2010-01E

ANTI-SPAM LAWS IN WESTERN COUNTRIES: A COMPARISON

Alysia Davies
Legal and Legislative Affairs Division

18 January 2010

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
SERVICE D'INFORMATION ET DE RECHERCHE PARLEMENTAIRES

The Parliamentary Information and Research Service of the Library of Parliament works exclusively for Parliament, conducting research and providing information for Committees and Members of the Senate and the House of Commons. This service is extended without partisan bias in such forms as Reports, Background Papers and Issue Reviews. Analysts in the Service are also available for personal consultation in their respective fields of expertise.

CE DOCUMENT EST AUSSI PUBLIÉ EN FRANÇAIS

CONTENTS

Page

CANADA
LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

ANTI-SPAM LAWS IN WESTERN COUNTRIES: A COMPARISON

Canada is the only G8 country that does not currently have specific anti-spam legislation. During the most recent session of the Parliament of Canada, a government bill to implement anti-spam legislation (Bill C-27, the Electronic Commerce Protection Act) reached the Standing Senate Committee on Transport and Communications before Parliament was prorogued on 30 December 2009 and it died on the *Order Paper*.[1]

Other countries have adopted models for their anti-spam legislation that share some similarities with Canada's proposed model, although there are certain differences in the areas of consent, exceptions and penalties. This paper will briefly outline some of the major features of anti-spam legislation in the United States, Australia, New Zealand, the European Union, and the United Kingdom.

UNITED STATES

The major federal anti-spam legislation in the United States is the *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003*, commonly known as the *CAN-SPAM Act*. It applies to commercial electronic mail messages, which are defined in section 3(2) as any commercial email with a "primary purpose" of commercial advertisement or promotion of a product or service, which is not an email relating to a business transaction or relationship.

The consent model used in the *CAN-SPAM Act* is opt-out (section 5), which means that consent to receive email can be considered implicit unless the recipient "opts out" and indicates he or she no longer wishes to receive such email. (This can be accomplished by various means, such as following the "unsubscribe" instructions at the end of a commercial email, or clicking on a link provided to facilitate opting out.) The law requires that a commercial electronic mail message include:

---

1 For a legislative summary of the bill, see Alysia Davies, *Bill C-27: Electronic Commerce Protection Act*, LS-645E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, rev. 13 November 2009, http://www2.parl.gc.ca/Sites/LOP/LegislativeSummaries/Bills_ls.asp?lang=E&ls=c27&source=library_prb&Parl=40&Ses=2.

(i) a functioning return email address or other Internet-based mechanism permitting the recipient to opt out, which remains functional for at least 30 days after the initial email was sent (section 5(a)(3)(A)(i) and (ii), and section 5(a)(5)(A)(ii));

(ii) "clear and conspicuous" identification that the message is an advertisement or solicitation (section 5(a)(5)(A)(i)); and

(iii) a valid physical postal address of the sender (section 5(a)(5)(A)(iii)).

There are various exceptions that permit certain types of emails to be sent in a different manner, as well as certain interactions between federal and state laws that remove other types of emails from federal jurisdiction. Emails related to an existing transaction or business relationship, such as those related to benefit plans, account balances, product recalls, upgrades, warranties, product safety, and subscriptions, are exceptions to the definition of "commercial electronic mail message," and do not have to follow the opt-out rules under the *CAN-SPAM Act*'s definition.

The *CAN-SPAM Act* does cover fraudulent or deceptive emails, but only to the extent that these emails are not already dealt with under state laws about other forms of computer crime. If a fraudulent or deceptive email falls under the state statutes as an integral part of another type of computer crime that is governed at the state level, the *CAN-SPAM Act* does not apply (see section 8(b)(2)(B)). However, the federal *CAN-SPAM Act* supersedes all state laws that specifically regulate spam email, so if the problematic nature of the email is based on its being spam alone, the federal statute governs in place of the state one. (This holds true even if the state anti-spam law is more restrictive than the federal one, as is the case in several states, including California.)

If there is a breach of the *CAN-SPAM Act*, there are administrative, civil and criminal penalties available, depending on which provisions are violated. Administrative actions are initiated by the Federal Trade Commission (FTC), the main enforcement body for the *CAN-SPAM Act*, since violations under the Act are considered to be unfair or deceptive trade acts or practices. Civil actions may be brought in the courts either by a state attorney general, or by an Internet Service Provider (ISP) under certain conditions, although no private right of action is available to an ordinary citizen. Criminal prosecutions are dealt with by the federal Department of Justice.

