



Journal of Information, Law & Technology

**Conference Paper**

**Anti-spam: a Comparative Appraisal of Canadian, European Union,  
and South African Regulatory Regimes**

Professor OS Sibanda  
College of Law, University of South Africa  
[sibanos@unisa.ac.za](mailto:sibanos@unisa.ac.za)

**Lex Informatica Conference, 21<sup>st</sup> – 23<sup>rd</sup> May 2008  
Pretoria, South Africa**

This is a **conference paper** published on 08 January 2009.

Sibanda, OS., 'Anit-spam: A Comparative Appraisal of Canadian, European Union, and South African Regulatory Regimes', 2008(2) *Journal of Information, Law & Technology (JILT)*, <[http://go.warwick.ac.uk/jilt/2008\\_2/sibanda](http://go.warwick.ac.uk/jilt/2008_2/sibanda)>

## **Abstract**

The huge commercial opportunities created by electronic technology and cyberspace are paralleled by certain risks and issues. A particular issue dealt with in this paper is unsolicited commercial communications or “spam” as it is commonly called. There is a continuing need for consumers to be protected from unwanted spam. The methodology of this paper is based on a comparative survey of the legislative and regulatory frameworks governing spam in Canada, the European Union, and South Africa.

## **Keywords**

Consumers, Commercial, Internet, Opt-out, Opt-in, Regulation, Spam

## **1. Introduction**

The use of electronic technology including e-mails, cellular phones, the Internet and cyberspace as contracting media in the modern commercial world is forever gaining momentum (Tang, 2007, p 42). The huge opportunities created by electronic technology have been paralleled by some innovative marketing practices. Consumers are flooded with countless numbers of business offers from all over the world, almost on a daily basis and many of which are unsolicited (Tladi, 2008, p 178). Different terms have been used to refer to spam. Geissler (2004, pp 24-31) uses the term such as ‘Unsolicited Bulk E-mail’ (UBE); ‘Unsolicited Commercial E-mail’ (UCE). From the onset the author would like to point out that the word ‘spam’ will, in this text, be used in its narrow sense to refer to unsolicited commercial communication (UCC).

According to Polanski (2007, p 403), unsolicited commercial communications, spam as it is often called, has become a global plague. The communication is regarded as ‘unsolicited’ because there exist no prior relationship between the recipient and the sender to justify such communication. Moreover, the recipient never explicitly agreed to receive such communication (generally, Solkin, 2001, pp 325-384). Put simply, the recipient has not given permission for the unsolicited communication to be sent to him or her.

There is a continuing need for consumers to be protected from unwanted or malicious spam by every national jurisdiction through more effective means, including more effective legislative intervention. This paper compares and examines the legislative and regulatory systems of spam in Canada, the European Union, and South Africa. The key issue in this survey is how these jurisdictions deal with the problem of errant spamming. Minimal or non-government intervention policy in favour of industry self-regulation, which was once the preferred method in Canada, for example, may prove to be ineffective. Since the requirements for the presentation of this paper does not allow an in-depth enquiry into all the measures designed to combat spam, the author will not deal with various technical, educational and administrative efforts to prevent spam.

## **2. Problems Created by Spam**

It has become increasingly difficult to tolerate spam, and to control and prevent it, even by using the most sophisticated of spam filters. The spammers, too, have become sophisticated and may easily bypass these filters, even the revered Optical Character Recognition (OCR) technology, which has been created to translate pictorial or graphical spam into computer fonts (Polanski, 2007, p 406).

The problems created by spam and the costs associated with combating it are clearly described as follows: (a) the recipient pays far more, in time and trouble as well as money, than the sender does (unlike unrequested advertising through the postal service); (b) the recipient must take the time to request removal from the mailing list, and most spammers claim to remove names on request but rarely do so; (c) many spammers use intermediate systems without authorization to avoid blocks set up to avoid them; (d) many spam messages are deceptive and partially or entirely fraudulent; and (e) the recipient ends up with the problem of technological spam filters that also block non-spam messages (Levine, <<http://spam.abuse.net/spambad.html>>; Delio, 2000, <<http://www.wired.com/news/infostructure/0,1377,61945-2,00.html>>). In South Africa the spam is reported to cost business “between R7 billion and R13 billion yearly in lost productivity” (Tladi, 2008, p 183).

