Brooklyn Law Review

Volume 84 | Issue 4 Article 6

6-21-2019

The King of the CASL: Canada's Anti-Spam Law Invades the United States

Arthur Shaykevich

The King of the CASL

CANADA'S ANTI-SPAM LAW INVADES THE UNITED STATES

"Canada will become a leader in anti-spam legislation among member countries . . . ."[1]

INTRODUCTION

Despite all the technological communication innovations that have developed since its creation, email remains the dominant communication channel for commercial purposes.[2] In fact, there is more commercial email traffic than for personal use.[3] The ease, cost, and monetization opportunities lead to some bad actors utilizing email for nefarious purposes. Comprising "[m]ore than half of inbound business email traffic" and costing end users an estimated $20 billion per year, unsolicited junk mail, also known as spam, is a big problem.[4]

---

[1] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2912 (Dec. 18, 2013). On November 4, 2015, Industry Canada was renamed Innovation, Science and Economic Development Canada (ISED). *See Machinery of Government Changes*, PRIVY COUNCIL OFF., https://www.canada.ca/en/privy-council/services/machinery-government-changes.html [https://perma.cc/B9KC-BT3K]. The two names are used interchangeably throughout the note.

[2] *See, e.g.*, *2017 Consumer Email Habits Report: What Do Your Customers Really Want?*, CAMPAIGN MONITOR, https://www.campaignmonitor.com/resources/guides/insights-research-report [https://perma.cc/6WCX-VF7B]; *Why Email Is Still King Among Digital Communication Channels*, EMAIL MONKS (Dec. 23, 2016), https://emailmonks.com/blog/email-marketing/email-is-king [https://perma.cc/Z9WA-AUSS].

[3] *See* RADICATI GRP., INC., EMAIL STATISTICS REPORT, 2015-2019, at 4 (Mar. 2015), https://www.radicati.com/wp/wp-content/uploads/2015/03/Email-Statistics-Report-2015-2019-Executive-Summary.pdf [https://perma.cc/AXW7-46W5].

[4] SYMANTEC INC., 2016 INTERNET SECURITY THREAT REPORT, vol. 21, 31 (Apr. 2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf [https://perma.cc/79PH-FGKB]; Justin M. Rao & David H. Reiley, *The Economics of Spam*, 26 J. ECON. PERSP. 87, 88 (2012). The term "spam" varies in meaning. For example, the term could be defined as: "[i]rrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc." *Spam*, OXFORD ENG. DICTIONARY, https://en.oxforddictionaries.com/definition/spam[https://perma.cc/7L9U-3ZU9]. Alternatively, spam could be defined more broadly, without focusing on mass mailing or on the content. *See, e.g.*, *Understanding Spam*, CONSTANT CONTACT (Feb. 12, 2018), https://knowledgebase.constantcontact.com/guides/KnowledgeBase/5635-understanding-spam [https://perma.cc/5RE9-399B?type=image] ("Spam is defined as any form of commercial email that is deemed unsolicited by the recipient, regardless of the content."). Further, the term "junk mail" is typically "defined as unsolicited advertising or promotional material received through mail or email . . . [and is generally] used interchangeably" with the term "spam." Aaron Charles, *The*

Internet Service Providers (ISPs) like Google's Gmail use ever more sophisticated spam-filtering technology to block spam,[5] and yet sixteen percent still gets through.[6] Despite the ISPs' efforts, "[s]pammers are finding other ways to reach their audiences."[7]

The resulting disruption and inconvenience to recipients can be profound. While the average user's email box is no longer full of Viagra advertisements or Nigerian prince scams,[8] ISPs cannot accurately find it all.[9] Worse, ISPs' aggressive spam identification efforts often result in an inadvertent misidentification of legitimate messages.[10] To thwart this problem, many countries have statutory laws dealing with spam.[11]

To combat spam in the United States, Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM),[12] with the Federal Trade Commission (FTC) having primary supplementary rulemaking authority and enforcement controls.[13] Among other requirements,

---

Difference Between Spam & Junk Mail, IT STILL WORKS, https://itstillworks.com/difference-between-spam-junk-mail-2138.html [https://perma.cc/KHZ4-APBG]. The inconsistency of this definition helps explain why in combatting spam, not everyone may be fighting the same enemy. When this note is referring to spam, it is referencing unsolicited, commercial email. Thus, dangerous emails from criminals such as phishing, as well as undesired nuisance emails from legitimate marketers, such as shopping advertising, are grouped together within the definition.

[5] *See, e.g.*, Frederic Lardinois, *Google Says Its Machine Learning Tech Now Blocks 99.9% of Gmail Spam and Phishing Messages*, TECH CRUNCH (May 23, 2017), https://techcrunch.com/2017/05/31/google-says-its-machine-learning-tech-now-blocks-99-9-of-gmail-spam-and-phishing-messages [https://perma.cc/8RCZ-2HEG]. It is also proper to acknowledge Spamhaus for its contribution to spam identification and reduction. *See About Spamhaus*, SPAMHAUS, https://www.spamhaus.org/organization [https://perma.cc/Z8NM-WNP5].

[6] *See* RADICATI, *supra* note 3. This number was calculated by dividing the 2015 average number of spam emails by the 2015 average number of emails received. The result is rounded up.

[7] SYMANTEC INC., *supra* note 4, at 31.

[8] *See, e.g.*, Oliver Burkeman, *Why the Spammers Are Winning: Thought the War on Junk Mail Was Over? Think Again*, GUARDIAN (Aug. 9, 2013, 6:59 PM EDT), https://www.theguardian.com/technology/2013/aug/09/why-spammers-are-winning-junk-mail [https://perma.cc/WFD3-KXEG].

[9] Not every mail server is as robust as Google's, thus the results depend on the quality of the average user's ISP. Further, if an individual or a business has its own mail server, a significant investment in email security is needed. *Cf. Barracuda Email Security Gateway*, BARRACUDA, https://www.barracuda.com/products/emailsecuritygateway [https://perma.cc/2NTZ-AD3S]. Thus, legitimate spam hitting an inbox remains a problem for many businesses without such tools.

[10] *See, e.g.*, *Get Your Emails Out of Spam*, KEYNECTUP (Oct. 7, 2015), https://www.keynectup.com/2015/10/get-your-emails-out-of-spam [https://perma.cc/S85B-79ET]. This may cause either: productivity loss as the user sifts through the spam folder or may cause a relevant message to be missed altogether.

[11] *See, e.g.*, *Email Anti-Spam Laws Around the World*, VERTICAL RESPONSE (Sept. 28, 2017), http://www.verticalresponse.com/blog/email-anti-spam-laws-around-the-world-infographic [https://perma.cc/SH2U-5XC5].

[12] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified as amended at 15 U.S.C. §§ 7701–7713 (2012 & Supp. V 2018)).

[13] 15 U.S.C. §§ 7702(3), 11.

the CAN-SPAM Act requires a commercial email sender to include an opt-out mechanism on any sent communication,[14] and to honor the email recipient's request to unsubscribe from further solicitations.[15] The Act, however, does not provide for individual recourse.[16] Due to the Act's lack of a private right of action and low enforcement rate, the U.S. anti-spam law has been largely criticized as ineffective.[17]

Canada passed a similar, but much broader anti-spam law called "Canada's Anti-Spam Legislation" (CASL).[18] As this law is now fully in effect, U.S.-based businesses should take notice regardless of whether they conduct business in Canada. CASL took effect July 1, 2014, with a focus on permission-based marketing—meaning, it is an "opt-in" regime and not an "opt-out" regime as used in CAN-SPAM.[19] While the purpose of CASL might have been "to encourage the growth of electronic commerce . . . [and simultaneously to] prohibit[] *damaging and deceptive* spam," it is legitimate businesses that endure the enforcement of this law because of the requirements associated with CASL compliance.[20] While maintaining an opt-out provision comparable to CAN-SPAM, CASL drastically distinguishes itself from CAN-SPAM, mainly because of its requirements for opt-in consent.[21] Above all, unlike CAN-SPAM, CASL has a provision for

---

[14] *Id.* § 7704(a)(3).

[15] *Id.* § 7704(a)(5)(ii).

[16] *Id.* § 7706.

[17] *See generally Is it Time to Can the CAN-SPAM Act?*, KREBSON SECURITY (July 2, 2017, 12:14 PM), https://krebsonsecurity.com/2017/07/is-it-time-to-can-the-can-spam-act [https://perma.cc/B9YC-NVA6] ("[C]ritics of the law often refer to it as the YOU-CAN-SPAM Act, charging that it essentially legalized spamming."); *see also* discussion *infra* Part II.

[18] Canadian Anti-Spam Legislation is a part of: An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c 23 (Can.) [hereinafter "Canadian Anti-Spam Legislation" or "CASL"]. CASL does not only deal with consent of electronic messages; rather, it also requires consent for altering transmission data and installation of computer software. *Id.* at §§ 7–8. Further, CASL contains various amendments. *Id.* at §§ 68–88. Those topics are outside the scope of this note.

[19] *See* discussion *infra* Part II.

[20] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2912 (Dec. 18, 2013); *see also* discussion *infra* Section I.C.

[21] *See* discussion *infra* Part II.

a private right of action,[22] although it is currently suspended.[23] It is likely that Canada will revise CASL in the near future.[24]

CASL has a geographical impact far beyond Canada because "[i]f a foreign company is sending commercial electronic messages to Canada . . . , CASL applies."[25] Because of geographic proximity, the United States is Canada's largest trade partner.[26] Therefore, Canadian law has a disproportionate extraterritorial impact on U.S. businesses when compared to other countries. For the U.S. businesses that reach into Canada, simply emailing a Canadian resident creates a compliance conundrum for cross-border communications. While obtaining consent is a good marketing practice, such practice was unnecessary under CAN-SPAM.[27] Depending on the business, Canada's email data is likely commingled with the U.S. data,[28] and is not easily severable without clear-cut instructions. Since an email address offers few clues to its owner's country of residence, customer segmentation is not possible without obtaining and maintaining far greater detail on the customer.

Unfortunately, Canada's lawmakers do not provide clear rules for data segmentation, and as a result, legitimate U.S.

---

[22] CASL, S.C. 2010, c 23 §§ 47–51 (Can.). In the U.S., the FCC through the Telephone Consumer Protection Act (TCPA) controls SMS text messaging compliance. *See In re* Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 18 FCC Rcd. 14014, 14115 (2003). The TCPA *does* allow for a private right of action. *Id.* at 14019. Even though in Canada, CASL governs SMS text messaging, this note's focus is on email compliance. Canada's extraterritorial reach onto SMS text messaging is a salient topic, albeit for a different day.

[23] Under CASL, a private right of action was scheduled to commence at the end of the law's three-year rollout period on July 1, 2017, and would have permitted individuals, or a class, to recover statutory damages of $200 per email; up to $1 million per day. CASL, S.C. 2010, c 23 §§ 47–51 (Can.). In acknowledging some flaws in the law, and to the chagrin of many attorneys, the Canadian parliament suspended the private right of action, less than a month before it was to take effect. *See* Press Release, Innovation, Sci. & Econ. Dev., Government of Canada Suspends Lawsuit Provision in Anti-Spam Legislation (June 7, 2017), https://www.canada.ca/en/innovation-science-economic-development/news/2017/06/government_of_canadasuspendslawsuitprovision inanti-spamlegislati.html [https://perma.cc/FP9W-PZSX].

[24] *See* discussion *infra* Section I.D.

[25] *Frequently Asked Questions: Canada's Anti-Spam Legislation*, GOV'T OF CAN., http://fightspam.gc.ca/eic/site/030.nsf/eng/00304.html#qB14 [https://perma.cc/SR3B-AGSE].

[26] *See, e.g.*, Karen Waksman, *Top Countries That Import U.S. Products by Dollar Value*, BALANCE (Apr. 28, 2018), https://www.thebalance.com/top-countries-that-import-u-s-products-3502316 [https://perma.cc/Q967-HBLH]. In fact, Canada's total trade with the U.S. is nearly eight times the amount of their next largest trade partner, China. *See Canada: Trade Statistics*, MICH. ST. U.: GLOBAL EDGE, https://globaledge.msu.edu/countries/canada/tradestats [https://perma.cc/QW2J-45H4] (In 2017, Canada's total trade with the U.S. was $541,034,482,428 and $72,848,885,113 with China).

