Fighting Spam
How Tough is the Canadian Legal Arsenal?
An Analysis in the Light of the U.S. CAN-SPAM Act

16 (2018) 2 Canadian Journal of Law and Technology 345-385

Serge Kablan*

Abstract

Following several countries, Canada recently passed Canada's Anti-Spam Legislation (CASL), in an attempt to tackle spam. The law aims to ''protect Canadians while ensuring that businesses can continue to compete in the global marketplace". For this purpose, CASL prohibits not only the sending of commercial electronic messages without consent, but also any alteration of transmission data in the course of a commercial activity. Moreover, the Act disallows the installation of a computer program on another person's computer system and the sending of commercial electronic messages following the installation. These three activities are prohibited unless the author or initiator has obtained the recipient's prior consent, either express or implied. This opt-in approach contrasts with the U.S. CANSPAM Acts opt-out regime, in force since 2004, which is known to offer to senders the chance to initiate contact and to recipients the option to unsubscribe or reject any subsequent commercial electronic message. Our paper intends to demonstrate that, notwithstanding the apparent difference in their respective approach, CASL and U.S. CAN-SPAM Act remain fundamentally similar in practical effect. This resemblance is good news, considering the profile and proximity of Canadian and American e-commerce economies. Thus, in spite of its detail and complexity, CASL may not be the most stringent anti-spam act as claimed, certainly not with the challenges related to its implementation and enforcement.

INTRODUCTION

In its 2014 *Internet Security Threat Report*, the Symantec Corporation [1] had estimated that for 2013 alone (that is, at the time Canada was on the verge of enacting

---

* Professor, FSA, Université Laval, Québec, Canada (serge.kablan@fsa.ulaval.ca). The author thanks the Office of Research and Creation (Université Laval), Joy Audet, and the CJLT's anonymous reviewer for their invaluable assistance in the production of this article. All the electronic citations are updated as of July 4, 2018.

1 Symantec Corporation, *Internet Security Threat Report 2014*, vol 19 (April 2014) at 14-15, online: <http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf> [ISTR 2014]; *Internet Security Threat Report 2018*, vol 23 (March 2018) at 73, online: <www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf>.

its anti-spam legislation) 29 billion spams were being sent daily in the world. The overall email spam rate was 66 per cent (this percentage dropped to 54.6 in 2017, according to the corporation's 2018 report). To counter this nuisance, the Organization for Economic Co-operation and Development (OECD) raised international cooperation and legislative harmonization as item No. 8 of its *Anti-Spam Toolkit*,[2] since spam shares attributes of cyberspace and, notably, makes light work of territoriality.[3] International cooperation and legislative harmonization are fundamental to the direction of the OECD to ensure that the laws to be enacted locally are effective.[4] According to the organization's guidelines, these laws should be concise and simple, and "put in place an effective sanction regime and appropriate standards of proof".[5]

The 2001 Budapest Convention on Cybercrime, which several non-member states of the Council of Europe, including Canada and the U.S., have signed, seeks to harmonize the rules regarding certain aspects of harmful cyberspace practices, such as computer forgery and computer fraud.[6] But the challenge of harmonization remains, and the absence of a comprehensive international instrument is not expected to alleviate states' need for homogeneity.[7] The Canadian anti-spam legislation should be tested from this perspective while, at the same time, one appreciates the severity of the solutions it puts in place. This law, entitled, *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage the exercise of commercial activities electronically and to amend the Canadian Radio-television Telecommunications Commissions Act, the Competition Act, the Personal Information Protection and Electronics Document Act and the Telecommunications Act* (hereinafter,

---

2 OECD, Joint ICCP-CCP Task Force on Spam, *Anti-Spam Toolkit of Recommended Policies and Measures*, Doc. No. DSTI/CP/ICCP/SPAM (2005)3 (2006 at 17 [OECD]. The organization's attention to spam is not an accident. It is motivated by spam's mutation, since spammers have gradually shifted from the initial purely advertising function of spam to a pervasive channel that paves the way for all sorts of illicit operations (fraud, spread of computer worms or viruses, propagation of malicious content, network alteration, etc.).

3 On the nature of cyberspace and the role of law, see Serge Kablan & Arthur Oulaï, "L'essence des approches du droit cyberspatial et l'opportunité de la co-régulation" (2009) 39 *RGD* 5.

4 The OECD shows the 8 elements of the Toolbox against spam: Element I: Regulatory Approaches; Element II: Enforcement; Element III: Industry-driven initiatives; Element IV: Technical Measures; Element V: Education and Awareness initiatives; Element VI: Cooperative partnerships; Element VII: Spam metrics; Element VIII: Global cooperation; OECD, *supra* note 2 at 73.

5 *Ibid.* at 25.

6 Council of Europe, Convention on Cybercrime, 23 November 2001, ETSNo. 185 at ss. 7-8 (entered into force 1 July 2004).

7 See, e.g., Pierre Trudel, France Abran&Gabriel Dupuis, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Rapport préparé pour la Direction des politiques du ministère des Services gouvernementaux du Québec, Montréal, Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique (2007); Arminda Bepko, "A State-by-State Comparison of Spam Laws" (2003-2004) Media L & Poly 20.

CASL)[8] allows Canada to catch up to other G7 countries in terms of legislative initiatives against spam.[9]

In fact, CASL is the culmination of a process that began in 2004 and involved Industry Canada[10] Working Group on spam (known as the "Spam Task Force"). The final report of the Working Group, released in May 2005, concluded that spam legislation was needed.[11] Bill C-27, which then became C-28, and most recently CASL,[12] implements this recommendation.

CASL has been in effect since July 2014.[13] At first sight, it appears particularly restrictive. The purpose of the Act is to promote e-commerce.[14] The way in which this is achieved is addressed in this article. More specifically, we examine the strength of the rules that intend to discourage infringements on the easy flow of communication and thereby support electronic commercial activities. The review we undertake puts into perspective the OECD guidelines.[15] In addition, the U.S. CAN-SPAM Act, in force since January 1, 2004,[16] will be considered, since Canada's e-commerce involves its American neighbour: as a matter of fact, the 2016 Canada Post whitepaper indicates that 53 per cent of Canadian online shoppers had made at least one cross-border purchase in 2015 (83 per cent had purchased from the U.S.).[17] On occasion, we will reference Australian

---

8 S.C. 2010, c. 23 [CASL]. CASL stands for "Canada's Anti-Spam Legislation." In its 2017 report, the Standing Committee on Industry, Science and Technology acknowledged that "[b]usinesses often fail to realize that the Act applies to them because their personnel do not think of their communications as "spam." By underlining spam rather than electronic commerce and communications, the name under which the Act is commonly known exacerbates this problem." [citations omitted] Thus, the committee recommends that "the Government of Canada [. . .] replace the phrase 'Canada's Anti-Spam Legislation' by the short title 'Electronic Commerce Protection Act' and the acronym 'CASL' by the acronym 'ECPA' in all guidance and enforcement materials as well as other publications on every support, including fightspam.gc.ca." See House of Commons, Standing Committee on Industry, Science and Technology, *Canada's Anti-Spam Legislation: Clarifications Are in Order*, (December 2017) at 5, 11 (Chair: Dan Ruimy).

9 Canada, Library of Parliament, "Legislative Summary of Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage the exercise of commercial activities electronically," by Alyssa Davies & Thomas J. Terrence, Publication No. 40-3-C28-F, revised 15 November 2012 (Ottawa: Library of Parliament, 2010) at 2-3.

10 Now Innovation, Science and Economic Development Canada (ISED).

11 Industry Canada Working Group on Spam, *Stopping Spam: Creating a Stronger, Safer Internet* (Ottawa: Industry Canada, 2005) at 3.

12 See the progress of the bill by consulting the database *LEGISinfo*, online: <www.parl.-ca/LegisInfo/BillDetails.aspx?billId=4543582&Mode=1&View=0&Language=E>.

13 The provisions dealing with the installation of computer programs came into force on 15 January 2015. Those concerning the private right of action are not yet in force at the time of publication of this article.

14 CASL, *supra* note 8, s. 3.

15 OECD, *supra* note 2.

16 *Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003,* 15 U.S.C. 37701-7713 (2004) [CAN-SPAM Act].

17 See Canada Post, "Growing E-commerce in Canada: Unlocking the online shopper opportunity," (2016) at 8, online: <www.canadapost.ca/web/assets/pdf/blogs/canadapo s t - g r o w i n g - e - c o m m e r c e - i n - c a n a d a - 2 0 1 6 _ e n . p d f ? e c i d = d i s -play%7Cpdn%7Ccs%7C104>.

law,[18] which is often presented as a model for the battle against spam.[19] The review will be conducted in two parts: (1) in light of the requirements and prohibitions introduced by CASL, and (2) in relation to the requirement of consent. In conclusion, we will briefly consider the recourses and penalties faced by offenders.

1. THE REQUIREMENTS AND PROHIBITIONS

CASL regulates three activities: first, the sending of commercial electronic messages (''CEMs") (1.1); second, the alteration of transmission data (1.2); and, third, the installation of computer programs (1.3).

1.1 The Rules for Commercial Electronic Messages

At issue from the outset is the meaning to be given to the phrase CEMs.[20] There is a double challenge to this, according to the OECD. One is related to the form or medium of CEMs; the other concerns their nature.[21] The first step is to determine whether a technology neutral approach should be favored or, if the law should target messages sent via specific technologies (or by specific methods, to use the expression of the International Telecommunications Union).[22] The first option has the advantage of being inclusive, in addition to widening the scope of the law. However, this option should not mean absolute neutrality, as the OECD believes:

> […] even with a technology neutral approach, it is worthwhile to evaluate which particular messaging media are being misused or have a strong potential to be misused in the future and ensure that they are appropriately addressed in the legislation.[23]

About the nature of the messages, it must be decided whether or not to emphasize the commercial dimension. Under one option, the scope of the law is narrower, but this does not prevent it from regulating a number of the current harms;[24] under the second option, the scope is more likely to raise constitutional concerns, notably related to the freedom of expression.[25] The choice of the Canadian government is revealed by analyzing the type of messages CASL intends to capture (1.1.1), the conditions it sets for sending these messages (1.1.2), and the situations excluded from these conditions (1.1.3).

---

18 *Spam Act 2003,* (Cth).

19 *Debates of the Senate—Official Report*, 39th Parl 2nd sess, vol 144:59 (13 May 2008) at 1329 [*Debates of the Senate*].

20 Derek E Bambauer, "A Comparative Analysis of Spam Laws: The Quest for a Model Law" (Background paper for the ITU WSIS Thematic Meeting on Cybersecurity, Geneva, Switzerland, 28 June—1 July 2005) Doc CYB/03 at 12.

21 OECD, *supra* note 2 at 26.

22 ITU, *supra* note 20.

23 OCDE, *supra* note 2, at 26. See for example the review of the rules governing the use of cookies (Part 2.1.3 of this article).

24 See, for example: Adam Massof, « Spam—Oy, What a Nuisance! » (2004) 2 BTLJ 1.

25 OECD, *supra* note 2 at 26. See also: Karen Ng, "Spam Legislation in Canada: Federalism, Freedom of Expression and the Regulation of the Internet" (2005) 2 U Ottawa L&Tech J 447.

1.1.1 The Targeted Messages

The CEM subject to CASL is the electronic message which has as its purpose or one of its purposes, the encouragement of participation in a commercial activity (Section 1(2)). By design, the Act does not indicate a particular technology that gives the message its electronic character. An electronic message is merely a message that is sent by any means of telecommunication (s. 1(1)). It is understandable that the Canadian government intended to follow the recommendations of the Spam Task Force, which encouraged such neutrality, and suggested that CEMs be considered as a whole (text, sound, voice, visual messages, etc.), including messages that come from the wireless communications sector.[26]

Under U.S. law, the commercial electronic mail message (hereinafter, ‘‘CEMM”) refers to a message sent to a single electronic mail address.[27] It was feared that this clarification of the support or technology of the message would force courts to rule on new media on an ongoing basis, unless the government committed to a gradual widening of the scope of the law, updating it regularly as new media emerged. However, case law has avoided this need. In the case of *MySpace, Inc., v. Wallace,*[28] it was alleged that advertisements from MySpace pages do not constitute CEMMs under the CAN-SPAM Act. The plaintiff submitted that the defendant had compromised 340,000 user accounts or *MySpace* profiles and sent some 400,000 spam messages to those network members. The defendant argued that these messages did not fall within the current scope of the Act, since the Act presupposed an e-mail address. It maintained that the addresses to which the MySpace messages were routed (inboxes within the MySpace network) did not have the required format of the domain name, which includes a string of characters such as *user@domain.com*.