## **3. Spam Regulatory and Legislative Measures**

### **3.1 South Africa**

#### **3.1.1 Spam Specific Legislative Interventions**

E-commerce in South Africa is governed primarily by the Electronic Communications and Transactions Act (ECTA) 25 of 2002, which came into force on 30 August 2002, as South Africa’s first comprehensive e-commerce legislation (Sibanda, 2008, p 321). The process of establishing the country’s first e-commerce law was initiated in 1999 by the Department of Communications, which sought to identify and determine the existing contract-specific or related legislation and decide on its appropriateness to e-commerce (ibid, p 322). The existing legislation was found not to adequately cater for e-commerce. The ECTA is modelled partly on the United Nations Commission on International Trade Law Model Law on E-Commerce (UNCITRAL Model Law) of 1996, which provides national legislatures with a ‘basic legal framework’ for enacting or revising their e-commerce laws (Faria, 2004, p 530; Sibanda, 2008, p 322). The ECTA aims to establish a formal regime and legal framework in order to define, develop, govern and regulate electronic commerce, and to protect consumers of e-commerce services (Sibanda, 2007, p 260; Sibanda, 2008, p 322).

Though not a specific anti-spam legislation, the ECTA sets out certain requirements that unsolicited communication must meet. Section 45 of ECTA provides as follows:

‘45. (1) Any person who sends unsolicited commercial communications to consumers, must provide the consumer

- a) with the option to cancel his or her subscription to the mailing list of that person; and
- b) with the identifying particulars of the source from which that person obtained the consumer's personal information, on request of the consumer.

(2) No agreement is concluded where a consumer has failed to respond to an unsolicited communication.

(3) Any person who fails to comply with or contravenes subsection (1) is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1).

(4) Any person who sends unsolicited commercial communications to a person who has advised the sender that such communications are unwelcome, is guilty of an offence and liable, on conviction, to the penalties prescribed in section 89(1)'.

It is clear from the provisions of section 45 of ECTA that, in South Africa, spamming is not per se illegal. The ECTA employs an approach of regulation rather than the prohibition of spam, subject to some penalties, including 12 months imprisonment, for non-compliance with the requirements of section 45(1). Be that as it may, the regulatory approach in South Africa remains unsatisfactory. It is for this and other reasons that there has been a call for the enactment of standalone anti-spam legislation (Geisler, 2004, p 121).

Section 45(1) of the ECTA only regulates the 'unsolicited commercial communications to consumer'. In effect, this means that any unsolicited communication that is not regarded as 'commercial' will not fall within the ambit of the regulation. What does the word 'commercial' entail? 'Commercial' is an elusive and fluid concept. A communication offering a commercial transaction will obviously be covered by the ECTA. But what about a communication which does not amount to offering a contract, but which has some vague commercial features? Furthermore, the regulatory protection of section 45 cannot be extended to legal persons. This is because the ECTA defines a 'consumer' as 'any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier'. The law as it now stands effectively says that a legal person, for example a company that receives unsolicited commercial communication is precluded from having recourse to section 45 of the ECTA.

In addition to the fact that the ECTA does not clearly define spam, a disconcerting characteristic of South African spam regulation is that it maintains an 'opt-out' approach. The ECTA leaves it to the recipient to opt to cancel communication of unsolicited communication (s 45(1) (a)). Perhaps this state of affairs may be explained by the fact that the ECTA primarily focuses on the functional equivalence of e-commerce and paper-based commerce. Also, spam was not viewed as a serious problem in South Africa when the ECTA was drafted in 2001. Be that as it may, opting out of unsolicited e-mails may be a costly onus for the consumer to discharge, and does not act as a real disincentive to the spammers. There is some solace in the fact that, in terms of section 45(2) of the ECTA, inaction by a consumer who has been bombarded with unsolicited communication shall not be deemed as acquiescence to the conclusion of a contract with a sender.

