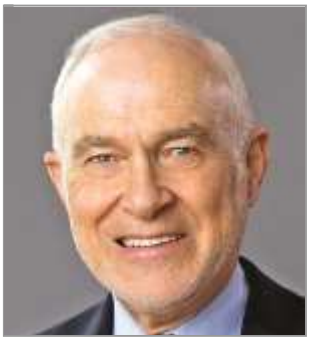
THE LAWYER'S DAILY

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

PIPEDA

Transfer for processing under PIPEDA a use, not a disclosure

By **David Young**



David Young

(July 31, 2019, 8:49 AM EDT) -- The key determination underlying the federal Office of the Privacy Commissioner's June re-launch of its Consultation on transfers for processing is whether a transfer to a data processor under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) is a use or a disclosure.

In its 2009 guidance document*, Guidelines for Processing Personal Data across Borders,* the OPC correctly described a transfer to a processor, as referred to in PIPEDA's Accountability Principle, as a use by an organization, not to be confused with a disclosure. The OPC now suggests that its 2009 interpretation was incorrect and that a transfer is a disclosure. In the context of modern-day outsourcing and data processing relationships, the significance of the distinction is critical — a disclosure requires consent by data subjects whereas a transfer does not.

The OPC's proposed new interpretation is not supported by principles of statutory interpretation — specifically consideration of the context in which the relevant terms are used and the intention of the relevant statutory provisions. Furthermore, it is not consistent with the accepted scheme of privacy protection reflected in PIPEDA and other Canadian private sector privacy laws, such as Alberta's *Personal Information Protection Act,* or the rules laid down in the EU's 1995 *Data Protection Directive* as carried forward into its successor, the *General Data Protection Regulation* (GDPR).

The plain wording of PIPEDA distinguishes between transfers and disclosures. The two terms are used separately and distinctively, by intention. Understanding of the intended meaning of the term "transfer" is drawn from within the Accountability Principle. That principle makes clear that an organization is responsible for personal information under its control or possession, including information transferred to a third party for processing.

In other words, information transferred remains within the control and legal possession of the transferring organization and that organization is responsible for ensuring the third party's protection of the information while processing it. The term "disclosure" is absent from the provision. As indicated by the 2009 guidance document, such transfers are simply a "use," limited to the purposes for which the information was originally collected.

A *disclosure* of personal information under PIPEDA changes control and possession of information — from the organization originally holding it (the "controller" under the GDPR) to another organization which is considered then to have "collected" the information. The data subject's consent is required, both for the disclosure by the first organization and for the collection by the second organization.

The purpose of the consent requirement is to enable the data subject to determine whether they accept the change of control and possession to the receiving organization. Once disclosed in this manner, the receiving organization (the new "controller") becomes subject to all of the PIPEDA rules respecting use and disclosure of that information, including the accountability rule.

By contrast, a transfer of information for processing, by the plain meaning and interpretation of the Accountability Principle, does not change control or legal possession of the information.

As opposed to a disclosure, a *use* of information is an activity that remains entirely within the responsibility of the organization originally holding the information. The Accountability Principle makes clear that such responsibility includes ensuring adequate protection when the information is provided (i.e. transferred) to a third party for processing. The third party does not acquire any ownership or control, but simply is authorized to perform certain services on behalf of the organization. This relationship between the organization and its third-party processor is clear from the plain meaning of the Accountability Principle.

Characterization of the relationship between an organization and its contracted service providers in this manner is consistent with international laws such as the GDPR. That law stipulates that notice to individuals regarding the processing of their data must include information regarding the identity of the controller and the nature of the processing but does not extend to providing information regarding contracted processors or requiring consent for the transfer of information to such processors. In other words, the control and responsibility character of the information does not change — the contracted processor relationship is invisible to the data subject.

The OPC supports its argument to include a transfer as a disclosure by reference to dictionary definitions and to other privacy legislation. However, it is clear from the rules of statutory interpretation that the meaning of legislation must be derived from the context in which terms are used, not simply by dictionary definitions read in isolation from that context.

Furthermore, other privacy legislation does not provide any clear guidance to support a conclusion that a transfer is to be considered a disclosure. Instead, it is predominantly consistent with the understood application of the transfer for processing rule, as reflected in the OPC's 2009 guidance.

Responses to the OPC's new consultation are requested to be submitted by Aug. 6, 2019.

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

Photo credit / Mike_Kiev ISTOCKPHOTO.COM

Interested in writing for us? To learn more about how you can add your voice to The Lawyer's Daily*, contact Analysis Editor Richard Skinulis at* Richard.Skinulis@lexisnexis.ca *or call 437- 828-6772.*