devised by the plaintiff in those proceedings, and not a computer program as such. This line of reasoning had no bearing here where there was no doubt that the parties were concerned about competing software products.

It may well be that these observations of the Court are not material to the findings it made, which were based upon the paucity of the evidence present. It is troubling, however, that in the face of such extensive identity between the two programs in question, and the fact that it took a considerable period of time to create E-call24.com, but only a very short period to create Phone Wizard, there was still no finding of infringement. It may be time that the decisions of the High Court in *Data Access* and *Autodesk* are revisited.

* Telephonic Communicators International Pty Limited v Motor Solutions Australia Pty Limited and others [2004] FCA 942 (21 July 2004)

1 See *AGL v Shortland* (1989) 17 IPR 99; *Telstra Corporation Limited* v *Royal & Sun Alliance Insurance Australia Limited* [2003] FCA 786 (1 August 2003), derived from older cases such as *Harman Pictures NV v Osborne* [1967] 1 WLR 723 [[1967] 2

2 All ER 324] (Ch) and *Zeccola v Universal City Studios Inc* (1982) 67 FLR 225 [46 ALR 189] as well as even older decisions.

3 Pars 25 - 26

4 Par 27, citing *Data Access Corporation* v *Powerflex Services Pty Limited* (1999) 202 CLR 1; 166 ALR 228; 73 ALJR 1435; 45 IPR 453, itself based upon *Autodesk Inc v Dyason* (1992) 173 CLR 330; 66 ALJR 233; 104 ALR 563; 22 IPR 163; [1992] AIPC 38,182 (¶90-855); see also *Autodesk Inc v Dyason [No 2]* (1993) 176 CLR 300; 67 ALJR 270; 111 ALR 385; 25 IPR 33.

5 See *University of London Press* v *University Tutorial Press* [1916] 2 Ch. 601

6 per Peterson J at 608

7 See *Kenrick* v *Lawrence* (1890) 25 QBD 99, but note *Desktop Marketing Systems Pty Ltd* v *Telstra Corporation Limited* (2002) FCR 491; (2002) 192 ALR 433; (2002) 55 IPR 1 (Full Court - Leave to appeal refused - Unreported, High Court 20 June 2003; per Hayne and Callinan JJ)

8 (2001) 114 FCR 324

9 Par 36

10 see *DP Anderson & Co Ltd v The Lieber Code Co* [1917] 2 KB 469; *Ager v Collingridge* (1886) 2 TLR 291

The CAN-SPAM Act of 2003: An end to Unsolicited Email?

Dr. John P. Geary & Dr. Dinesh S. Dave, Appalachian State University, North Carolina

John P. Geary is from the Department of Finance, Banking and Insurance, and Dinesh S. Dave is from the Department of Computer Information Systems, of John A. Walker College of Business, Appalachian State University in Boone, North Carolina.

Introduction

The rapid increase in unsolicited commercial electronic mail (SPAM) on the Internet has not only proven an annoyance to users but has the potential to impact the efficiency of global commercial transmissions on the Web. Unsolicited email poses a particular problem for Internet service providers (**ISPs**) who have to respond to customer complaints and the possible loss of business. Many Internet access services have been forced to add increased infrastructure and incur the attendant costs. Much of the unwanted mail contains deceptive and untruthful claims about advertised goods and services that confuse consumers and contribute to fraudulent activities on the Web. Responding to these problems, many states enacted legislation whose purpose was to protect recipients from deceptive spam and decrease its volume on the Internet. These state statutes were not that effective because of consistency and jurisdictional issues. What was needed was a national effort to control the onslaught of unsolicited email and to discourage professional bulk mailers or "spammers" with legislation that contained severe penalties. In this paper, we examine pertinent sections of the CAN-SPAM Act, its probable impact on commercial advertising, and investigate the Act's efficiency.

Discussion

The CAN-SPAM ACT:

In order to address the issues of unsolicited mail on the Web, Congress passed the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," Pub. L. No. 108-187 **(CAN-SPAM Act)** and President Bush signed it into law on December 16, 2003. It went into effect on January 1, 2004. Section 2(a) of the CAN-SPAM-Act sets out the findings and concerns of Congress relating to unsolicited commercial electronic mail and its impact on commerce and the Internet.

The following are the concerns and findings of the United States Congress:

(1) Electronic mail has become an important means of communication utilized by many Americans and offers unique opportunities for the growth of global commerce.

(2) The rapid increase in unsolicited commercial mail not only results in storage and time costs to recipients but much of it contains fraudulent or deceptive information.

(3) Some unsolicited email contains sexually explicit materials that many recipients find offensive.