That said, South Africa's approach to spam ignores the fact that spam is a growing menace in South Africa, and can be offensive and intolerable. For example, an interview study conducted with scholars at the University of Cape Town, South Africa on six Internet Service Providers (IPS) averaged the amount of spam received daily to be approximately 50% of incoming email. The study also revealed that 51% of the people interviewed found spam offensive (Chigona, Bheekun, Spath, Derakhashani and Van Belle, pp 287-288 <<http://www.commerce.uct.ac.za/InformationSystems>>). What aggravates the

situation is that responding to spam is costly to recipients. And the problem becomes more costly and time-consuming if it involves having to clear the receiving system of viruses. Unfortunately, technology service providers in South Africa, such as the Wireless Application Provider Association (WASPA) which regulates the South African SMS messaging industry, had eagerly implemented the opt-out approach as the preferable approach as contained in section 5 of its Code of Conduct (Wireless Application Service Providers' Association Code of Conduct, 2008 <[http://www.waspa.org.za/code/waspa\\_coc\\_6.1.pdf](http://www.waspa.org.za/code/waspa_coc_6.1.pdf)>)

### **3.1.2 General Legislative Interventions**

The shortcomings of the ECTA anti-spam regulations notwithstanding, there are several other approaches that may be followed in order to deal with spam in South Africa. One such approach is treating spam as an unlawful business practice. Section 49 of the ECTA allows consumers to lodge a complaint for an unlawful business practice with the Consumer Affairs Committee established under the Consumer Affairs (Unfair Business Practices) Act of 71 of 1988. In the absence of specific anti-spam legislation, the practice has been to look to general laws which have a bearing on spamming and related activities, or which may be interpreted as a means of combating spam.

A spammer may also be prosecuted for statutory forgery under the provisions of the ECTA and other legislation. In terms of section 86(2) of the ECTA, any intentional and authorized interference with data in a manner that causes such data to be modified amounts to a criminal offence. In a situation whereby a consumer has opted out of the unsolicited communication but still continues to receive such communication to an extent that such communication crashes or jams the e-mail server, for example, the spammer may be charged with cyber crime. This is because the incessant communication and consequent server crash amounts to unauthorized interference with data which under section 86(2) of the ECTA, is an offence.

The same incessant conduct by the spammer may fall foul of the law of nuisance. Though the term nuisance, which is derived from English law, is traditionally used in the context of the repeated unreasonable use of land by one neighbour at the expense of another, it may be extended to cover repeated spamming activities. After all, spamming may well be, in essence, the unreasonable use of electronic media which, as in the case of land, occurs at the expense of another in the form damage to the server. In this respect, it is damage that is emphasised, because damage is the essential element of the law of nuisance.

## **3.2 Canada**

### **3.2.1 Spam Specific Legislative Interventions**

Canada is yet to enact an anti-spam legislation. However, in January 2003 Industry Canada released a discussion paper, exactly 42 months after it had released its first position paper on spam in January 1999. The discussion paper shone a light on the possibility of anti-spam legislation in Canada, and marked the jettisoning of Canada's 'hands-off' spam policy. The discussion paper was followed in 2004 by the unveiling

of the anti-spam action plan (Industry Canada, 2004 <[http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h\\_gv00246e-htm](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e-htm)>), which set the foundation for the establishment of the national anti-spam task force. In 2005 the task force released its recommendations on anti-spam legislation for Canada.