In fact, s. 7702(5) of the CAN-SPAM Act does specifically refer to this characteristic,[29] but the electronic mail address is interpreted broadly. According to the U.S. District Court of Central California, the electronic mail address designates any destination to which an electronic mail can be sent. As a consequence, reference in s. 7702(5) to the standard format of the electronic mail address and the domain name would essentially be indicative only. The court was of the view that the government had not intended to restrict this provision, aware as it was of the state of the art in technology and of the outlook for its development.[30] The broad interpretation this court adopted was echoed in the judgment of *Facebook Inc. v. MaxBounty Inc.,*[31] and elsewhere,[32] leaving

---

26 Working Group on Spam, *supra* note 11 at 21.

27 CAN-SPAM Act, *supra* note 16 ss. 7702(2)(A), 7702(2)(C), 7702(6).

28 *MySpace, Inc., v. Wallace,* 498 F. Supp.2d 1293 (C.D. Cal. 2007) [*Wallace*].

29 CAN-SPAM Act, *supra* note 16, ss. 7702(5): “The term ‘electronic mail address’ means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the ‘local part’) and a reference to an Internet domain (commonly referred to as the ‘domain part’), whether or not displayed, to which an electronic mail message can be sent or delivered.”

30 *Wallace*, *supra* note 28 at 1300.

31 *Facebook, Inc. v. MaxBounty, Inc.,* 274 F.R.D. 279 (N.D. Cal. 2011) at paras. 238-284.

32 *Joffe v. Acacia Mortg. Corp.,* 211 Ariz. 325 (Ariz. Ct. App. 2005).

few dissimilarities with the Canadian law, where the approach that advocates regulation according to technology was rejected in favor of an expansive and more neutral approach.

As a further matter, to be subject to the CAN-SPAM Act, the primary purpose of the CEMM must be commercial. The primary purpose is commercial when the message is exclusively commercial advertising or promotes a product or service. If the message includes other content (for example when the message encompasses content that is transactional or relational, in addition to promotional content),[33] the recipient must reasonably interpret the subject line of the message to determine if its primary purpose is commercial. In the cases where the message conveys material other than transactional or relational content, in addition to promotional content, not only can the subject line of the message be interpreted to determine its nature, but the body of the message may also be taken into consideration.[34]

Unlike U.S. law, the Canadian legislation is not expressly related to the *primary purpose* of the message. Its scope seems to be much broader, since CASL targets messages which have as their *purpose*, *or one of their purposes*, the encouragement of participation in a commercial activity. In determining whether this purpose is present in the message, reasonable consideration must be given to internal and external elements of the message. The content of the message or any website or other database to which the message gives access, are expressly recited in s. 1(2). The information about a contact person referred to in the message may also indicate a commercial purpose. One must emphasize the following point: in themselves, these elements of s. 1(2) do not seem essential.[35] What is decisive is the expected action from the recipient, that he or she participates in a certain commercial activity. This interpretation emerges more explicitly from the U.S. CAN-SPAM Act, which mentions the same elements and may have inspired the Canadian provision:

> The inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such a message to be treated as a commercial electronic mail message for purposes of this Act if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service.[36]

CASL provides a non-exhaustive list of CEMs that are intended to encourage participation in a commercial activity (s. 1(2)(a)-(c)).[37] This is the case for messages involving an offer to buy, sell, barter, or lease a product, good, or service, and for messages that offer, announce or promote a potential business, investment or transaction. For purposes of s. 1(2)(d), the electronic message which ‘‘promotes a person” by representing him or her as a person who performs or has the intention to perform the

---

33 See CAN-SPAM Act, *supra* note 16, s. 7702(17(A).

34 See *Primary purpose*, 16 CFR s. 316.3 (2008).

35 ITU, *supra* note 20.

36 CAN-SPAM Act, *supra* note 16, s. 7702(2)(D).

37 The Australian legislation specifically targets 12 activities. It provides, however, that other activities could be included in the Regulations. See: *SpamAct 2003*, *supra* note 18, s. 6.

enumerated acts, also has this commercial nature. An electronic message that includes a request for consent to send a CEM is likewise considered to be commercial (s. 1 (3)). As such, it is prohibited, unless the sender has previously obtained the recipient's consent. The parliamentary proceedings highlight the impasse created by this rule of prior consent. This rule represents one of the main differences with the U.S. model, which offers senders a chance to initiate contact and recipients the option to reject commercial electronic messages thereafter.[38] In the opinion of some parliamentarians, implementing s. 1(3) would put a merchant in an impossible situation:

> That, unfortunately, raises what I would call a catch 22. No one can send a message without getting consent and no one can send a message asking for consent because that would be a commercial message.[39]

Thus, the means of contact available to Canadian companies would be limited: "Anyone who wishes to establish a business relationship with another person must now do so via the telephone or mail, or meet the individual in person. They could not send a simple email."[40]

It is worth recalling the Belgian solution in this respect:

> [R]egulatory authorities […] consider that a request for consent may be addressed by electronic mail. They rely on the fact that the Act requires prior consent solely in the case of electronic mail sent for advertising purposes. An electronic mail message whose purpose is to seek consent is not by definition an advertisement and therefore it would not be subject to the requirement of prior consent.[41]

Moreover, beyond what is enumerated in s. 1(2) and (3) of CASL, one might well question the exact criterion which qualifies an activity and thus an electronic message as commercial. As suggested earlier, it may be appropriate to take account of intrinsic and extrinsic elements of the message, but it remains difficult to know under which principles these elements should be evaluated. CASL is silent on this matter. The idea of commercial activity is nevertheless a central feature of the law, for obvious reasons. First, because it restricts the reach of the Act. If the statute had targeted electronic messages in general, freedom of expression would have likely suffered disproportionately. But the OECD warns: "Limiting the scope of spam legislation to commercial messages only may lead to the omission of most harmful spam. For example, a million spam messages promoting a political or religious idea can be as invasive and disturbing as a million messages

---

38 House of Commons, Standing Committee on Industry, Science and Technology, *Proceedings of the House and its committees*, 40th Leg, 3rd sess, No. 43 (2 November 2010) at 3 (Andre Leduc). See, e.g., CAN-SPAM Act, *supra* note 16, s. 7704(a)(4). Also, Sylvia Mercado Kierkegaard, "War Against Spam: AComparative Analysis of the U.S. and the European Legal Approach" (2005) 2 Communications of the IIMA 47 at 52.

39 *House of Commons Debates*, 40th Parl, 2nd sess, vol 144, No. 53 (7 May 2009) at 3249 (Derek Lee).

40 *House of Commons Debates*, 40th Parl, 2nd sess, vol 144, No. 105 (2 November 2009) at 6477 (Robert Vincent).

41 Arthur Oulaï, « La place du consentement dans l'encadrement de la cyberpublicité au Canada » in Pierre-Claude Lafond, ed, *La publicité, arme de persuasion massive : les défis de l'encadrement législatif* (Cowansville : E´ ditions Yvon Blais 2012) 123 at 155 [free translation].

promoting an herbal remedy."[42] Second, by emphasizing electronic messages that promote participation in a commercial activity, the Canadian federal parliament avoids potential constitutional challenges to its legislative authority, since it has jurisdiction in the area of trade and commerce.[43]

That being said, CASL assumes the commercial nature of the transactions listed in s. 1(2) and (3), without engaging in any definition of their "commerciality." Similarly, s. 1(1) merely states that transactions with a commercial nature (such as those listed) fall within the scope of CASL, regardless of whether or not they are carried out[44] with the purpose of making a profit.[45] The scope of CASL is thereby fully expanded, reaching almost all organizations (when engaging in a commercial activity),[46] including provincial and federal Crown corporations.[47]

Under European law, the wording seems more precise. For example, the Parliamentary directive on privacy and electronic communications[48] regulates unsolicited communications for *direct marketing* purposes.[49] In transposing s. 13 of that directive, which prohibits this type of communication when the persons to whom it is addressed have not previously agreed to receive it, s. 22 of the French *Law regarding Confidence in the Digital Economy* (hereinafter, "LEN")[50] gives the meaning of *direct marketing*: "[d]irect marketing is the sending of any message intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services".

---

42 OECD, *supra* note 2 at 26-27.

43 Canada, Innovation, Science and Economic Development, *Bill C-28* (Ottawa: 2010) at 1 (unpublished) [ISED].

44 Where conducted by a "person," person within the meaning of s. 1(1) of CASL, *supra* note 8, is any "natural person, partnership, corporation, organization, association, trustee, executor, liquidator of a succession, administrator, receiver or legal representative."

45 The *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 3 [PIPEDA] also evokes the notion of "commercial activity." Its definition is not far from that of CASL, with some exceptions (e.g. fundraising, which enjoys special treatment in CASL). For the purposes of this Act, a commercial activity is "any regular activity and any isolated act of a commercial character in nature, including the selling, bartering or leasing of donor lists, membership or collection fund" (s. 2(1)).

46 ISED, *supra* note 43. For purposes of CASL however, commercial activity does not relate to an act or transaction that is performed with a view to the following four objectives: compliance with the law, public safety, protection of Canada or conduct of international affairs and defense (s. 1(1) and (4)).

47 Section 4 of CASL, *supra* note 8, for example, stipulates that "This Act is binding on any corporation that is expressly declared by or under any Act of Parliament or of the legislature of a province to be an agent of Her Majesty, when the corporation is acting as such in the course of any commercial activity."

48 EC, *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*, [2002] OJ, L 201/37. See also EC, *Directive 2009/136/EC of the European Parliament of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the implementation of the legislation onconsumer protection*, [2009] OJ, L 337/11.

49 EC Directive 2002/58/EC, *supra* note 48, see, e.g., paras. 40-42.

50 *Loi no. 2004-575 du 21 June 2004 pour la confiance dans l'economie numérique,* ss. 13.1, 13.3. JO, 22 June 2004, 11168 [LEN] [free translation].

The European directive on electronic commerce may also be mentioned. This instrument refers to *commercial communication* to mean "any form of communication intended to promote, directly or indirectly, goods, services, or the image of a company, organization or person having a commercial, industrial or craft activity or pursuing a regulated profession."[51] Perhaps a similar wording, or wording modelled after the U.S. anti-spam law (which targets commercial advertising or promotion of products or services), would have allowed a clearer distinction between electronic messages subject to CASL, the sending of which must meet the specific conditions analyzed below, and messages that escape these requirements. Without criteria other than the generic terms commercial activity, the enumerative approach of CASL necessarily leaves uncertainties.[52]

1.1.2 Conditions for Sending Messages

A first prohibition concerns spam or unsolicited electronic messages (it should be noted that the word spam is not used in the Act). Section 6(1) of CASL makes it illegal to send a CEM to an electronic address,[53] except with prior consent of the recipient and on condition that the sender provides information about its identity and an unsubscribe mechanism. The Act considers a CEM to be sent once the transmission of the message is initiated, regardless of whether or not the electronic address to which it is sent exists and whether or not the message reaches the desired destination (s. 6(4)). The challenges underlying the international dimension of CEMs appear clearly here, notably as to what extent spammers operating from foreign countries are subject to the prohibition of s. 6(1) of CASL. In one of the texts initially debated, Bill S-235, the drafters tried to address the issue and counter what they perceived as a weakness in anti-spam laws, by targeting the person who ultimately benefits financially from the CEM.[54] The financial benefit and the presumption it implies were not formally inserted into the final version of CASL, except partially, for determining the amount of the penalty for violations.[55] Perhaps the Act has

---

51 Certain communications are excluded. See especially EC, *Directive 2000/31/EC of the European parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, [2000] OJ, L178 at ss. 7, 2(f).

52 Oulaï, *supra* note 41 at 153.

53 It is worth clarifying that the electronic address to whichCASLrefers receives a relatively broad definition and avoids the description of the CAN-SPAM Act. Here, electronic address (in digital, alphabetical, or alphanumeric form) includes any address of an email, instant message, telephone account, or any other "similar account" (s. 1(1)). The Canadian Radio-television and Telecommunications Commission (CRTC) explains that "similar accounts" may include new media if a review in practice reveals characteristics other than those of broadcast media: "Whether a 'similar account' is an electronic address depends on the specific circumstances of the account in question. For example, a typical advertisement placed on a website or blog post would not be captured. In addition, whether communication using social media fits the definition of 'electronic address,' must be determined on a case-by-case basis, depending upon, for example, how the specific social media platform in question functions and is used. For example, a Facebook wall post would not be captured. However, messages sent to other users using a social media messaging system (e.g., Facebook messaging and LinkedIn messaging), would qualify as sending messages to 'electronic addresses.'" See ISED, *supra* note 43 at 10.

54 See *Spam Act 2003*, *supra* note 18, ss. 7, 16.

55 See, e.g., CASL, *supra* note 8, s. 20(3)(e).

nevertheless adopted the spirit, since s. 6(1) focuses not only on the person who sends the CEM, but also on the person who allows such a message to be sent. Even with this, one wonders how CASL would tackle situations where the beneficiary of the mailing or the financial interest is abroad. How will that person be identified and then punished for any offence, since its actions also technically bring the Canadian anti-spam law into play? Indeed, like the Australian law,[56] CASL applies whenever the computer system[57] used to access the electronic message is located in Canada,[58] whether or not the sender or the beneficiary is operating from a foreign country.