[27] *See* discussion *infra* Part II.

[28] *See generally* Bonnie Massa, *How to Get All Your Customer Data into a Single Database in 5 Easy Steps*, MASSA & CO. (Oct. 18, 2016), http://massainc.com/customer-data-into-a-single-database-in-5-easy-steps [https://perma.cc/S826-BN32] (encouraging the creation of a single, centralized, database).

businesses are vulnerable to CASL violation claims, even if they attempt segmentation. This note argues that but for the fortuitous event of the suspension of the private right of action mentioned above,[29] U.S. businesses of all sizes would be under continuous threat of litigation under CASL.[30] As this note shows, it is quite easy for a U.S. business to violate CASL by inadvertently sending an email into Canada.[31] Hence, while the private right of action is suspended, and while Canada's government considers CASL changes, the timing is ripe for Canada to create a workable foreign exemption.[32] Since CASL is destined to change, this note proposes clear-cut and unburdensome compliance rules for foreign email senders that would qualify for an exemption. Until such an exemption exists, however, U.S. businesses should take notice of the consequences of failing to comply. "While the problem of spam, like the [i]nternet itself, is global in scope,"[33] Canada should not be in the position of controlling U.S. commerce to such a degree.

This note proceeds in the following parts. Part I dives into the complex rules of CASL, the exemptions, as well as the documentation requirements and enforcement of the law. Part II briefly discusses CAN-SPAM and contrasts the relevant CAN-SPAM provisions with CASL. Part III details why U.S. businesses are at risk and explains why reliance on the current CASL regulatory exemption for foreign entities or on the due diligence defense is foolhardy.[34] Part IV proposes practical solutions for Canada to implement in order to strike the right balance between compliance and reality. The note concludes by requesting the FTC to take notice of the status quo's dire consequences and urges FTC involvement if Canada will not address the noted risk.

---

[29] Press Release, Innovation, Sci. & Econ. Dev., *supra* note 23.

[30] This note is not anti-private right of action. Quite the opposite. Any law, however, let alone one with the magnitude of CASL, needs to be buttoned-up; concrete; unambiguous; and adequate to provide notice of compliance. CASL, while well meaning, suffers from multiple ambiguities. *See* Barry Sookman, *Michael Geist's Defense of Canada's Indefensible Anti-Spam Law CASL*, BARRYSOOKMAN.COM (July 14, 2014), http://www.barrysookman.com/2014/07/14/michael-geists-defense-of-canadas-indefensible-anti-spam-law-casl [https://perma.cc/YVT5-DUBN].

[31] *See* discussion *infra* Part III.

[32] *See* discussion *infra* Section II.D.

[33] INDUS. CAN. TASK FORCE ON SPAM, STOPPING SPAM: CREATING A STRONGER, SAFER INTERNET 16 (2005), http://publications.gc.ca/collections/Collection/Iu64-24-2005 E.pdf [https://perma.cc/XM7Z-M3VA].

[34] *See* Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175, § 3(f) (Can.).

I. OVERVIEW OF CANADA'S ANTI-SPAM LEGISLATION (CASL)

Following a task force report which concluded that "[s]pam impedes the efficient use of the [i]nternet for personal and business communications, and threatens the growth and acceptance of legitimate e-commerce,"[35] Bill C-28, otherwise known as CASL, received Royal Assent[36] on December 10, 2010, and took effect July 1, 2014.[37] CASL instantly became "the toughest law of its kind" with its focus on consent-based marketing for any electronic commercial message.[38] Following the passage of CASL, one needs to obtain either express or implied consent to send an electronic message.[39] With the overall goal "to encourage the growth of electronic commerce by ensuring confidence and trust in the online marketplace,"[40] CASL forced legitimate businesses to expend extensive resources while attempting to adjust their marketing practices for compliance.[41]

---

[35] INDUS. CAN. TASK FORCE ON SPAM, *supra* note 33, at 7.

[36] *See, e.g.*, Susan Munroe, *The Monarch's Royal Assent Turns Bills into Laws in Canada*, THOUGHT CO. (July 30, 2017), https://www.thoughtco.com/royal-assent-508477 [https://perma.cc/A3QD-6BCU] ("In Canada, 'royal assent' is the symbolic final stage of the legislative process by which a bill becomes law.").

[37] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2913 (Dec. 18, 2013); *see also* Chris Bennett, Tamara Hunter & David Spratley, *Getting Ready for Canada's Anti-Spam Legislation (CASL) - Try Green Regs and Spam (Even If You Do Not Like Them)*, DLA PIPER DAVIS LLP PRIVACY L. BULL. (Mar. 7, 2013), https://www.dlapiper.com/en/canada/insights/publications/2013/03/getting-ready-for-canadas-antispam-legislation-c__ [https://perma.cc/U7B4-SAQU] ("There have been many delays for the [Canadian] Federal Government in bringing CASL into effect . . . ."). CASL had a three-year transitional period for businesses to adjust their practices and to obtain express consent from their customers. *See* CASL, S.C. 2010, c 23 § 66 (Can.); *Canada's Anti-Spam Legislation Order*, SI/2013-81000-2-1795 (Can.); Kelly Ann Smith, *Video Transcript: Information Power Point Session on Canada's Anti-Spam Legislation*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N (June 10, 2014), http://www.galaxytext.com/information-power-point-session-on-canadas-anti-spam-legislation [https://perma.cc/K568-8MA4]. The final portion of CASL, the private right of action, was to take effect on July 1, 2017 but was suspended. *See* Press Release, Innovation, Sci. & Econ. Dev., *supra* note 23.

[38] Barry B. Sookman & Puneet Soni, *CASL Applies to You Even If You Aren't in Canada*, MCCARTHY TÉTRAULT LLP (Mar. 11, 2014), https://www.lexology.com/library/detail.aspx?g=7c4fd0eb-fe55-4098-bf66-6bbf0a9ba8c7 [https://perma.cc/RD77-6UXW]. CASL also regulates the installation of computer programs and in-transit alteration of transmission data. *See* CASL, S.C. 2010, c 23 §§ 7–8 (Can.). These complex parts of CASL are worthy of their own note and raise concerns similar to the ones addressed here.

[39] CASL, S.C. 2010, c 23 §§ 10(1), 10(9) (Can.).

[40] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. at 2914.

[41] Michael G. Osborne, *The Great Anti-Spam Cash Grab*, FIN. POST (Dec. 9, 2015, 11:09 AM EST), http://business.financialpost.com/opinion/the-great-anti-spam-cash-grab [https://perma.cc/VL2C-4ZCM]. CASL did indeed encourage compliance with "37% reduction in spam originating in Canada," and "29% reduction in all email received by Canadians, spam and legitimate" in its first year. 2015 Q1: SECURITY THREAT REPORT, CLOUDMARK 6 (2015), https://www.cloudmark.com/en/register/threat-reports/report_15q1 [https://perma.cc/7BX6-UYB3].

CASL applies when a Commercial Electronic Message (CEM) is sent or received in Canada.[42] "Under CASL, a CEM is a message [e.g., an email, SMS text message, or a message on social media], that encourages participation in a commercial activity."[43] Further, the department of Innovation, Science and Economic Development Canada (ISED)[44] clarified a message as a CEM if "one of [its] purposes [is] to encourage participation in a commercial activity."[45] Therefore, CASL would consider a transactional message, such as a purchase confirmation containing links to related items, a CEM.[46] CASL does not have a *de minimis* exception, thus a single message could place the sender in violation.[47] The Canadian Radio-television and Telecommunications Commission (CRTC) is the agency responsible for regulations pertaining to content and form, while the Governor-in-Council (GIC) through the ISED may make regulations pertaining to defining CASL's usage of its consent requirements.[48]

A. CASL's Provisions: Form, Content, and Consent

CASL requires that a message must "identi[fy] the person who sent the message . . . [or] on whose behalf it is sent."[49] To do that, the CRTC requires each electronic message to include the sender's name and, "if the message is sent on behalf of another person, the name [of] the person on whose behalf the message is sent."[50] Additionally, senders must list secondary identifying information of either a mailing address,

---

[42] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. at 2914.

[43] Alex Ilhan, *CASL and Email Marketing: What You Need to Know*, EMAILONACID (July 11, 2014), https://www.emailonacid.com/blog/article/industry-news/casl_and_email_marketing_what_you_need_to_know [https://perma.cc/E8D3-T4NM]. This note's primary focus is email.

[44] The ISED is a federal government department whose responsibilities include managing the Governor-in-Council's (GIC) CASL regulations. *See* CASL, S.C. 2010, c 23 § 64(1) (Can.); *see also Home—Innovation, Science and Economic Development Canada*, GOV'T OF CAN., https://www.canada.ca/en/innovation-science-economic-development.html [https://perma.cc/URE8-R78H]; Susan Munroe, *Understanding Governor in Council Appointments in Canada*, THOUGHT CO. (Mar. 5, 2019), https://www.thoughtco.com/governor-in-council-508241 [https://perma.cc/VBK2-E9U2].

[45] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. at 2923.

[46] *See id.* at 2923–24.

[47] *See* Barry Sookman, *CASL: The Unofficial FAQ, Regulatory Impact Statement, and Compliance Guideline* (July 14, 2015), http://www.barrysookman.com/2015/01/14/casl-the-unofficial-faq-regulatory-impact-statement-and-compliance-guideline [https://perma.cc/K73J-ESNH].

[48] CASL, S.C. 2010, c 23 § 64 (Can.). Industry Canada is the former name of ISED. *See Machinery of Government Changes*, *supra* note 1.

[49] CASL, S.C. 2010, c 23 § 6(2)(a) (Can.).

[50] SOLOWAY WRIGHT, WHAT YOU NEED TO KNOW ABOUT THE NEW CANADA ANTI-SPAM LAW 3, http://cla.ca/wp-content/uploads/What-You-Need-to-Know-About-the-New-Canada-Anti-Spam-Legislation-April-24-2014-for-members.pdf [https://perma.cc/5QJM-RGNF]; *see also* Electronic Commerce Protection Regulations, SOR/2012-36 146 C. Gaz. 730, 731 (Mar. 28, 2012).

telephone, or a website.[51] CASL also requires "for an unsubscribe mechanism to be 'readily performed;' it must be accessed without difficulty or delay, and should be simple, quick, [at no cost to the recipient], and easy for the consumer to use."[52] Outside of these form and content requirements, CASL's main provisions focus on ensuring that a sender obtained either express or implied consent from the recipient before deployment of a CEM.[53]

One way for senders to comply with the consent requirement is through express consent.[54] Express consent is a permission from the recipient, which allows a sender to deploy electronic communications to the receiver once "a person has clearly agreed to receive a CEM, either in writing or orally."[55] Businesses cannot bundle the request for such consent to receive CEMs, however, into standard terms and conditions; rather, request for consent needs to be conspicuously apart.[56] Additionally, the request for consent must be clear and contain a statement notifying the recipient that they "may withdraw their consent at any time."[57] Further, users must perform an action to consent to a message.[58] Toggling—or pre-checking an agreement of consent terms for sending a CEM—does not demonstrate consent.[59] Once a business procures express consent, it remains valid in perpetuity until the customer revokes it through the unsubscribe mechanism.[60] Moreover, unless the sender can rely on implied consent to send an email requesting consent, CASL treats *the email itself* as a CEM.[61]

---

[51] Electronic Commerce Protection Regulations, SOR/2012-36 146 C. Gaz. at 731. A P.O. Box satisfies the address requirement. *See Guidelines on the Interpretation of the Electronic Commerce Protection Regulations*, Compliance & Enf't Info. Bull., CRTC 2012-548 ¶ 9 (Can.) (Oct. 10, 2012), https://www.crtc.gc.ca/eng/archive/2012/2012-548.pdf [https://perma.cc/9AGQ-Q52A] [hereinafter "CRTC Bulletin 2012-548"]. In addition, CRTC allows for this information to be placed on a website as long as a prominent link is clearly displayed on the message. Electronic Commerce Protection Regulations, SOR/2012-36 146 C. Gaz. at 731. The listed information must be valid for a minimum of sixty days after the message is sent. CASL, S.C. 2010, c 23 § 6(3) (Can.).

[52] CASL, S.C. 2010, c 23 § 11(a)(1) (Can.); CRTC Bulletin 2012-548, *supra* note 51, at § 11.