### 3.2.2 General Legislative Interventions

In the absence of anti-spam specific legislation, the practice has been to look to general laws which have a bearing on spamming and related activities, or which may be interpreted as a means of combating spamming. In Canada, this includes the following Acts: the Competition Act: Revised Statutes of Canada 1985, C-34, which prohibits deceptive practices through information that is ‘false or misleading in material respect’ with a view to promoting goods or business interests; the Telecommunications Act of 1993, in so far as it empowers the Telecommunications Commission, which interestingly has powers equivalent to those of the Canadian superior courts in terms of section 55(c), ‘to prohibit...the provision of unsolicited telecommunications to the extent that the Commission considers it necessary to prevent undue inconvenience or nuisance...’ (s 41); and several provisions of the Criminal Code 1985 including section 380, which resembles the infamous Nigerian 491 scam that are designed to combat defrauding of ‘any property, money or valuable security or any service’, and section 372(1), which covers the dissemination of false and injurious messages through a ‘letter, telegram, telephone, cable, [and] radio’.

In its first criminal spam case, *R v Hamilton*<sup>1</sup>, Canada unsuccessfully tried to prosecute, under section 464 of the Criminal Code, a spammer who sent e-mails offering to sell information on how to make homemade bombs, how to generate credit card numbers, and how to break into private homes. The problem with the criminal approach to spam is that such a case needs to be dealt with first as an ordinary criminal offence and the proscription of the offence should be satisfied. The Crown in *R v Hamilton* was unsuccessful because it could not prove the intent element of the crime. According to the trial court, the spammer did not really intend for the recipients of his mail to use the information. Moreover, the spammer’s motivation was money and not crime, as required by section 464 of the Code. The trial judgment, and a similar judgment by the Court of Appeal for Alberta ((2003), 25 Alta (4th ) 1, 2003 ABCA 255) were recently confirmed by the Supreme Court of Canada in *R v. Hamilton*<sup>2</sup>, when it dismissed the Crown’s further appeal.

## 3.3 European Union

### 3.3.1 Spam Specific Legislative Interventions

The European Union is one of the few regions that have overcome the dearth of regulation of Internet advertising. Moreover, as yet there exist no Internet-specific regulations that may be adapted to deal with spamming activities. Commercial communication and advertising is dealt with under the Directive 2000/31/EC on electronic commerce. In a provision that may be construed as equating commercial

---

<sup>1</sup> (2002) 3 Alta. L.R (4th) 147, 2002 ABQB 15

<sup>2</sup> [2005] 2 S.C.R. 432, 2005 SCC, par. 79-86

communication with advertising, the Directive defines 'commercial communication' as 'any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing commercial, industrial or craft activity or exercising a regulated profession'. This Directive should be read with directives on misleading and comparative advertising (OJ L 149/22 11.06.2005; OJ L 250/17 19.09.1984).

The Directive on electronic commerce permitted spam, subject to a simple condition that spammers shall make their e-mails clearly identifiable as spam and to enquire whether a person was listed in the opt-out register before sending such a person an unsolicited mail. According to Polanski (2007, p 404), the spam opt-out registers were 'unfortunate' because they 'serve mainly as a source of confirmed e-mail addresses for spammers'.

In 2002 the European Union introduced a hybrid approach to control advertising and therefore spamming. Firstly, the opt-in model registry model is introduced pursuant to Article 13(1) of the Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communication sector (OJ L 201/37 31.07.2002). It applies primarily in the context of business to consumer (B2C) communications. In terms of Article 13(1), it is now required that prior consent be obtained from natural persons beforehand for the purposes of 'direct marketing' through automated calling machines (fax). This requirement, according to recital 40, also covers advertising through short messaging systems messages (SMS). Related to this opt-in approach what is commonly referred to as the 'soft opt-in approach' in that it allows the maintenance of an opt-out registry system in marketing forms that are 'more costly for the sender and impose no financial costs on subscribers and users', and in 'pre-existing relationships'. The second approach, which is essentially an exception-based opt-out system, applies to B2B relationships. Since Article 13(1) read with Article 13(5) applies to B2C communication because of its explicit reference to 'natural persons', it stands that an opt-out approach applies by inference in business to business (B2B) communications.

### **3.3.2 Prohibition of False and Deceptive Communications**

An important provision in the Directive 2002/58/EC is the prohibition, under Article 13(4), of the sending of electronic mail for the purposes of direct marketing (as permitted under Article 13(2)) whereby the identity of the sender is concealed or disguised, or without the sender providing a valid e-mail address to which the 'recipient may request that such communication cease'.

