Volume 3, Number 1 *2004*

Allied Academies
International Conference

New Orleans, Louisiana
April 7-10, 2004

Academy of Strategic E-Commerce

PROCEEDINGS

Volume 3, Number 1 *2004*

Table of Contents

WHAT MAKES UP A BLOG? AN EXPLORATORY LOOK AT THE CONTENT OF WEB-LOGS 1
Charlotte A. Allen, Stephen F. Austin State University

A LONGITUDINAL ANALYSIS OF THE PRIVACY POLICIES OF THE FORTUNE E-50 FIRMS 3
Harlan L. Etheridge, University of Louisiana at Lafayette
Kathy H. Y. Hsu, University of Louisiana at Lafayette

CAN-SPAM ACT OF 2003: HOW FAR DID CONGRESS GO? 5
Sandra E. McKay, Southeastern Louisiana University
John W. Yeargain, Southeastern Louisiana University
Randall P. Settoon, Southeastern Louisiana University

THE IMPACT OF DISCONTINUOUSLY INNOVATIVE TECHNOLOGICAL MARKETS ON CONSUMER SATISFACTION 11
Newell D. Wright, James Madison University
Val Larsen, James Madison University
Irvine Clarke III, James Madison University

Authors' Index 12

WHAT MAKES UP A BLOG? AN EXPLORATORY LOOK AT THE CONTENT OF WEB-LOGS

Charlotte A. Allen, Stephen F. Austin State University
caallen@sfasu.edu

ABSTRACT

Did you see what her blog said? Welcome to the new Internet subculture of blogs and bloggers. Blogs, a version of an online diary with commentary on current news topics, are read by millions of online consumers internationally. This paper is an exploratory look into what makes up a blog. The findings from a content analysis of the top blogs is presented along with suggestions for future research in the area.

A LONGITUDINAL ANALYSIS OF THE PRIVACY POLICIES OF THE FORTUNE E-50 FIRMS

Harlan L. Etheridge, University of Louisiana at Lafayette
Harlan@louisiana.edu
Kathy H. Y. Hsu, University of Louisiana at Lafayette
Kathy@louisiana.edu

ABSTRACT

Online privacy is a major concern of individuals spending time on the Internet. Companies that want to be successful in conducting business on the Internet must be responsive in promoting the trust and confidence of on-line commerce. A privacy notice is a written statement advising the public of the collection and use of personally identifiable information and security practices of a firm. A privacy policy allows consumers to know that the business follows ethical practices in the treatment of their personally identifiable information, and helps increase consumer confidence in the Web as a safe place to shop. A good privacy notice is easy to find, easy to read, and comprehensively explains all of the firm's online information practices. This notice provides online visitors an opportunity to make informed decisions about the collection and use of their information. In this study, we use data collected from the 2000 and 2003 online privacy policies of the Fortune e50 firms, fifty firms that are representative of the Internet economy, to provide a longitudinal analysis of the extent to which online firms are committed to protect online consumer privacy.

We found that most Fortune e50 firms provide basic information about online consumer privacy; however, certain important aspects of online consumer privacy are lacking in the privacy policies of the Fortune e50 firms. We also found that the disclosures in the online privacy policies of the Fortune e50 increased from 2000 to 2003. However, several areas of disclosure are still in need of improvement, particularly information related to consumer choice about data use, the privacy of data collected via email, and children's online privacy.

CAN-SPAM ACT OF 2003: HOW FAR DID CONGRESS GO?

Sandra E. McKay, Southeastern Louisiana University
smckay@selu.edu
John W. Yeargain, Southeastern Louisiana University
jyeargain@selu.edu
Randall P. Settoon, Southeastern Louisiana University
rsettoon@selu.edu

ABSTRACT

With the growing use of the internet for unsolicited commercial electronic mail (spam), many individuals and businesses are complaining about the time and effort necessary to delete such material from personal and business computers. Although filtering has been tried, it seems the senders of such unwanted mail have found ways around such blocks. To attempt to meet the growing demand for a legal method to control and discourage the unwelcome growth of unsolicited email, bills were introduced in both the House of Representatives and the Senate of the United States to try to regulate such activities.

This paper will examine the Can-Spam Act of 2003 and point out its salient features.

