

CASL is Not CAN-SPAM

Learn the difference between the two and remove risk of non-compliance.

Canada's anti-spam legislation ([CASL](#)) has been in effect since July 1, 2014. Fines under CASL have been well publicized, and can reach as high as \$10 million for businesses and may be broadened to include the over-reaching personal vicarious liability of officers and directors. Many small to mid-size organizations, including media owners, find it challenging to adapt to CASL's overly prescriptive rules. In order to be compliant under CASL, media owners need to adopt new technologies and processes. [An overview of what media owners should be aware of can be found here.](#)

What are some differences between CASL and CAN-SPAM?

A distinguishing difference between [CAN-SPAM \(Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003\)](#) and CASL is the former is an opt-out model, while the latter is primarily an opt-in model. With an opt-out model, it is easier for media brand owners to imply consent for electronic messages until the recipient has opted-out. With an opt-in model, an individual actively communicates their consent, usually by clicking a subscription button or sending an email to authorize receipt of electronic messages.

Under CASL, a media brand or marketer from outside of Canada will not be compliant if a computer system located in Canada is used to either send or access the commercial electronic message (CASL Section 12 (1)). This means a U.S.-based organization sending an e-newsletter to a recipient in Canada requires consent. Compliance will likely not be an issue if this same Canadian recipient was traveling in the U.S. and the electronic message was not sent through a Canadian-based server; however, this is difficult for an organization to determine. Media owners should be cautious when recipients are expected to access electronic communication in Canada or elsewhere. Remember: The burden to prove CASL compliance is with the media owner (CASL section 13).

CASL rules mandate all electronic messaging contain an unsubscribe mechanism that must remain active for at least 60 days (CASL Section 11 (2)), and allow recipients to unsubscribe without difficulty and delay (Electronic Commerce Protection Regulations (CRTC) (SOR/2012-36, section 3)). While CAN-SPAM requires the unsubscribe mechanism to remain active for at least 30 days, both pieces of legislation require organizations to permanently remove recipients within 10 business days upon notification (CASL Section 11 (3)). Under CAN-SPAM and CASL, outbound communication requires media owners to state their company name and physical postal address; however, CASL also requires a contact name of sender, as well as a telephone number and email address or web address ([Electronic Commerce Protection Regulations \(CRTC\), SOR/2012-36, section 2 \(1\)](#)).

CASL includes vicarious liability provisions for which liability extends to an organization's executives if employees or agents acted within the scope of their employment. Liability also extends to officers and directors if they directed, authorized, assented to, acquiesced



in or participated in the offending conduct. CASL will also allow a person to take civil actions against a brand owner that is found in violation of CASL. Penalties for violating CASL are strict; the maximum penalty for a violation is \$1,000,000 for an individual, and \$10,000,000 in the case of any other individual (brand owner) (CASL section 20 (4)).

Media owners based in Canada or elsewhere must be extremely careful when sending electronic messages. A U.S.-based media owner who is CAN-SPAM compliant and certain all of their email communication will be accessed outside of Canada is likely to be CASL compliant; however, media owners should conduct a full assessment of their electronic communication practices to determine the scope of changes to be made with policies, procedures and technologies. Under CASL, violations go beyond email, and include SMS and instant messaging, social networking, applications and voice over internet protocol (VOIP).

Should a complaint be pursued under CASL by CRTC, it is the responsibility of the media owner to prove compliance. Media owners are at risk of not complying with CASL. A third-party evaluation of media owners' electronic messaging with customers, prospects and other constituents is one of the keys to limiting liability. [Independent organizations, including BPA, and its Canadian division CCAB, provide compliance checks to mitigate media owners' liability in the event of a CASL infraction](#) or investigation.

To learn more about CASL – Guard, BPA/CCAB's service to assess and reduce risk under CASL, or BPA/CCAB's media audits, please contact [Tim Peel](#). The contents described above are intended to be used as an aide for compliancy under CASL, and should not be construed as formal advice which should solely be relied on.

###

About BPA Worldwide/CCAB. BPA Worldwide, and CCAB, its Canadian division, is in the business of providing assurance. For 80+ years as a not-for-profit assurance service provider, BPA was originally created by advertisers, advertising agencies and the media industry to audit audience claims used in the buying and selling of advertising. Today, in addition to auditing audience claims, through its iCompli service, BPA verifies compliance to defined government, industry, and organizational standards as well as adherence to privacy, data protection and sustainability guidelines and best practices. Performing nearly 3,800 audits in over 20 countries, BPA is a trusted resource for compliance and assurance services. Its latest offering, Ad iCompli, measures and scores online ad campaign performance for business and consumer marketers.

For more information on BPA and its services, please visit the [website](#).