The Canadian privacy landscape *is* different!

While the world continues to shrink and organizations take advantage of the reduction and diminution of trade barriers, it's not surprising that we found ourselves more and more often dealing with the movement of people around the globe in order to get jobs done. Gone are the days where you limited your search for employment to within your geographic vicinity. Nowadays, more than ever, it's common for people to apply for and get jobs for organizations that are anywhere but in our backyard.

So, it's not surprising that those tasked with the job of screening potential candidates are asked to look into the background of people currently living outside of the United States or who have lived outside of the U.S. in the past. And, it's equally not surprising that a good number of candidates come from Canada.

However, while the trend is likely to continue, there are some important things to remember about the Canadian landscape when it comes to screening those Canucks.

One of the most significant considerations is the fact that Canadian privacy laws are markedly different than in the United States. The following is a simple primer to help get you thinking about what this landscape looks like.

Unlike the United States, Canada has comprehensive privacy laws that cover all aspects of personal information handling. While this is true of the public sector as well as the private sector, this paper will concentrate on identifying the private sector laws.

Nationally, Canadians avail themselves of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). This law governs the collection, use and disclosure of all personal information so long as the transaction is considered to be a commercial activity. To complicate matters, people in British Columbia, Alberta and Quebec have additional private sector laws that might supersede PIPEDA depending on the nature of the activity in question.

Regardless of which laws apply, it is often said that there are two overriding and general obligations:

1. that the collection, use and disclosure of personal information be considered appropriate by the reasonable person. This is often referred to as the "reasonableness" standard.
2. that, for the most part, the collection, use and disclosure of personal information only occur with the informed consent of the person to whom the information belongs.

It's important to keep in mind that *both* of these overriding obligations have to be met. You must be acting both reasonably *and* with consent. And, while it might often be the case where you can demonstrate that you were acting reasonably because you had consent, it's not necessarily the case.

While these two obligations may appear simple at first, there are a myriad of complicating factors one has to consider when dealing with a Canadian's privacy rights.

For example, when determining if the collection of personal information meets the reasonableness standard, Canadian laws emphasize the principle of minimum data collection. And, to be clear, Canadian regulators strictly enforce this notion. In most instances, you will only meet the test for this principle if:

1. the collection of information is necessary to meet a specific need
2. the collection of information is going to be effective in meeting that need
3. you can demonstrate that the loss of privacy is proportionate to the benefit gained through the collection of the information
4. you have exhausted any other means of achieving your goal without the information

Another important point worth mentioning in this brief article is that Canadian laws are based on 10 privacy principles (the minimal collection one mentioned above being one of them). These include: being accountable, identifying the purpose for the collection, collecting only that which is necessary, obtaining consent, limiting use and disclosure, safeguarding the information, keeping the information only for as long as necessary, begin open and transparent about what you do with the information, and providing a mechanism for people to challenge your information handling practices.

Lastly, Canadian laws are enforced by Privacy Commissioners who have powerful rights of investigation. Some argue that their enforcement sanctions are not as severe as in some European countries, but there is a movement afoot in Canada to add monetary fines for non-compliance. And, just because an organization may be located outside of Canada does not mean that they don't have to comply. The Federal Court of Canada has already ruled that Canadian privacy laws extend beyond the borders and must be followed by any organization dealing with the personal information of Canadians.

Kris Klein is a partner in the boutique firm, nNovation LLP (www.nnovation.com). He is one of Canada's most known and respected experts in privacy law. He teaches the privacy law course at Ottawa University' Law School and is a member of the IAPP's faculty that provides privacy training to organizations around the world. He is widely published and also produces the invaluable resource Privacy Scan (www.privacyscan.ca).

Kris will be speaking about Canadian privacy issues at the upcoming NAPBS conference in Nashville. His talk will cover some of the more unexpected issues that arise when screening Canadians such as the restrictions on collection publicly available data, when and why the Social Insurance Number can be collected and what the rules are with respect to the transborder movement of personal information.