

# Employee Data and Consent

**The federal government has proposed amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA). This article focuses on one of the significant changes: the elimination of the consent requirement for employee data. Readers who have built privacy protections based on the 10 privacy principles should not face extraordinary challenges in adjusting their programs to prepare for these legislative changes.**

As this is my first column, I would like to begin by discussing the way that I approach the practice of privacy as a former operations manager and business process improvement project manager. It can be characterized by a couple well-known sayings:

■ **The perfect is the enemy of the good.<sup>1</sup>**

This might seem counter-intuitive to a payroll person, as your role is to ensure every pay statement is accurate. However, privacy rules can apply differently to each situation, so trying to create a privacy program that will be right for all people in all circumstances is a recipe for failure. Your goal is to implement privacy protections that most people most of the time will accept as reasonable.

■ **You can't manage what you can't measure.** The privacy protections are

reflected in the activities done, or not done, by an organization. The outcomes of these activities can provide feedback on the effectiveness of the program.<sup>2</sup>

How do you, as a payroll professional, translate this into guidance about the way that you do your job on a day-to-day basis? As it happens, the federal government recently introduced Bill C-29, An Act to amend the *Personal Information Protection and Electronic Documents Act*, which includes a number of provisions that are directly impact payroll privacy. The rest of the column will look at one of the proposed changes—consent—and its operational consequences for payroll professionals.

First, if and when the new amendments to PIPEDA take effect, they directly affect you only if you are a federal work, undertaking or business (FWUB). (A quick rule of thumb is that if you are covered by the *Canada Labour Code*, instead of provincial standards, you are probably a FWUB.)

That being said, PIPEDA is often used by privacy professionals as a guideline for best practices where no specific provincial regulation or collective agreement exists. So even if you are not federally regulated, PIPEDA changes affecting payroll may still change your department's goals or deliverables.

**What's changed:** The definition of consent and the necessity for consent in the employment context.

The new legislation states that, "... the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting." This, I believe, significantly reduces the circumstances

1 From Voltaire's *Dictionnaire philosophique* (1764).

2 A useful blog, "10 Things to Know about Privacy Metrics," can be found at <http://michaelpower.ca/2010/03/10-things-to-know-about-privacy-metrics>.

in which “opt-out” or “assumed” consent could be regarded as valid.

For payroll practitioners, the impact on this may be somewhat mitigated by another change. If the bill passes as it reads now, employee consent will not be required to collect, use or disclose their personal information if that collection use or disclosure is necessary to establish, manage or terminate the employment relationship. However, the employer must notify employees so they are aware that data is being used for these purposes. You should also note that the amendments propose to expand the definition of employee personal information to include applicants for employment.

## Operational Impact

■ **Data:** If you have not already done so, you will need to do an inventory of the employee information you have and categorize how you use it as necessary for the employment relationship (for example, social insurance number used for statutory remittances) or not (for example, home contact information used for a social club).

■ **Policy and procedure:** You will need to schedule a review and update of your employee privacy policy and related procedures and forms. Where these policies and procedures impact other departments, you may need to initiate a new project or projects to deal with implementing the changes. At minimum, you will need to change the wording on most or all of the consent forms that you currently use from “signature of consent” to “signature acknowledging notification.”

■ **Communications:** You will need to prepare a communications plan. For senior management, you should prepare an estimate of the resources required to maintain compliance. This can be based on your initial assessment of data changes and policy changes above. For line managers, you will need

to prepare messaging and training on how to respond to employee concerns about “losing” consent. You may need to work with IT to update your information systems. You may also need to discuss with your payroll service or software vendor how they are planning to address the changes in PIPEDA.

Finally, and most importantly, you will need to prepare communications for all staff to make sure employees are notified in a timely manner about the changes that affect them. While you do not want to cause a panic, you should also ensure you are not minimizing legitimate concerns. The communication should preferably include a timeline and a FAQ document that applies to your particular employee population.

This change to consent is just one of a significant number of changes to PIPEDA.<sup>3</sup> An upcoming column will deal with another significant change: mandatory breach notification requirements.

At the end of the day, protecting employee privacy is one of the best ways that an employer can demonstrate respect for

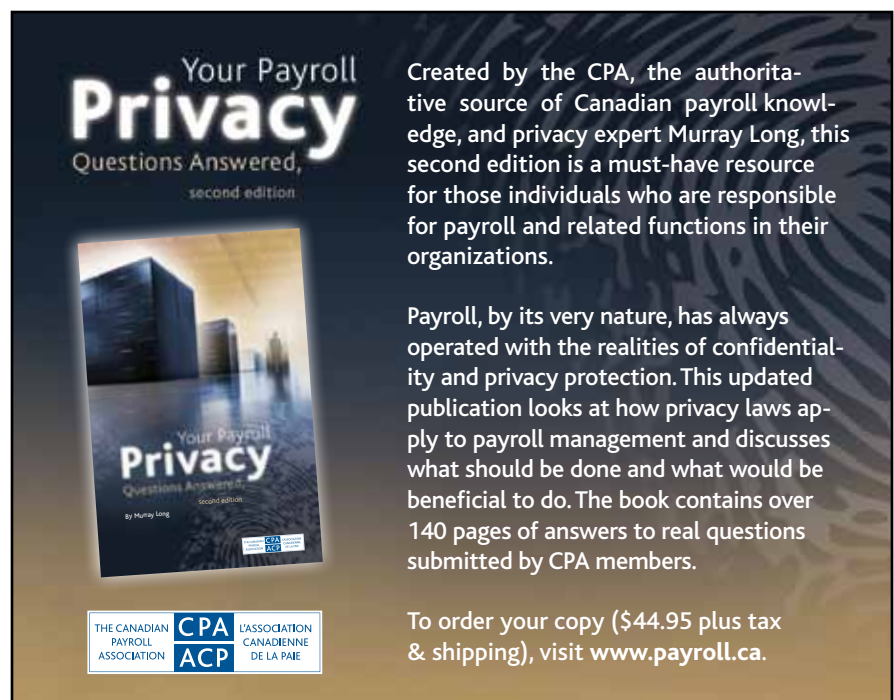
employees, which in turn will have positive impacts on employee engagement. Good privacy is good business. ■

---

<sup>3</sup> One of the best sources for information on the proposed PIPEDA changes is David Fraser, a Halifax lawyer, whose Canadian Privacy Law Blog is a must read for privacy professionals. He has posted a “red-line” version of the proposed changes on his blog at <http://blog.privacylawyer.ca/2010/05/markup-of-bill-c-28-and-bill-c-29.html>. For his overview of all the changes, visit <http://www.slaw.ca/2010/05/26/overview-of-proposed-pipeda-amendments/>. For the Industry Canada press release, visit <http://www.ic.gc.ca/eic/site/icc1.nsf/eng/05596.html>.

*John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at [www.wunderlich.ca](http://www.wunderlich.ca).*

**Notice:** This column reflects solely the opinions of the author. Individuals are encouraged to seek qualified legal advice on points of law or matters of interpretation.



Created by the CPA, the authoritative source of Canadian payroll knowledge, and privacy expert Murray Long, this second edition is a must-have resource for those individuals who are responsible for payroll and related functions in their organizations.

Payroll, by its very nature, has always operated with the realities of confidentiality and privacy protection. This updated publication looks at how privacy laws apply to payroll management and discusses what should be done and what would be beneficial to do. The book contains over 140 pages of answers to real questions submitted by CPA members.

To order your copy (\$44.95 plus tax & shipping), visit [www.payroll.ca](http://www.payroll.ca).