THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

In-House Counsel

Facebook data scandal raises stakes for PIPEDA overhaul

By **David Young**

David Young

(March 28, 2018, 8:32 AM EDT) -- On Feb. 28, the House of Commons Standing Committee on Access to Information, Privacy and Ethics published its report of the review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The committee's report focuses on responding to technological change. However, in light of the current Facebook data "scandal," the question is, can the law ever keep pace with technology?

The committee's review was informed firstly, by the dramatic changes in technology since 2000 — when it became law — and secondly, by the European Union's new *General Data Protection Directive* (GDPR), which becomes law this May.

The committee's recommendations import a major overhaul of PIPEDA. However, it is not clear what direction legislative amendment will take — will it be a wholesale rewrite, or just selective changes? How the government responds to the technology revolution and the trajectory for reform will be watched closely.

The report's two focuses — PIPEDA's *consent rule,* and online *reputation* — drill down to a critical examination of how protective a privacy law can, or should, be. The recent exposé of the "breach" of Facebook users' data is instructive by the light it is shining on data collection practices and permissions generally. However, a more basic issue is whether privacy laws can ever be expected to adequately address such practices, or is there place now for another level of regulation?

It is helpful to recall that PIPEDA's origins were very much aligned with responding to the challenges of technology when, 20 years ago, the need to facilitate the "information highway" was a critical goal of government policy. PIPEDA's genealogy can be traced back to the OECD's 1980 *Privacy Principles* — developed specifically to respond to the new challenges of computers and information technology. PIPEDA is based on a voluntary code, and sought to respond to these challenges by adopting what continues to be a very flexible document. However, is it flexible enough to respond to the increasingly rapid pace of technological change?

The consent rule is the focus of widely diverging policy responses to technology, reflected in the testimony of witnesses before the committee, and in its recommendations. In large measure, consent may be shown to be at the heart of the Facebook data scandal. We don't know all the facts yet but initial reports indicate that the FB terms and conditions — including privacy permissions — allowed app developers to collect not only the personal information of users but also of their friends. This example of a wide-ranging "consent" imbedded in an app's terms and conditions — likely never read — points up the risks of

enabling expansive and unexpected uses for data collected on social networks and other online media.

The committee's central recommendation is that consent remain the core element of the privacy regime, stating that, "respect for personal autonomy requires that individuals be free to decide for themselves what to do with their personal information." However, the committee acknowledged that real and explicit consent has become more difficult to obtain.

The committee also made specific recommendations which, when viewed together, appear to diverge in the level of the privacy protections that should exist. While on one hand it recommended that opt-in consent be implemented as a default for secondary uses — which could limit the scope for apps to use information for ancillary purposes, it also recommended expanding the scope for publicly available information to include that posted on public web sites — which could extend to postings with low privacy settings such as on Facebook and other social media.

Another recommendation is to consider eliminating the consent requirement for "legitimate business interests." Would "legitimate business interests" include any uses disclosed in an app's terms and conditions, for which no consent would be required?

A yet further recommendation addressed greater clarity in algorithmic applications — such as may have been used with the Facebook data in targeting voters and influencing elections. As can be seen from the committee's report, there are diverging views as to the direction that the privacy laws should take. These are policy decisions that must be addressed if there is any realistic expectation that privacy laws will be effective in providing adequate protections for users of the evolving technology idioms.

David Young is principal at David Young Law*, a privacy and regulatory counsel practice in Toronto.*

Photo credit / ValeryBrozhinsky ISTOCKPHOTO.COM