[53] CASL, S.C. 2010, c 23 § 10 (Can.).

[54] *Id.* § 10(1).

[55] *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://www.crtc.gc.ca/eng/com500/guide.htm [https://perma.cc/Y5VA-M9SH].

[56] CRTC Bulletin 2012-548, *supra* note 51, at ¶ 31.

[57] Smith, *supra* note 37; *see also* CRTC Bulletin 2012-548, *supra* note 51, at ¶ 31.

[58] CRTC Bulletin 2012-548, *supra* note 51, at ¶ 31.

[59] *Guidelines on the Use of Toggling as a Means of Obtaining Express Consent Under Canada's Anti-Spam Legislation*, Compliance and Enf't Info. Bull., CRTC SOR/2012-549 ¶¶ 4–6 (Can.) (Oct. 10, 2012), https://crtc.gc.ca/eng/archive/2012/2012-549.pdf [https://perma.cc/MK4F-D4MJ].

[60] *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, *supra* note 55.

[61] *Id.*

Consent can also be implied through three circumstances: (1) an existing business relationship; (2) conspicuous publication; and (3) a "business card" exemption.[62] In a case where someone made a purchase, accepted a business opportunity, or entered into a contract, implied consent is assumed, and is valid for two years or until the consent is withdrawn.[63] For an existing business relationship, the two-year countdown commences from the finality of the relationship, and any subsequent activity restarts the window of consent.[64] In addition, a business relationship is also created in response to a query or a complaint, but only for six months.[65] Furthermore, CASL finds implied consent for messages sent to a member of a social club or to an association.[66] Consent can also be implied from a "conspicuous publication"—a public posting of an electronic address, or through an individualized disclosure of information; e.g., handing someone a business card.[67] CASL allows a sender to rely on such implied consent, as long as the provided information does not contain a statement from the recipient disallowing electronic messages, and if "the message is relevant to the person's . . . business or official capacity."[68]

Additionally, CASL allows for consent to be captured for the purpose of sharing the data with unknown third parties.[69] A third party may use the email and rely on such transferred consent, provided that they identify the party that received the original consent and follow CASL's form requirements.[70] Further requirements attach, however, once a recipient unsubscribes from the third party. First, the third party must pass the user's choice back to the original party.[71] Next, the original party in turn must notify all other parties with whom they previously shared this address.[72] And finally, all the connected parties must remove the

---

[62] CASL, S.C. 2010, c 23 § 10(9) (Can.); *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, *supra* note 55.

[63] CASL, S.C. 2010, c 23 § 10(10) (Can.).

[64] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2924 (Dec. 18, 2013).

[65] CASL, S.C. 2010, c 23 § 10(10)(e) (Can.); Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(b) (Can.) Industry Canada expanded "inquiry" in the regulations to include a "query." CRTC distinguished this CASL provision from the GIC Regulations by focusing on the purpose of the message. If the message contained a financial component, CASL's form requirements needed to remain, else, the message would be excluded from CASL requirements altogether. *See* Smith, *supra* note 37.

[66] CASL, S.C. 2010, c 23 § 10(13)(c) (Can.); Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 7 (Can.).

[67] CASL, S.C. 2010, c 23 § 10(9)(b)–(c) (Can.).

[68] *Id.*; *see also From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, *supra* note 55.

[69] CASL, S.C. 2010, c 23 § 10(2)(b) (Can.).

[70] Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 5(1).

[71] *Id.* § 5(2).

[72] *Id.* § 5(3).

electronic address from future communications.[73] Third parties should be cautious, however, because the CRTC recently clarified that intermediaries can be subject to accessorial liability.[74]

B. Exemptions to CASL

In an effort to limit CASL's reach beyond statutory intent, the GIC implemented certain notable exemptions to its applicability, as well as provided regulations on the exceptions carved by CASL itself.[75] First, as distinguished from an existing business relationship, which requires implied consent, CASL stipulates exceptions for communications within a "family relationship" or within a "personal relationship."[76] The GIC defined these exceptions narrowly, thus some direct connection is necessary for the definition of a relationship to take effect.[77] Next, a business employee, sending a CEM in relation to his or her employment is exempt from CASL requirements.[78] Similarly, business-to-business communications between companies are exempt, as long as a relationship is present "and the message concerns the activities of the organization."[79] Moreover, consent requirements are suspended in the case of a person with any existing relationship recommending a product or service to another.[80] The sender of the communications must comply with CASL's form requirements and stipulate from

---

[73] *Id.* §§ 5(2)–(4). Depending on the consent verbiage, it is possible to capture third-party consent separately from the original party consent. In such a case, only sharing must halt, but the original party itself can continue to send communications until a direct unsubscribe occurs. *See* Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2915–16 (Dec. 18, 2013).

[74] *Guidelines on the Commission's Approach to Section 9 of Canada's Anti-Spam legislation*, Compliance and Enf't Info. Bull., CRTC SOR/2018-415 (Can.) (Nov. 5, 2018), https://crtc.gc.ca/eng/archive/2018/2018-415.pdf [https://perma.cc/2MT7-JBJF]; *see also* Barry Sookman, *CRTC's Troubling Guidelines on CASL Accessorial Liability* (Nov. 7, 2018), https://www.barrysookman.com/2018/11/07/crtcs-troubling-guidelines-on-casl-accessorial-liability [https://perma.cc/W9MT-GCMZ] ("[T]he CRTC apparently seeks to impose liability even on completely innocent intermediaries with no actual or constructive knowledge that their products, services, or tools are being used to violate CASL.").

[75] CASL, S.C. 2010, c 23 § 64(1) (Can.); Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 2.

[76] CASL, S.C. 2010, c 23 § 6(5)(a) (Can.).

[77] Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 2 (Can.); *Frequently Asked Questions About Canada's Anti-Spam Legislation*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://www.crtc.gc.ca/eng/com500/faq500.htm [https://perma.cc/H4B2-6SPC] ("[U]se of buttons available on social media websites—such as clicking 'like', . . . [or] accepting someone as a '[f]riend' . . . will generally be insufficient to constitute a personal relationship.").

[78] Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(a)(i) (Can.).

[79] *Id.* § 3(a)(ii). The GIC Regulations do not define what "activities of the organization" entail.

[80] *Id.* § 4.

whom the referral came. Only one message, however, could be sent to a prospective client under this set of circumstances.[81] Without a response or further consent from the recipient, the sender must cease all subsequent communications.[82]

An additional exemption is for messages sent from a secure account, such as a bank account, as long as it is only a one-way communication stream.[83] The GIC Regulations also provide exemptions for charitable solicitations and for messages sent on behalf of a political party.[84] Likewise, any communications sent to enforce a legal right, such as in a case of debt recovery, are exempt from CASL.[85] Finally, the GIC includes an exemption for messages that the sender reasonably believes will be delivered to a foreign country and that complies with that country's spam laws—a major focus of this note.[86]

C. Documentation Requirements and Enforcement Provisions

In the case of an alleged CASL violation, the "onus [is on the business] to prove consent."[87] Thus, businesses need to keep certain historical records for each past, current, and prospective customer. For example, to prove express consent, the "record of the date, time, purpose, and manner of that consent [must be] stored in a database."[88] In addition to tracking the timestamp of a recipient's action, to prove reliance on a conspicuous publication, the CRTC recommends for a business to "record screenshots or have a contemporaneous record of the publication."[89] In order for a business to rely on the due diligence defense, the CRTC created guidelines for a corporate compliance program that suggests for businesses to create a CASL corporate training program, a complaint handling system, an audit program, and a written policy manual.[90]

---

[81] Electronic Commerce Protection Regulations, 147 C. Gaz. 2907, 2914 (Dec. 18, 2013) (Can.).

[82] *Frequently Asked Questions About Canada's Anti-Spam Legislation*, *supra* note 77 ("Only one CEM may be sent without obtaining the consent of the recipient of the message.").

[83] Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(e) (Can.).

[84] *Id.* §§ 3(g)–(h).

[85] *Id.* § 3(c).

[86] *Id.* § 3(f); *see* discussion *infra* Section III.A.

[87] *Canada's Anti-Spam Legislation (Infographics): What Constitutes a Commercial Electronic Message (CEM)?*, *supra* note 43.

[88] CRTC Bulletin 2012-548, *supra* note 51, at ¶ 26.

[89] *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, *supra* note 55.

[90] *Guidelines to Help Businesses Develop Corporate Compliance Programs*, Compliance & Enf't Info. Bull., CRTC 2014-326 (Can.) (June 19, 2014), http://www.crtc.gc.ca/eng/archive/2014/2014-326.pdf [https://perma.cc/F7ZU-F68K]. In addition, the CRTC instructs businesses to keep detailed records of their:

The CRTC is the agency tasked with primary enforcement responsibility of non-compliant CEMs.[91] CASL includes provisions for the CRTC to consider multiple factors when determining the penalty to apply,[92] but allows for stiff administrative penalties per violation of $1,000,000 per individual and $10,000,000 per business.[93] CASL further allows anyone to "enter into an undertaking at any time," and if one has done so before the CRTC's violation notice, then "no notice of violation may be served on them in connection with . . . the undertaking."[94] Further, CASL provisions for vicarious liability, and for potential personal liability for corporate directors and officers in connection with a CASL violation.[95] CASL also created a private right of action, with statutory damages up to "$200 for each [CEM] contravention, . . . not exceeding $1,000,000" per day.[96] On June 7, 2017, less than a month before its effective date, the ISED acknowledged some flaws in CASL and suspended the private right of action provision.[97]

D. Potential Changes to CASL

The ISED acknowledged that "businesses . . . should have reasonable ways to communicate electronically with Canadians. . . .

> commercial electronic message policies and procedures; all contemporaneous unsubscribe requests and resulting actions; all evidence of express consent (e.g. audio recordings or completed forms) from consumers who agree to receive commercial electronic messages; commercial electronic message recipient consent logs; commercial electronic message scripts; CEM campaign records; staff training documents; other business procedures; and official financial records.

From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent, *supra* note 55.

[91] *Canada's Anti-Spam Legislation: Enforcement*, GOV'T OF CAN. (June 13, 2017), http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00026.html [https://perma.cc/FV52-SXT8].

[92] CASL, S.C. 2010, c 23 § 20(3) (Can.).

[93] *Id.* § 20(4); *see also* EMAIL EXPERIENCE COUNCIL, A DIGITAL MARKETER'S GUIDE TO CANADA'S ANTI-SPAM LAW "CASL" 9–10 (2017), https://emailexperience.org/wp-content/uploads/2017/04/CASL_guidance-1.pdf [https://perma.cc/94HG-HDSS].

[94] CASL, S.C. 2010, c 23 § 21 (Can.); *see Undertaking*, BLACK'S LAW DICTIONARY (10th ed. 2014). For an example of an undertaking, see *Undertaking: Rogers Media Inc.*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N (Nov. 20, 2015), https://crtc.gc.ca/eng/archive/2015/ut151120.htm [https://perma.cc/6HBY-X4WR] (Rogers Media Inc. entered into an undertaking with the CRTC by agreeing to pay $200,000 and implementing compliance measures.).

[95] CASL, S.C. 2010, c 23 § 31–32. For an example where CRTC penalized an individual, see *Compliance and Enforcement Decision CRTC 2017-65*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N (Mar. 9, 2017), https://crtc.gc.ca/eng/archive/2017/2017-65.htm [https://perma.cc/Z7XB-3ZMA].

[96] CASL, S.C. 2010, c 23 § 51(1)(i) (Can.); *see also* EMAIL EXPERIENCE COUNCIL, *supra* note 93, at 9 ("Each 'send instance' can be considered a violation, so the penalties can add up quickly.").

[97] *See supra* note 23 and accompanying text.

