Blaney McMurtry LLP

PUBLICATION

Canada's Anti-Spam Law and Social Media: Marketers Advised to Proceed with Caution

Date: June 03, 2014
Lawyers You Should Know: H. Todd Greenbloom

Original Newsletter(s) this article was published in: Blaneys on Business: June 2014

"In every life we have some trouble; when you worry, you make it double; Don't worry, be happy."[1]

Marketers using social media may be happy and not worried about Canada's Anti-Spam Legislation (CASL)[2] because they think it may not apply to them. But, they should be cautious. Although social media advertising has the possibility of being CASL- exempt, CASL compliance may be required for various steps along the way.

CASL, the majority of which comes into force July 1, prohibits the sending of commercial electronic messages (CEM) to an electronic address unless the message complies with CASL (e.g. identify the sender, obtain consent and provide an unsubscribe mechanism). Users of social media marketing may not worry and may be happy because they are not *sending* messages and because they are not sending anything to an email account, an instant messaging account, a telephone account or a similar account.

Although the message in the Bobby McFerrin song is to be happy and not worry, despite having some trouble, and even if he "might have to litigate", people using social media for commercial purposes may have some trouble with CASL. So, they should be aware of CASL and how it might apply to social media.

On the Government of Canada's website for CASL, the following observation was made (emphasis added):

"These violations can include spam, malware, spyware, address harvesting and false or misleading representations involving the use of any means of telecommunications, Short Message Services (SMS or text messaging), ***social networking***, websites, uniform resource locators (URL) and other locators, applications, blogs, and Voice over Internet Protocol (VoIP).

Canada's anti-spam law takes a technology-neutral approach, so that all forms of commercial electronic messages sent by any means of telecommunications are captured under the new law."

As a starting point, any marketing endeavour, even on social media, will be a CEM, given that it is a message that "encourage[s] participation in a commercial activity" and, in all likelihood, is offering a sale of a good or service or is advertising the sale of a good or service.

In a general situation, the next question is whether or not the CEM is sent to an electronic address. According to the frequently asked questions (FAQs) provided by the CRTC[3], a social network account may fall into the class category of an electronic address (i.e. a similar account to email accounts, phone accounts and instant messaging accounts). In particular the answer provided by CRTC is:

"For example, a typical advertisement placed on a website or blog post would not be captured. In addition, whether communication using social media fits the definition of "electronic address," must be determined on a case-by-case basis, depending upon, for example, how the specific social media platform in question functions and is used. For example, a Facebook wall post would not be captured. However, messages sent to other users using a social media messaging system (e.g., Facebook messaging and LinkedIn messaging), would qualify as sending messages to "electronic addresses." Websites, blogs and micro-blogging would typically not be considered to be electronic addresses."

Even if messaging services on a social media site are not used to broadcast messages and, instead, reliance is placed primarily on the audience seeking out the message so that the originator of the message is not *sending* a message, caution should be exercised to ensure that social media are not used to send a CEM or, if CEMs are sent through social media, that they are sent in compliance with CASL (i.e. identify the sender, obtain consent and provide an unsubscribe mechanism).

Anyone using social media should be aware of how the particular site functions and, especially, what features are being used. Any time that the audience is receiving content passively (i.e. it does not go to the place where the information is stored), the originator may be sending an electronic message, especially if that message encourages participation in a commercial activity. An example of a possible sending of a CEM can be seen in an investigation of Facebook by the Privacy Commissioner[4].

The complainant alleged that Facebook was using social plug-ins ("buttons and boxes designed to display certain Facebook functionality on third-party websites", for example the "Like" or "Recommend" icons) to share his personal information without his knowledge and consent. When a Facebook user accesses a social plug-in while logged onto Facebook, the user sees personalized content in the social plug-in that highlights any activity that his or her friends may have initiated on that site, such as recommending a news article on a news website. Facebook described the mechanism as follows:

- a social plug-in is contained within an “iframe” on websites that host the social plug-in, which causes the user’s web browser to retrieve the contents of the iframe directly from Facebook; the iframe is essentially the third party renting space on its site to Facebook;
- the social plug-in acts as a portal to Facebook for the user, but it does not provide the third party site hosting the plug-in with any access to Facebook user data;
- the respective web server will receive a request for a file and send the requested content back to the computer requesting the file; if a user is logged-in to Facebook when visiting the applicable website, Facebook’s iframe will load with personalized content gathered from the Facebook user’s profile. This information does not travel to the applicable website but rather directly from Facebook to the user.