It is true that the U.S. law prohibits unsolicited electronic messages *a posteriori*, or after the recipient has expressed his or her objection to receiving further messages. But the legislation is no less interested in the initiator of the messages. As a matter of fact, this prohibition *ex post* focuses on the person whose product, service or website is advertised or promoted by the CEMM and who identified the recipients and provided their electronic mail addresses. The U.S. reasoning uses the notion of *protected computer,*[59] which also raises the international issue of spam. In the CAN-SPAM Act, the term has the meaning of s. 1030(e)(2)(B) of title 18 of the *United States Code.*[60]

Section 6(1) of CASL prohibits the sending of CEMs to electronic addresses unless certain substantive and procedural requirements are met.

1.1.2.1 The Substantive Conditions

CASL raises two substantive issues: (a) foremost, the necessity for consent, and (b) the content of CEMs.

(a) Prior Consent of the Recipient

Under CASL, any person to whom a CEM is sent must have previously agreed to receive it. This is the approach referred to as opt-in. The recipient can give his or her consent expressly, and in some cases, consent can be implied (s. 6(1)(a)). Both the European Directive on privacy and electronic communications and the Australian Spam Act have this requirement,[61] but not the U.S. CANSPAM Act which uses the opt-out model. In that model, the recipient's consent is presumed and remains as long as he or she does

---

56 See: *Spam Act 2003*, *supra* note 18, ss. 7, 16.

57 CASL, *supra* note 8, s. 1(1) adopts the definition set out in s. 342.1(2) of the *Criminal Code of Canada*, R.S.C. 1985, c. C-46 on the computer, which is envisaged as a "device or group of devices connected or related to each other, which one or more of them: a) contains computer programs or other computer data; b) pursuant to computer programs, (i) performs logic and control functions, (ii) may perform any other function."

58 There is also a contravention if the computer used to send the CEMis located in Canada. See CASL, *supra* note 8, s. 12(1).

59 CAN-SPAM Act, *supra* note 16, s. 7704(a)(1).

60 "T]he term "protected computer" means a computer—which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." See CAN-SPAM Act, *supra* note 16, s. 7702(13). As in Canada, the intermediary which participates in the sending by furnishing the telecommunication services ("through an automatic technical process") is not of concern: CAN-SPAM Act, *supra* note 16, s. 7702(9), (15); CASL, *supra* note 8, s. 6(7).

61 *Spam Act* 2003, *supra* note 18, s. 16; EC Directive 2002/58/EC, *supra* note 48 s. 13.

not withdraw.[62] The International Telecommunications Union (ITU) has drawn attention to some implications of opt-in and opt-out: opt-in focuses legislative efforts on defining the processes needed to manage the recipient's consent, that is, the mechanisms for obtaining, recording and revoking consent; opt-out emphasizes the choice of the recipient not to receive further CEMs and how to make this choice effective.[63]

The process of the opt-in approach as implemented under CASL will be discussed hereafter. It should, however, be borne in mind that the ITU cautions about some detrimental effects arising from a possible coexistence of opt-in and opt-out models in neighboring markets such as Canada and the United States. The warning recalls the usefulness of harmonization: "Variation in opt-in versus opt-out approaches makes cross-border efforts hard since an offense in an opt-in regime may be legal in an opt-out one."[64] Serious other constraints to cope with are revealed by the OECD regarding the opt-out approach. These constraints seem inimical to consumer protection:

- It transfers the burden of effort and cost to the consumer.
- In order to unsubscribe, the email must be opened and responded to, which is contrary to good e-security practice, unless the e-mail is from a known and trusted source.
- Unsubscribe links are often non-functional.
- It places the evidentiary burden upon the recipient of the message.[65]

The opt-in regime where the recipient openly expresses consent has its advantages, notably in the area of privacy or by transferring the evidentiary burden to the sender. But it remains just as limited, according to the OECD outline which highlights issues regarding the means of recording consent and freedom of expression:

- Difficulty in keeping records of consent received by business. The absence of such records may significantly restrict the potential pool of recipients who can be targeted for otherwise legitimate messaging.
- Restricts "commercial free speech".
- Could result in devoting enforcement resources to areas where consumers are not financially harmed.[66]

That said, the requirement of consent in the electronic context is not new to Canadian law, and CASL forces coordination with previous Acts. For instance, under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[67] "[c]onsent is required for the collection of personal information and the subsequent use or disclosure of this information [...]." [68] Arrangements for consent under PIPEDA preempt any provision of any other Act, in the absence of express derogation in the other Act[69]. Such

---

62 OECD, *supra* note 2 at 9; 27ff.
63 ITU, *supra* note 20 at 17.
64 *Ibid.* at 27.
65 OECD, *supra* note 2, at 28.
66 *Ibid.*
67 PIPEDA, *supra* note 45, s. 3.
68 *Ibid*, Schedule 1, s. 4.3.1.
69 *Ibid*, s. 4(3).

derogation was unavoidable for CASL. The drafters explain that the narrower scope of the CASL consent regime compared to PIPEDA involved a "coordinating provision" (in this case, s. 2 of CASL) to give primacy to CASL over incompatible provisions of PIPEDA.[70] The earlier remarks of the Canadian Bar Association (CBA) with respect to Bill C-27 (that became CASL) apply here. The CBA deplored the legislative choice "[…] to treat certain commercial online activity differently and more restrictively than other commercial activity currently subject to privacy laws."[71]

Once consent is obtained, the sender must ensure that the CEM it is sending reflects the minimum content required by CASL.

(b) Compulsory Content of the Commercial Electronic Message

Professor A. Oulaï explains that in CASL, there is no obligation to identify advertising specifically, as there is in French law.[72] Relying on the professor's analysis, such an identification may be useful. It would allow a prompt distinction (that is to say, right on receipt of the messages) between advertising and other content.[73] CASL does not impose this duty with regard to advertising, nor does it retain it for commercial messages in general. Conceivably, the government instead seized the opportunity of prior consent to achieve the objective of content identification, that is consumer information (for instance, s. 10(1)(a) of the Act requires that the purpose be disclosed for which consent is sought). But even with this, content identification at the start would still be useful. The debate on this matter, which has yet to be conducted regarding CASL, has evolved to content labeling by keywords or abbreviations entered in the subject line of messages. This proposal may have practical advantages, according to an assessment by the OECD:

> The utilization of specific wording, or labels, to allow users to distinguish between advertising and other personal and professional e-mail, could be useful in the fight against spam. In terms of e-mail, labelling is the use of standard words in the message header or subject line that clearly identifies the content of the message, for example, the use of "ADV" for advertising and "ADLT" for adult content. Such a mechanism means that recipients are able to distinguish between advertising material and other e-mail traffic. It would also enable the more efficient and effective use of filtering systems.[74]

The CAN-SPAM Act adopts this labeling approach with respect to commercial electronic messages containing sexually oriented material. The prescription is strict; any person who initiates the transmission of a message of this nature must include in the nineteen

---

70 Standing Committee supra note 28 at 1. See also CASL, *supra* note 28, s. 2. Under US law, see CAN-SPAMAct, *supra* note 16, s. 7701(b); DavidESorkin, "Spam Legislation in the United States" (2003) *Journal of Computer and Information Law* 3 at 11; Katherine Wong, "The Future of Spam Litigation after *Omega World Travel v. Mummagraphics*" (2007) 2 H JL & Tech 459 at ff466.

71 Letter from the Canadian Bar Association to House of Commons Committee on Industry, Science and Technology (15 September 2009) at 2-3, online: <www.cba.org/Our-Work/Submissions-(1)/Submissions/2009/Bill-C-27-—-em-Electronic-Commerce-Protection-Act>.

72 Oulaï, *supra* note 41, at 137. See also LEN, *supra* note 50, ss. 20, 21.

73 *Ibid*, at 134.

74 OECD, *supra* note 2 at 33.

characters of the subject line, the specific wording ‘‘SEXUALLY EXPLICIT:” in capital letters.[75] In addition, U.S. law prohibits rendering any of this material immediately visible upon opening the message.[76] But let us not forget the limits of content labeling or tagging. The OECD, in particular, warns that its effectiveness remains subject to the international harmonization of labels and a standardization of their use.[77] Similarly, the Federal Trade Commission, responsible for the implementation of CAN-SPAM Act, is not convinced of the usefulness of the approach, at least of the idea of extending tagging to all subjects. In a report to the U.S. Congress published in 2005,[78] the Commission denied one of the alleged main benefits. It rejected the claim that labeling would facilitate content filtering and, ultimately, contribute significantly to curb spam. The report shows compliance rates altogether insignificant (“two percent of email messages that the Commission reviewed contained an “ADV” label in their subject lines.” [79]). It suggests that the experience of the American states which have chosen this legislative approach is not conclusive.

But even though content labeling is not extended to all subjects, for the apparent benefit of the U.S. marketing industry,[80] the obligation remains for anyone who wishes to initiate the transmission of a CEMM to make a clear and conspicuous indication that the message is an advertisement or solicitation.[81]Additionally, the initiator must not perform this transmission if it has actual or constructive knowledge that the subject line of the message is likely to induce error on the part of the recipient.[82]

Under CASL, the focus is turned elsewhere. Attention is given to the information in the hands of the recipient, which concerns three areas. The first two are related to the identity and coordinates of the person sending the CEM and, when applicable, that of those (such as affiliates) on behalf of whom the CEM is sent (s. 6(2)(a)).[83] As in U.S. law,[84] it is about disclosing the origin of the CEM. The sender must indicate its name, mailing address (including street address, post office box, rural route, or general delivery), either the phone number at which the recipient can access a service agent or a voice messaging service, its e-mail, or website address. Contact information must remain valid for at least

---

75 *Requirement to place warning labels on commercial electronic mail that contains sexually oriented material*, 16 CFR s 316.4(a)(1) (2008). The regulator says: “The phrase “SEXUALLY-EXPLICIT” comprises 17 characters, including the dash between the two words. The colon (:) and the space following the phrase are the 18th and 19th characters.”

76 See: *U.S. v. Impulse Media Group*, CV05-1285RSL (W.D. Wash. 2007).

77 OECD, *supra* note 2 at 33.

78 Federal Trade Commission, *Subject Line Labeling as a Weapon Against Spam: A CANSPAM Report to Congress* (Washington, DC: Federal Trade Commission, 2005) at 6.

79 *Ibid.*

80 Andrea Slane, “Home Is where the Internet Connection Is: Law, Spam and the Protection of Personal Space” (2005) 2 U Ottawa L & Tech J. 255 at 279-280.

81 CAN-SPAM Act, *supra* note 16, s. 7704(a)(5)(i).

82 *Ibid*, s. 7704(a)(2).

83 Intermediaries are not affected by these rules, that is to say, those whose primary function is to facilitate CEMs distribution without influencing their content or recipients’ choice. See Canadian Radio-television and Telecommunications Commission, “Guidelines on the interpretation of the Electronic Commerce Protection Regulations (CRTC),” Compliance Enforcement Information Bulletin CRTC 2012-548 (Ottawa: CRTC, 2012).

84 See CAN-SPAM Act, *supra* note 16, ss. 7703, 7704.

60 days after the CEM has been sent.[85] A minimum period of 30 days was originally required and thus justified: "[t]o avoid having spammers change their address every day, which they all otherwise do, the information […] must remain valid for at least 30 days after the commercial electronic message has been sent."[86] ISED considers 60 days to be more reasonable to allow the recipient to decide whether to continue receiving CEMs, withdraw consent or report to the CRTC when such consent is missing from the start. In the latter case, the delay would allow the CRTC enough time to examine the claim.[87]

Thirdly, the sender must describe an unsubscribe mechanism, which is to say, explain how or by what process the recipient can withdraw consent (s. 6(2)(c)).[88] The provision of all such information must respect several formal conditions.

1.1.2.2 The Formal Conditions

It is permissible for the sender to display the required information (including the unsubscribe mechanism) on a web page, in cases where it is not practicable to insert it into the CEM.[89] The web page must then be "readily accessible" and available at "no cost." As for the hyperlink to the information and the information itself, the established standard commands a wording that is "clearly and prominently" readable. A rough draft of CASL Regulations proposed to circumscribe this obligation more strictly: accessibility of the web page was to be provided as a *single click*, unless a method of equivalent efficiency was employed.[90] Nonetheless, references to the internet, via a web page, and to the click option had been criticized. It was argued that not all communication terminals captured by CASL enable access to the internet, taking into account technical or even purely circumstantial constraints. We think of a user whose mobile device may technically access the internet, but the telecommunications service to which he or she subscribes does not provide such access. This user could well receive SMS (Short Message Service) CEMs but would ultimately be unable to access the mandatory information if this information is displayed on a web page to which the message refers. In addition, one could doubt the universal nature of clicking, since it is incompatible with a number of communication devices.[91]

While the CRTC welcomed these remarks, and had undertaken to rely on the fact that "a more technology neutral wording is appropriate to accommodate the different technology platforms available currently and in the future,"[92] the commission took out only the click (and methods of equivalent effectiveness) in the final version of the

---

85 *Electronic Commerce Protection Regulations (CRTC),* SOR/2012-36, s. 2(1). See also CAN-SPAM Act*, supra* note 16, s. 7704(a)(5)(ii).