Certain other agencies are also involved in enforcing the *CAN-SPAM Act*, depending on what kind of institution may have committed a violation and whether it already has an enforcement body associated with its activities. For example, if a national bank is a spammer, the Office of the Comptroller of the Currency will be the enforcement body for the purposes of the *CAN-SPAM Act*. If a broker or dealer is a spammer, the Securities and Exchange Commission will become involved. Other potential enforcement bodies include the Federal Communications Commission, the Farm Credit Administration, the Secretary of Agriculture and/or the Secretary of Transportation, among others, in connection with regulated activities in particular sectors of the economy (section 7(b)).

In terms of penalties, criminal violations of the *CAN-SPAM Act*, which include various fraudulent acts such as falsifying email header information and gaining unauthorized access to computers to use them for spamming, are punishable by fines under the criminal provisions of Title 18 of the *United States Code* and/or a prison term of up to five years, three years or one year, depending on the nature of the offence. It is also possible to seek forfeiture of a spammer's assets in criminal cases (section 4). In civil cases, statutory damages of up to either $1,000,000 or $2,000,000 may be awarded, depending on whether the action is brought by an ISP or a state attorney, plus aggravated damages where warranted (sections 7(f) and (g)). With respect to administrative actions, the FTC has its normal powers under the *Federal Trade Commission Act* (section 7(d)), which appear to include the ability to either issue administrative orders (the violation of which can result in a fine of up to $11,000 per violation), or prosecute certain cases before the courts in a manner similar to the Department of Justice.[2] Injunctions may also be issued (section 7(f)(2)).

AUSTRALIA

In Australia, spam is regulated by the *Spam Act 2003*. The activity to which it applies is described in detail – the Act's definition of "commercial electronic message" covers a message sent using an Internet or other carriage service to an email account or an instant messaging, telephone or similar account (section 5) and relating to a specific list of commercial

---

2 Federal Trade Commission, "A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority," rev. July 2008, http://www.ftc.gov/ogc/brfovrvw.shtm.

purposes (section 6). (It does not, however, include faxes or telephone voice calls.)[3] The term "message" is further defined to specify that it includes text, data, speech, music, other sounds, visual images (animated or otherwise), or any other form of information (section 4).

The specified list of purposes that render a message "commercial" include: advertising; promoting or offering to supply goods, services, land or an interest in land; or a business opportunity for investment. Any message that is intended to dishonestly obtain a gain, financial advantage or property belonging to another person by means of deception is also included in the definition (section 6).

The exceptions to this definition are listed in Schedule 1 to the Act, titled "Designated commercial electronic messages." While these exceptions must, like commercial email message senders, still include information about the individual or organization that authorized the sending of the message (in compliance with section 17 of the Act), they do not have to observe the section 16 ban on unsolicited communications or the section 18 requirement to include a means of unsubscribing.

The exceptions include messages that contain "no more than factual information," accompanied by certain specific features such as contact information of the sender and author, that are not commercial (Schedule 1, section 2), as well as any messages authorized by government bodies, registered political parties, religious organizations, and charities (Schedule 1, section 3). Another exception consists of messages sent by educational institutions to students or alumni (Schedule 1, section 4). Further exceptions may be specified by regulation (Schedule 1, section 5).

The consent model is detailed in Schedule 2 to the Act, which focuses on an opt-out regime. Consent can be inferred from the conduct of an individual or organization, as well as their business and other relationships (Schedule 2, section 2). There is also a "conspicuous publication" provision which states that although electronic message addresses cannot be harvested for use merely because they are publicly posted, they may be used to contact certain categories of people. A specific list of examples includes addresses publicly posted in an official capacity for employees, directors, partners, and holders of a statutory office (Schedule 2, sections 4(2)(a) and (b)). However, if those addresses are posted with a disclaimer indicating that the account-holder does not wish to receive unsolicited commercial electronic messages, then they cannot be harvested for that purpose (Schedule 2, section 4(2)(d)).

---

3 See section 5(5) of the Act and section 2.1 of the *Spam Regulations 2004*.

Enforcement is pursued via the courts, specifically the Federal Court of Australia, which can award civil penalties for violations of the Act, as well as compensation to any victims, and/or forfeiture of any financial benefit to the Crown where warranted. The courts may also order injunctions, and accept undertakings from violators to cease certain types of activity. Court actions are initiated and prosecuted by the Australian Communications and Media Authority (ACMA), the main enforcement body for the Act (section 26). Where the Court determines that a third party has been a victim of a violation of the Act, either the ACMA or that third party may apply for compensation for the victim to be paid in addition to the civil penalties (section 28).

The amount of the penalty can vary depending on whether the violator has a prior record, whether it is an individual or a body corporate, and which provision of the Act has been violated (section 25(1)). The penalties are expressed in the form of "penalty units," an Australian term for a fine specified by the Crown which is revised and updated on a regular basis. The highest penalties are for cases where a violator has sent unsolicited commercial electronic messages, or has aided, abetted, counselled, procured, induced, been knowingly concerned in or conspired with others to send such messages. In such a case, the maximum penalty for an individual without a prior record is 20 penalty units per violation, to a maximum of 400 penalty units per day for multiple violations. The maximum penalty for a corporation without a prior record is 100 penalty units per violation to a maximum of 2,000 penalty units per day for multiple violations. (The maximums increase if the violator has a prior record.) The current federal penalty unit in Australia is A$110,[4] which would make a civil penalty of 400 units worth A$44,000, and one of 2,000 units worth A$220,000.

