“Innovation” is the rallying cry of our time. It’s more than a buzzword. It’s a strategy. It’s a ground up movement with few rules. Consumers, corporations and public sector organizations are racing to tap into the gold rush of technological innovation.

While innovation happens in organizations of all sizes, the energy we are feeling in the marketplace is coming from start-up companies. Companies that are populated by Millennials who are coming of age and starting to make their mark on the world. These engines of innovation are found in the incubators and accelerators that are attached to educational institutions in every major city in Canada and the United States.

Much of the innovation is at the front end of technology where there is a seismic shift in the human/machine interface. This includes mobile, social media, the Internet of Things, wearables and medical devices. These apps and devices are poised to become the gateways into our health information infrastructures.

On the back end, small start-up companies are starting to accumulate mountains of personal information in their cloud-based systems. This information has value. There is a tremendous impetus to “monetize” this data as part of the start-up business model.

As is common in technology, the pace of change is moving faster that society’s ability to address the social impacts of technological developments. This is true of privacy. Like it or not, technological innovation raises serious questions about privacy. Privacy breaches can hurt people. Virtual muggings in the forms of identity theft, cyberbullying and other forms of cybercrime are on the dark side of this virtual landscape.

But there’s good news. Privacy doesn’t have to be a boat-anchor. Privacy is about common sense. Privacy is nothing more than good information management and good customer service. As Dr. Ann Cavoukian points out in her Privacy by Design principles, privacy isn’t a zero-sum game. You don’t have to trade privacy for technological innovation. You can have both.

So what what advice can we give to start-ups to help them build and operate privacy-friendly solutions?

1. Know what privacy laws apply to you and your customers.

Start-ups face a bewildering array of privacy legislation, especially those who are selling their products and services across the country or into the United States. In Canada alone there are more than 30 separate federal, provincial and territorial privacy laws in effect. What laws apply to you depends on where you are and who you’re selling to.

Are you selling direct to consumers or private businesses? Then the federal Personal Information Protection and Electronic Documents Act (PIPEDA) may apply to you. Are you selling to healthcare providers in Canada? Then as many as 12 provincial and territorial privacy laws may apply to you and your customers. Are you selling to healthcare organizations in Texas? You’ll be caught by the US federal Health Insurance Portability and Accountability Act (HIPAA) AND the Texas Medical Records Privacy Act.

Privacy laws set the ground rules for information management. At 50,000 feet they all look the same. But on the ground where you are writing code, they can be quite different.

2. Conduct a privacy impact assessment

You need to understand the privacy risks associated with your products and services. The privacy impact assessment (PIA) is a structured risk management methodology that looks at the environment in which your app or device will operate, how it is used, and how data flows through the technical and business processes. You don’t want to over-engineer your app or device. The PIA will help identify real hotspots where privacy and security countermeasures may be needed. For a deeper dive into security issues, a threat and risk assessment (TRA) may be needed.

The PIA is also an important marketing tool. You can use it to demonstrate to your customers that you take privacy seriously.

3. Build privacy and security protective features into your products and services.

Based on your PIA and TRA risk assessments, you need to build in safeguards and countermeasures to ensure the protection of personal information from real identified risks. These measures could include encryption, access control, strong authentication, consent management and virus protection. Processes to detect vulnerabilities and implement bug fixes and patches are also needed.

4. Implement a privacy management program.

If you collect, store or manage personal information as part of your service you need a privacy management program. Begin by appointing a privacy officer... a real human being who is responsible for implementing the privacy program. For a start-up this won’t be a full time position. The person needs to have the authority and personality to make privacy happen in your company.

Create a privacy policy. In fact, create two. One to be posted on your website advising your customers of their privacy rights, and a second operational privacy policy that sets the ground rules for your staff.

Make everyone who handles personal information sign a confidentiality agreement. Ensure that they understand
their obligation to keep personal information confidential and the consequences of breaching customer privacy.

Provide privacy and security awareness training for everyone. Anyone can leave a door or a workstation open. Make sure that everyone is aware of privacy and security enhancing behaviours and what to do if they witness or suspect a privacy breach.

Most important, create a culture of privacy. Make privacy a core value of your company. Make sure that everyone knows that privacy is good for business.

5. Be ready for a privacy breach.

Despite your best efforts, your company may be the victim of a privacy breach. There are lots of bad guys out there… hackers, hacktivists, identity thieves and disgruntled or opportunistic employees. How well or how poorly you handle a breach could mean the difference between survival or failure for your start-up company.

Establish a breach management protocol… step by step procedures and responsibilities for those tasked with managing the breach. Train responsible staff on breach procedures. Test the protocol regularly using desktop exercises. Most jurisdictions in Canada and the United States require that you notify affected customers and, in some cases, regulatory authorities. Think about how you’re going to tell your customers that they are victims of a breach.

Who cares about privacy?

Privacy is one of those subjects that nobody thinks about until something goes very wrong. The whole point of understanding the law, assessing your risk, implementing privacy and security features in your products and services and implementing a privacy management program is to avoid privacy breaches and violations of customer privacy rights. Trust me. If something goes wrong, lots of people including your customers, your regulators, your investors and your board of directors will care.

Turning it around: the privacy advantage.

But let’s not dwell on the negative. Privacy is an area where start-up companies can differentiate themselves. It’s a feature to be promoted. This is especially true in healthcare where the customers will include healthcare providers who have very specific legislative mandates to protect privacy.

Where to go from here?

To help start-up companies to get out the gate, I have created a privacy library in the form of a wiki with links to privacy legislation in Canada and other countries, and best practice guidelines from around the world. The URL for the wiki is www.privacyhorizon.wikispaces.com.

And remember the bottom line… Privacy is good for business!