86 *Debates of the Senate, supra* note 19 at 1328.

87 ISED, *supra* note 43 at 29.

88 See Part 2.3 of this article.

89 SOR/2012-36, *supra* note 85, ss. 2(2), (3).

90 Canadian Radio-television and Telecommunications Commission, "Call for Comments on Draft Electronic Commerce Protection Regulations (CRTC)," Telecom Notice of Consultation CRTC 2011-400 (Ottawa: CRTC, 2011) Annex at s. 2(2).

91 Canadian Radio-television and Telecommunications Commission, "Electronic Commerce Protection Regulations (CRTC)," Telecom Regulatory Policy CRTC 2012-183 (Ottawa: CRTC, 2012) at para. 9.

92 *Ibid,* s. 21.

Regulations. The reference to web pages remains, with a pressing need, we believe, to clarify the meaning of the obligation to render such pages "readily accessible."[93] The same word, *readily*, is used in conjunction with the unsubscribe mechanism: not only must the sender describe this mechanism clearly and prominently, but s. 3(2) of Regulation SOR/2012- 36 specifies that the mechanism itself must be able to be ''readily performed." As will be discussed further on, the CRTC is more eloquent in this regard, and perhaps its interpretation[94] could bring to life the meaning of this expression when associated to web pages.

To summarize, CASL prohibits the sending of a CEM to an electronic address, unless the recipient has given prior consent, as long as the message allows the recipient to identify and communicate with the sender, in addition to providing a compliant unsubscribe mechanism. These general requirements, nevertheless, include several exclusions that are worth considering.

1.1.3 Excluded Messages

Certain exclusions are general (1.1.3.1); others are partial (1.1.3.2).

1.1.3.1 Messages Receiving a Full Exemption

It is not required to obtain the recipient's prior consent, nor to disclose the sender's identity as prescribed or to comply with the unsubscribe mechanism provisions, where a natural person sending a CEM has a personal or family relationship with the recipient.[95] This rule applies equally to any CEM that constitutes solely an inquiry or application regarding the recipient's commercial activities, and certain other messages whose category and sending circumstances are specified in the Regulations. These include a CEM sent from Canada where the sender has reasonable grounds to believe that it will be accessed in a foreign state covered by the Regulations;[96] a CEM sent by or on behalf of a registered charity, if the main objective is fundraising; and a CEM sent by or on behalf of candidates or political organizations with the primary purpose of soliciting political contributions, whether monetary or not.[97]

The last two exceptions were missing in the 2013 draft Regulations, drawing the attention of some stakeholders, including the Association of Universities and Colleges of

---

93 For further study of the concept of accessibility of contractual provisions in electronic commerce, see Serge Kablan & Edward O Onana, "Formation du contrat électronique : L'acceptation entre mutations et orthodoxie" (2015) 1 Ottawa L Rev 63 at ff 108.

94 See Part 2.3 of this article.

95 Section 6(5)(a)-(b) of CASL, *supra* note 8, also recall the exception of paragraph 7 regarding carriers that provide a telecommunications service to enable the transmission of the message. Broadcasting companies (for everything related to broadcasting) are exempted as well. Advertisements of these companies remain subject to the *Broadcasting Act* (see CASL, *supra* note 8, s. 5).

96 The message must nevertheless comply with anti-spam law of that State. This law must be analogous to CASL, which imposes on the sender a certain diligence. See *Electronic Commerce Protection Regulations*, SOR/2013-221, Schedule 1.

97 Other CEMs are concerned. See SOR/2013-221, *supra* note 96, s. 3; CASL, *supra* note 8, s. 6(8) (live voice telemarketing and telemarketing by facsimile. Currently governed by s. 41 of the *Telecommunications Act*, S.C. 1993, c. 38, these activities could later be subject to CASL).

Canada (now Universities Canada — UC). UC was concerned with not being able to determine whether certain communications from universities in the pursuit of their educational goals would be treated as spam.[98] One way to counter these uncertainties, UC submitted with limited success, would be to give a full exemption to universities and charities. The association suggested as well going beyond the current exemption for fundraising messaging and even exceeding the solution set out in Australian Schedule I, which excludes messages sent by educational institutions to specific groups, comprising students, alumni, and household members.[99]

The exception for personal or family relationships also raises concerns. First, as defined in the Governor General in Council Regulations, the sender and recipient have family relationships if they are related to one another through marriage, common-law partnership, or any legal parent-child relationship. Moreover, the parties must have had a direct, voluntary two-way communication.[100] The original draft Regulations published on January 5, 2013, were more inclusive, encompassing individuals with common grandparents, as well as uncles, aunts, cousins, nieces, and nephews.[101] Secondly, as with family relationships, personal relationships assume a direct, voluntary two-way communication. The personal nature of the relationship should reasonably appear from these communications, taking into account certain indicators, such as shared interests, experiences, opinions and information, frequency of communications, the fact that parties may meet in person, etc.[102]

Some authors are convinced that these requirements could render the Canadian anti-spam law unconstitutional, because they make the Act too restrictive. Professors Crowne and Provato, in particular, have reviewed CASL in the light of s. 2(b) of the *Canadian Charter of Rights and Freedoms* (the "*Charter*").[103] To them, the Act fails to pass this test, considering its effects on communications and ordinary relationships and its impact in general.[104]

Section 2(b) of the *Charter* describes certain fundamental freedoms protected by the Constitution: "Freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication." In light of the case law of the Supreme Court of Canada,[105] the authors claim that a CEM under CASL constitutes an "expression"

---

98 Such as recruiting students. See letter from Association of Universities and Colleges of Canada to Industry Canada (4 February 2013).

99 *Spam Act 2003*, *supra* note 18, Schedule 1—Designated commercial electronic messages, s. 4.

100 SOR/2013-221, *supra* note 96, s. 3(a).

101 Electronic Commerce Protection Regulations — Regulatory Impact Analysis Statement, (2013) C Gaz I 29 (see s. 2(a) of the draft regulations).

102 *Ibid,* s. 3(b).

103 *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act, 1982 UK,* 1982, c. 11, s. 2(b) [*Charter*].

104 Emir Crowne & Stephanie Provato, "Canada's Anti-Spam Legislation: A Constitutional Analysis" (2014) 1 John Marshall J Info Tech & Privacy L 1.

105 The authors cite: *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927, [1989] S.C.J. No. 36, 1989 CarswellQue 115F, 1989 CarswellQue 115,15 A.C.W.S. (3d) 121 (S.C.C.); *Ford v. Quebec (Attorney General)*, [1988] 2 S.C.R. 712, 1988 CarswellQue 155F, 1988 CarswellQue 155, [1988] S.C.J. No. 88 (S.C.C.) [*Ford*]; Crowne & Provato, *supra* note 104 at 12-13.

protected by the *Charter*.[106] They then set out to determine if CASL complies with s. 1 of the *Charter*, by checking if the constraints that the Act imposes are "reasonable limits […] as can be demonstrably justified in a free and democratic society."[107] In its decision in *R. v. Oakes*, the Supreme Court of Canada restates the cumulative criteria for analysis, among which is the requirement that the legislation under scrutiny "[…] should impair 'as little as possible' the right or freedom in question […]."[108] The decision rendered by the U.S. Supreme Court in the case of *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York*[109] provides a framework for comparative analysis, for deciding whether the CAN-SPAM Act respects the First Amendment of the U.S. Constitution.[110] Some authors hold the belief that CAN-SPAM complies whith the First Amendment, on the ground that it is no more restrictive than necessary: ''the registry was narrowly tailored because it restricted 'only speech that contributes to the problems the government seeks to redress.'"[111]

By contrast, according to Crowne and Provato, the way family relationships are defined and organized under CASL clearly undermines this principle. As rightly suggested, it can hardly be justified, even from the perspective of fighting spam, that first cousins are by definition people with whom one has no "family relationships." Nonetheless, CASL limits freedom of expression accordingly by making illicit any CEMs that are sent between first cousins, unless the prescribed formalities are satisfied.[112] This vision of family relationships is said to be so narrow that it restricts communications and harmless ordinary relations, prompting the authors to question the proportionality between these effects and the objectives the law is pursuing. The definition of personal relationships is similarly flawed because of its vagueness. Surprisingly, it derogates from the principle of technology neutrality usually demonstrated by CASL. The authors make the following assertion:

> This definition is imprecise. It relies on a vague appeal to reasonableness and a series of non-limiting factors that appear to restrict "personal relationships" to only close friends. Thus, under CASL, many friends, colleagues, and acquaintances will not fit within the definition of acceptable recipients of communication […] While CASL is intended to be technologically neutral, the factor that examines whether the parties have met in person is evidence that it still favors traditional relationships over virtual ones. Thus, CASL has the negative effect of restricting

---

106 *Ford, supra* note 105, cited by Crowne & Provato, *supra* note 104. See especially para 59 of the judgment.

107 *Charter*, *supra* note 103, s. 1. See also Crowne & Provato, *supra* note 104 at 17.

108 *R. v. Oakes,* [1986] 1 S.C.R. 103, 1986 CarswellOnt 1001, 1986 CarswellOnt 95, [1986] S.C.J. No. 7, 26 D.L.R. (4th) 200 (S.C.C.), cited by Crowne & Provato, *supra* note 104.

109 447 U.S. 557 (1980).

110 Vivek Arora, "The CAN-SPAM Act: An Inadequate Attempt to Deal with a Growing Problem" (2006) Colum JL & Soc Probs 299 at 305-306. See also: Jameel Harb, "*White Buffalo Ventures, LLC v. University of Texas at Austin*: the CAN-SPAM Act & the Limitations of Legislative Spam Controls" (2006) BTLJ 531 at 537.

111 Vivek Arora, *supra* note 110.

112 Crowne & Provato, *supra* note 104 at 17.

> and hindering harmless communications, potentially stunting social networking.[113]

We believe that the CRTC's warning about social media does favor traditional relationships. At least, the Commission doubts the strength of certain relationships emerging from social media. It states for instance that "using social media or sharing the same network does not necessarily reveal a personal relationship between individuals. The mere use of buttons available on social media websites — such as clicking "like", voting for or against a link or post, accepting someone as a "Friend", or clicking "Follow"— will generally be insufficient to constitute a personal relationship."[114]

While these restrictions to freedom of expression would likely be challenged, the final impact of CASL is already substantially modified by the partial exclusions it grants.

1.1.3.2 Partial Exemptions

For some CEMs, CASL removes the obligation to seek prior consent. These CEMs must however comply with the other sending conditions, by providing identification information about the sender and the unsubscribe mechanism. Beneficiaries of this partial exclusion are CEMs falling within the circumstances
listed in s. 6(6)(a)-(f).[115]

This list is imported from U.S. law where it defines "transactional or relationship messages".[116] The Canadian Regulations add to that list a CEM following a referral.[117] In this latter case, two conditions must be met. First, the individual who recommends a party (e.g., a potential customer) to another person (e.g., an online retailer who will eventually send the CEM) must have an existing business, non-business, family, or personal relationship with both parties. The potential customer must be a natural person and the exemption to obtaining prior consent applies only to the first CEM sent by the retailer following the referral. Second, this initial CEM must disclose the full name of the person who made the referral (apparently, to allow the recipient to differentiate the CEM from typical spam messages),[118] and stipulate that the message follows a referral. The Regulations do not clearly specify the aim of this first message, except to say that it is for

---

113 *Ibid,* at 18.

114 CRTC 2012-548, *supra* note 83.

115 That is, the response to a request for a price quote or estimate; messages that are intended to facilitate, complete, or confirm a commercial operation that the recipients have previously agreed to enter into; messages that provide information on warranties, recalls, or safety for a good or service used or bought; messages that provide factual information about an ongoing relationship (subscription, registration, account, loan, or similar relationship); messages that provide information on the status of an employee of the recipients or their beneficiaries; messages which deliver a product/service under the terms of a transaction the parties have previously entered into.

116 Under the CAN-SPAM Act, these messages are not considered as CEMMs. See *supra* note 16, ss. 7702(2)(B), 7702(17): "*The term 'commercial electronic mail message' does not include a transactional or relationship message.*" See also *Primary purpose*, 16 CFR s. 316.3(b)-(c) [2008]; *U.S. v. Rad* 559 Fed.Appx. 148 (Third Cir. 2014).