The maximum penalties for other violations of the Act, such as not including accurate sender information, are lower.

NEW ZEALAND

New Zealand's anti-spam activities are regulated under the *Unsolicited Electronic Messages Act 2007*. It contains many similarities to the Australian legislation, with some particular refinements of its own.

---

4 *Crimes Act 1914*, Section 4AA.

A commercial electronic message is defined as a message, using a telecommunications service and sent to an electronic address, to market or promote goods, services, land, an interest in land or a business or investment opportunity, or to assist or enable dishonest financial advantage or gain, whether via direct communication or a link (sections 5 and 6). As with the Australian legislation, an electronic message includes a message sent to an email account or an instant messaging, telephone or similar account, but does not include voice calls and faxes (Schedule to the Act). It also includes all the specific forms of information such as text, video and sound that are listed in the Australian legislation (section 4).

The New Zealand legislation provides a very specific list of exceptions to what constitutes a commercial electronic message (section 6). Not included in the definition are messages that:

- provide a quote or estimate for goods and services requested by the recipient;
- facilitate, complete or confirm an agreed-upon commercial transaction;
- provide warranty information, product recall information or safety/security information about goods or services purchased by the recipient;
- provide notification of factual information about a subscription, membership, account, loan or similar ongoing relationship;
- provide information directly related to an employment relationship or benefit plan;
- deliver goods or services, such as product upgrades, that the recipient is entitled to receive under a previous transaction;
- provide the recipient with information about goods or services from a government body or court/tribunal;
- fulfill other purposes specified by the regulations.

Commercial electronic messages must contain the usual requirements of accurate sender information and an unsubscribe facility, and cannot be unsolicited (sections 9–11).

The consent model in the Act is an opt-out model, which allows consent to be inferred from the conduct, business and other relationships of the persons concerned, in addition to any other circumstances specified by regulation (section 4). The Act also contains the “conspicuous publication” provision, which allows electronic addresses to be harvested if they have been placed publicly online in an official capacity without a disclaimer indicating that they are not to be used for unsolicited electronic messages (section 4).

Enforcement duties are carried out by the Department of Internal Affairs, which has an Anti-Spam Compliance Unit that takes complaints and carries out investigations.[5] It can issue warnings and infringement notices, and accept undertakings from a violator (section 19(b) and (c)). This unit is also responsible for applying to the courts to obtain remedies for violations of the Act (section 19(c)). Matters under the Act may be taken to the District Court or the High Court, depending on the type of violation (sections 37 and 38 of the Act).

In addition, a private right of action is available in New Zealand to any person affected by a violation of the Act (section 19(a)), and the Department's enforcement unit may apply to join in any such action (section 19(c)).

The courts can impose civil penalties for a violation of the Act of up to NZ$200,000 for a person or NZ$500,000 for an organization (sections 45 and 48), as well as awarding compensation and/or damages as the circumstances warrant (sections 46 and 48).

EUROPEAN UNION

European Union (EU) directives are required to be implemented into legislation in all of the 27 member countries. The EU *Directive on privacy and electronic communications*[6] was introduced in 2002, and its key components have since been incorporated into various forms of national legislation in the member countries, including in the United Kingdom, which will be discussed at further length in the next section of this paper.

The *Directive on privacy and electronic communications* builds upon and interacts with an earlier directive from 1995, the *Data Protection Directive*,[7] which laid the template for privacy legislation in all of the member countries. The *Data Protection Directive* anticipated some of the issues with spam, and contained general principles that continue to be applied in the spam-fighting context.

---

5 New Zealand Department of Internal Affairs, "Anti-Spam," http://www.dia.govt.nz/DIAwebsite.nsf/wpg_URL/Services-Anti-Spam-Index.

6 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, OJ L 201, 31.7.2002, pp. 37–47.

7 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive)*, OJ L 281, 23.11.1995, pp. 31–50.

The EU directives apply to all direct marketing communications by automatic calling machines, fax or email (Article 13(1) of the *Directive on privacy and electronic communications*).

The consent model is opt-in, based on the precedent already established by the *Data Protection Directive*, which has used an opt-in model based on express consent in situations involving electronic privacy from its inception. This principle has been incorporated and widely implemented in all of the countries under EU jurisdiction (Article 13 of the *Directive on privacy and electronic communications*, Article 14(b) of the *Data Protection Directive*).

