RECENT PRIVACY CONCERNS CALL FOR INCREASED TRANSPARENCY AND CONTROL

Posted on April 26, 2018

Categories: Insights, Publications

In the midst of the Cambridge Analytica data scandal, businesses should consider whether their data handling practices are consistent with user expectations.

Facebook recently announced upcoming changes to its privacy policies to give its users more control over what information may be collected, used and shared with third parties.

The changes will first take effect in Europe in response to the EU's new General Data Protection Regulation. Eventually, all users, regardless of their location, will be asked to review and make choices regarding Facebook's use of their data.

Users will be asked to decide whether:

- to permit Facebook to use data from partners, such as websites and apps that collect information about what users like, to tailor advertisements;
- to continue to share political, religious, and relationship information, and whether to allow Facebook to use this information; and
- users in EU and Canada want to opt into Facebook's facial recognition technology.

Facebook's facial recognition technology detects untagged faces and prompts both the person posting an image and the users appearing in it to apply the relevant name tags. It also helps Facebook detect when a third party is using a stolen photo, and is used to make "new friends" suggestions to users. For now, users outside of the EU and Canada will continue to be subject to the use of facial recognition unless they opt out of the system.

These privacy changes are a part of Facebook's requirement to comply with the EU laws that require explicit permission from users, and the broader push to address concerns over Facebook's handling of user data. In 2012, Facebook had to withdraw the use of facial recognition technology in EU due to objections from data privacy groups. In Canada, facial technology will be offered for the first time since its launch in 2011.

Canadian privacy law also generally requires individuals to consent to the collection of their personal

information and for organizations to be transparent regarding their use and disclosure practices. Express consent is required to collect biometric information.[1]

The Cambridge Analytica data scandal highlights the necessity for organizations to be transparent about the type of personal information that they collect, the reasons for doing so and to whom such information may be shared. Facebook already faces a class action lawsuit in the U.S. for collecting or storing users' biometric information without prior notification and consent.

Businesses should continue to review and update their privacy policies and practices to ensure compliance with applicable privacy legislation and consistency with the reasonable expectations of their customers.

by Mitch Koczerginski and Guneev Bhinder, Student-at-Law

[1] The Office of the Privacy Commissioner of Canada, "Guidelines for Identification and Authentication" (2016).

A Cautionary Note