## **4. Conclusion**

Unsolicited commercial communication is a problem world-wide. Efforts have been taken in different jurisdictions to protect consumers from unwanted and unsolicited communications. This brief survey of the position in South Africa, European Union, and Canada revealed that such a protection may be afforded through an anti-spam specific legislation or through applying the general laws which may be interpreted and used as tools to combat spamming. In South Africa, for example, spamming is not per

se illegal. The country employs a regulatory approach backed by a threat of penalties, which includes imprisonment for non-compliance with the regulatory requirements contained in section 45(1) of ECTA. Moreover, ECTA established an opt-out system placing a burden on consumers to inform senders of their disinterest in receiving the information.

The European Union maintains a mixed regulatory approach to spam activities. The approach, which is rather interesting, includes the opt-in model in B2C pursuant to the Directive concerning the processing of personal data and the protection of privacy in the electronic communication sector, most importantly business prior consent of the consumer before sending the consumer marketing information. In B2B cases it would seem that the European Union allows the opt-out approach. Canada seems to be effectively having recourse to general laws in its fight against malicious spam.

## References

An Anti-Spam Action Plan for Canada, Industry Canada, May 2004 <[http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h\\_gv00246e-htm](http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00246e-htm)> accessed on 3 February 2007

Baumer, D L and Poindexter, J (2004), *Legal Environment of Business in the Information Age* (Africa: Frazer Press)

Chigona, W, Bheekun, A, Spath, M, Derakhashani, S and Van Belle, J, 'Perceptions on SPAM in a South African context', *Internet and Information Technology in Modern Organisations: Challenges & Answers* <<http://www.commerce.uct.ac.za/InformationSystems/Staff/PersonalPages/jvbelle/pubs/IBIMA05%20Cairo%2069.pdf>>, accessed on 3 March 2008

Delio, M (2000), 'Spam Filters Grab Good With Bad', *Wired News*, 19 January 2000, <<http://www.wired.com/news/infostructure/0,1377,61945-2,00.html>> accessed on 3 February 2007

Faria, J A E (2004), 'e-Commerce and International harmonisation: Time to go Beyond the Functional Equivalence', *SA Mercantile LJ*, p 429

Geissler, M L (2004), *Bulk Unsolicited Electronic Messages (SPAM): A South African Perspective* (unpublished LLD Thesis, Pretoria: University of South Africa)

General Assembly Resolution 51/162 of 16 December 1996: United Nations Commission on International Trade Law Model Law on E-Commerce (UNCITRAL Model Law) from <<http://www.uncitral.org/en-index.htm>>

Polanski, P P (2007), 'Spam, Spamdexing and Regulation of Internet Advertising' in Kierkegaard, S (ed.) *International Law and Trade – Bridging the East-West Divide* (Ankara Bar association Press, Ankara)



Sibanda, OS (2007), 'Choice of Law, Jurisdiction, and Recognition and Enforcement in E-commerce in South Africa' in Kierkegaard, S (ed.) *Cyberlaw and Security Privacy* (International Association of IT Lawyers)

Sibanda, OS (2008), 'The Strict approach to party autonomy and choice of law in e-contracts in South Africa: Does the approach render South Africa an unacceptable jurisdiction?', *De Jure*, p 320

Tang, Z (2007), 'Online dispute resolution – An effective dispute resolution system for electronic consumer contracts', *Computer Law and Security Report*, p 43

Tladi (2008), 'The Regulation of Unsolicited Commercial Communications (SPAM): Is the Opt-Out Mechanism Effective?', *SALJ*, p 178

Wireless Application Service Providers' Association Code of Conduct, July 2008  
<[http://www.waspa.org.za/code/waspa\\_coc\\_6.1.pdf](http://www.waspa.org.za/code/waspa_coc_6.1.pdf)> accessed on 19 November 2008.