INTRODUCTION

Spam is becoming a growing source of concern among legitimate electronic marketers, businesses, and individuals. There are concerns about the impact of spam on network bandwidth, network storage costs, and user productivity. Spam currently accounts for about 40 percent of all email activity, which is an increase of 32 percent since 2001. Unsolicited commercial electronic mail poses network security problems to government and businesses via viruses and worms. The increasing amount of spam has resulted in a decline in consumer trust of legitimate email marketers. (Findings, Reduction in Distribution of Spam Act, 2003). The receipt of spam results in costs to receivers who cannot refuse to accept such mail, incur costs for storage, and for accessing, reviewing, and discarding such items. The alarming increase in unwanted email will increase monetary costs to Internet access providers, businesses, and nonprofit institutions as they struggle to handle increasing volume and face further expenditures to handle such unwanted growth. This growth is shifting costs from the senders of spam to the Internet access service. In order to avoid liability, spam senders are disguising their addresses to prevent recipients from negatively responding (Findings, Anti-Spam Act of 2003). Despite the fact that Congress enacted legislation to regulate spam, there is concern that it will have limited effect because most of the spam is sent by overseas entities, which are beyond the reach of United States jurisdiction (McCullagh, April 10, 2003).

PROPOSALS

There were two bills in the Senate, two in the House, plus proposals from the Federal Trade Commission to strengthen the ability of the federal government to discourage spam both by civil and criminal penalties. In the Senate, both bills had powerful bi-partisan supporters. The Can-Spam Act was sponsored by Senators Conrad Burns, R-Mont., and Ron Wyden, D-Ore., who serve on the Commerce Committee. The Criminal Spam Act (CSA) was sponsored by Senators Oren Hatch, R-Ut., and Patrick Leahy, D-Vt., who serve on the Judiciary Committee. Both Microsoft and Yahoo supported the Can-Spam bill (McCullagh, D. June 19, 2003). The Can-Spam Act sought to regulate interstate commerce by imposing limitations and penalties on the sending of unsolicited commercial email via the Internet. It gives authority to the Federal Trade Commission (FTC) to enforce its provisions with appropriate regulations. It declares criminal the sending of spam with fraudulent routing information and proposes a fine or imprisonment for not more than 1 year, or both. The use of deceptive subject headings is prohibited. There must be a method for the recipient to opt-out of receiving further spam from the sender which the sender has 10 business days with which to comply. The sender must include in its message a physical postal address. The attorneys-general of the states may enforce the provisions of this act in federal district court in their respective states. The damages may be multiplied by $10 per each separately addressed message with a cap of $500,000, unless the court finds the sender knowingly committed the acts, in which case the court may increase damages up to $1.5 million. Attorney fees may also be assessed if the state is successful in its civil action against the spam sender. The Criminal Spam Act (CSA) would punish repeat spammers with a maximum of 5 years in federal prison and fines up to $25,000 per day. Can-Spam would jail first offenders with up to 3 years and repeat offenders with up to five year terms. The Senate Commerce Committee approved the Can-Spam Act with the provisions that the FTC and Internet service providers could sue spammers who use false email headers, or do not let recipients opt-out, or send spam to email addresses obtained by crawling the web (McCullagh, June 19, 2003).

The two mail House bills in play for controlling spam were the Anti-Spam Act sponsored by 33 Democrats and 20 Republicans and the Reduction in Distribution of Spam Act (RID Spam) sponsored by 19 Republicans and 2 Democrats. The main difference between the two bills was a political one. The Anti-Spam Act would permit class action lawsuits whereas the RID Spam Act expressly prohibited such suits. Trial lawyers favor class action suits and heavily contribute to Democratic candidates. A Common Cause study of the 2000 elections estimated that trial lawyers favored the Democratic Party over the Republican Party by a 40-1 margin for soft money contributions. Since the RID Spam act was sponsored by two Republican committee chairmen, Energy and Commerce - Billy Tauzin and Judiciary - James Sensenbrenner, who control the two committees to which anti-spam legislation was assigned, this was the bill that was favored to make it out of the House. This proposal included criminal sanctions for spammers who use fraudulent headers or send unlabeled pornographic solicitations, but it did not give the FTC as much authority as the Anti-Spam Act. Both bills permitted spammers to send unsolicited bulk email provided an opt-out provision was included. Some critics have noted that this permits email marketers to send spam until the recipient opts-out. So, some liberal Democrats are proposing an opt-in requirement, which is opposed by legitimate commercial marketers, that would forbid any unsolicited commercial email unless a prior business relationship exists (McCullagh, July 9, 2003). This opt-in requirement

has been ruled by the Supreme Court in other cases to be an unconstitutional First Amendment violation whereas the court has approved of less intrusive ways to protect privacy such as posting "No Solicitors or Peddlers Invited" (Schaumburg, 1980). This is why the court will probably uphold the federal Do Not Call statute.

Some legislators attempted to broaden these proposals to include unsolicited marketing messages sent to wireless devices and cell phones using means other than email. This expansion of coverage of the acts would necessitate more time in committee for study, testimony, and drafting. All of the proposed bills exempted from regulation any type of spam from politicians, charitable, religious or nonprofit organizations (McCullagh, July 9).