117 SOR/2013-221, *supra* note 96, s. 4(1).

118 Regulatory Impact Analysis Statement, Canada supra note 101, s. 6 (proposed exemptions to address stakeholder concerns).

contact. A question remains whether it should be designed to seek or confirm consent or for outright promotional purposes. In the face of such ambiguity, senders would have every interest in favouring the latter hypothesis, which is less restrictive, since it gives an opportunity to promote and sell while mitigating the requirement of consent.

These rules have been criticized, and comments by parliamentarians like Charmaine Borg are worth noting. The former member argued that the provisions were contrary to the opt-in model promoted in CASL, which suggests that one can not consent on behalf of a third party. Ms. Borg had detected a weakness in this scheme, a risk of a certain abuse.[119] On closer inspection, the loophole in CASL seems real, even though only the first CEM following a referral is exempt from consent. One expects that advertisers will quickly seize the golden opportunity to do viral marketing.[120] The reasoning is simple: under CASL, one can not send a CEM without the recipient's prior consent, and the request for consent is itself regarded as a CEM and therefore subject to prior consent; but the prior consent requirement is waived for the first CEM following a referral. The consequence, perfectly embodied by viral marketing, is very likely: urging existing customers (through discount offers, direct subsidies, etc.) to refer potential customers from their respective networks (whether business, private, family, or personal) to whom the first CEM would be sent. If these referrals are successful, each new client could in turn provide new referrals, and the following clients as well, extending the campaign into infinity, at least theoretically.

A referral is as simple as passing along to the advertiser the third party's contact information.[121] It may be sufficient to use the tools of viral marketing. We think of electronic forms to collect and forward e-mail addresses of the referees (possibly without the referees' knowledge).[122] CASL is therefore, in the end, closer to the U.S. CAN-SPAM Act in indirectly providing to senders the coveted "chance to initiate contact"![123] This outcome is surprising, given the government's initial choice to require consent and place

---

119 See letter from Ms. Charmaine Borg, former MP for Terrebonne — Blainville, to Mr. Christian Paradis (8 February 2013) entitled "Antispam Regulations."

120 Service public fédéral, économie, PME, classes moyennes et énergie, "La légalité du marketing viral" Direction générale Régulation et Organisation du Marché (September 2005) (Belgium); see also: MS Poorvika & NV Kavitha, "A Study on Impact of Viral Marketing on Consumers" (2014) 4 International Journal Of Marketing, Financial Services & Management Research 150; J Phelps, et al, "Viral Marketing or Electronic Word-of-Mouth Advertising: Examining Consumer Responses and Motivations to Pass Along Email" (2004) Journal of Advertising Research 333.

121 *Regulatory Impact Analysis Statement, supra* note 101, s. 4.

122 One may wonder if the disclosure of a third-party email addresses may violate the provisions of other legislation. About that, it is worth recalling CASL, *supra* note 8, s. 2: "In the event of a conflict between a provision of this Act and a provision of Part 1 of the *Personal Information Protection and Electronic Documents Act*, the provision of this Act operates despite the provision of that Part, to the extent of the conflict."

123 The FTC announced new rule provisions on May 12, 2008. These provisions cover a number of topics, including "Forward-to-a-Friend" Email Campaigns "in which someone either receives a commercial e-mail message and forwards the e-mail to another person, or uses a Web-based mechanism to forward a link to or copy of a Web page to another person. The SBP explains that, as a general matter, if the seller offers something of value in exchange for forwarding a commercial message, the seller must comply with the Act's requirements, such as honoring opt-out requests." See 16 CFR part 316 (2008).

the opt-in mechanism at the heart of the regime. This choice involves two other matters that should be understood before analyzing the mechanism of consent: transmission data and computer programs.

1.2 Rules for Transmission Data and Computers

For simplicity, we study the rules for transmission data (1.2.1) before those relating to computer programs (1.2.2).

1.2.1 Transmission Data

A second prohibition introduced by CASL relates to transmission data, meaning signs, signals, symbols, or concepts regarding or necessary for the transmission of a telecommunications service.[124] Electronic addresses are among these data, including the date and time which a message is sent, the size of any attached file, the SMTP protocol used, the unique identification number of the message, the IP addresses and service providers involved, the number of attachments, etc.[125]

Section 7(1) prohibits the alteration of these data in the course of commercial activities in a way that the corresponding message would be delivered to a destination other than or in addition to that specified by the sender. It is explained that the provision is intended to counter phenomena like pharming. Pharming is an online fraud that involves altering CEM transmission data to redirect parties to a malicious or illegitimate URL where, by deception, they are induced to disclose their personal information.[126] Here, the prohibition does not apply to telecommunications service providers who modify transmission data for purposes of network management (s. 7(2)). Similarly, alteration of transmission data is permitted with express consent of the sender or recipient of the corresponding message. The latter could give this consent, for example, by allowing the message to be intercepted by an email filter.[127] But there must be an unsubscribe mechanism: "an electronic address to which [the person who gave their consent] may send notice of the withdrawal of their consent."[128] Finally, the alteration of transmission data is permissible if it is in accordance with a court order.[129]

Under the CAN-SPAM Act, certain requirements on header information aim to combat "fraud and related activity in connection with electronic mail," and, more specifically, predatory and abusive messages.[130] The definition of header information resembles that of transmission data in CASL. It includes information that allows location of the source and the destination of an electronic message. It also comprises routing information, the domain name and address of origin, as well as "any other information that appears in the line identification [identification field], or purporting to identify a

---

124 CASL, *supra* note 8, s. 1(1).

125 For an illustration, see Google "Gmail Help—Trace an e-mail with its full headers," online: <support.google.com/mail/answer/29436?hl=en>.

126 ISED, *supra* note 43 at 36. See also: Gouvernement du Canada, "Risques de cybersecurité," online: <www.pensezcybersecurite.gc.ca/cnt/rsks/index-fr.aspx>.

127 *Ibid.*

128 See CASL, *supra* note 8, s. 11(4)(a).

129 *Ibid*, s. 7(1)(b).

130 CAN-SPAM Act, *supra* note 16, s. 7703.

person initiating the message."[131] According to s. 4§7703(a)(3) of the Act, whoever materially falsifies[132] header information of more than 100 CEMMs during a 24-hour period, more than 1,000 CEMMs in a 30-day period, or over 10,000 CEMMs through a 1-year period, and intentionally initiates the transmission of these messages, may be punished by fine and/or imprisonment. Header information is materially falsified if the alteration impairs the ability to identify, locate, or respond to the initiator of the CEMM or to investigate the alleged violation.[133]

Other provisions of U.S. law generally prohibit header information that is materially false or misleading, such as when this information does not identify accurately the protected computer[134] used to transmit that message.[135] The initiator of a CEMM who knowingly uses another protected computer to relay or retransmit the message so as to conceal its true origin and prevent any communication back to him or her, is caught by this prohibition.[136] This particular situation is discussed in the case of *Facebook, Inc. v. Power Ventures, Inc., et al.,*[137] and the outcome will inevitably help to clarity the meaning of the provision. In this case, to promote its services, the defendant (Power) initiated a campaign that allowed users of the plaintiff (Facebook) to refer members of their network. Following these referrals, invitation e-mails were sent to the prospects from Facebook servers, suggesting that these messages, which use an address including the extension @facebookmail.com, came from Facebook. The district court ruled that this process contravened the CAN-SPAM Act. Header information of the CEMMs was misleading, since it did not specifically identify the actual initiator of these messages, nor did it allow the recipients to communicate directly with him or her.[138] The defendant, however, appealed this verdict and the *Electronic Frontier Foundation* (EFF) filed an *amicus* brief in support of the defendant.[139] At the very least, the EFF claimed that the court erred in adopting a purely technical approach, which deduces liability from mere material error. Supported by various authorities,[140] the EFF submitted that it was necessary to assess the misleading nature of header information by taking into consideration the general context of the CEMMs. For this purpose, the relevant information (identity, contact information of the initiator, etc.,) must be sought in the other elements of the message, such as the presence of an opt-out option or the message

---

131 *Ibid*, s. 7702 (8).

132 *United States v. Kilbride,* 507 F. Supp. 2d 1051, 1064 (D. Ariz. 2007).

133 CAN-SPAMAct, *supra* note 16 s. 7703(d)(2). See *U.S. v. Kilbride*, 584 F.3d 1240 (9th Cir. 2009).

134 *Supra* note 58.

135 CAN-SPAM Act, *supra* note 16, s. 7704(a)(1).

136 *Ibid*, s. 7704(a)(1)(C), 7704(a)(6). Section 7704(a)(1)(A) mentions also the case where certain information (the original address, for example) had been obtained fraudulently.

137 *Facebook, Inc., v. Power Ventures, Inc., et al.,* United States District Court, N.D. California, San Jose Division, No. C 08-05780 JW.

138 *Ibid,* at paras 12-13.

139 *Ibid*, (Amicus Curiae Brief of Electronic Frontier Foundation in Support of Defendants-Appellants) [EFF].

140 See *Omega World Travel, Inc. v. Mummagraphics*, Inc., 469 F.3d 348 (4th Cir. 2006) [*Omega*], cited by EFF, *ibid* at 27.

text itself and any references it includes.[141]

The United States Court of Appeals hold that the messages at issue were not materially misleading.[142] First, the court explained that within the meaning of the CAN-SPAM Act, "more than one person may be considered to have initiated a message." In this action, it does appear that Power's users, Power, and Facebook all initiated the messages: "A Power user gave Power permission to share a promotion, Power then accessed that user's Facebook data, and Facebook crafted and caused form e-mails to be sent to recipients." The court accordingly concluded that "Because Facebook (among others) initiated the messages, the 'from' line accurately identified [Facebook as] a person who initiated the messages." Second, by design, the messages at issue did not impair the ability of a reasonable recipient to contact or respond to the initiator.

All things considered, the reach of the CAN-SPAM Act remains broader than that of Canadian law regarding header information, as the former governs the alteration or falsification of this information as well as situations where it is simply false or misleading.[143]

Furthermore, there is a relative difference between the two laws regarding the prohibition pertaining to computers, including those used for the transmission of CEMs/CEMMs.

1.2.2 Computer Programs

Under the CAN-SPAM Act, it is an offense to gain unauthorized access to a protected computer and initiate the transmission of multiple CEMMs by or from this computer. The rule is stated as follows:

> Whoever, in or affecting interstate or foreign commerce, knowingly—
>
> > (1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer, […] or conspires to do so, shall be punished as provided in subsection (b).[144]

In substance, s. 8(1) of CASL remains close to this provision, although the Canadian prohibition clearly distinguishes two activities, with a slightly wider scope. First, s. 8(1) prohibits, within the framework of commercial activities, the installation of a computer program in another person's computer system, except if the owner of the computer or

---

141 *Ibid* at paras 27-28.

142 *Facebook, Inc. v. Power Ventures, Inc.,* 844 F.3d 1058, 1065 (9th Cir. 2016), cert. denied, 138 S. Ct. 313, 199 L. Ed. 2d 206 (2017).

143 See Omega, *supra* note 143. ("Inaccuracies in e-mail headers referring to non-functional e-mail address as sender and an Internet domain not linked to sender did not make the headers materially false or materially misleading and, therefore, did not violate [CAN-SPAM Act]."); *Silverstein v. Experienced Internet.com., Inc.* 266 Fed.Appx. 678 (9th Cir. 2008) (e-mails' use of domain name of professional networking website or of fictitious "from" names were not materially false or misleading); *Silverstein v. Keynetics, Inc.,* 2018 WL 1164715 (9th Cir, 2018).

144 CAN-SPAM Act, *supra* note 16, s. 7704(a)(1)-(2).

an authorized user, such as an employee, has given his or her express consent to this installation and is provided with an unsubscribe mechanism.[145] Secondly, CASL prohibits, under the same conditions, the sending of a CEM from that computer system once the program has been installed.

Obviously, the first activity excludes personal installations. Even so, whether the computer program is used or could be used to send CEMs is irrelevant. The letter of s. 8(1) suggests that the program is subject to the rigor of the law as soon as its installation is considered to occur in the context of a commercial activity. Parliament thus seems to insert into CASL a matter not necessarily related to spam, as "computer program" is given the meaning of s. 342.1(2) of the *Criminal Code* which includes without distinction all "computer data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function." This is the case for softwares in desktops or laptops, smart phones, smart watches, game consoles,[146] smart glasses, etc.[147] The purview of the Act is, therefore, considerably expanded.

