THE COMMON LAWYER

Why "Privacy" Should (Also) Be On Your Mind

By Justin M. Jakubiak and Sean Nouch

THERE IS LIKELY still one thing on everybody's mind right now; but do not worry, we are not going to talk about that (for today at least). With that said, we hope you continue to stay safe and resilient in the face of these strange times.

With new federal privacy legislation moving through the pipeline, and the increase in online sales (car sales especially), dealers and businesses alike should put their mind to whether they have adequate privacy policies in place to comply with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

PIPEDA applies to private-sector organizations across Canada (including provincially regulated businesses in Ontario) that collect, use or disclose personal information in the course of commercial activity. This means that PIPEDA applies to the handling of your customers' personal information - notably, it does not apply to your employees' personal information, unless you are a federally regulated organization.

Businesses, and auto dealers specifically, deal with all kinds of personal information on a regular basis that would be subject to PIPEDA, including: addresses, driver's licenses, SINs, insurance, banking and credit card information. With a move to online sales, and with many employees working from home, this personal information is now being held by businesses and their employees in more places than just the office or on an internal server. Even if your business already has privacy policies in place, you should reassess whether those policies are still adequate given the changing operational landscape we find ourselves in, and whether your staff require some fresh training and reminders regarding their responsibilities.

PIPEDA Principles

Businesses must follow these 10 fair information principles that form the ground rules for the collection, use and disclosure of personal information:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

Accountability – Privacy Officials

Businesses are responsible for the personal information they collect, and they should designate a "privacy official" to spearhead compliance efforts. The privacy official should be mainly responsible for ensuring that their business complies with PIPEDA, and would develop the business' privacy policies and best practices to protect personal information that the business controls. The privacy official's name should be displayed internally, as well as externally to the public, such as on the company's website, so that all employees and customers know who they may go to for issues concerning personal information accuracy, individual access to personal information and compliance challenges.

A good place to start for privacy officials would be to conduct a privacy impact assessment and threat analysis to assess your business's personal information handling practices, including current or new initiatives, such as online sales or WFH policies. Privacy officials should ask the "5 Ws" about how the business handles collection, use, disclosure, access, security and disposal of their customers' personal information to help develop policies and procedures.

The privacy official should ensure that all staff are trained to understand their organization's privacy policies, what valid and meaningful consent is, and how to deal with privacy complaints/inquiries from customers. Even if employees have been trained, refreshers are a great tool to assist employees and to explain how the policies may apply to employees working from home. Additionally, the privacy official should ensure through contractual measures that third parties (like service providers in another jurisdiction) who have access to the personal information a business collects use similar PIPEDA-compliant privacy measures.

Identifying Purposes and Consent

A key element of the PIPEDA principles is that you must obtain valid, informed, implied or express (express is preferred), consent before collecting, using or disclosing customers' personal information. Personal information should only be collected, used or disclosed for the reasonable purposes that were identified when obtaining consent and generally should be limited to what is necessary to complete the transaction in question, like obtaining personal financial information when financing a vehicle or adding a third-party warranty.

A great place to obtain explicit consent would be on the contracts your customers sign, like a bill of sale, a lease agreement, or a service/repair work order. This clause should inform the customer about what information is being collected, the purposes for the collection, use and disclosure of the personal information, and if any personal information will be shared with third parties and for what purpose (if the information is shared for purposes other than those necessary to complete the transaction). All privacy policies should be made public and easily accessible so customers understand what they are consenting to.

Data Breaches

Big and small businesses have a duty to keep a record of, and in some cases, report breaches of security involving personal information they control (including information disclosed to a third-party who suffered the breach), if it is reasonable to believe that the breach poses a real risk of "significant harm" to an individual. To identify what is considered significant harm, businesses should consider the sensitivity of the breached information and the probability that the information has been or will be misused. For example, if financial information was breached that could affect someone's credit score, this would constitute significant harm.

A business that has suffered a breach that meets the significant harm standard must, as soon as feasible, report the breach to the Office of the

Privacy Commissioner of Canada, the affected individuals, and to any other organization/government institution that may be able to reduce/mitigate the harm. Even if the breach does not reach the level of significant harm, the business must keep a record of the breach, including: the date, general description of the breach, type of information breached, and whether or not the breach was reported.

Liability for Privacy Violations

Aside from the reputational risk and trust concerns which could plague businesses who mishandle their customers' personal information, there can be serious legal and financial consequences as well.

While PIPEDA has been criticized for lacking adequate enforcement teeth, businesses may also be held liable for privacy violations civilly, through the tort of "intrusion upon seclusion", as recognized in the case of *Jones v. Tsige*. The elements of this tort are: (1) the individual's conduct must be intentional (includes recklessness); (2) the individual must have invaded one's private affairs, without lawful justification; and (3) a reasonable person would regard this invasion as highly offensive causing distress, humiliation, or anguish. It is important to note that a litigant need not prove actual harm to make out the tort, and may be awarded up to $20,000 for "moral damages", which may be compounded if the tort is brought in a class action lawsuit.

In the business context, this tort has been raised in actions where rogue employees misuse personal information collected by the business (see *Evans v. The Bank of Nova Scotia*), or where the business was subject to a data breach by a third-party hacker (see *Agnew-Americano v. Equifax Canada Co.*). The courts have considered that businesses can, in principle, be held vicariously liable for the actions of their employees or even the actions of third-party hackers, if they do not implement proper safeguards limiting/monitoring access to personal information or by recklessly enabling a hacker attack on a company database.

Generally, the more sensitive the information (e.g. financial information), the more safeguards should be in place, as there is a greater risk of harm to the individual. Examples of proper safeguards to avoid breaches and liability for such breaches include:

- implementing a security policy
- using physical measures (e.g. locking filing cabinets/offices)
- updated technological tools (e.g. new passwords, encryptions, firewalls)
- organizational controls (e.g. security clearances, limiting/monitoring who can access personal information, staff training)

New Legislation – Bigger Fines and a Private Right of Action

The Federal Government introduced Bill C-11, the *Digital Charter Implementation Act, 2020* in November, 2020 which, if passed, will essentially overhaul and replace most of PIPEDA with the new *Consumer Privacy Protection Act* ("CPPA"). The CPPA will mirror the principles from PIPEDA, but also introduce stiffer penalties of up to $10,000,000 or $25,000,000 for breaches or offences, and give a private right of action to individuals to sue businesses in respect of violations of the CPPA.

While this new legislation will not be enacted for some time, businesses should make sure adequate privacy policies are in place in anticipation of this legislative change and the greater potential for regulatory and civil liability.

Conclusion

Now more than ever, sensitive personal information is being held in a variety of places: in the office, at employee home offices, or on internal or sometimes external employee devices and servers (e.g. personal employee phones). The risks of misuse and data breaches of personal information are much greater, and businesses should reassess their privacy policies to ensure they are up-to-date within the new landscape that their business operates in.

Businesses will not only suffer potential legal liability in the future if they do not have adequate privacy policies, but may also risk reputational damages from customers and the public at large for potentially mishandling personal information. As attitudes shift towards a greater emphasis on privacy, businesses can also utilize their commitment to privacy as a competitive advantage over their competitors. ■