(4) The increasing volume of such unsolicited mail can impose significant monetary costs on Internet servers and access providers, and other commercial and non-profit organizations.

(5) Many senders of bulk unsolicited email practice techniques to disguise the source and subject

matter of such mail and obtain electronic mail addresses using devious means.

(6) Some senders of mail provide no mechanism for recipients to unsubscribe or "opt out" of receiving future messages, or refuse to honour such requests.

(7) Federal legislation will not solve the problem alone; there must be improvements in technology and cooperation with other countries.

The CAN-SPAM Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content of an Internet web site operated for a commercial purpose)".[1] This is a broad definition and seems to apply whether or not the recipient requested such information. Transactional and relationship messages are excluded. These particular types of messages include confirmation of a previous commercial transaction, warranty or recall notices, account balance information and product updates or upgrades.[2] The Act applies to any "sender" who "initiates [a commercial electronic mail message] and whose product, service or Internet web site is advertised or promoted by the message".[3] Political and charitable messages are not covered under the Act.

The CAN-SPAM Act amends Chapter 47, Title 18 of the United States Code to make it a crime to access a protected computer without authorization and transmit multiple electronic mail messages with the intent to mislead recipients as to their origin. This makes it unlawful to transmit non-traceable messages in this context. Furthermore, it is specifically unlawful to materially falsify header information[4] or to falsify the identity of the registrant for five or more electronic mail accounts or two or more domain names.[5] Offences are punishable by a fine or imprisonment for up to five years, or both.[6]

Major Protections under the CAN-SPAM Act:

Section Five of the Act sets out the major protections for commercial email users and recipients. These are as follows:

(1) It is unlawful for a sender to transmit commercial, transactional or relationship messages that contain header information that is materially false or misleading. Commercial email that contains a subject heading that is likely to mislead the recipient about a material fact regarding the contents of the message is prohibited.[7]

(2) A commercial email message must contain a functioning return email address conspicuously displayed which the recipient can use to request not to receive future email. The return address must remain functioning for at least thirty days after the initial transmission.[8] This "opt out" provision allows the recipient to unsubscribe and request to receive no further messages. The sender must comply with the request within ten business days after receipt of such request.[9]

(3) All commercial email messages must include:

  (a) clear and conspicuous notice that the message is an advertisement;

  (b) disclosure that the recipient may "opt out" of further messages; and

  (c) the postal address of the sender. The name of the sender is not required. This provision does not apply if the recipient has given prior affirmative consent to receive such messages.[10]

(4) In an attempt to discourage bulk mailers, the Act defines as an aggravated violation the use of "harvesting" of email addresses from an Internet web site or an online service operated by another person. Aggravated violations carry additional civil and criminal penalties.[11]

(5) Sexually oriented material transmitted by email must contain in the subject heading a warning of its contents as stipulated by the Federal Trade Commission. In order to view the material, the recipient must take some further action to access it. This is to prevent the receipt of such material when there is no consent.[12]

Implications of the Act:

Businesses may be liable under the act if they allow the promotion of trade or business by a third party who uses false or deceptive header information in the advertisement. Liability would apply if the business knew or should have known that its goods or services were being promoted by such a message. Additionally, the business must receive or expect to receive an economic benefit from the advertising and take no reasonable action to prevent its transmission. Commercial entities must investigate third party advertising of their products or services and take proper precautions.[13]

Violation of the CAN-SPAM Act is an unfair or deceptive practice enforced by the FTC or certain other federal agencies with specific jurisdiction. The Act carries criminal and civil penalties. Private individuals have no standing to sue under the Act but the Attorney General of each state may bring a civil action on behalf of state residents for actual monetary loss or statutory damages, whichever is greater.[14] Statutory damages are set at up to $250 per prohibited email, not to exceed $2,000,000. The court may increase the damage award by an amount of not more than three times if it is determined that the violations were aggravated and wanton. The court at its discretion may award costs and attorney's fees.[15] An Internet service provider harmed by a violation may bring a civil action for actual or statutory damages. Statutory damages are computed by multiplying the number of violations by up to $100 (in some instances $25), not to exceed $1,000,000. Treble damages and attorney's fees are available.[16]

Civil Action

The four major ISPs in the United States wasted little time in filing

lawsuits under the CAN-SPAM Act.[17] This anti-spam alliance consists of EarthLink, America Online, Microsoft and Yahoo. EarthLink filed a typical type of civil action in October 2004, charging the defendants with deceptive practices in transmitting millions of emails advertising prescription drugs and mortgage rates. EarthLink alleges that the defendants violated the CAN-SPAM Act by falsifying email addresses, failing to include the sender's email address, not providing an "opt out" option, selling consumer email addresses and using automated programs to produce email addresses (dictionary attacks). EarthLink is seeking injunctive relief and damages against the two spammers, hoping to put them out of business.[18]