The other activity covered by s. 8(1) of CASL is closer to the spirit of s. 7704(a)(1) of CAN-SPAM Act.[148] This is the sending of CEMs following the installation of a computer program in another person's computer system. Just as in the CAN-SPAM Act, through the definition of protected computer, a requirement of territoriality exists in Canadian law. Section 8(1) of CASL is contravened in each of the following three situations: first, when the computer system is located in Canada at the time of the alleged acts; second, when the perpetrator is in Canada at that time; third, when the perpetrator acts on the instructions of a person who is in Canada at the time these instructions are given.[149]

Up to this point, CASL seems not very different from the CAN-SPAM Act, despite some differences in its scope. CASL takes a wide-ranging approach with respect to CEM. This approach creates prohibitions that may transcend what is necessary to fight spam, potentially exposing the Act to judicial challenges. The CAN-SPAM Act enlarges its reach, in turn, regarding transmission data, but is again surpassed by CASL with respect to computer programs. The U.S. law keeps its focus on this point on fighting spam, unlike the Canadian law.

More fundamentally, both laws have in common the requirement of consent. It is true that they frame commercial electronic messages from different perspectives, with CASL subscribing to the opt-in model and the CAN-SPAM Act to opt-out. But the exclusions provided by the Canadian Regulations, particularly the one that authorizes the sending of CEMs following referrals, impairs the effect of the regime intended by the creators of the law. As a result, CASL indirectly offers senders the opportunity to initiate

---

145 See Part 2.3 of this article. As for transmission data, the prohibition does not apply if the installation is in accordance with a court order.

146 See, e.g., *R. c. Hamel*, 2011 QCCQ 11103, 2011 CarswellQue 10168 (C.Q.) at para 21.

147 In its judgment *R. v. Fearon*, [2014] 3 S.C.R. 621, 2014 CSC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203, [2014] S.C.J. No. 77 (S.C.C.), the Supreme Court of Canada deals with computers (in general) and these devices as similar devices or functional equivalents (for some).

148 At least, if it is considered that sending a CEM from a protected third-party computer may require the installation of a computer program.

149 CASL, *supra* note 8, s. 8(2).

contact, just as is the case under the CAN-SPAM Act. The ostensible strictness of CASL is thereby greatly attenuated. One is reminded of the parody that once served to denounce the CAN-SPAM Act: "You Can Spam Act."[150]

It remains to be seen if the similarities between CASL and the CAN-SPAM Act persist in the way they formulate the procedures for obtaining and managing consent.

2. THE TERMS AND CONDITIONS OF CONSENT

Where consent is required for sending a commercial electronic message (s. 6 of CASL), altering transmission data (s. 7) or installing a computer program (s. 8), the will of the recipient must be explicitly stated (2.1). But consent can also be implied under certain circumstances (2.2). In all cases, there must be an option to unsubscribe or a mechanism for the person who has given his or her consent to withdraw it (2.3).

2.1 Obtaining and Managing Express Consent

CAN-SPAM Act uses the term *Affirmative Consent* with regard to CEMMs. Section 15 USC 7702(1) provides this definition:

> AFFIRMATIVE CONSENT. —The term "affirmative consent", when used with respect to a commercial electronic mail message, means that—(A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

For its part, CASL does not directly define consent or express consent. It gives more attention to the way it should be obtained. Nevertheless, a case involving Google and its operating system, Android, shows that there may be uncertainty about the meaning of consent, as in contexts involving mobile communication apps.[151] The case arose under PIPEDA, but since CASL finds some of its roots in this Act, the example is still relevant.

Pursuant to Principle 4.3.3 laid out in Schedule 1 of PIPEDA, "An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes." The complainant in the case alleged that Google had compelled him to grant several "permissions" before he was able to use the app Google Search. A number of these permissions, according to the complainant, were

---

150 See, e.g., Steve Linford, "United States set to Legalize Spamming on January 1, 2004," SPAMHAUS (22 November 2003), online: <www.spamhaus.org/news/article/150/united-states-set-to-legalize-spamming-on-january-1-2004>.

151 Canada, Office of the Privacy Commissioner, ''Report of Findings underPIPEDA," No. 2014-008 (2014), online: <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2014/pipeda-2014-008/>.

not necessary for the use he intended for the app, such as to enable it to place calls, send SMS, take pictures, make videos, etc. In its response, Google explained, to the satisfaction of the Office of the Privacy Commissioner of Canada (hereinafter, the "Commissioner"), that "the permissions requested by an app describe the app's technical capabilities, and not necessarily its actual behaviors."[152] The Commissioner could not conclude that the disputed permissions added up to a consent that would allow Google to go above and beyond what was necessary for its service. The conclusion is this:

> In general, requiring a user to grant a permission to an app is not equivalent to requiring that user to consent to the collection, use or disclosure of the personal information associated with the permission. As such, requiring agreement to a permission would not represent a contravention of Principle 4.3.3 of the Act; however, nor would it necessarily represent consent to any collection, use or disclosure of personal information.[153]

If *permission* is not necessarily *consent*, it may be useful to seek certainty as to the definition of consent, including under CASL. As in the U.S. (with the term "affirmative consent"), the French legislature engages in such clarification. Section 22 of the LEN gives this definition of consent: "consent means any expression of free, specific and informed will, by which a person agrees to the use of his or her personal data for direct marketing purposes." (Free translation).

With regard to formalities, pursuant to the age-old principle that requires an informed decision, CASL directs the person seeking express consent under ss. 6, 7, and 8 to make his or her request under strict conditions as to substance and form (2.1.1). Special terms apply to situations where the request is made on behalf of a third party whose identity is unknown (2.1.2). Finally, there is another peculiarity relating to computer programs (2.1.3).

2.1.1 The Wording of the Request for Consent

The first test any request for express consent must meet is standard, as already set out in other legislation, such as PIPEDA. According to this Act, for the collection of personal information to be lawful, not only must the purposes of the collection be disclosed, but it is necessary for the person giving consent to "reasonably understand" these purposes.[154] CASL establishes the same principle in s. 10(a). It stipulates, in addition to the unsubscribe mechanism that must be provided, the obligation for the entity seeking consent to disclose its identity and contact details or those of the person on whose behalf consent is sought.[155]

The request for consent must use simple and clear words. The choice is left whether the request is made orally, as in PIPEDA,[156] on paper, or electronically (e.g., by means of

---

152 *Ibid*, at para 68.

153 *Ibid*, at para 69.

154 PIPEDA, *supra* note 45, Schedule 1, s. 4.3.2.

155 CASL, *supra* note 8, s. 10(1)(b); SOR 2012-36, *supra* note 85, s. 4.

156 PIPEDA, *supra* note 45, Appendix 1, para 4.3.7.

an electronic form). The alternative thus offered seems useful to prevent the additional costs and frustrations that a solution requiring a written form would have caused businesses and consumers.[157] The first option nevertheless raises the inevitable issue of proof of consent, which, fortunately, the CRTC attempts to mitigate by admitting that the expression of will could be ascertained or verified by an independent third party or by a "complete and unedited audio recording of the consent."[158] These terms are reminiscent of the CRTC Unsolicited Telecommunications Rules.[159] In the second option, especially when an electronic method is used to obtain consent, the relevant information must be verifiable in order for the obligation to be validly fulfilled.[160] Like the rules on unsolicited telecommunications, s. 13 of CASL provides that the burden of proof is upon the person alleging consent.

A separate request for consent must be submitted for each of the three activities covered by CASL (e.g., sending CEMs, altering transmission data, installing computer programs).[161] According to the CRTC *Guidelines on the Interpretation of the Electronic Commerce Protection Regulations,* this requirement does not mean that a new request is needed whenever an action under one of the three activities is intended. Consent is more about each activity considered as a whole: when a consumer gives consent for CEMs, this acceptance applies to all specified CEMs, but does not allow alteration of transmission data nor installation of computer programs. This is supposed to give the consumer the opportunity to agree to be party to only one or two of these activities, unless he or she accepts or rejects them all.[162] In addition, in the interest of clarity, the CRTC requires that the request for consent be presented separately from the General Terms of Use or the General Terms of Sale.[163] Thus, the consumer would consent to be bound by these general conditions and, if necessary, consent separately to each of the three activities of CASL. This idea of separate consent was considered unreasonable and unnecessary by some stakeholders, but the CRTC still believed in its relevance.[164] In practice, however, the procedure of online consent is considerably more onerous, mainly since electronic contracts often involve acceptance of some additional clauses (distinct from the general conditions).[165] One has to wonder if this really protects the consumer.

To the request for express consent, the response of the consumer must use actions that allow a positive or explicit manifestation of the will; it is not sufficient, for example, to rely on pre-checked boxes presuming consent unless stated otherwise.[166] The CRTC has

---

157 See CRTC 2012-183, *supra* note 91, s. 25.

158 CRTC 2012-548, *supra* note 83at para 23.

159 Canadian Radio-television and Telecommunications Commission, "Unsolicited Telecommunications Rules," online: <crtc.gc.ca/eng/trules-reglest.htm>. See PartVon the express consent.

160 CRTC 2012-548, *supra* note 83 at para 25.

161 *Ibid*.

162 *Ibid*, at paras 14-15.

163 *Ibid,* at para 16.

164 *CRTC* 2012-183, *supra* note 91, s. 27.

165 Kablan & Onana, *supra* note 93 at 105.

166 Canadian Radio-television and Telecommunications Commission, "Guidelines on the use of toggling as a means of obtaining express consent under Canada's anti-spam legislation," Compliance and Enforcement Information Bulletin 2012-549 (Ottawa: CRTC, 2012) at para 4.

approved two techniques that are, however, barely technologically neutral (therefore, difficult to apply to all communication devices): on the one hand, checking a box before confirming an online transaction (for example, the purchase of software); on the other hand, entering one's e-mail address in a dedicated field to express consent to receive CEMs.[167] To complete the process, an acknowledgment of receipt must be sent to the person who gave consent.[168] Moreover, the use of hyperlinks within the text mandating action from the consumer does not seem to matter. At least, the CRTC guidelines allow the latter to be redirected to secondary pages where useful information for the decision-making may be posted.[169]

2.1.2 Consent on Behalf of a Third Party

CASL addresses the instance where a person is seeking express consent on behalf of another person whose identity is not known at the time of the request.[170] One can possibly equate the CASL provision with the principle of *affirmative consent* of the CAN-SPAM Act indicated above.[171] Consent in this case (e.g., under U.S. law) covers the situation where, in the course of business, the commercial electronic mail message originates from a party other than the party to whom consent was first given. The recipient must have received a clear and conspicuous notice, at the time consent was communicated, that his or her electronic mail address could be transferred to the third party for the purpose of initiating the sending of commercial electronic mail messages. These messages must also comply with the other requirements (e.g., regarding identification of the sender and the opt-out mechanism).[172]

Canadian law has some complex peculiarities (although the basic idea remains the same as in the CAN-SPAM Act) when at least three parties are involved: first, the person requesting express consent (for example, a marketing firm); next, the recipient who consents; and finally, the third party on whose behalf consent is sought and who is eventually entitled to rely on this consent ("the authorized person" or "partner"). The rights and obligations of these three parties are strictly laid down in s. 10(2) of CASL and s. 5 of the *Electronic Commerce Protection Regulations*.[173] Foremost, the marketing firm seeking express consent on behalf of an unidentified third party must reveal its own identity. It may authorize any person or partner to use the resulting consent, on the condition that its identity is established as the person who obtained the original consent. Furthermore, the authorized person or partner who sends a CEM in this context is

---

167 *Ibid*, at para 8.

168 *Ibid*.

169 About the use of hyperlinks under s. 1435 of Québec Civil Code, *Union des consommateurs c. Dell Computer Corp*., [2007] 2 S.C.R. 801, 2007 SCC 34, 2007 CarswellQue 6310, 2007 CarswellQue 6311, [2007] S.C.J. No. 34 (S.C.C.). The Supreme Court of Canada ruled that a "clause that requires operations of such complexity that its text is not reasonably accessible can not be considered as part of the contract." See Serge Kablan& Arthur, Oulaï "La formalisation du devoir d'information dans les contrats de cyberconsommation : analyse de la solution québécoise," (2009) RDMcGill 627 at 658ff.

170 CASL, *supra* note 8, s. 10(2).

171 CAN-SPAM Act, *supra* note 16, s. 7702(1).

172 *Ibid.* See also s. 7704(a)(4)(B).

173 SOR /2013-221, *supra* note 96.

required to identify itself and provide an unsubscribe mechanism consistent with s. 11 of CASL. [174]

Communication between the person who obtains consent and the partners it authorizes must be unhampered. The former ensures that the latter notify him as soon as the recipient's consent is withdrawn. Similarly, when receiving an unsubscribe notice concerning an authorized partner, the person who obtained consent must immediately notify this partner and comply with the request. [175] Behind this (rather restrictive) set of rules, there is the purpose, certainly justified, of protecting consumer privacy and allowing effective control over the use of a person's electronic address, even with regard to unknown third parties. The obligation regarding the unsubscribe mechanism which must be both simple and functional is consistent with this objective, the ultimate responsibility of which is on the person seeking express consent.