[and CASL needs to] strik[e] the right balance,"[98] and on September 26, 2017, the House of Commons commenced a review of CASL.[99] Many testified on CASL's inadequacies. For example, Rogers Communications, Inc., a Canadian communications and media company, lamented that sending a roaming notification to a customer requires an unsubscribe option under CASL.[100] Another witness, a marketing company, testified to "the economic burden that CASL compliance is placing on many Canadian businesses."[101] It is notable that none of these witnesses represented U.S. interests. On December 12, 2017, the ISED Committee adopted a recommendations report and requested the Canadian government's response.[102] None of its thirteen recommendations call for drastic changes, rather, the purpose of the recommendations was to provide clarifications to the law, and to educate the public.[103]

For illustration, the Committee Report desired to ensure the definitions of "commercial electronic message," "implied consent," and "express consent" "[were] clear and . . . do not create unintended cost of compliance."[104] Additionally, "[t]he Committee recommend[ed] that the Government of Canada further investigate the impact of implementing the private right of action . . . . [and to] consider if an award of damages should be based on proof of tangible harm."[105] There was a notable supplementary opinion rejecting drastic changes and

---

[98] Government of Canada Suspends Lawsuit Provision in Anti-Spam Legislation, *supra* note 23.

[99] *Statutory Review of CASL*, HOUSE OF COMMONS STANDING COMM. ON INDUS., SCI. & TECH., https://www.ourcommons.ca/Committees/en/INDU/StudyActivity?studyActivityId=9659639 [https://perma.cc/3FU4-5PLA].

[100] *Standing Committee on Industry, Science and Technology: Statutory Review of Canada's Anti-Spam Legislation*, 42 Parl. 1st Sess. Num. 76, at 7–8 (Oct. 17, 2017) (statement of Deborah Evans, Associate Chief Privacy Officer, Rogers Communications Inc.), https://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9163185/INDUEV76-E.PDF [https://perma.cc/J9ZL-SSQL].

[101] *Standing Committee on Industry, Science and Technology: Statutory Review of Canada's Anti-Spam Legislation*, 42 Parl. 1st Sess. Num. 82, at 2 (Oct. 5, 2017) (statement of Kim Arsenault, Senior Dir., Client Services, Inbox Marketer), http://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9237086/INDUEV82-E.PDF [https://perma.cc/58U3-R2PC].

[102] HOUSE OF COMMONS, REPORT OF THE STANDING COMMITTEE ON INDUSTRY, SCIENCE AND TECHNOLOGY: CANADA'S ANTI-SPAM LEGISLATION: CLARIFICATIONS ARE IN ORDER, 42 Parl. 1st Sess., at 35 (2017) (Can.), https://www.ourcommons.ca/Content/Committee/421/INDU/Reports/RP9330839/indurp10/indurp10-e.pdf [https://perma.cc/2CMN-4RPV] [hereinafter The Committee Report].

[103] *Id.* at 3–5. The Committee Report also recommended replacing CASL's name with Electronic Commerce Protection Act (ECPA). *Id.* at 5.

[104] *Id.* at 3. The Committee pointed to testimony on the deficiencies with the current definitions. For example, all witnesses agreed that "purely administrative and transactional electronic messages should not fall under the definition of a CEM." *Id.* at 24. The committee also noted the testimony requesting simplification and clarification of express and implied consent requirements. *Id.* at 21.

[105] *Id.* at 4.

recommending keeping the private right of action as is, albeit, with a one-year grace period.[106]

On April 16, 2018, the government of Canada responded to the report, agreeing that some changes are warranted, but calling for further research.[107] Additionally, it stated that "[a] decision on the private right of action will be part of the broader considerations that the government pursues through consultation with key stakeholders, thereby ensuring the CASL is effective, balanced, and delivers for Canadians."[108] Based on the response, it is unclear what the future holds, however, it is likely that CASL at its core will be retained.[109] Yet, any future changes to CASL provide a sound opportunity for the GIC to incorporate a foreign sender exemption.[110]

II. U.S. ANTI-SPAM LAW: WHAT IS DIFFERENT FROM CASL?

In the United States, the CAN-SPAM Act is the primary commercial anti-spam law.[111] As this section progresses in contrasting CAN-SPAM with CASL, it is important to recognize that CAN-SPAM has existed since 2004.[112] After fifteen years of adoption,

---

[106] *Id.* at 38 (statement of Brian Masse M.P., Windsor West, NDP Innovation, Sci. & Econ. Dev. Critic).

[107] Government Response to the Tenth Report of the Standing Committee on Industry, Science and Technology, to Dan Ruimy, M.P., Chair of the Standing Comm. on Indus., Sci. and Tech. (Apr. 16, 2018), https://www.ourcommons.ca/content/Committee/421/INDU/GovResponse/RP9762984/421_INDU_Rpt10_GR/421_INDU_Rpt10_GR-e.pdf [https://perma.cc/5XCV-VGN8].

[108] *Id.* at 5.

[109] None of the thirteen recommendations touched on CASL's extraterritorial reach. Thus, it is probable that the issues discussed in this note will remain as-is. *See* The Committee Report, *supra* note 102, at 3–5; *see also* Michael Geist, *Industry Committee Calls for CASL Clarification, Rejects Demands for Anti-Spam Law Overhaul* (Dec. 15, 2017), http://www.michaelgeist.ca/2017/12/industry-committee-calls-casl-clarification-rejects-demands-anti-spam-law-overhaul [https://perma.cc/EWV2-4L2U]; *infra* Section III.C.

[110] *See infra* Part III.

[111] *See* CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified as amended at 15 U.S.C. § 7701-7714 (2012 & Supp. V 2018)). The law expressly preempts states from passing spam laws "except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." *Id.* at § 7707(b). There has been a lot of litigation on this topic, mainly in California, which allows for select private right of action for such violations. *See* CAL. BUS. & PROF. CODE § 17529.5(b)(1)(A)(iii) (West 2019); *see also* Balsam v. Trancos, Inc., 138 Cal. Rptr. 3d 108, 123 (Cal. Ct. App. 2012) ("Accordingly, we will affirm the award of liquidated damages to Balsam. The award is neither inconsistent with the statute . . . nor preempted by federal law."), *as modified on denial of reh'g* (Mar. 21, 2012); Daniel Balsam, DANHATESSPAM, http://www.danhatesspam.com [https://perma.cc/B74K-U8WW]. For background on this topic, see Roger Allan Ford, Comment, *Preemption of State Spam Laws by the Federal Can-Spam Act*, 72 U. CHI. L. REV. 355, 355 (2005).

[112] *See* 15 U.S.C. § 7701–14.

any drastic shift to the anti-spam law, as presented in CASL, is likely to be difficult for some businesses and disruptive to others.[113]

The FTC publicizes certain rules and provisions to enforce compliance with the Act.[114] Among other requirements, the CAN-SPAM Act requires a commercial email sender to include an opt-out mechanism on any sent communication[115] and to honor the email recipient's request to unsubscribe from further solicitations.[116] Additionally, the FTC controls most of CAN-SPAM's enforcement, and currently threatens a hefty $41,484 penalty per violation and even criminal prosecution;[117] but with the low enforcement rate, its bark is worse than its bite.[118] CAN-SPAM also allows state enforcement actions,[119] as well as enforcement by the ISPs,[120] but

---

[113] *See* Sookman & Soni, *supra* note 38 ("For many [non-Canadian] organizations, compliance will require development of new databases, modification of computer systems, changes to websites, user interfaces, and contracting processes and disclosures of information.").

[114] These rules include defining "primary purpose." 16 C.F.R. § 316.3 (2019). Additional publicized rules are: labeling rules for sexually oriented messages, *id.* § 316.4; prohibition from charging fees to unsubscribe, *id.* § 316.5; and a severability clause. *Id.* § 316.6.

[115] *See* 15 U.S.C. § 7704(a)(3)(A)(i); *CAN-SPAM Rule*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/can-spam-rule [https://perma.cc/S4ZK-N44U] ("The CAN-SPAM Act applies almost exclusively to 'commercial electronic mail messages.'").

[116] 15 U.S.C. § 7704(a)(5)(ii). The other requirements prohibit misleading 'from' line in the email; prohibit misleading subject headings; requires clear identification of the nature of the email; and a valid physical address of the sender. *See* 15 U.S.C. § 7704(a)(1)–(5).

[117] *See* 15 U.S.C. § 7704(b)(d)(5); *CAN-SPAM Act: A Compliance Guide for Business*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business [https://perma.cc/69NM-X32S]. The penalty before the adjustment was $16,000. Press Release, *FTC Raises Civil Penalty Maximums to Adjust for Inflation*, FED. TRADE COMM'N (June 29, 2016), https://www.ftc.gov/news-events/press-releases/2016/06/ftc-raises-civil-penalty-maximums-adjust-inflation [https://perma.cc/ARE6-9TJ9].

[118] *See* XMission, L.C., Comment Letter on the Regulatory Review of the CAN-SPAM Rule (Aug. 31, 2017) [hereinafter "XMission Comment"], https://www.ftc.gov/system/files/documents/public_comments/2017/08/00088-141227.pdf [https://perma.cc/J5L5-6LAR] ("In the 14 years of the CAN-SPAM's existence, there appear to have been only twenty-six CAN-SPAM actions filed by various branches of the government."). Other agencies presumably include other federal agencies that could enforce CAN-SPAM. *See* 15 U.S.C. § 7706(b). In fact, primarily due to lack of enforcement, some sources suggest that a recipient should *not* unsubscribe, as that would provide notice of a working email address, which in turn will only exacerbate spam. *See* Alan Zeichick, *5 Things You Should Know About Email Unsubscribe Links Before You Click*, SOPHOS: NAKED SECURITY (Sept. 4, 2014), https://nakedsecurity.sophos.com/2014/09/04/5-things-you-should-know-about-email-unsubscribe-links-before-clicking [https://perma.cc/9SM5-HJQC].

[119] State recovery includes actual or statutory damages up to $250 per email, up to $2 million total. In addition, there are treble damages for a "willful[ ] and knowing[ ]" violation. 15 U.S.C. § 7706(f)(3).

[120] ISP recovery includes actual or statutory damages of $100 per email for a header violation; and $25 for other violations, with a $1 million cap on recovery. Similar to state enforcement actions, treble damages are allowed as well. 15 U.S.C. § 7706(g)(3). ISPs have a difficult time enforcing CAN-SPAM because the law places an additional burden to prove intent by the violator. *See id.* at § 7706(g)(2); XMission Comment, *supra* note 118 ("In every lawsuit . . . , the [d]efendant relied heavily on the definition of 'Procure' set forth in 7706(g)(2) in order to pass responsibility to other[s].").

does not allow for a private right of action. Because of its "opt-out" construction and lack of a private enforcement mechanism, compliance with CAN-SPAM is not onerous, but consequently is generally regarded as less effective at controlling spam than similar legislation in other countries.[121] Recently, the law underwent a ten-year mandatory review, with the FTC unanimously voting to keep the law as is.[122]

There are many differences between CAN-SPAM and CASL, however, a few are especially notable.[123] First, in contrast with CASL, CAN-SPAM limits the definition of a CEM to an email with a commercial "primary purpose,"[124] thereby allowing certain transactional messages to contain marketing content.[125] Also, in contrast to CASL's opt-in consent requirements,[126] CAN-SPAM allows for senders to deploy messages until the recipient opts out from further emails.[127] CAN-SPAM does not have significant limitations around email procurement, thus enabling businesses to design their own methods of email marketing to a prospect or customer, until an opt-out occurs.[128] Further, unlike CASL, there is no complex propagation requirement between data-sharing parties—once a user removes consent, a business simply must stop sharing it.[129]

More telling, because CAN-SPAM does not contain a consent requirement, onerous documentation is unnecessary, while CASL requires the development of "extensive, expensive, corporate compliance programs . . . [which] can easily cost tens of thousands of dollars in legal and consulting fees, not to mention

---

[121] *See* KREBSON SECURITY, *supra* note 17 ("[C]ritics of the law often refer to it as the YOU-CAN-SPAM Act, charging that it essentially legalized spamming."); *see also Email Anti-Spam Laws Around the World*, *supra* note 11 (showing global anti-spam laws requiring consent).

[122] Press Release, Fed. Trade Comm'n, FTC Completes Review of CAN-SPAM Rule (Feb. 12, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftc-completes-review-can-spam-rule [https://perma.cc/A7ZQ-QAX8]; CAN-SPAM Rule, 82 Fed. Reg. 29,254 (June 28, 2017).