Criminal Action

There have been state criminal prosecutions of spammers for violating state anti-spam laws. Two North Carolina residents were found guilty on three felony counts for violating Virginia's anti-spam law. The Virginia law is similar to the CAN-SPAM Act in that is prohibits fraudulent email and untraceable routing information. A New York State Court found a defendant guilty of sending 850 million spam messages using stolen identities in violation of New York's identity theft law. The defendant was sentenced to three and a half to seven years in prison.[19] The CAN-SPAM Act now preempts state law that regulated commercial electronic mail, with the exception of fraud or computer crimes. The extent of federal preemption in this area will have to be determined by the courts.

The FTC filed the first criminal charges under the CAN-SPAM Act against two spam operations for allegedly including false and deceptive claims in commercial email messages, attempting to obscure their identities and not including "opt out provisions" in the messages.[20]

The Act directs the FTC, no later than twenty-four months after the date of enactment, to submit a report on the effectiveness and enforcement of the legislation. Topics that must be included in the report are:

- an analysis of technological and marketplace developments that may impact the effectiveness of the Act;
- how commercial electronic mail should be addressed if it originates or is transmitted in other countries and suggestions for initiatives that the U.S. Government could pursue through negotiations with other nations; and
- recommendations for protecting consumers and children from viewing obscene or pornographic material.[21]

In addition, Congress specifically directs the Federal Communications Commission, in consultation with the FTC, to issue regulations within 270 days to protect consumers from unsolicited mobile service commercial messages.[22]

Conclusions

The CAN-SPAM Act, in existence for just over a year, has come under increasing criticism. MX Logic reports that in 2004, 97% of spam failed to comply with the Act and the volume of spam increased, amounting to 77% of all email traffic.[23] The Act has cleared up some ambiguities and put the commercial and advertising community on notice of what is expected of them. Although litigation under the Act has been commenced, to date there is still no case law interpreting the statute or its application. While there have been prosecutions under state law, much of this state legislation has been preempted, with the exception of certain anti-fraud provisions.

One of the problems in regulating spam is that unsolicited email is transmitted on the World Wide Web which is international in scope. The CAN-SPAM Act has no jurisdiction abroad and a great deal of spam comes from overseas. In addition, spammers can outsource messages to multiple providers located out of the United States or gain access to an innocent party's computer to transmit millions of messages. The lure of spam is that it is easy and inexpensive to transmit. One commentator has observed: "A spammer can send and email advertisement to one million people at a cost of only $100, he or she will make a 10% profit if just 11 customers respond and pay $10 each".[24]

The heart of the CAN-SPAM Act is deception. Most legitimate marketers have or are in the process of complying with the law. It needs to be emphasized that spam is lawful but senders need to be mindful of the prohibitions against fraud, the required disclosure information that is to be included in the message and the inclusion of an "opt out" mechanism. There are software programs available that can assist "high volume emailers" in complying with requests to "opt out" of further mail. Samples of spam related transactions should also be preserved in the event of lawsuits.[25] As litigation increases and the required FTC reports are filed with the US Congress, the effectiveness of the Act will be gauged and new methods to control unsolicited email considered. Many recipients have turned to technology for help and are using filters and other devices to exclude unwanted messages and this may well be the preferred method rather than extensive legislation and regulation. Certainly, international cooperation will be required to combat the increased flow of unwanted email messages.

1 CAN-SPAM Act, Sec. 3(2)(A)

2 CAN-SPAM Act, Sec. 3(17)(A)

3 CAN-SPAM Act, Sec. 3(16)(A

4 The term 'header information' is defined to mean "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message", see Sec 3(8).