RESULT

On October 22, 2003, the Senate voted 97-0 to approve the Can-Spam Act (Bridis, 2003). When it reached the House of Representatives it was referred to Representative Tauzin's Energy and Commerce Committee. In short order, it emerged from his committee with amendments that attached the features of his RID Spam bill to the Can-Spam bill. The House voted 392-5 in favor of the bill as amended (Thomas, 2003), and the Senate concurred. President Bush signed the bill into law on December 16, 2003. It became effective January 1, 2004.

As enacted the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 or Can-Spam Act of 2003 provides for criminal penalties of up to five years imprisonment for previous convictions under federal or state law involving multiple commercial electronic mail messages or unauthorized access to a computer system. A fine or imprisonment for up to three years, or both, would be assessed for those convicted of obtaining 20 or more falsified email account registrations, or 10 or more falsified domain name registrations; and the volume of email messages exceeded 2,500 in any 24-hour period, 25,000 during any 30-day period, or 250,000 during any 1-year period. The offender would also forfeit any proceeds, property, or equipment obtained from such offense (Can-Spam Act, Section 4).

Section 5 of the Act (15 U.S.C. 7704) prohibits the transmission of false or misleading information. Thus, header information which includes a domain name or Internet Protocol address which was obtained by false representations is materially misleading. Subject headings which are deceptive as defined by the Federal Trade Commission Act are prohibited. There must be a return address which enables the recipient of commercial email to submit a request not to receive future messages from the sender. This is the opt-out provision. Once the sender receives the opt-out message, it has 10 business days to act upon the request. The sender may not sell, lease, or transfer the addresses of those recipients who have opted out of its commercial email messages. All commercial email messages must contain clear and conspicuous notice that they are advertisements, an opt-out provision, and a valid physical postal address of the sender. It is illegal for a sender of commercial email to obtain recipient email addresses by automated means from an Internet web site or proprietary online service belonging to another person who includes a notice stating that it does not sell or lease its addresses to others for use in sending email messages. The FTC is given the authority to modify the 10-business day period if it deems it necessary for good faith compliance with the opt out provision by commercial senders. Senders of sexually oriented material are required to include in the subject heading notices required by the FTC. No warning is necessary if the

recipient has given prior consent to receive such material. The FTC in consultation with the Attorney-General has 120 days from January 1, 2004, to issue marks or notices to be included in sexually explicit commercial email. These notices will be published in the Federal Register. Thereafter, anyone who knowingly violates this standard shall be fined or imprisoned for up to 5 years or both.

Section 6 of the act (15 U.S.C. 7705) forbids businesses to send commercial email with false or misleading transmission information knowingly through a third party. It is assumed that the business knew of the wrongful intentions of the sender if the business owns a 50 percent or greater interest in the person that violated this section.

Section 7 (15 U.S.C. 7706) defines violations of this act as unfair and deceptive practices and authorizes the FTC to enforce violations as if they had occurred under the Federal Trade Commission Act (15 U.S.C. 57). Other federal agencies are given authority to enforce these provisions over commercial email senders under their respective jurisdictions. So, national banks are regulated by the Office of the Comptroller of the Currency; savings associations by the Director of the Office of Thrift Supervision; federal credit unions by the Board of the National Credit Union Administration; brokers and dealers of securities by the Securities and Exchange Commission; insurance companies by state insurance authority; air carriers by the Secretary of Transportation; radio and television stations by the Federal Communications Commission. The FTC may use its usual powers against those who violate this act. Thus, it may issue cease and desist orders and injunctions without having to prove intent of the party charged with a violation. The attorney general of a state may bring a civil action on behalf of the state's citizens in a federal district court in the state. The damages shall be determined by multiplying the number of violations (each separately addressed message received by a state resident) to a maximum of $250. The maximum fine cannot exceed 2 million dollars unless the court finds aggravating circumstances, such as willful violation, in which case the damages may be increased to up to three times the damages. The court may also award attorney fees to the state for a successful action. However, before the state attorney general can bring an action he must notify the FTC or appropriate federal agency. The FTC shall have the right to intervene and to remove the action to another United States district court. If there is an FTC action currently before the court, the state attorney general may not bring an action against a defendant already named in the FTC action. Internet access providers may also bring actions against those who violate section 5 (15 U.S.C. 7704) of this act to enjoin further violations and recover damages up to $100 per each separate address transmitted over its facilities. The court may also find aggravating circumstances and increase the damage award up to three times. Attorney fees may also be recovered by the successful Internet access provider.

Section 8 (15 U.S.C. 7707) exercises the doctrine of preemption. It specifically states that the Can-Spam Act supersedes any state statute or regulation covering commercial email.