[123] *See generally Key Differences Between US and Canadian Anti-Spam Laws*, MCMILLAN LLP (Apr. 2014), http://mcmillan.ca/Files/172403_Key%20Differences%20between%20US%20and%20Canadian%20Anti-Spam%20Laws.pdf [https://perma.cc/24ET-FX42] (discussing in depth the differences between the two countries' Spam laws). For an in-depth look at CAN-SPAM, see Mark W. Brennan, Hogan Lovells US LLP, *Complying with the CAN-SPAM Act*, LEXIS NEXIS (Nov. 8, 2016), https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2016/11/08/complying-with-the-can-spam-act.aspx [https://perma.cc/4M8E-XAVE].

[124] 16 C.F.R. § 316.3 (2018).

[125] *Id.* § 316.3(a)(2); *see* discussion *supra* Part I.

[126] *See* discussion *supra* Section I.A.

[127] Without consent, however, a sender must include a "clear and conspicuous identification that the message is an advertisement or solicitation." 15 U.S.C. § 7704(a)(5)(i) (2018). Further, consent is required for CEMs sent to wireless providers' domains. *See* 47 C.F.R. § 64.3100 (a)(1) (2018).

[128] With the exception of statutory limitations on automated email harvesting and on dictionary attacks. 15 U.S.C. § 7704(b)(1).

[129] *See supra* notes 69–74 and accompanying text; 15 U.S.C. § 7704(a)(4)(A)(iv).

lost productivity."[130] Additionally, CASL impacts other forms of communication, such as social networks and text messaging, while CAN-SPAM applies purely to emails.[131] Moreover, under CASL, officers and corporate directors could be personally and vicariously liable for violations in contrast to CAN-SPAM.[132] Finally, unlike CAN-SPAM, CASL has provisions for a private right of action, albeit it is currently suspended during the parliamentary review period.[133] Beyond the rule comparison, after fifteen years of compliance, U.S. businesses are used to CAN-SPAM adherence.[134]

III. U.S. BUSINESSES NEED TO BE CONCERNED WITH CASL

CASL's regulatory body, ISED, clarified that only emails which are sent from Canada's servers or accessed in Canada are subject to CASL.[135] ISED, however, left no doubt that CASL's consent and "unsubscribe requirements . . . apply (i) to foreign messages including those sent by foreign organizations to Canadian recipients (whether customers, or proposed customers or otherwise), and (ii) to messages that are stored on foreign servers and accessed from Canada."[136] Thus, legitimate American businesses that reach into Canada must follow the law of the land and abide by CASL.

This leads to a simple, but important question: How does a U.S. business know they reached into Canada? If we are dealing with a physical address, the answer is clear: postal codes.[137] An

---

[130] Osborne, *supra* note 41; *see* discussion *supra* notes 87–97 and accompanying text. CAN-SPAM does require ceasing all sharing and sales of an email address that opted out. 15 U.S.C. § 7704(a)(4)(A)(iv).

[131] *See* definition of "electronic address" and "electronic message". CASL, S.C. 2010, c 23 (Can.). In the U.S., the FCC through the TCPA governs text messaging. *See In re* Rules & Regulations Implementing the Telephone Consumer Protection Act of 1991, 18 FCC Rcd. 14014, 14115 (2003).

[132] *See* discussion *supra* Section I.C.

[133] Press Release, Innovation, Sci. & Econ. Dev. Can., *supra* note 23 ("The [g]overnment supports . . . eliminating any unintended consequences for organizations that have legitimate reasons for communicating electronically with Canadians. For that reason, the [g]overnment will ask a parliamentary committee to review the legislation.").

[134] *See supra* note 111.

[135] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2914 (Dec. 18, 2013) ("The provision of CASL that addresses sending CEMs only applies where the CEM is sent from Canada or accessed in Canada. It does not apply when the CEM is simply routed through Canada."). Email routing is best understood by analogizing it to a post office. The post office does not route a letter if they deliver it directly to a person's home. A temporary change of address request, on the other hand, does require the post office to route the mail. For an in-depth discussion of email routing, see *Email Routing Services*, WEBSERVIO, https://www.webservio.com/custom-email-solutions/email-management/email-routing-services.html [https://perma.cc/U9QC-H9BC].

[136] Sookman & Soni, *supra* note 38.

[137] Unlike numeric zip codes in the USA, Canada utilizes alphanumeric postal codes. Susan Munroe, *Postal Codes for Canada*, THOUGHT CO. (Jan. 31, 2019), https://www.thought

email address, however, transcends geographical boundaries as a generic email domain, such as @yahoo.com or @gmail.com, says nothing regarding the recipient's location. Without additional data points, a sender might not even be aware that a Canadian is being targeted for offers when an electronic message is sent—in potential violation of CASL.

A. Rely on These Provisions at Your Own Risk

The Canadian government offered U.S. businesses a glimmer of hope when the GIC passed a regulatory exemption to CASL for foreign states.[138] Additionally, CASL contains a due diligence defense provision.[139] Unfortunately, because CASL places the burden of proof with the sender,[140] neither is likely to substantially help a U.S. business in a fight against a claim of a CASL violation.

Section (3)(f) of the GIC Regulations states that CASL's electronic messages provision does not apply to a commercial electronic message

> if the person who sends the message or causes or permits it to be sent reasonably believes the message will be accessed in a foreign state that is listed in the schedule and the message conforms to the law of the foreign state that addresses conduct that is substantially similar to conduct prohibited under section 6 of the Act.[141]

While to the naked eye, and to some sources, this exemption suggests that Section (3)(f) might protect CAN-SPAM compliant U.S. businesses in case of contention,[142] as detailed below, there is

---

co.com/postal-codes-for-canada-510814 [https://perma.cc/459U-LC6L]. This makes for an easy country differentiator.

138 Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(f) (Can.).

139 CASL, S.C. 2010, c 23 § 33 (Can.).

140 *Id.* § 13 (Can.).

141 Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(f) (Can.). As originally proposed, the verbiage to the exemption was applicable for a message

> that is sent from a computer system located outside Canada and that *relates to a product, good, service or organization located or provided outside Canada* that is accessed using a computer system located in Canada if the person sending the message did not know and could not reasonably be expected to know that the message would be accessed using a computer system located in Canada.

Electronic Commerce Protection Regulations, 147 C. Gaz. 29, 38 (proposed Jan. 5, 2013) (emphasis added). This verbiage seems to have fewer gaps than the current regulation and would likely have been better suited to protect U.S. interests. In view that an exemption for emailing Canadian visitors was "not necessary," the Governor-in-Council modified the verbiage. Electronic Commerce Protection Regulations, 147 C. Gaz., SOR/2013-221, 2907, 2927 (Dec. 18, 2013). The GIC did not include an explanation behind this reasoning.

142 *See, e.g.*, David Fraser, *Complying with Canada's Anti-Spam Law (CASL) Foreign Organizations Doing Business in Canada Need to Pay Attention*, MCINNES COOPER (Aug. 1, 2014), http://www.mcinnescooper.com/publications/legal-update-complying-with-

sufficient room for alternate interpretations. Thus, such reliance is unadvisable.

First, an argument can be made that Industry Canada's intention for Section (3)(f) was to apply it only to *Canadian*, and not to foreign, senders.[143] Indeed, Industry Canada seemingly confirmed as much when it stated that the purpose of Section (3)(f) was "[t]o reduce regulatory duplication in situations where CEMs are sent from Canada to other states that have their own regulatory requirements, the Regulations exempt messages *sent from Canada* to" countries listed in the schedule, including the United States.[144] Therefore, it can be argued that senders from foreign countries are in fact excluded from Section (3)(f) protections.

Furthermore, a more basic argument could be made, in that as defined by CASL, U.S. businesses are excluded from the word "person" altogether. CASL defines a "person" as "an individual, partnership, corporation, organization, association, trustee, administrator, executor, liquidator of a succession, receiver or legal representative."[145] Is there room to fit in a foreign entity within this translation? Not if utilizing the statutory canon of *expressio unius est exclusio alterius*—the inclusion of one term, excludes another.[146] In fact, the statutory definition does not even contain a general term, so that the statutory canon of *ejusdem*

---

canadas-anti-spam-law-casl-foreign-organizations-doing-business-in-canada-need-to-pay-attention [https://perma.cc/WN64-PSSC]; WORLD COUNCIL OF CREDIT UNIONS, CANADA'S ANTI-SPAM LEGISLATION AND NON-CANADIAN CREDIT UNIONS 4–5 (July 3, 2014), http://www.woccu.org/documents/CASL_for_Non-Canadians [https://perma.cc/U324-GY3W].

[143] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. at 2921 ("Another issue concerns the ability *for businesses in Canada* to send CEMs *to recipients* outside of the country. . . . In order to address this issue, an exclusion is provided in these Regulations *for messages sent from Canada to foreign states* and in compliance with local laws that regulate essentially the same conduct that is prohibited under section 6, notably, the United States . . . .") (emphasis added).

[144] *Id.* at 2914 (emphasis added). The CRTC initially took on a similar view that the Section (3)(f) "provision excludes some CEMs sent from Canada to a foreign country." Smith, *supra* note 37. The CRTC adjusted this interpretation, which now states that CEMs "sent to recipients in Canada from another country must comply with CASL." *Frequently Asked Questions About Canada's Anti-Spam Legislation*, *supra* note 77. Since the CRTC has no authority over non-form consent requirements, its interpretation is not binding. CASL, S.C. 2010, c 23 § 64 (Can.).

[145] CASL, S.C. 2010, c 23 § 1(1) (Can.).

[146] *Expressio unius est exclusio alterius*, BLACK'S LAW DICTIONARY (10th ed. 2014). *Compare* the above definition of "person" *with Memorandum of Understanding Between the United States Federal Trade Commission and the CRTC on Mutual Assistance in the Enforcement of Laws on Commercial Email and Telemarketing*, CAN. RADIO-TELEVISION & TELECOMM. COMM'N (Mar. 24, 2016), http://crtc.gc.ca/eng/internet/ftc.htm [https://perma.cc/MWG6-5LPL] [hereinafter "Memorandum of Understanding"] ("'Person' means any natural person or legal entity, including corporations, unincorporated associations, or partnerships, existing under or authorized by the laws of the United States, its States, or its Territories, or the laws of Canada.").

generis could be applied.[147] Thus, if a court were to rely solely on the plain meaning, CASL's definition of a "person" likely excludes a U.S. entity. Concededly, this argument is unlikely to hold because Canada generally relies on legislative intent in its statutory interpretation, and contrary to intent, such application would likely invalidate many provisions of CASL's desired reach on foreign senders.[148] Nevertheless, this faulty wording is noteworthy and showcases Canada's aloofness towards CASL's impact on foreign countries.

Assuming *arguendo* that Section (3)(f) applies to foreign senders, its efficacy is also up for debate. Section (3)(f) applies to someone with a reasonable belief that "the message will be accessed in a foreign state."[149] The CRTC clarified that "reasonabl[e] belie[f] is [analyzed under] the reasonable person test."[150] According to Black's Law Dictionary, a reasonable person is prudent and behaves in a way that society expects.[151] How would a reasonable *foreign* email sender behave? As an illustration, would a local store in Florida with no online purchase capability be considered "reasonable" if it obtained a local email list and ended up reaching into Canada? A reasonable person in such a case might know that more than four million "snowbirds" visit Florida from Canada each year,[152] hence the likelihood of targeting them once they return to Canada.[153] This set of facts might have the potential to force coastal Florida businesses into CASL compliance as it could negate the reasonable person analysis of Section (3)(f). The point is that nothing is clear, and without regulatory or legislative intervention, it will be up to the CRTC or the court system to interpret the law—a situation that U.S. businesses accused of noncompliance might wish to avoid. It

---

147 *Ejusdem generis*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("[W]hen a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same class as those listed."); *cf.* Air Travellers Security Charge Act, S.C. 2002, c 9, art 5 § 2 (Can.) ("'Person' means an individual, partnership, corporation, trust or estate, or a body that is a society, union, club, association, commission *or other organization of any kind whatever*.") (emphasis added).

148 *See, e.g.*, Interpretation Act, R.S.A. 2000, c I-8, § 10 (Can.) ("An enactment . . . shall be given the fair, large and liberal construction and interpretation that best ensures the attainment of its objects.").

149 Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(f) (Can.).

150 Smith, *supra* note 37.

151 *Reasonable Person*, BLACK'S LAW DICTIONARY (10th ed. 2014).