5 CAN-SPAM Act, 4,(a)(1)-(4).

6 CAN-SPAM Act, 4,(b)

7 CAN-SPAM Act, 5(a)(1)-(2).

8 CAN-SPAM Act, 5(a)(3).

9 CAN-SPAM Act, (5)(a)(4).

10 CAN-SPAM Act, 5(a)(5).

11 CAN-SPAM Act, 5(a)(6)(b).

12 CAN-SPAM Act, (5)(a)(6)(d)(A)

13 CAN-SPAM Act, 6(a)(1)(2)(3).

14 CAN-SPAM Act, 7(f)(1).

15 CAN-SPAM Act, (7)(f)(3)

16 CAN-SPAM Act, (7)(g)(1)(3).

17 Washington Post, 4 January, 2005, LEXIS/NEXIS: http://web.Lexis-Nexis.com/universe/docu...vb&_md5=b6e4885519d764b54ab4534c9741adb6

18 PR News Wire Association, 28 October 2004, LEXIS/NEXIS: http://web.Lexis-Nexis.com/universe/docu...VA&_md5=aecce21d74917b44d37cc38c2cb9c17f

19 Facts on File World News Digest, 31 December 2004, LEXIS/NEXIS: http://web.Lexis/Nexis.com/universe/docu... V6&md5=8103b9672551011ef375cf04b5992c32

20 The Computer and Internet Lawyer, July 2004, LEXIS/NEXIS: http://web.Lexis-Nexis.com/universe/docu...Vb&_md5=01f4e2e7bf9486d5637efb25bd04646c.

21 CAN-SPAM Act, Sec. (10)(b).

22 CAN-SPAM Act, Sec. 14(b).

23 Business Wire, 3 January 2005, LEXIS/NEXIS: http://web.Lexis-Nexis.com/universe /docu...Vb&_md5=b419b94b241be69c164c8cc359ca2d9c

24 The Internet News Letter, 4 November 2004, LEXIS/NEXIS: http://web.Lexis-Nexix.com/univese/docu...VA&_md5=27aa5ab05b0d683190abc5b84699796d

25 Legal Times, 1 November 2004, LEXIS/NEXIS: http://web.Lexis-Nexis.com/universe/docu...VA&_md5=0031789efdcb46222c06c65623cd27c8

Review: Promises to Keep: technology, law and the future of entertainment*

Rob Bhalla, NSW Crime Commission

Rob Bhalla is a solicitor at the NSW Crime Commission.

Some time soon, the mere fact that you possess a gold credit card could mark you out as someone forced to pay substantially more for that next Kylie album, than would other citizens content with rather less shiny forms of plastic.

Welcome to the world of extreme price discrimination for digital content, one of the "culturally corrosive" scenarios mapped out by William W. Fisher, the Hale and Dorr Professor of Intellectual Property Law at Harvard Law School, in his book, *Promises to Keep: technology, law and the future of entertainment* (Stanford Law and Politics 2004).

In an effort to avoid such a result, and to restore order to what he sees as rapidly disintegrating intellectual property protection for digital entertainment, Fisher has produced a detailed analysis of the "alternative compensation system". The proposal is a veritable free-for-all, for the consumer at least.

Digital content would be made freely available to consumers using broadband Internet connections to download content to use as they saw fit. Freed from just passively consuming content, Fisher paints a future where instead, consumers are thoroughly engaged – changing it, editing it, incorporating it into their own works and then even redistributing it. He describes this "semiotic democracy" as one where "the public at large ... participate ... actively in the construction of their cultural environment."

Fisher advocates that the current system, whereby artists are remunerated (sometimes barely) from the sale of CDs and DVDs, be replaced by a system where artists are paid according to how often their songs or movies are played or watched. A government body would determine whose work was being consumed, and then distribute funds raised by a tax on, for example, broadband charges and CD burners.

Fisher, writing in the United States (US), readily acknowledges and explores the problems that this proposal would encounter. Among them, the fact that a government body is involved in remunerating artists, including sometimes controversial artists (think pornography); and, perhaps most fatally, that it seems impossible to imagine Congress, responsible for the *Digital Millennium Copyright Act*, or the entertainment industry as currently constituted, acquiescing to such heresy. Indeed, the RIAA is already preparing ammunition ("Do you want Government to set the price for music – for Beethoven?"), and Bill Gates opined in a recent interview, "There are some new modern-day sort of communists who want to get rid of the incentive for musicians and moviemakers and software makers under various guises."

Amid the name-calling, Fisher has written a highly commendable book, accessible to both the professional and non-professional reader; like any good tutor, his enthusiasm for the subject is infectious. Along the way toward describing the centrepiece alternative compensation system, Fisher also details and discusses other (perhaps more likely) outcomes.

Given the alignment of Australian and US intellectual property protection rules under the recent Free Trade Agreement, it will be important for practitioners here to be aware of, and participate in, the debate in the US. There is no doubt that this book represents an important contribution to that debate, which will only intensify as both the US Supreme Court (in the *Grokster* litigation) and the Australian Federal Court (the *Kazaa* litigation) get ready to rule on peer-to-peer file sharing networks during 2005.

* Review of William W. Fisher's Promises to Keep: technology, law and the future of entertainment (Stanford Law and Politics 2004)