In that particular investigation, Facebook was absolved of any wrong doing since Facebook did not share or sell the information collected by the company when a Facebook user visited a website with a social plug-in, and also since Facebook adequately disclosed the collection and use of plug-in.

That investigation predates CASL and CASL was not a consideration. The same facts under CASL, however, should have the same result. Some may try and argue that since a website’s content is being transmitted to a Facebook user (albeit directly from Facebook), the argument would be that information from a website promoting a commercial activity is being ***sent*** to a user indirectly through Facebook as an intermediary. In these circumstances the CEM may not be CASL-compliant since the opt-out mechanism (i.e. using the plug-in while not logged on to a Facebook account) may be akin to default consent, which is not sufficient, and prescribed information that identifies the person who sent the message (the social media site) and the person on whose behalf it is sent (the host website) might not be properly set out.

Persons using social media to market must be very careful about how they build their social media networks to ensure compliance with CASL. An electronic message, by definition, includes an electronic message that contains a request for consent to send a CEM. As a result, inviting someone to join your network electronically could be seen as the sending of an electronic message asking for consent, which is problematic.

One of the elements in guides to launching successful social media campaigns is the promotion of the campaign. The manner in which the campaign is promoted could be subject to CASL. Some promotional suggestions are CASL neutral (e.g. publicize in non electronic newsletters, conventional advertising, word of mouth) while others may require CASL compliance (e.g. email announcements).

“The general purpose of Canada's Anti-spam Legislation is to encourage the growth of electronic commerce by ensuring confidence and trust in the online marketplace. To do so, the Act prohibits damaging and deceptive spam, spyware, malicious code, botnets, and other related network threats.”[5] The European Network and Information Security Agency (EINSA) has published a number of studies that involve social networking services (SNSs) and has identified a number of potential risks that would be in line with the objectives of CASL, including the following:

“Threat SN.2 Secondary data collection: as well as data knowingly disclosed in a profile, SN members disclose personal information using the network itself: e.g. length of connections, other users’ profiles visited and messages sent. SNSs provide a central repository accessible to a single provider. The high value of SNSs suggests that such data is being used to considerable financial gain.

“Threat SN.7 SNS spam: unsolicited messages propagated using SNSs. This is a growing phenomenon with several SNS-specific features.[6]

and

“Another study shows that not only are these third parties increasing their tracking of users, but that they can now link these traces with identifiers and personal information via online social networks [Krish2009a].”[7]

In response to these problems the European Union proposed legislation that would require the “erasure of personal data relating to [a person] and the abstention from further dissemination of such data.”[8]

Although this legislation has not been passed, its principals are being adopted by at least one court[9]. The court balanced the individual’s rights to the protection of their data and to privacy against interests of the operator of the search engine and the general interest in freedom of information.[10] The European court chose privacy over freedom of information.

That same conclusion may not be reached in Canada. The Supreme Court of Canada recently determined that Alberta privacy legislation’s “broad limitations on freedom of expression are not demonstrably justified because its limitations on expression are disproportionate to the benefits the legislation seeks to promote.”[11] That being said, over time Canada might adopt the right to be forgotten.

In summary, as we indicated earlier, social media advertising has the possibility of being CASL-exempt. Caution should be exercised, however, as CASL compliance may be required for various steps along the way.

Also if reliance is being placed on social media marketing, the legal landscape should be monitored regularly so that that one is prepared for things like the European right to be forgotten.

---

[1] Chorus from Bobby McFerrin’s “Don’t worry, Be Happy.”
[2] 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).

[3] The CRTC (the Canadian Radio-television and Telecommunications Commission) is one of the government agencies supervising CASL.
[4] No evidence Facebook shares personal information with other sites via social plug-ins, investigation finds, 2011 CanLII 93087 (PCC).
[5] Regulatory Impact Analysis Statement, Industry Canada, Electronic Commerce Protection Regulations.
[6] ENISA Position Paper No.1 Security Issues and Recommendations for Online Social Networks, Giles Hogben, ENISA, October 2007.
[7] European Network and Information Security Agency, "Privacy considerations of online behavioural tracking" published on October 19, 2012.
[8] Section 17 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data *(General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD)*.
[9] Despite the opinion of Advocate General Kääskinen, delivered on 25 June 2013 (1) Case C 131/12, *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD)* Mario Costeja González to the contrary the Court (Grand Chamber) determined that data that is "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased' [para 94] and Google was required to "remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person" [ruling para 3]. In other words Google was required to erase the links to the data in question so that while the information itself was not erased the ability to access it was.
[10] *Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD)*, para 91.
[11] Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, 2013 SCC 62, [2013] 3 S.C.R. 733, para 18.