152 Thad Moore, *How the Canadian Dollar's Plunge Is Hurting Florida Snowbirds*, TAMPA BAY TIMES (Feb. 9, 2016, 11:51 AM), http://www.tampabay.com/news/business/tourism/how-the-canadian-dollars-plunge-is-hurting-florida-snowbirds/2264552 [https://perma.cc/LX75-CWQY].

153 Even if the Florida business in the example receives express consent from a snowbird to email, CASL's onerous documentation requirements would be triggered. *See* notes 87–90 and accompanying text.

is unfortunate that the GIC applied an objective standard to a law which requires concreteness to ensure compliance. Ironically, since it is difficult to know where the recipient behind an email address resides, the "reasonable belief" may be that an innocuous CASL violation is a near certainty.[154]

In addition to Section (3)(f), CASL includes a defense that "[a] person must not be found to be liable for a violation if they establish that they exercised due diligence to prevent the commission of the violation."[155] While it is certainly useful, "exercis[ing] due diligence" implies action,[156] thus *not* implementing any segmentation prevents the utility of the defense. Moreover, since the burden of proof lies with the sender,[157] the sender needs to keep records. To keep up with the CRTC's massive documentation requests,[158] a business would need to invest significant resources to their procedures, documentation, and data capture practices—in a nutshell: follow CASL.

Even if both Section (3)(f) and due diligence apply to a set of facts, they are *defenses*.[159] U.S. businesses need *reasonable* notice and concrete data segmentation rules to avoid being placed in the position of needing a defense in the first place. Yet neither is forthcoming.

B. Choices, Choices, Choices: What Is a U.S. Business to Do?

While no business is the same, there are seemingly three main ways that U.S. businesses can choose to interact with CASL. First, a business might elect to apply CASL requirements to all of its email campaigns, irrespective of geography. A business might also go the other extreme and disregard the law altogether, either because of ignorance or a belief that they are not emailing into Canada. Finally, companies that do business in Canada may decide to parse U.S. emails from Canadian emails to comply with CASL in Canada and CAN-SPAM in the United States.

A company may decide to apply the strictest requirements, satisfying both CASL and CAN-SPAM. Indeed, "[t]he best marketing strategies start with making sure you're getting permission before adding new contacts to your email

---

154 *See* discussion *infra* Section III.B.

155 CASL, S.C. 2010, c 23 § 33 (Can.).

156 *Id.*

157 *Id.* § 13.

158 *See supra* notes 87–90 and accompanying text.

159 Technically, Section (3)(f) is an exemption, although due to its reliance on the reasonable person standard, it behaves in practice as a defense. *See supra* notes 149–1154 and accompanying text.

list."[160] Here, businesses are ripe to utilize the due diligence defense in any accusation of a violation,[161] and to lower their overall legal risks, but at what cost? CASL is larger than opt-in marketing, and such a conservative approach may place a business at a competitive disadvantage.[162] Further, other aspects of CASL suffer from many interpretive uncertainties in need of resolution.[163] These businesses inherit the law's growing pains and any consequences which may result. Yet for U.S. businesses, this option seems to be the lesser of evils.

The other end of the spectrum is ignoring CASL altogether. In fact, many U.S. businesses may not even realize that a portion of their target audience resides in Canada. Consider a U.S. business that honestly believes their target audience is not in Canada and ignores CASL. Even if such a belief has merit, there is undoubtedly an inherent risk of unintended messages going to Canada. For example, an email address could change ownership after a period of inactivity with some email service providers[164] or through a non-renewal of a domain with a mail server.[165] Thus, it is not implausible that a Canadian resident could register an email address that once belonged to a U.S. resident. Given that a single unconsented CEM violates CASL,[166] such a situation places the sender out of compliance. Additionally, any imperfections in the captured email address, such as a typo, could lead to the same result.

---

[160] Ryan Pinkham, *Email Marketing Best Practices: 125 Links to Help You Be a Better Marketer*, CONSTANT CONTACT, https://blogs.constantcontact.com/email-marketing-best-practices-2 [https://perma.cc/43T9-YAHR].

[161] CASL, S.C. 2010, c 23 § 33 (Can.).

[162] For instance, the inability to conduct campaigns to prior customers beyond two years; or to engage in email sharing, without the limiting data sharing requirements; the inability to reach out via social media to potential prospects; etc.

[163] Discussing all of CASL's inadequacies could fill a book and is out of scope for this note. *See* Sookman, *supra* note 47; Osborne, *supra* note 41. There is also a persuasive argument that CASL's "'ban-all' approach" violates the Canadian Constitutional Right to freedom of speech. *See* Emir Crowne & Stephanie Provato, *Canada's Anti-Spam Legislation: A Constitutional Analysis*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 1, 1 (2014).

[164] *See* Caroline Shahar, *Yahoo Is Closing Down Inactive Accounts: Here's What You Should Do*, CONSTANT CONTACT (July 10, 2013), https://blogs.constantcontact.com/yahoo-shutting-down-accounts [https://perma.cc/C723-SW7U] (referencing Yahoo's shutdown of accounts due to only 12 months of inactivity and making the email address available for re-registration to the public); *see also* Tony Redmond, *Recycled Email Addresses and Outlook Nicknames*, WINDOWS IT PRO (Apr. 14, 2016), http://windowsitpro.com/blog/recycled-email-addresses-and-outlook-nicknames [https://perma.cc/P4LH-2C6P] (noting that Microsoft recycles email addresses).

[165] *See* QUORA, *What Happens With My Email When Domain Expires?*, https://www.quora.com/What-happens-with-my-email-when-domain-expires [https://perma.cc/CZ8C-FGRL].

[166] Sookman, *supra* note 47 ("[U]nlike more reasonable legislation in other countries, even a single message can be a CEM. There is no requirement that messages be sent in bulk and there is no *de minimis* exception for single emails in CASL.").

Ironically, it is California—the state with the most progressive U.S. data privacy legislation[167]—that creates a unique conundrum because California and Canada share an abbreviation, "CA." The possibilities for innocuous CASL violations are endless. For example, a study showed that thirty-two percent of U.S. residents think they are interacting with California when they see a ".ca" domain extension.[168] It is conceivable that a U.S. business would make a similar mistake and send an email to someone in Canada. California also presents unique typo opportunities because many of the state's government agencies and municipalities utilize third-level domain of ".ca.gov."[169] A simple domain extension error that flips "email@californiaagency.ca.gov" to "email@californiaagency.gov.ca" or "email@californiaagency.ca" sends the email into Canada. For illustration, one could readily see how easy it is to mistype "governor@governor.ca.gov" to "governor@governor.ca," thereby switching the recipient from a California governor to a Canadian domain owner.[170] Hence, businesses that ignore CASL altogether might reach into Canada and place themselves at regulatory risk.[171]

Another choice that a business could pursue is to treat Canadian and U.S. emails differently. This ideal option follows CAN-SPAM for U.S. data, while complying with CASL for Canadian electronic addresses.[172] Creating such a split, however,

---

[167] Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/95SX-U47A].

[168] Alicia Thomas, *32% of Americans Think .CA Represents a California-Based Website [Study]*, SEARCH ENGINE PEOPLE (Dec. 21, 2015), https://www.searchenginepeople.com/blog/15124-ca-california-canada-domain.html [https://perma.cc/8SA7-CADW].

[169] One can reach many examples through the main site, CA.GOV, https://www.ca.gov [https://perma.cc/4K7A-AZ4L].

[170] This is not a hypothetical. See Wuyee.org, where a similar typo is readily visible ("jerry.brown@gov.ca"). *ECE Advocacy Phone & Email Scripts*, WUYEE, https://www.wuyee.org/s/ECE_Advocacy_PhoneEmail_Scripts.pdf [https://perma.cc/A7BC-CXPZ]. The domain "gov.ca" is indeed registered, ironically by the Canadian government. *See Whois Record for Gov.ca*, WHOIS, http://whois.domaintools.com/gov.ca [https://perma.cc/MXE4-DU98]. A ".ca" domain must be owned by someone with a Canadian presence. *See Policies, Rules, and Procedures*, CIRA, https://cira.ca/sites/default/files/public/policy/cprregistrants-en.pdf [https://perma.cc/36G6-ESRV].

[171] *See* discussion *supra* Section III.A. A business might rely on the "reasonably believes" exemption. It will be hard to rely on the due diligence defense in this case, as no "diligence" for CASL compliance is present.

[172] *Compare, e.g.*, *Premier Rewards Gold Card Application*, AM. EXPRESS, https://www.americanexpress.com/us/credit-cards/card-application/apply/rose-gold-card/25330-10-0?pmccode=784&intlink=US-Acq-Shop-Consumer-CardDetails-RoseGold-Prospect-Apply-RoseGold-Header [https://perma.cc/KN3Y-X9U6] (U.S. credit card application requiring an email address) *with American Express® Gold Rewards Card Application*, AM. EXPRESS, https://global.americanexpress.com/acq/intl/dpa/canlac/can/pers/begin.do?perform=IntlEapp:CAN:en_gold_charge&parent=A00000KW0U&intlink=ca-en-amex-cardshop-details-apply-americanExpressGoldRewardsCard-top [https://perma.cc/HU4B-BPUF] (In contrast to the U.S. credit card application, a comparable, CASL compliant credit card application in Canada clearly stipulates that providing an email address is optional.).

is difficult for many U.S. businesses because they lack technological prowess.[173] Depending on the business, collected data points could include a physical address, customer name, and phone number,[174] although many service-based businesses collect only email addresses.[175] Thus, it is unsurprising that "a lot of businesses dump all contacts into one, unfiltered email list [and] send the same email to the entire list of subscribers, without any distinction."[176] Indeed, with such limited data, it is nearly impossible to determine with complete certainty if an enrollee is Canadian. After all, an email address does not point to a location on a map.[177] Consequently, without clear-cut satisfactory instructions, any data separation from a commingled database is unlikely to be perfect.[178] Even for a large company with all the resources, directionless application of segmentation strategy is akin to dart throwing.

Additionally, those businesses with commingled databases are unlikely to take advantage of the implied consent provisions of CASL, and instead, are likely to rely only on the express provisions in their communication with Canadian customers.[179] This is because to rely on implied consent, a business needs to maintain certain analytical data points such as time stamps of last activity and purchase or inquiry history to determine if an existing business relationship exists.[180] Because complex database additions would be difficult for many businesses, such businesses are likely to only use express consent, thereby marketing to fewer people and limiting

---

[173] *See, e.g.*, Eric Rosenbaum, *You'll Be Shocked to Learn How Many Small Businesses Still Don't Have a Website*, CNBC (June 29, 2017, 1:16 PM EDT), https://www.cnbc.com/2017/06/14/tech-help-wanted-about-half-of-small-businesses-dont-have-a-website.html [https://perma.cc/6TQ9-VEUH] (Surprisingly, nearly half of all businesses do not have a website at all, while only a third utilize a website to communicate with customers, while only twenty-six percent utilize email marketing.).

[174] *See* Leah Hamilton, *Legal Requirements for Email Marketing*, TERMS FEED (Oct. 23, 2016), https://termsfeed.com/blog/legal-requirements-email-marketing [https://perma.cc/FXP6-E3CQ] (listing types of information a website might collect).

[175] *See, e.g.*, CRUNCHBASE, https://www.crunchbase.com/register [https://perma.cc/K8B4-VZ25]. Presumably, some of these sites collect pertinent underlying data such as the IP address, and the date and time stamp of enrollment.

[176] Derek Miller, *Small Business Email Marketing—Part Two: Leveraging Your Email Lists*, SCORE (Oct. 31, 2016), https://www.score.org/blog/small-business-email-marketing-part-two-leveraging-your-email-lists. [https://perma.cc/4LFW-7ZLU].

[177] *See, e.g.*, *Yahoo Account Enrollment*, YAHOO, https://login.yahoo.com/account/create [https://perma.cc/FLJ6-SRMP] (Canadians could freely register a @yahoo.com email address).

[178] *See* Lauren Smith, *Send Targeted Messages with Geolocation, Device, and Engagement Data*, LITMUS (Sept. 29, 2014), https://litmus.com/blog/send-targeted-messages-with-geolocation-device-and-engagement-data [https://perma.cc/FME6-CKA7] (discussing successful email data segmentation strategies based on location).

[179] *See* discussion *supra* Section I.A.