2.1.3 The Case of Computer Programs

The following paragraph of the parliamentary proceedings is striking, as the provisions on computer programs appeared to be innovative [though, reality is more nuanced]:

> What sets this spam legislation apart from everybody else's is clauses 8 and 9, which are new pretty much to the world. Whereas we've learned from the rest of the world, in this particular case the rest of the world will be learning from us over the next few years.[176]

In particular, where it is mandatory to obtain express consent for the installation of a computer program, or after installing or having installed such a program in a computer system, for the sending of CEMs from that computer system (s. 8(1)(a)) [177]the person

---

174 See Part 2.3 of this article.

175 CASL, *supra* note 8, s. 11(3). In an attempt to reassure the parties about these formalities which, arguably, it knows are onerous, ISED felt compelled to make this clarification: "Some stakeholders expressed concern that these Regulations would require third parties to allow the recipient to withdraw their consent to receive messages directly from the person who acquired the third-party consent. To be clear, there is no requirement for the third parties to provide the opportunity to withdraw consent from all commercial messages directly from the person who acquired consent; the requirement is limited to removal of consent to receive messages from third parties." See Industry Canada, "Regulatory Impact Analysis Statement, Electronic Commerce Protection Regulations, "online: <combattrelepourriel.gc.ca/eic/site/030.nsf/eng/00271.html>. Thus, two contexts are distinguished: it is indeed possible that the person who obtained express consent from the recipient on behalf of third parties whose identities were unknown at the time of the request (the first context) would have obtained separately, for their own account, express consent to send CEMs to the same recipient (the second context). Withdrawal of consent in the first context (consent obtained on behalf of third parties) only affects that context and does not apply to the second context (consent obtained on one's own account). This allows the person involved to continue sending CEMsto the recipient despite the withdrawal, at least as long as consent is not withdrawn in the second context as well.

176 Standing Committee, *supra* note 38 at 6.

177 As with sending CEMs under s. 6, the scope of s. 8(1) includes a geographical restriction, at least the need for link with Canada in order to apply. Thus, the person who, without express consent, installs a computer program in another person's computer, or which sends a CEM by this computer after

seeking consent must comply with a number of additional requirements (that is, in addition to those set out in s. 10(1)). [178] On the one hand[179], the person seeking consent must "clearly and simply describe, in general terms, the function and purpose of the computer program that is to be installed if the consent is given." (s. 10(3)). [180] On the other hand, s. 10(4) introduces specific requirements for any program intended to fulfill any one of the functions listed in s. 10(5) of CASL or by the Regulations. [181] According to s. 10(4), the person seeking express consent for the installation of such a program in another person's computer system, and who knows and intends that the program will cause the computer to operate in a manner contrary to the reasonable expectations of the owner or an authorized user, must: (1) describe the program's material elements that perform the functions listed and (2) bring these elements to the recipient's attention. Once again, this must be done "clearly and prominently, and separately and apart from the license agreement."

The formalities are even more restrictive: s. 5 of Regulation SOR/2012-36 stipulates that the computer program's material elements performing the specified functions must be brought to the attention of the recipient separately from any other information provided in the request for consent. In addition, the applicant has the obligation to obtain an "acknowledgement in writing" (either on paper or electronically) from the recipient certifying that he or she understands fully what is to be done to him or her. That is to say, the recipient understands and agrees that the computer program will perform the functions described in the request. One wonders how this will translate into practice, and whether the software industry, or even the consumer himself, will keep up with such rules. In the meantime, the CRTC describes the following implementation procedure:

---

installing the program, violates the Act if: (1) the computer is located in Canada at the time the acts were committed; (2) the perpetrator is in Canada at that time; or (3) the perpetrator acts on the instructions of a person who is in Canada at the time he gives these instructions. See CASL, *supra* note 8, s. 8(2).

178 See Part 2.1.1 of this article on the formulation of the request for consent. CRTC 2012-183, *supra* note 91, s. 4(e) is also applicable. This provision mandates the unsubscribe mechanism.

179 Alongside information that may be specified by Regulations.

180 Under CASL, *supra* note 8, s. 10(7), it is not necessary to meet these requirements or the requirements of s. 10(1) when updating a program initially installed or used with the recipient's express consent, if he is entitled to the update.

181 Namely: (a) collecting personal information stored on the computer system; (b) interfering with the owner's or an authorized user's control of the computer system; (c) changing or interfering with settings, preferences, or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system; (d) changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts, or interferes with lawful access to or use of that data by the owner or an authorized user of the computer system; (e) causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system; (f) installing a computer program that may be activated by a third party without the knowledge of the owner or an authorized user of the computer system; and (g) performing any other function specified in the Regulations. The provision excludes programs that, while performing any of these functions, are only intended to collect, use, or disclose transmission data or perform other operations prescribed by the Regulations. See CASL, *supra* note 8, s. 10(6). CASL, *supra* note 8, s. 11(5) should be taken into account.

> The Commission considers that an example of an acceptable means of obtaining consent pursuant to section 5 of the Regulations would be an icon or an empty toggle box, separate from the license agreement and other requests for consent, that would need to be actively clicked or checked, as applicable, in order to indicate consent to one, several, or all of the functions listed in Section 10(5) of the Act, as applicable, provided that the date, time, purpose, and manner of that consent is stored in a database.[182]

It should be considered to what extent this procedure is compatible with current technologies. From another angle, it is surprising that CASL assumes express consent or, more precisely, decides that a person ''is considered to expressly consent" when the installation concerns computer programs such as cookies, HTML code, or JavaScripts (s. 10(8)).[183] In other countries, it is different, and for good reason. In European law, for example, the request for consent for the installation and reading of cookies is divided into two strictly marked components: first, the complete information of the recipient, including information about the specific functions of the program (in simple and conspicuous terms, separately from the General Conditions or the Terms of Service); second, the ability of the recipient to demonstrate, by a positive action, willingness to accept or reject cookies. [184] Furthermore, to minimize the risk (to which one is necessarily exposed) of losing the record of the consent that was given, the French authority for the protection of personal data, the *Commission Nationale de l'Informatique et des Libertés* (CNIL), limited to 13 months the lifetime of cookies and, consequently, the lifetime of any associated consent. A new request for consent is therefore needed after this period.[185]

The focus on these particular computer programs is explained as follows. Cookies are routinely mentioned in association with consumer tracking, profiling, and targeting.[186] The 2015 Web Privacy Census by Altaweel, Good, and Hoofnagle showed that together, the top 100 most popular websites placed over 6,000 HTTP cookies on users' computers

---

182 CRTC 2012-548, *supra* note 83 at para 31.

183 While the presumption justifiably applies to other programs (e.g. programs installed by telecommunications service providers for the security of their networks or to correct a defect in a computer), it seems especially problematic when it concerns "cookies" and similar programs.

184 EC, *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, a) amended by 2009/136/EC* [2002] OJL201 at art 5(3); in French law: *Loi no 78-17 de 6 janvier 1978*, JO: 7 January 1978, 227, art 32(11).

185 See Commission Nationale de l'Informatique et des Libertés, online: <www.cnil.fr>.

186 For example: Meredith Whipple "Regulating Consumer Profiling: Going Beyond Behavioral Advertising" (2013) LBJ J Public Affairs 89 at 90; see alsoMAyenson et al, "Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning" (2011) [unpublished, online at <>]. Recital 30 of the new general regulation on the protection of data states: ''Individuals may be associated, by the devices, applications, tools and protocols they use, online identifiers such as IP addresses and cookies (''cookies") or other identifiers, e.g., radio frequency identification tags. These IDs can leave traces, especially when combined with unique identifiers and other information received by the servers can be used to create profiles of individuals and to identify these people." See EC, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,* [2016] OJ, L 119/1.

when the users were merely visiting their homepages.[187] For many governments, alerting the consumer of the phenomenon and, possibly, restoring some control over the consumer's data, seem to accord with an approach that favours consent given positively, not assumed.

Although it deviates from this approach,[188] notwithstanding the clearly invasive nature of these programs, CASL sets out the following condition in s. 10(8)(b): the presumption of express consent is in effect if "the person's conduct is such that it is reasonable to believe that they consent to the program's installation." Thus, a person who configures his or her computer to prohibit the installation of these programs would rebut the presumption. But can one assume that the average consumer knows how, technically, to block the installation of Flash cookies or similar programs? Undoubtedly, a consumer with low digital literacy will, by default, authorize installation of programs of which he or she never suspected either the existence nor the tracking features.

All of that described, the Act distinguishes the situation of a "person considered to expressly consent" from contexts of implied consent.

2.2 The Contexts of Implied Consent

Section 6 of CASL addresses implied consent. It may be recalled that under this provision, it is prohibited to send a CEM, or to cause or permit a CEM to be sent, to an electronic address, unless the recipient has consented to receive it. Consent for this is either express or implied. When it is express, it follows the previously analyzed provisions. Implied consent must fit one of the contexts of s. 10(9): this is the case when sending is in the interests of an existing business or non-business relationship; or is consequential to the conspicuous publication of the recipient's electronic address, without restriction on unsolicited messages; or following the recipient's communication of his or her electronic address, again without restriction regarding unsolicited messages.

The level of detail about some of the contexts of s. 10(9) is impressive, maybe even excessive. For example, in defining an existing business relationship, the legislation chooses an enumerative approach and lays out an inventory of situations that appears to be exhaustive. However, this catalogue could, in practice, only be indicative, given the lack of more precise criteria. Section 10(10) explains that "existing business relationship" refers to a "business relationship" arising from any of the five following situations:

(1) the purchase or lease of a "product, goods, a service, land or an interest or right in land";
(2) the bartering of one of these things;
(3) an "inquiry or application" about one of these things or a business opportunity, investment, or gaming (the scope of the inquiry is not otherwise specified, except for an indication that it may be a request for information);
(4) the acceptance of such a business opportunity;

---

[187] Ibrahim Altaweel, Nathaniel Good, & Chris Jay Hoofnagle, "Web Privacy Census," Technology Science, online: <techscience.org/a/2015121502>.

[188] The manner of implementing the approach can obviously be problematic, given the widespread use of cookies.

(5) any contract concluded in writing.

The relatively wide range of the fifth situation (any contract concluded in writing) calls into question the usefulness of the list, at least partially. If any written contract for anything is ultimately included, one wonders how helpful it is to specifically list purchase, lease, bartering of goods, products, lands, etc. It may be
that these listed contracts are considered even if they are oral. But then, why only them?

Another detail: the parties must be aware of not only one, but of two separate time constraints, two years (24 months) and six months, to determine if a business relationship is "existing." The two-year period concerns a business relationship resulting from the listed situations, except for an "inquiry or application", which is subject to the six-month period. The basis for this distinction is not clear, nor is the choice of the terms of 24 and six months. In practice, there is implied consent to sending a CEM, for example, when the sender and recipient have entered into a contract (such as a purchase, lease, or barter) and the contract is in force or has expired within two years preceding the sending of the CEM.[189] Where there is an "inquiry or application" for information about a product, among other things, the parties are considered to have a business relationship at the time the CEM is sent (and, therefore, the sender had the recipient's implied consent to send it) if the recipient sent an inquiry or application for information within the six months preceding the CEM. We would underline that a message that constitutes a response to such a request for information is excluded from the need for any consent (express or implied) pursuant to s. 6(6).

A final enumeration, whose usefulness is marginal at best, offers a short list of organizations which "are considered to be businesses," and thus likely to have business relationships: cooperatives and similarly described organizations.[190] But the term "commercial activity" is already subject to a definition sufficiently broad to include these organizations.

Grasping the scope of an "existing non-business relationship" requires parties to pay similar attention to a number of details. These relations concern specific entities.[191] As previously noted, a registered charity, a political party or organization, or a candidate for a publicly elected office, is, in principle, excluded from s. 6 of CASL when sending CEMs and, thus, from the formality of prior consent.[192] But this exclusion applies only where the main purpose of the message is to raise funds for the charity's activities or to seek contributions in accordance with electoral law. In other situations, these entities remain subject to CASL when sending a CEM and may benefit from invoking an existing nonbusiness relationship. CASL considers that such a relationship is ongoing where the

---

189 The buyer of a business sold when it had an existing business relationship with a person is deemed to have a business relationship with that person within that company. See CASL, *supra* note 8, s. 10(12).

190 See CASL, *supra* note 8, s. 10(11).

191 Namely (1) a registered charity; (2) a political party or organization; (3) a candidate for a publicly elected office; (4) a club, association or volunteer organization. See CASL, supra note 8, s. 10(13)(c) and SOR 2013-221, *supra* note 96, s. 7.

192 SOR 2013-221, *supra* note 96, s. 3.

recipient offered the entity a gift or donation, volunteered for it, or adhered to it (such as being accepted as a member) during the two years preceding the CEM. [193]

As we will see in the last segment of our analysis, the technicality of these rules and the possible implementation challenges they raise reflect on the unsubscribe mechanism and the withdrawal of consent, which are two of the essential pieces of the control the government intended to put in the hands of consumers. One senses, nevertheless, a desire to add flexibility to a process that operates in a diversified and quickly evolving technological context.

