by John Wunderlich

What Did You Say You Were Doing with that Data?

Can you match use to purpose?

Trust is not built by what you say, but rather, by what you do. Much the same can be said about privacy. It's relatively easy to write a privacy policy; however, it's hard to execute a robust privacy program. The most important part of any privacy program is the answer to the question, "How do we use personally identifiable information?"

In the life cycle of employee personal information, an organization spends by far the most time on "use" and the corresponding efforts to implement security measures to protect privacy (see the column in the May/June issue). If you have taken due care to minimize the collection of personally identifiable information, you might feel you are in a pretty good position. However, have you also considered the disclosure of the information?

For our purposes, disclosure occurs when personally identifiable information under your custody and control moves out of your custody and control. This does not include the third party processing of your own data; the use of a payroll service bureau, for example, does not qualify as a disclosure. However, transferring information about employees to the Canada Revenue Agency does. The rule of thumb that I use to distinguish between "use" and "disclosure" is whether the third party is doing something that fulfills the purposes for which the organization collected the information.

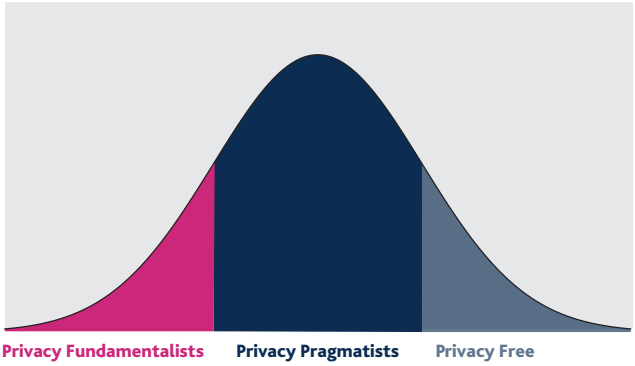
Inevitably, employee data must be disclosed, and disclosure increases your risk and must be properly managed. When you disclose information to a third party, there are a number of steps you can take to minimize the risk and ensure minimal impact on employee morale and organizational commitment should a breach occur.

Third parties collecting information are often dedicated purpose organizations, and one of the reasons organizations trust them is because they have dedicated information security and privacy teams. You minimize your risks of privacy breaches when you take advantage of another organization's strengths. However, it still important that you disclose the minimum amount of information you have to, and you have a clear contract or agreement specifying their privacy and security obligations.

Longtime readers and those well trained in privacy will remember

that one of the privacy principles is openness. To minimize the impact on employees, your organization should be open about disclosures. Employees should never be surprised to learn that their information is in the custody and control of another organization. People who are surprised to find out their information has been shared are much more likely to complain about the organization that shared it. So before you disclose their information, take reasonable steps to ensure employees are aware of what is being done with their information.

The chart below represents what research tells us about how people feel about their privacy.



The great majority of people are "privacy pragmatists"; they accept that privacy may be reduced in return for certain services and/or benefits, but they expect that organizations will exercise reasonable due diligence. Then there are people who are "privacy free." They are not sensitive about the privacy of their information. Finally, there are the "privacy fundamentalists"; they will not share their information unless required to do so, and they have very high expectations of what is required for exercise due diligence.

It is important to remember that these broad categories describe personality types. In other words, you cannot necessarily persuade people to change their views on what is and is not reasonable to share. This reinforces the need for openness in most circumstances, as it is much easier to deal with objections before the information is disclosed than afterwards.

With respect to disclosures to government bodies, you must ensure you exercise due diligence. When a representative from a government agency requests a disclosure of information, ask under what authority the request is being made if it is unclear. For example, if you receive a phone call asking for information about an employee, you may ask to receive the request in writing, with the specific authority making the request indicated.

It may be that the government agency has the authority to ask, but not require, a disclosure. When you are presented with a court order or a subpoena, you have no choice but to comply. However, other requests do not have the same force. In those cases, it is at the discretion of your organization. This is why privacy policies will often have the phrase, "unless authorized or required by law."

You must consider your commitment to employees and their privacy. Is the request a normal or routine one? Should it be normal or routine? And finally, if you accede to the request, will it lead to more requests? If your organization's privacy policy doesn't give you guidance on these issues, perhaps it's time to update your privacy policy.

We live in an information economy, and you will be disclosing personal information about employees. You can ensure you have done your privacy due diligence if you are able to identify every disclosure and how it conforms to the rules outlined in your organization's privacy policy.

That way, when a breach occurs (as you have to assume one will), no one will be surprised to find their information in the hands of a third party, and employees' trust in your respect for their privacy will be undiminished.

Send your questions and feedback to **john@wunderlich.ca**. Include **"CPA Life Cycle"** in the subject line.

John Wunderlich is an information privacy and security consultant, based in Toronto. For more information, check out his intermittently updated website at http://compliance.wunderlich.ca. ■