There is an exception in the *Directive on privacy and electronic communications*, which permits email contact information consensually provided by customers in the context of the sale of a product or service to be used for direct marketing of similar products or services by that same company, on an opt-out consent basis. However, the customer must be given the opportunity to opt out at the time of the collection of this email contact information in the first instance, as well as via any later contact (Article 13(2) and Preamble – Article 41 of the *Directive on privacy and electronic communications*).

It should be noted that this exception is for "electronic contact details for electronic mail" only and is not applicable to direct marketing via the other methods covered in Article 13 of the *Directive on privacy and electronic communications*, i.e., fax or automatic calling machines. Opt-in consent remains the standard for these. The handling of person-to-person marketing calls is left to national discretion to some degree, within the framework of existing privacy legislation (Preamble – Article 42 of the *Directive on privacy and electronic communications*).

"Electronic mail" is defined as "any text, voice, sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient" (Article 2 of the *Directive on privacy and electronic communications*).

There is also a distinction in European law between a "natural person," i.e., a person, and a "legal person," which includes a corporation or other organization. Privacy is considered to be a right under the European legal framework, and the consent provisions are designed to protect the rights of all individual "natural persons" who may be the recipients of direct marketing, regardless of the sender or medium. In cases where a "legal person," i.e., a corporation or organization in general, rather than an actual individual person, is the recipient of

direct marketing attempts, the member countries are given more discretion to regulate their own solutions, such as allowing companies to join an opt-out register to prevent receipt of such attempts. However, some protection is required to be legislated for them as well, whatever form it may take (Article 13(5) and Preamble – Article 45 of the *Directive on privacy and electronic communications*).

Sending direct marketing email via a disguised or concealed identity, or without an opt-out unsubscribe mechanism, is prohibited (Article 13(4) of the *Directive on privacy and electronic communications*).

Enforcement bodies and penalties are left to be designated by the national legislation in each member country.

UNITED KINGDOM

As with the European Union legislation, the United Kingdom's anti-spam rules build upon the privacy legislation framework it already has in place. The EU *Directive on privacy and electronic communications* has been incorporated into British law by means of the *Privacy and Electronic Communications (EC Directive) Regulations 2003* ("the Regulations"), which interact with the UK's pre-existing *Data Protection Act 1998* ("the Act") to provide specific anti-spam measures.

The British anti-spam rules apply to all direct marketing communications by automatic calling machines, fax or email (which includes text, voice, sound or image sent via electronic communications). The British have exercised their national discretion to include voice-to-voice telephone calls in their rules as well (sections 2 and 19–23 of the Regulations).

As prescribed by the EU directive, and consistent with the data privacy approach used throughout Europe, the consent model is opt-in (sections 19–22 of the Regulations and 7–12 of the Act). As per the EU directive, there is an exception – email contact information that is consensually provided by customers in the context of the sale or negotiations for sale of a product or service may be used for direct marketing of similar products or services on an opt-out basis (section 22 of the Regulations). It would appear that do-not-call registries and do-not-fax registries are also in operation (sections 25 and 26 of the Regulations).

It is prohibited to send an email covered by the Regulations without including an accurate identity for the sender and a valid address for unsubscribing (section 23 of the Regulations).

Enforcement is provided by Britain's Information Commissioner, who oversees both the Act and the Regulations, and who investigates complaints and makes findings in the form of various types of "notices" (sections 31–32 of the Regulations and Part V of the Act). The findings of the Commissioner may be appealed to the Information Tribunal, which can hear appeals on any decision notices, information notices, enforcement notices, and special information notices issued by the Commissioner (section 48 of the Act). Further appeals may be made to the courts on points of law only (section 49 of the Act).

Failure to comply with any notice issued by the Information Commissioner is a criminal offence subject to prosecution and a penalty fine up to the statutory maximum, which is currently £5,000 in England and Wales, and £10,000 in Scotland[8] (sections 47 and 60 of the Act).[9]

A private right of action is also available through the courts to any person wishing to claim damages resulting from a violation of the Regulations (section 30 of the Regulations).

---

8 *Criminal Justice Act 1982*, s. 74, as read with the *Magistrates' Courts Act 1980*, s. 32(9) (for England and Wales), as amended by the *Criminal Justice Act 1991*, s. 17; *Criminal Procedure (Scotland) Act 1995*, s. 225(8), as amended (for Scotland).

9 The only instance in which a different penalty amount may be imposed under the Act is for obstruction of or failure to provide assistance with the execution of a warrant or the inspection of overseas information systems by the Commissioner. The fine in this case can go up to the top level of the standard scale (a different measure than the statutory maximum), which is £5,000 in England, Scotland and Wales (*Criminal Justice Act 1982*, s. 37, as substituted by the *Criminal Justice Act 1991*, s. 17 (for England and Wales) and by the *Criminal Procedure (Scotland) Act 1995*, s. 225 (for Scotland)).