

CONTACT INFORMATION POSTED ON WEBSITES NOT NECESSARILY UP FOR GRABS

Posted on December 19, 2019

Categories: [Insights](#), [Publications](#)

Recently released investigation findings of the Office of the Privacy Commissioner of Canada (the “OPC”)^[1] highlight several issues surrounding the use of personal information posted on websites.

The Facts

Grey House Publishing Canada (“Grey House”) produces and sells access to annual print and electronic directories across a number of fields.

The complainant alleged that Grey House collected his contact information from the website of a local chapter of a Canadian non-profit education association (the “Association”). The website listed the complainant’s contact information and invited those with questions about the club to contact the complainant. The complainant was not an officer, director or employee of the Association at the time.

Grey House added the complainant’s contact information to an e-mail distribution list, which it sold to Economic and Social Development Canada (“ESDC”). ESDC then used the distribution list to send the complainant e-mails promoting nominations for a volunteer award.

The Complainant’s Position

The complainant took the position that Grey House’s actions violated the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”).^[2]

In particular, the complainant argued that he had not consented to the collection, use and disclosure of his personal information by third parties and that his personal information was not “publicly available” (as defined in PIPEDA) simply because it was posted on a website.

Grey House’s Position

Grey House admitted that it collected the contact information of senior directors of associations when compiling entries for its directories.

Grey House justified its actions on the basis that:

- The complainant's personal information was "business contact information", and that PIPEDA therefore did not apply;
- Grey House was not conducting a commercial activity (as defined in PIPEDA) because the complainant's information was ultimately used by ESDC for the non-commercial purpose of promoting nominations for volunteer awards; and
- There was implied consent to this collection, use and disclosure of personal information by virtue of the information being "publicly available" on a website with no statement limiting its use.

The OPC's Findings

(a) Business Contact Information

PIPEDA defines business contact information as any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession. It can include, for example, a person's name, title, work address, work telephone number, or work email address.

Part 1 of PIPEDA does not apply to the collection, use or disclosure of business contact information solely for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession.

The OPC found that the complainant's contact information was not business contact information in this case, as he was not a director of the Association at the time his information was given to ESDC. The complainant's personal information was only included on the local chapter webpage to respond to general inquiries from local members and the public who may be interested in the Association.

(b) Commercial Activity

PIPEDA defines commercial activity as being any transaction, act or conduct that is of a commercial character, including the selling of donor, membership or other fundraising lists.

The OPC swiftly rejected Grey House's argument that it was not conducting a commercial activity, as Grey House sold the e-mail distribution list to the ESDC for a fee. It was not the ultimate use of the information by the ESDC that mattered, rather the character of the activity undertaken by Grey House itself.

(c) Publicly Available Information

Finally, the OPC found that Grey House had not obtained consent from the complainant to collect, use or

disclose his personal information. In particular, the OPC rejected Grey House's argument that the complainant's express consent was not required by virtue of his email address being "publicly available".

Publicly available information is defined quite narrowly in the Regulations to PIPEDA^[3] as including specific information appearing in, for example, telephone directories, professional or business directories, magazines, books or newspapers.

The OPC found that the information posted on the local chapter website was not "publicly available" within the meaning of the Regulations, and therefore the complainant's consent (express or implied) was required for the collection, use and disclosure of his personal information for Grey House's purposes.

Though the information was of a less sensitive nature, and the complainant freely chose to release the information to the public on a website, the OPC noted that the complainant could not have expected a third party to collect his information, insert it into a national database and sell that information to the federal government. Accordingly, Grey House could not rely on this exception to PIPEDA's consent requirements.

Takeaways for Your Business

As tempting as it may be, organizations should be very cautious about collecting, using or disclosing personal information posted on websites. This is the case even when an organization manually sources personal information from websites and does not "scrape" such information in bulk by electronic means.

The definition of "publicly available information" is not as intuitive as one may think. A recent white paper regarding potential changes to PIPEDA has suggested that the definition of publicly available information in the Regulations would be "explored", citing criticism of the current Regulations as being outdated and in need of updating to reflect the current digital age.^[4] It therefore remains to be seen whether the scope of this exemption will be extended to include personal information posted on a wider variety of digital platforms.

In addition to privacy law concerns, organizations should also consider the implications of Canada's anti-spam legislation (commonly referred to as "CASL") which prohibits "address harvesting", or the collection of email addresses through the use of a computer program that scrapes websites and assembles lists of addresses to be used for marketing purposes.

by Kristen Pennington and Troy Hilson, Student-At-Law

[1] "Directory company lacked consent to publish complainant's personal information", [PIPEDA Case Summary #2019-006](#).^[ps2id id='1' target='']

[2] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.^[ps2id id='2' target='']

[3] *Regulations Specifying Publicly Available Information*, SOR/2001-7.^[ps2id id='3' target='']

[4] [Proposals to modernize the *Personal Information Protection and Electronic Documents Act*](#), Innovation, Science and Economic Development Canada.[ps2id id='4' target='']

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

© McMillan LLP 2019