Yukon Information and Privacy Commissioner

BACKGROUNDER

Bill No. 24, the *Access to Information and Protection of Privacy Act*, was tabled in the Yukon Legislative Assembly on October 3, 2018.

Positive changes

Although the draft ATIPP Act has many new features, the fundamental privacy and access to information rights afforded to citizens across Canada have been preserved. Public bodies would have expanded authority to collect, use and disclose personal information for an integrated service, data-linking, and the creation and maintenance of a personal identity service. In her 2015 ATIPP Act recommendations document, the IPC recognized the need to allow for innovation and recommended many of the changes now included in Bill 24. These modifications are necessary in the age of the digital information economy. There are benefits to citizens that come from using and sharing personal information for program and service delivery.

The IPC's recommendations document also stated that expanded authority to support innovation must be balanced with adequate controls, including effective oversight, to ensure the privacy rights of citizens. Bill 24 incorporates many of these controls. There is a reasonable amount of rigour built into the legislation to prevent an improper exercise of this authority and this will reduce privacy risks. The controls, which will contribute to achieving the recommended balance, include:

- Public bodies must have privacy management programs.
- Public bodies must submit privacy impact assessments (PIAs) to the Information and Privacy Commissioner (IPC) for integrated services, data-linking and when establishing an identity service.
- Public bodies must report breaches of privacy to affected individuals and to the IPC, when there is a risk of significant harm to those individuals.
- The IPC's powers would be expanded, giving the office the power to make "own motion" complaints (rather than waiting for a citizen to make a complaint) and to conduct privacy compliance audits.

In terms of access to information, Bill 24 facilitates more transparency by public bodies and mandates that certain records and information be made publicly accessible. This too is positive.

Improvements still needed

While there are many positive changes contained in Bill 24, the IPC has a number of concerns.

It is up to complainants to go to court if a public body rejects a recommendation made by the IPC.

Under the draft legislation, if the IPC makes a recommendation to a public body and the public body rejects it, it is up to the complainant to take the public body to court. This is unsatisfactory. Complainants should not have to foot the Bill to go to court and fight for their rights against a public body. The recommendation from the IPC was to establish an alternate level of adjudication with order-making power. The IPC could refer a matter to this adjudicator when recommendations are rejected. Alternatively, the IPC recommended that the Yukon look at adopting the solution used in Newfoundland and Labrador's ATIPP Act, which requires the public body to go to court to refuse a recommendation. Neither of these recommendations were accepted.

The information security obligations of public bodies are not contained within the legislation.

Ensuring adequate security for personal information is fundamental. Bill 24 does not specify the information security controls that a public body must have in place to adequately protect the personal information it holds. Instead, the government's plan is to set out these requirements in the regulations. However, regulations can be easily changed. Because adequate security is an essential element to privacy protection, these requirements should be embedded within the legislation, rather than in regulations.

The legislation introduces the use of protocols to exercise authority, placing too much power in one person's hands.

Under Bill 24, the Access and Privacy Officer (APO), an employee of the Yukon government, can issue and use protocols to define the "scope and description of a program or activity of a public body" and "determine when PIAs must be conducted," as well as other matters. The APO also has authority to decide whether to accept or reject an access request. This places a significant amount of power in the hands of a single government employee. The degree to which this power may negatively impact citizens' rights must be carefully considered.

The Bill's offence provisions may not be strong enough to encourage compliance.

The offence provisions in access and privacy legislation operate as a deterrent to non-compliance. In Bill 24, the threshold for an offence is lowered from "willful" to "knowing." This is positive. However, the fines for being found guilty of an offence are too low. In addition,

there is no offence for a public body's non-compliance. This could mean that the offences in Bill 24 may not serve the deterrence function. This may be balanced out, however, by the addition of a term of imprisonment for up to six months if a "person" is found guilty.

There is no offence for failure to notify affected individuals about a breach of privacy.

Bill 24 does not include an offence for failure to notify individuals about a breach of their personal information when there is a risk of significant harm to them as a result of the breach. Because of the pervasiveness of privacy breaches and the ease with which large amounts of personal information can be breached, most modern privacy laws include privacy breach notification provisions with failure to notify being an offence. (The Yukon's *Health Information Privacy and Management Act* is a good example of this.) Failure to notify individuals about a risk of significant harm can have significant consequences for them. However, under Bill 24, when a public body fails to meet this obligation, there are no consequences for the public body. To remedy this, Bill 24 should include an offence when required notification does not occur.

Public bodies have too much authority to collect, use and disclose information in the public domain.

The ability of public bodies to collect, use and disclose personal information that is publicly available, or contained within a reputable public source, raises concerns. The ubiquitous use of social media has led to a large amount of personal information that may be considered "publicly available" or contained within a "reputable public source." If there are fears that public bodies can collect this information, use it for their own purposes, and disclose it, this may have a chilling effect on citizens and negatively impact their right to participate in social media and other public activity. The ability of public bodies to collect personal information from a public source, then use it and disclose it should be reconsidered for these reasons. If this ability remains, it will require careful monitoring, in order to safeguard the privacy rights of citizens.

Bill 24 does not apply to municipalities.

The draft legislation provides the option to include Yukon municipalities, after it is proclaimed and in force. In the view of the IPC, municipalities should be subject to this legislation as soon as it goes into effect, given that they are, in essence, public bodies. Citizens should have the same ability to access information held by municipalities as they do with other public bodies. In addition, municipalities hold a significant amount of personal information that should be subject to the same level of protection as other public bodies. Citizens should be able to exercise their privacy rights in respect of the personal information collected, used and disclosed by municipalities. Not having municipalities subject to the legislation is a gap that significantly affects the access and privacy rights of Yukoners and others.