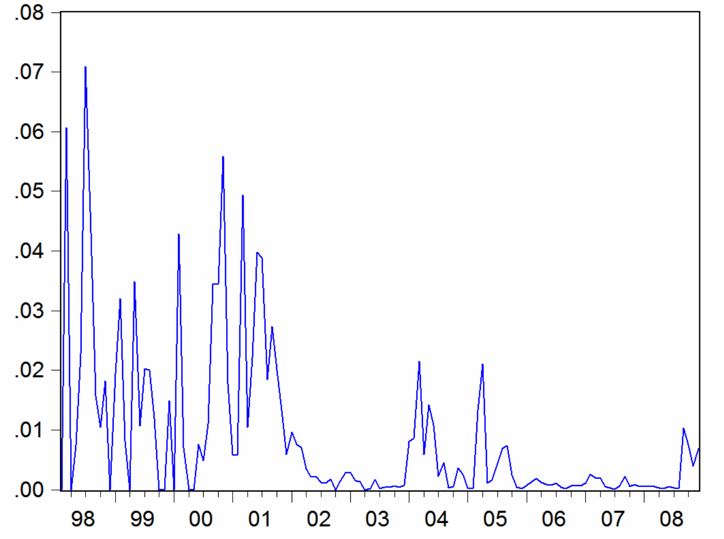


Figure B.6 Line chart for percentage compliance with unsubscribe option per month, 1998-2008

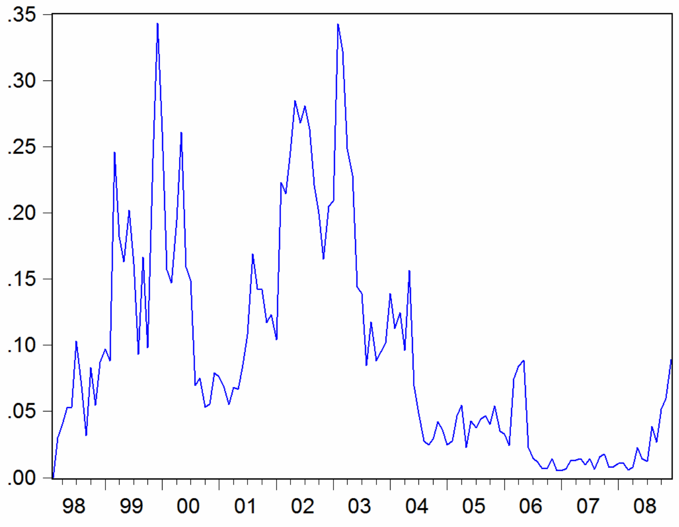


Figure B.7 Line chart for percentage compliance with notice of advertisement per month, 1998-2008

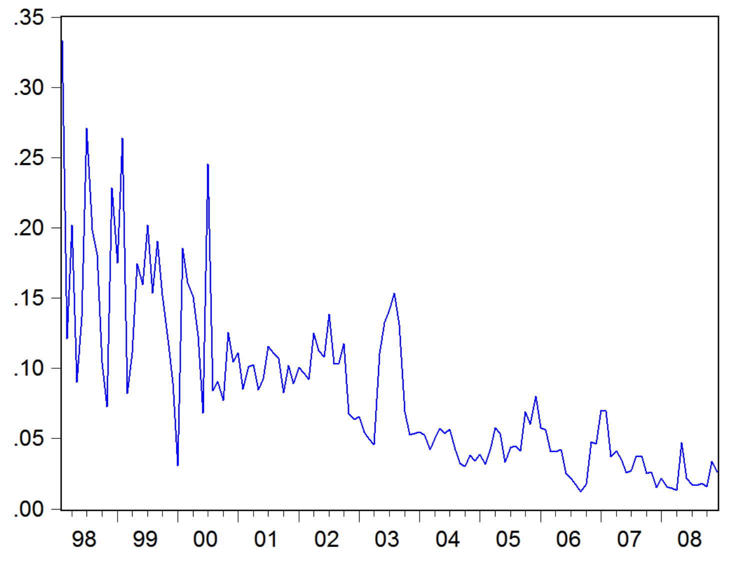
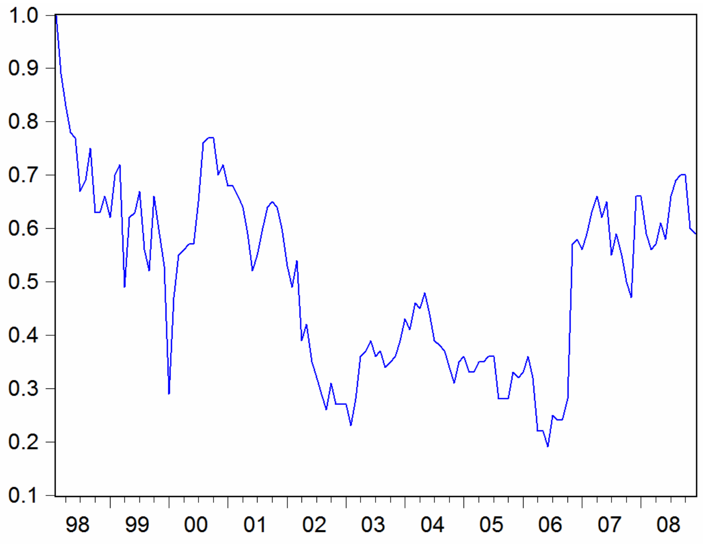


Figure B.8 Line chart for percentage of messages sent from the US per month, 1998-2008


1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
98
99
00
01
02
03
04
05
06
07
08