[180] *See* discussion *supra* Section I.C.

themselves of potential business as they trade off regulatory cost for opportunity cost.[181]

Moreover, acquiring new customers through email marketing, while attempting to maintain such a data split, creates additional concerns. A marketer must be conscious as to the source of their prospect list.[182] For example, a U.S. business could purchase email lists for prospecting,[183] but with CASL's complicated compliance provisions on third party consent sharing, that business needs to be extra cognizant of the source of a company's email procurement methods.[184] Otherwise, it may be the purchaser and data user who will be in violation of the law, as "the sender of a CEM has the onus of proving consent."[185]

Seemingly, CASL seeps into U.S. business practices regardless of whether the sender's focus is customer contacts or acquisitions. Without an ideal option, each business should evaluate its own risk tolerance and pick its poison. This note recommends that U.S. businesses—especially those using email marketing to acquire customers—cautiously mitigate the risk by implementing CASL requirements into their marketing programs and treat it as the de facto anti-spam law in the United States.

C. Private Right of Action: A Lucky Break or a Temporary Reprieve?

Should U.S. businesses care about this law if the current enforcement is unlikely? U.S. marketers of all sizes, especially those with Canadian assets, dodged a bullet from a foreseeable flood of class action filings,[186] and from the need to defend

---

[181] EMAIL EXPERIENCE COUNCIL, *supra* note 93, at 6–7 ("[S]ome companies are only employing express consent . . . because of concerns about . . . enforcement . . . [and] costs, time and resources to track requirements of both implied and express consent for new clients; otherwise might need to employ complex tracking measures and protocols for different groups/categories.").

[182] *Cf.* Dan Nedelko, *One List to Rule Them All: CASL Edition*, HONEYPOT MKTG. (July 15, 2014), https://honeypotmarketing.com/casl-list-segmentation-lotr [https://perma.cc/S2WG-G9SN].

[183] *See, e.g.*, INFO USA, https://www.infousa.com [https://perma.cc/S9LS-WPEX]. Note: While this practice is legal in the U.S., it is not considered a marketing best practice. *See* Teradata Perspectives, *Best Practices for Email Marketing: The Three Levels of Consent*, FORBES (June 23, 2015, 5:14 PM), https://www.forbes.com/sites/teradata/2015/06/23/best-practices-for-email-marketing-the-three-levels-of-consent. [https://perma.cc/CG5C-AKFJ]. This example is used for ease of illustration. Other hypothetical scenarios such as a business sale would be equally appropriate.

[184] *See* discussion *supra* Section I.A.

[185] *From Canada's Anti-Spam Legislation (CASL) Guidance on Implied Consent*, *supra* note 55.

[186] *Cf. Enforcing the Canada Anti-Spam Legislation (CASL) Against U.S. Companies*, KLEIN MOYNIHAN TURCO, http://www.kleinmoynihan.com/enforcing-the-canada-anti-spam-legislation-casl-against-u-s-companies [https://perma.cc/372E-WJGN] ("In theory,

themselves and settle against complaints due to inadvertent cross-border reach, when the ISED suspended the private right of action.[187] Without a private right of action, enforcement by the CRTC is unlikely against legitimate U.S. businesses for two reasons. First, the CRTC has limited resources. This is evidenced by the fact that the CRTC launched only "more than [thirty]" investigations out of over 1.1 million complaints.[188] Such lack of enforcement is reminiscent of the FTC's CAN-SPAM.[189] Second, what helps U.S. businesses is the verbiage in the Memorandum of Understanding between the CRTC and the FTC acknowledging that "cooperation [is] focus[ed] on those [c]overed [v]iolations most serious in nature."[190] Seemingly, without the private right of action, U.S. (and likely Canadian) entities might get a reprieve from enforcement.

Despite the current state of enforcement, U.S. businesses should be troubled by the unsettled status quo. After all, the private right of action could return.[191] The ISED cannot suspend this law in perpetuity, only the Canadian Parliament can as the private right of action provision is part of CASL itself and not

---

Canadian plaintiffs can bring class action lawsuits in the state where the U.S. business is incorporated or has a principal place of business, or even in Canada, under the theory that the U.S. business purposely availed itself of jurisdiction in Canada by sending CEMs into Canada. Canadian judgments can . . . generally be enforced in the U.S. pursuant to the Uniform Foreign Money Judgments Recognition Act.").

[187] Government of Canada Suspends Lawsuit Provision in Anti-Spam Legislation, *supra* note 23.

[188] Standing Committee on Industry, Science and Technology: Statutory Review of Canada's Anti-Spam Legislation, 42 Parl. 1st Sess. Num. 72, at 5, 7 (Sept. 26, 2017) (statement of Mr. Neil Barratt, Dir., Elec. Comm. Enf't, Can. Radio-television & Telecomm. Comm'n), http://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9112618/INDUEV72-E.PDF [https://perma.cc/P5JY-27FK]. The CRTC issued only "a half a dozen notices of [a] violation. . . . [and] more than 10 warning letters." *Id.* at 7. Additionally, since 2015 until the writing of this note, the CRTC influenced only eight undertakings. *See* Undertakings 2015—Compliance and Enforcement of Canada's Anti-Spam Legislation, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://crtc.gc.ca/eng/com500/ut2015.htm [https://perma.cc/Y2DP-VMP9]; Undertakings 2016—Compliance and Enforcement of Canada's Anti-Spam Legislation, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://crtc.gc.ca/eng/com500/ut2016.htm [https://perma.cc/W3UN-VLSP]; Undertakings 2017—Compliance and Enforcement of Canada's Anti-Spam Legislation, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://crtc.gc.ca/eng/com500/ut2017.htm [https://perma.cc/XZP2-FX4V]; Undertakings 2018—Compliance and Enforcement of Canada's Anti-Spam Legislation, CAN. RADIO-TELEVISION & TELECOMM. COMM'N, http://crtc.gc.ca/eng/com500/ut2018.htm [https://perma.cc/2ZXS-8DAL].

[189] *See* XMission Comment, *supra* note 118.

[190] *Memorandum of Understanding*, *supra* note 146.

[191] *See* Government Response to the Tenth Report of the Standing Committee on Industry, *supra* note 107, at 5 ("The government agrees to investigate further the impact of implementing the private right of action and to consider options for its implementation, including whether awards of damages should be based on proof of tangible harm. A decision on the private right of action will be part of the broader considerations that the government pursues through consultation with key stakeholders, thereby ensuring the CASL is effective, balanced, and delivers for Canadians.").

the regulations.[192] Thus, either the Canadian Parliament will formally change the private right of action provision, or it will return in some moderated form.[193]

Moreover, it is tough to gauge political implications. It is unlikely that Canada's Government will desire to drastically curtail CASL. With the EU passing the General Data Protection Regulation (GDPR),[194] the government may not wish to appear lenient on consumer protection laws. Additionally, the upcoming 2019 federal elections may bring an incremental level of uncertainty.[195] At the time of CASL's nascent beginnings, when the Conservative Party led, the government thought it a good idea to add a private right of action not to the discretion of the GIC, but into the law itself.[196] In 2015, the Liberal Party formed a majority government.[197] It was not until 2017 that the Minister of INDU, a Liberal, suspended the private right of action.[198] Hypothetically, if the Conservative Party wins the 2019 election, it is possible that CASL review is treated with different gloves. Alternatively, the government may ultimately side with the Committee Report's Supplementary Opinion, which advocated that "the private right of action of this legislation should be enforced, as is, and not studied further. . . . with a grace period of one year or less."[199] Additionally, while the United States and Canada have historically had a close relationship, the current geopolitical landscape could alter this, resulting in a situation such as a trade war.[200] The government may then instruct the CRTC to conduct more rigorous extraterritorial enforcement.

---

[192] *See Standing Committee on Industry, Science and Technology: Statutory Review of Canada's Anti-Spam Legislation*, 42 Parl. 1st Sess. Num. 75, at 8 (Oct. 5, 2017) (statement of Barry Sookman, Partner, McCarthy Tétrault), http://www.ourcommons.ca/Content/Committee/421/INDU/Evidence/EV9148519/INDUEV75-E.PDF [https://perma.cc/7CTW-T9HE] ("Only Parliament can address . . . [the private right of action] because it's in the legislation, and at some point, it has to come into force or be killed or amended.").

[193] *See* discussion *supra* Section I.D.

[194] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive, recital 23, 95/46/EC, 2016 O.J. (L 119/1).

[195] *See* Chris Young, *Federal Election 2019: Navdeep Bains Becomes 1st Liberal Candidate to Be Nominated*, CAN. PRESS (June 27, 2018, 8:44 PM), https://globalnews.ca/news/4301776/federal-election-2019-navdeep-bains-nomination [https://perma.cc/H4R7-D5ZX].

[196] CASL, S.C. 2010, c 23 § 47–51 (Can.); Electronic Commerce Protection Regulations, SOR/2013-221 147 C. Gaz. 2907, 2912–13 (Dec. 18, 2013); *Conservative Party of Canada*, ENCYC. BRITANNICA (Mar. 8, 2019), https://www.britannica.com/topic/Conservative-Party-of-Canada [https://perma.cc/L8WG-HYS4].

[197] *Conservative Party of Canada*, *supra* note 196.

[198] *See Government of Canada Suspends Lawsuit Provision in Anti-Spam Legislation*, *supra* note 23; Young, *supra* note 195.

[199] The Committee Report, *supra* note 102, at 38.

[200] *See* Jack M. Mintz, *Canada Has Already Picked a Losing Strategy for Trump's Trade War*, FIN. POST (July 12, 2018, 8:20 AM EDT), https://business.

Furthermore, larger U.S. businesses may have more to worry about than CRTC enforcement. Failure of adhering to CASL regulations may create reputational risk. This may "have an adverse impact on a company's reputation thereby affecting its revenue."[201] For publicly traded companies, this could trigger requisite disclosure of material risk.[202] Since regulatory and reputational risks could turn material, companies typically discuss them on their Form 10-K annual report.[203]

All of this makes it unwise for U.S. businesses to depend on macroeconomic factors and on a foreign government and its agencies to determine its marketing fate. Yet, this is the situation U.S. businesses face today. U.S. businesses should acknowledge the risk and analyze their best course of action, which may ultimately be to follow CASL.

IV. A PATH TO ADJUST CASL'S EXTRATERRITORIAL REACH

Due to the ambiguity of Section (3)(f), as well as the overarching "ban-all" approach, CASL engulfs U.S. electronic message senders, many with limited Canadian interaction, to whom this law should not apply. Without change, a reactivation of CASL's private right of action would be an international travesty created by the Canadian government. This is because U.S. businesses would be under the threat of litigation and settlement extortion from even the most innocuous violations of CASL, which are bound to occur.[204]

U.S. businesses need direction on how to reasonably conform their marketing practices to CASL—a "reasonable" request. Further, the ISED Committee acknowledged that "improving awareness and understanding of [CASL] and its regulations" is necessary for its adoption.[205] Presumably, U.S. businesses require a similar treatment.[206] Yet, the ISED Committee's focus is to "increase

---

financialpost.com/opinion/jack-mintz-canada-has-already-picked-a-losing-strategy-for-trumps-trade-war [https://perma.cc/JT7V-ZYK9].

[201] Jonas Sickler, *What Is Reputational Risk and How to Manage It*, REPUTATION MGMT. BLOG (Apr. 27, 2019), https://www.reputationmanagement.com/blog/reputational-risk [https://perma.cc/LK2U-5YWX].

[202] FAST Act Modernization and Simplification of Regulation S-K, Release No. 33-10618; 34-85381, 84 Fed. Reg. 12,674, 12,688–89 (Apr. 2, 2019) (codified at 17 C.F.R. § 229.105 (2019)).

[203] *See, e.g.*, NIKE, 2018 FORM 10-K 66 (2018) ("[T]he adoption of new laws or regulations, or changes in the interpretation of existing laws or regulations, may result in significant unanticipated legal and reputational risks.").

[204] *See supra* notes 149–154, 167–171 and accompanying text.

[205] The Committee Report, *supra* note 102, at 4.

[206] Since CAN-SPAM adherence existed since 2004, one could argue that U.S. businesses need *more* training than Canadian ones. *See* discussion *supra* Part II.

efforts to educate *Canadians*."[207] Who is then responsible to educate U.S. businesses on CASL?