2.3 The Unsubscribe Mechanism and the Withdrawal of Consent

Consumers must be able to unsubscribe or withdraw their consent if already given for an activity covered by CASL, that is, the sending of CEMs (s. 6(2)(c)); alteration of transmission data (s. 7(1)(a)); and installation of computer programs (s. 8(1)(a)). The ‘‘unsubscribe mechanism” is mentioned with regard to the first activity. Thus, the Act refers to a mechanism that would allow the recipient to indicate, without charge, the wish to no longer receive any CEMs, or a category of CEMs in particular, from the sender. Certain characteristics are required of the mechanism must be identical to those used to send the CEM. If not practicable, the mechanism may be based on any suitable electronic method. In addition, the mechanism should specify an electronic address or a link to a web page where the consumer can indicate his or her wish. The address and link should be active for at least 60 days after the transmission of the message. This amount of time is justified as it ensures recipients enough time to unsubscribe without imposing an excessive burden on businesses. [194]This period is shorter under the CAN-SPAM Act: it is set at 30 days.[195]

Section 3(2) of Regulations CRTC 2012-183 provides that an unsubscribe mechanism “must be able to be readily performed. [196] In practice, this means that the mechanism is “accessed without difficulty or delay, and should be simple, quick, and easy for the consumer to use.” [197] The CRTC states that responding to a CEM by tapping the word “STOP” or “Unsubscribe,” in the case of short message service (SMS), is an acceptable way to unsubscribe from receiving CEMs. [198] The sender must respond to the wish to unsubscribe without delay, not later than 10 working days after notification (s. 11(3) of CASL). Reading the preparatory works of CASL, it appears that the 10-day period, which is

---

193 CASL, *supra* note 8, s. 10(14). Regarding club membership, association, etc., the two-year period starts on the day the membership terminates. When the purchase or use is spread out over time, the computation of time begins at the expiration of this period.

194 ISED, *supra* note 43; annotations of s. 11(2).

195 CAN-SPAM ACT, *supra* note 16, s. 5(3). U.S. lawmakers will not impute to the sender a temporary unavailability due to technical problems beyond its control, if these problems are fixed within a reasonable time.

196 See Canadian Radio-television and Telecommunication Commission, “Undertaking: Mr. Halazon and TCC,” File No. 9090-2015-00414 (12 June 2017), online: <www.crtc.gc.ca/eng/archive/2017/ut170612.htm>.

197 CRTC 2012-548, *supra* note 83 at paras 11-12.

198 *Ibid*.

the same as that provided by the CAN-SPAM Act,[199] was added to accommodate the rare companies whose updating of mailing lists is not yet automated.[200]

The Canadian legislation uses the term "withdrawal of consent" in relation to the two other activities regulated by CASL (s. 11(4) and (5)). In the case of alteration of transmission data, the withdrawal follows a "notice of withdrawal of consent" and the sender of the CEMs must execute it promptly (i.e. within 10 working days after receiving it). The form and content of the notice are not specified in the Act. We only know that an "electronic address" must be provided where the notice can be sent at any time during the validity of the express consent.

In the case of a computer program, withdrawal of consent takes the form of a "request to remove or disable" the program, which can also be sent to an "electronic address," at any time during the year following installation. This refers to a program whose functions are described in s. 10(5) of the Act (collection of personal information; interference with the owner's control of the computer system, etc.) if the person who gave their express consent believes that the functions, purposes, or impact of the program were not correctly described at the time of consent. In this case, the person who had the express consent must remove or disable the program as soon as possible, at no charge. It is an open question whether the removal could be requested for other reasons.

CONCLUSION

A study by Professor Wall, *Digital Realism and the Governance of Spam as Cybercrime*, is instructive regarding the impact of anti-spam laws.[201] It puts into perspective three legislative instruments enacted in 2002, 2003 and 2004: the European Directive of July 12, 2002 on the protection of privacy in the electronic communications sector; in Britain, the *Privacy and Electronic Communications (EC Directive) Regulations 2003*, and the U.S. CAN-SPAM Act, in force in 2004. In the study, the overall levels of spam observed after the introduction of these instruments reflect a heavy uptrend. CASL was also followed by a wave of spam that allegedly has not been seen in the five years prior to enactment in Canada.[202] This raises the question of whether a legislative arsenal is

---

199 CAN-SPAM Act, *supra* note 16, s. 5(4)(A)(i).

200 House of Commons, Standing Committee on Industry, Science and Technology, Proceedings of the House and its committees, 40th Leg, 3rd sess,No 43 (2 November 2010) at 4.

201 David S Wall, "Digital Realism and the Governance of Spam as Cybercrime" (2005) 4 EU J Crim Pol'y & Research 309 at 316.

202 Karim Benessaieh, "La plus grosse vague de pourriels en cinq ans," La Presse (14 octobre 2016), online: <www.lapresse.ca/techno/actualites/201610/14/01-5030339-la-plusgros-vague-de-pourriels-en-cinq-ans.php>. However, the 2017 report of the Standing Committee on Industry, Science and Technology states that: "since the Act came into force in 2014, Innovation, Science and Economic Development Canada (ISED) observes that the amount of spam originating from Canada has decreased by more than a third. Moreover, while Canada figured among the top five spam-producing countries before the Act came into force, it now no longer appears among the top 10 or even top 20." The organization immediately adds: "Whether the Act effectively reduced spam originating from Canada is difficult to ascertain." [citations omitted]. See Standing Committee, *supra* note 8 at 8.

relevant in tackling spam. Further, Professor Wall's study also shows a dramatic decline (about 68 per cent) in spam levels from April-May 2004. However, we should make no mistake: Professor Wall explains that this drop is not the result of a delayed impact of the legislation, but a direct consequence of improved technology, such as software whose main function is to prevent messages identified as spam from reaching the inbox of users. A relatively low proportion of spam managed to circumvent these filters over the period of the study.

If technology seems more effective in reducing the amount of spam, the role of law is not to be neglected, as it transcends the issue of number of unsolicited messages, according to Professor Wall:

> […] while the direct impact of law upon behavior may be limited, law has nevertheless played an important, though not exclusive role in the governance of spam. Under the 'shadow of law,' technology is effective in shaping the architecture(s) to reduce spam receipts, but its shadow also strengthens social values against spammers and shapes the market against them.[203]

Although "shaping the architectures" is not the immediate objective of CASL, we believe that nothing prevents the agencies responsible for its implementation from pushing stakeholders in this direction. This can be done, for instance, by focusing on the communication protocol used for email, that is, the simple mail transfer protocol ("SMTP"). The idea of rewriting or enhancing this protocol to screen out spam springs to mind.[204]

For the time being, the argument that CASL is the most stringent law in the world in the fight against spam must be discarded. Our analysis does show a breadth of scope, strict prohibitions, complex consent management procedures (the implementation of which is certainly a challenge), two remedies for infringement, and visibly severe penalties (ss. 20 and 51). On the one hand, the statute authorizes an action administered by the CRTC with a penalty cap of $1 million for a violation by an individual and $10 million for any other person.[205] CASL states that the penalty is not to punish but to promote compliance with the Act[206]. On the other hand, a private right of action (PRA) is provided to allow any person claiming to be affected by an act or omission which constitutes a

---

203 Wall, *supra* note 201 at 12.

204 See: Federal Trade Commission, Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress, December 2005, at 18-19, online: <www.ifap.ru/pr/2005/051223aa.pdf>.

205 CASL, *supra* note 8, s. 20(4). For comparison, see especiallyCAN-SPAM Act, *supra* note 16, s. 7(f)(3)(B): "For any violation of Section 5 (other than Section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $2,000,000. (C) The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if […]."

206 CASL, *supra* note 8, s. 20(2). Also, when an "offence" (non-compliance with a demand pursuant to s. 15 or a notice issued under s. 17, or contravention of s. 19(4)) is committed by a corporation, its officers, directors, agents or mandataries who directed, authorized, assented or acquiesced to or participated in the offence are parties to and liable. Similarly, a person is liable for the offence of their employee or agent during employment or mandate. As a defense, they can prove that they have taken all due diligence to prevent the offence. See CASL, *supra* note 8, ss. 42-46.

violation of CASL or s. 5 of PIPEDA to apply to the court for an order against its author.[207] The court may order compensation in an amount equal to the actual loss or damage suffered or expenses incurred and $200 per contravention of s. 6 of CASL (about sending a CEM without prior consent) and up to $1 million per each day on which a contravention occurred. For contravention of s. 7 (concerning alteration of transmission data) and s. 8 of CASL (relating to installation of computer program), the penalty may reach a maximum of $1 million for each day on which a contravention occurred.[208] This PRA[209] was to come into effect on July 1, 2017. With less than a month to go, on June 7, 2017, Canada announced that it was suspending its implementation. Apparently, it is seeking a balance that CASL fails to guarantee in its current version:

> Canadians deserve an effective law that protects them from spam and other electronic threats that lead to harassment, identity theft and fraud. At the same time, Canadian businesses, charities and non-profit groups should not have to bear the burden of unnecessary red tape and costs to comply with the legislation.
>
> The Government supports a balanced approach that protects the interests of consumers while eliminating any unintended consequences for organizations that have legitimate reasons for communicating electronically with Canadians.
>
> For that reason, the Government will ask a parliamentary committee to review the legislation, in keeping with the existing provisions of CASL.[210]

The Standing Committee on Industry, Science and Technology "recommends that the Government of Canada further investigate the impact of implementing the private right of action, once changes and clarifications have been implemented to the Act and its regulations. At the same time, it could consider if an award of damages should be based

---

207 CASL, *supra* note 8, s. 47.

208 Ditto for contraventions of s. 9, subject to subparas (iv) and (v). Also s. 51(1)(iv)-(vii).

209 Under s. 7(g)(1) of the CAN-SPAM Act, *supra* note 16, action is open to ISPs "A provider of Internet access service adversely affected by a violation of Section 5(a)(1), 5(b), or 5(d), or a pattern or practice that violates paragraph (2), (3), (4), or (5) of Section 5(a), may bring a civil action [. . .]"; See also s. 7(g)(3)(B): "For any violation of Section 5 (other than Section 5(a)(1)), the amount determined under subparagraph (A) may not exceed $1,000,000. (C) The court may increase a damage award to an amount equal to not more than three times the amount otherwise available under this paragraph if […]." See also *Gordon v. Virtumundo, Inc.*, 575 F.3d 1040 (9th Cir. 2009) [*Gordon*]; *Xmission, L.C. v. Adknowledge, Inc.,* No. 2:15-CV-00277, 2016WL3746528 (D. Utah 2016), citing *Gordon*: "Plaintiff lacked standing to bring a private action for CAN-SPAM because no real harm was suffered and Plaintiff did "not fit any reasonable definition of an 'Internet access service'"; *Gordon v. John* 1-10 Does 459 Fed.Appx. 681(9th Cir, 2011): "Consumer who had received unsolicited commercial email or spam from marketers was not an 'internet access provider,' as required to have standing to bring suit under CAN—SPAM Act."

210 Innovation, Science and Economic Development Canada, News Release, "Government of Canada suspends lawsuit provision in anti-spam legislation," (7 June 2017), online: <https://www.canada.ca/en/innovation-science-economic-development/news/2017/06/government_of_canadasuspendslawsuitprovisioninanti-spamlegislati.html>.

on proof of tangible harm." [211] By indefinitely suspending these provisions, which are described as "the toughest" of CASL, it has been said that Canada has, for all intents and purposes, "declawed" the law. [212]

To us, other choices of the government also significantly moderate the purported strictness of the Act. There is, of course, the exemption for CEMs following a referral. Through it, the Canadian legislation moves away from the opt-in approach and therefore brings CASL closer to the U.S. CAN-SPAM Act. It indirectly provides senders with a golden opportunity to initiate contact, perhaps to try to sell. Since the U.S. anti-spam law was criticized for being permissive, it is strange to see CASL follow its path although this brings some homogeneity in the rules governing their neighbouring markets. On another note, some definitions may face judicial review, such as the restrictive definition of family relationships. The provisions about computer programs, which initially appeared innovative, also moderate the purported strictness of CASL; especially the indulgence they convey about cookies and other tracers, matters that still create concern for other governments.

After all, it is our view that CASL's objective to enhance consumer protection is highly laudable. Hopefully, the ongoing review of the provisions and operation of the Act will lead to some amendments consistent with this aim.

---

211 Standing Committee, supra note 8 at 4, (Recommendation 10).

212 Jean-François Codère, "Ottawa dégriffe la loi antipourriel," La Presse (8 juin 2017), online: <www.lapresse.ca/techno/internet/201706/08/01-5105492-ottawa-degriffe-la-loi-antipourriel.php>.