Section 9 (15 U.S.C. 7709) orders the FTC to report back to Congress within two years regarding the effectiveness and enforcement of the Can-Spam Act and to make recommendations for any modifications. The Congress specifically wants the report to address changes in devices through which consumers receive email, how to handle commercial email that originates in other nations, and options for protecting children from obscene email.

Section 10 (15 U.S.C. 7710) orders the FTC to send to the Congress within 9 months from date of enactment (December 16, 2003) a report that sets out a method for rewarding those persons

who give information about violations of the act. The reward should be not less than 20 percent of the civil penalty to the person who identifies the wrongdoer and supplies information that leads to the successful collection of a civil penalty by the FTC. Also, within 18 months the FTC shall report to Congress a plan for requiring commercial email to be identified from its subject line by means of compliance with Internet Engineering Task Force Standards the use of the characters "ADV"(advertisement) in the subject line or other comparable identifier.

Section 11 (15 U.S.C. 7711) authorizes the FTC to issue regulations to implement the act. However, the FTC is not authorized under section 5(a)(5)(A) covering identification of advertisement, opt-out provision, and physical postal address of sender to include any specific words, characters, marks, or labels in commercial email or to specify any particular part of the message to include such requirements, e.g., subject line or body.

Section 12 (15 U.S.C. 7712) orders the Federal Communications Commission (FCC) in consultation with the FTC to issue rules within 270 days to protect consumers from unwanted mobile service commercial messages. The FCC shall give subscribers of commercial mobile services a way to avoid receiving commercial messages unless the subscriber has given prior authorization to the sender; allow subscribers to indicate via their mobile service a desire not to receive future commercial messages from the sender; or allow subscribers to opt-out at time of subscribing and in any billing.

CONCLUSION

By its exercise of the preemption doctrine in the Can-Spam Act the federal act nullified state statutes which sought to control spam in some individual states. The states which had passed spam acts were Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Michigan, Missouri, Nevada, New Mexico, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Utah, Virginia, Washington, West Virginia, Wisconsin, and Wyoming. These states which had mandated "ADV" on the subject line must now wait for the FTC to publish its regulations(Spam laws).

REFERENCES

Anti-Spam Act of 2003, H.R. 2515, 108th Congress.

Bridis, Ted (2003, October 23). Senate approves limits on 'spam', Baton Rouge *Advocate*, 5A.

Can-Spam Act of 2003, S. 877, 108th Congress. Retrieved February 29, 2003, from http://web.lexis-nexis.com/universe/document .

McCullagh, D. (2003). Antispam bill gets a second go. Retrieved April 10, 2003, from http://news.com.com/2110-1028-1019430.html .

McCullagh, D. (2003). Spam fight divides on party lines. Retrieved July 9, 2003, from http://news.com.com/2100-1028-1024385.html .

McCullagh, D. (2003). Spam goes through Capital mincer. Retrieved June 19, 2003, from http://new.com.com/2100-1028-1019430.html .

Reduction in Distribution of Spam Act of 2003, H.R. 2214, 108th Congress.

Schaumburg v. Citizens for Better Environment (1980). 444 U.S. 620, 63 L.Ed. 2d 73, at 89.

Spam laws. Retrieved February 23, 2003, from http://www.spamlaws.com/statelaws .

Thomas Voting Reports (2003, November 23). Louisiana tally, Baton Rouge *Sunday Advocate*, 17A.

THE IMPACT OF DISCONTINUOUSLY INNOVATIVE TECHNOLOGICAL MARKETS ON CONSUMER SATISFACTION

Newell D. Wright, James Madison University
wrightnd@jmu.edu
Val Larsen, James Madison University
larsenwv@jmu.edu
Irvine Clarke III, James Madison University
clarkeix@jmu.edu

ABSTRACT

Marketers in discontinuously innovative technological markets face special difficulties in meeting consumer needs and creating consumer satisfaction. It is not simply a matter of a market orientation, nor is it adequately explained by the expectancy/disconfirmation theory of consumer satisfaction (Oliver 1980). Marketers instead must deal with technological, technemic, and network constraints that can make it nearly impossible to satisfy most consumers when a product is first introduced. Since product transparency and functionality are generally limited, technophilic consumers with a high gizmo orientation should be the initial target. Companies should take care to match the product, at each stage of its introduction into the marketplace with a target group whose expectations and typical satisfactions are fitted to the product's current degree of transparency and functionality.

The authors would like to thank the Commonwealth Information Security Center at James Madison University for supporting this research.

Authors' Index

Allen, C.A 1
Clarke, I 11
Etheridge, H.L. 3
Hsu, K.H.Y 3
Larsen, V 11
McKay, S.E 5
Settoon, R.P 5
Wright, N.D 11
Yeargain, J.W 5