A. A Proposal to Canada

The first order for Canada before any private right of action reactivation is to absolve foreign senders from innocuous de minimis violations. Fortunately, "[t]o fix this dilemma . . . one does not need a bulldozer, but a scalpel."[208] The ISED could clarify the Section (3)(f) reasonable belief ambiguity comparable to the EU's GDPR. Recital 23 clarifies that the GDPR requirements apply to foreign senders

> where the processing activities are *related to* offering goods or services to [EU residents] irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is *apparent* that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. . . . [F]actors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[209]

While imperfect, the GDPR offers U.S. businesses greater protection against unintended violations than CASL because a sender's intent is implied through the electronic message's content.[210] If Canada would implement such a provision, a local Florida business marketing their local store—as in the earlier example—may be exempt,[211] as would inadvertently mistyped emails. Here, the message content itself would act as a facially apparent defense, likely limiting the legal risk because it would deter frivolous complaints.

Such a change would be a large improvement over the status quo, yet is likely insufficient. Legitimate U.S. businesses

---

[207] The Committee Report, *supra* note 102, at 4 (emphasis added).

[208] Charles S. Wood, Note, *Cannibal Cop Out: Why Lenity Is a Necessary, Yet Unworkable Solution in Interpreting the Computer Fraud and Abuse Act*, 82 BROOK. L. REV. 1849, 1889 (2017). The below recommendation does not resolve CASL impact through other channels, such as social media. Here, the risk to U.S. businesses is likely contained since the social platforms themselves are likely to police compliance and have the means to do so.

[209] Regulation 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive, recital 23, 95/46/EC, 2016 O.J. (L 119/1), Rec. 23 (emphasis added).

[210] *See id.*

[211] *See supra* notes 149–154 and accompanying text.

need concrete CASL rules, as opposed to its currently unfettered interpretation. The Canadian Parliament granted the GIC authority to regulate "circumstances in which [CEMs] are sent."[212] Thus, there need not be a parliamentary amendment to CASL, the ISED could recommend the proposed changes to the GIC.[213] Therefore, this note recommends for the GIC to define and create a regulatory structure for a foreign email sender to implement.[214]

The Canadian government must remember that due to the nature of an email, a one hundred percent compliance rate is unrealistic.[215] To achieve ultimate success, compliance of CASL cannot fully depend on the senders themselves and will require some assistance from the recipient. Further, the proposals below are purposefully designed to be minimally intrusive to the senders in that their implementation involves limited technological investment, without the onerous paperwork currently demanded by CASL.[216] On the other hand, the balanced proposal maximizes CASL's efficacy because implementing the below proposal would limit the unintended reach of the law, and would allow the CRTC to effortlessly discern foreign CASL violators from complying parties.

The first order is simple. The GIC needs to define a reasonable segmentation strategy for foreign senders. First, if a business collects a physical address, then any email address associated with the Canadian postal code should be excluded from the CASL exemption. Likewise, CASL should govern any email address with a ".ca" extension.

Admittedly, the Canadian government will be unsatisfied with limiting foreign senders to the above rules, as it would open legal doors to spammers to target generic domain extensions such as ".com." To that end, Canada should implement a Do-Not-Email Registry for foreign senders. The U.S. previously vetted a Do-Not-Email Registry and "determined that [the] spammers would most likely use . . . [it] for verifying the validity of email addresses."[217]

---

[212] CASL, S.C. 2010, c 23 § 64(1)(c) (Can.).

[213] *See generally* Canada's Anti-Spam Legislation Regulations, SOR/2013-81000-2-175 § 3(f) (Can.) ("His Excellency the Governor General in Council, on the recommendation of the Minister of Industry . . . .").

[214] It may be argued that many portions of the below recommendations could simply be defined through guidance by the CRTC. Undoubtedly, such an outcome would be welcomed, however, the CRTC's authority to do so may be questioned. Thus, the recommendation is to define this exemption through the GIC Regulations.

[215] *See* discussion *supra* Section III.B.

[216] *See* discussion *supra* Section I.C.

[217] FED. TRADE COMM'N, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS *i* (2004).

With this in mind, this note proposes a domain only registry,[218] whereby a verified domain owner or a certified representative would add their respective domain to the registry. Except for an overriding CASL-compliant consent for a specific email address, foreign senders would remove all electronic addresses matching to any domains to be suppressed, from all their CEM initiatives.[219] This change would significantly reduce the chances of an undesired CEM landing into Canada and grant Canadians greater flexibility and control in managing undesired emails.

This leaves the issues of country identification with the recipients holding email addresses from popular providers such as Google's Gmail or Microsoft's Outlook. It is generally impossible to tell the country of origin,[220] and therefore a balanced middle ground is needed. The purpose of CASL is "to encourage . . . confidence and trust in the online marketplace" and to deter "damaging and deceptive . . . network threats."[221] Even here, there is a method to do both, and to that end, Canada should require CEM senders to enable mail authentication.[222] An "authentication associates a clear sender identity with a message and then enables a recipient to validate that the sender with that identity is in fact authorized to send the message."[223] In a nutshell, authentication acts like a peephole—enabling the ISPs to determine who is at the door, before allowing them in. Further, the popular ISPs generally contain filtering options for their users, which Canadian users, in turn, could utilize to block or redirect CEMs as an alternative to the unsubscribe

---

[218] This should include a rule preventing ISPs that provide email addresses to others from adding themselves to such a registry. Further, the registry must be limited to Canadian-owned domains.

[219] A simple illustration: A, an owner of the domain "abc.com" is a Canadian citizen and places this domain name in the Do-Not-Email Registry. B, a U.S. marketer wishes to send a CEM, and after a domain name match, determines that there are two email addresses on the file with this domain: def@abc.com and ghi@abc.com. This gives notice to B, that abc.com is a Canadian domain. B, in turn, determines that def@abc.com has purchased an item in the last year. Thus, B decides to send an email to def@abc.com and remove ghi@abc.com from the campaign. Alternatively, if B is not CASL compliant in terms of keeping to the consent requirements, or wishes to avoid Canada, B could drop both emails altogether. While this might prevent A, or A's email assignee from receiving some CEMs that A would desire; such is the consequence for placing a domain on the registry.

[220] *See* discussion *supra* Section III.B.

[221] Electronic Commerce Protection Regulations, SOR/2013-221, 147 C. Gaz. 2907, 2912 (Dec. 18, 2013).

[222] For a background on the three ways to authenticate: DMARC, SPF, and DKIM, see Lisa Weintraub Schifferle, *Want to Stop Phishers? Use Email Authentication*, FED. TRADE COMM'N (Mar. 3, 2017, 9:10 AM), https://www.ftc.gov/news-events/blogs/business-blog/2017/03/want-stop-phishers-use-email-authentication [https://perma.cc/QR77-CLBA].

[223] ELLEN SIEGEL, CONSTANT CONTACT, THE WHAT, WHY, AND HOW OF EMAIL AUTHENTICATION 1 (2008), https://www.constantcontact.com/aka/docs/pdf/whitepaper_authentication.pdf [https://perma.cc/BP7A-F7LA].

option.[224] Those users adamant about not receiving such mail altogether should switch to a ".ca" domain, as CASL never meant to apply to such a limiting degree to legitimate messages.

In summary: A foreign sender would satisfy CASL requirements if the sender (1) removes non-consenting recipients with a known Canadian physical address (if applicable); (2) removes all non-consenting ".ca" domain names; (3) accesses the Do-Not-Email Registry and removes all non-consenting email addresses matching the domain in the database; and (4) the sender adds authentication to the incoming messages, allowing the ISP to determine the sender's identity. Furthermore, the CRTC will need to work with the FTC to publicize CASL and the updated requirements in the United States. An educated user base will probably lead to faster adoption and serve as adequate notice to U.S. businesses because of the complex nature of CASL.

B. A Message to the FTC

It is evident that the FTC failed to perceive cross-border implications on U.S. businesses when it signed a Memorandum of Understanding with the CRTC, pledging compliance.[225] In June 2017, when the FTC announced a review of CAN-SPAM as part of their ten-year regulatory review schedule,[226] it requested written comments on thirty-eight pre-written questions, including subparts.[227] Question thirteen asked whether CAN-SPAM "overlap[s] or conflict[s] with other federal, state, or local laws or regulations? If so, how?"[228] This question should have been rewritten by including "foreign countries," because as this note conveyed, CASL should be viewed as the de facto anti-spam law in the United States.

Yet, an opportunity to cure this oversight is available. CASL's statutory overhaul will commence and changes are likely.[229] Once that occurs, the FTC should exercise the "Changes in Applicable Laws" provision,[230] which states that "in the event of significant modification to . . . [CASL, Canada and the U.S.]

---

[224] *See, e.g.*, *Create Rules to Filter Your Emails*, GOOGLE, https://support.google.com/mail/answer/6579?hl=en [https://perma.cc/PUT4-6X8W] (click on "Create a filter" hyperlink).

[225] *See generally Memorandum of Understanding*, *supra* note 146 ("RECOGNIZING the importance of developing a global and coordinated approach to address unlawful commercial email and telemarketing, and the threats that they pose to consumers and their confidence in these critical communication systems." Yet, CASL's application is beyond those that pose a threat to consumers.).

[226] Regulatory Review Schedule, 82 Fed. Reg. 29,259, 29, 259–60 (June 28, 2017).

[227] CAN-SPAM Rule, 82 Fed. Reg 29,254, 29, 254–55 (June 28, 2017).

[228] *Id.* at 29,255.

[229] *See* discussion *supra* Section I.D.

[230] *Memorandum of Understanding*, *supra* note 146.

intend to consult promptly, and, if possible, prior to the entry into force of such enactments, to determine whether to modify this Memorandum."[231] This timing provides for a perfect opportunity for dialogue regarding CASL between the two countries. In "[recognizing] the importance of developing a global and coordinated approach to address unlawful commercial email," Canada's partnership with the United States is needed to ensure compliance.[232] Surely, the FTC's expression of concern, and discussing the future of the Memorandum, would go a long way in influencing change to CASL's cross-border reach.

CONCLUSION

Canada is surely correct to call "[s]pam . . . a multifaceted, global problem."[233] But if spam is global, then so is any law in an attempt to regulate it. Canada's spam law in its current form impedes on legitimate business practices of the United States, who comply with the imperfect, yet ubiquitous CAN-SPAM. CAN-SPAM and CASL compliance are like night and day. Thus, unless Canada clarifies the foreign requirements for compliance or U.S. businesses adopt it as the de facto anti-spam law, U.S. interests will continue to be at risk.[234] Therefore, Canada should revisit CASL regulations from a foreign compliance lens. Moreover, CASL should be a cautionary tale, as a reminder to all countries to keep their international neighbors in mind when creating laws with extraterritorial reach. This is not the game of Risk.[235]

Arthur Shaykevich[†]

---

[231] *Id.*

[232] *Id.*

[233] INDUS. CAN. TASK FORCE ON SPAM, *supra* note 33, at 42.

[234] *See* discussion *supra* Section IV.A.

[235] Risk is a strategy board game of "global domination" by Hasbro. *See Risk Rules*, WIZARDS, http://media.wizards.com/2015/downloads/ah/Risk_rules.pdf [https://perma.cc/6EJV-Q7L5].

[†] J.D. Candidate, Brooklyn Law School, 2020; M.B.A. Yeshiva University, 2016; B.S. Binghamton University 2001. Thank you to Allison M. Cunneen, Alexander S. Mendelson, Chloe M. Gordils, and the entire *Brooklyn Law Review* staff for making this publication possible. Thank you to David A. Straite, Esq. for his valuable feedback during the selection process, and to Hon. Timothy S. Driscoll for teaching me the art of legal writing. My deepest gratitude to my partner, Michelle Shaykevich, for her companionship and for intellectually challenging me to be my very best. I additionally wish to thank my mother, Faina Shaykevich, for her unconditional love and endless encouragement, and Jeff and Alla Malamut for their care that made it all possible. With deep appreciation to Jonathan, Rosabella, Aaron, Boris, Helen, Esther, Michael, Dima, Adam, Hopas, Vita, Alex, and the rest of my family and friends for their understanding, or at the very least, tolerance. I am also grateful to Phuong, Adam, David, Leslie, and all of my Citi colleagues for their support. Finally, I wish to acknowledge the big man upstairs because I have been blessed with the opportunity to find my calling in life and to chase my dreams.