Top 10 Privacy Law Developments of 2017

December 19, 2017
David Elder, Michael Rosenstock

Playing catchup on 2017 developments in Canadian privacy law? Here's a list of our Top 10:

1. **Supreme Court deals blow to choice of forum provisions in consumer contracts**
   In *Douez v. Facebook*, a divided Supreme Court refused to enforce an otherwise valid forum selection clause in Facebook's terms of use agreement which would have required the plaintiff to sue Facebook for an alleged privacy breach in California rather than in British Columbia. The majority determined that unequal bargaining power between the parties and the quasi-constitutional nature of privacy rights provided "strong cause" not to enforce the clause. The decision casts into doubt a range of consumer contracts that purported to have consumers contract out of provincial jurisdiction.

2. **CASL: private right of action suspended, reform recommended**
   In June 2017, the government slammed the brakes on implementing ss. 47-51 of Canada's Anti-Spam Legislation (CASL), which would have allowed individuals to sue organizations for breaches of CASL and related sections of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and the *Competition Act*. With potential damage awards of up to $1 million per day, businesses and not-for-profits voiced concern that the private right of action could have serious unintended consequences. The government asked the Standing Committee on Industry, Science and Technology (INDU) to review the provision, as part of a more general statute-mandated review of CASL.

   In December, the Committee tabled its report following its review of CASL and the private right of action. INDU heard from 40 witnesses, many of whom were severely critical of the law. The Committee stopped short of making specific recommendations as to how CASL's provisions might be amended, but made 13 general recommendations for clarification, including with respect to key terms such as "commercial electronic message", the implied and express consent provisions, and how CASL applies to charities and non-profits. INDU also recommended that consideration of the coming into force of the private right of action should await an assessment of the impact of these recommended clarifications.

3. **Supreme Court confirms privacy of text messages**
   In *R. v. Marakah* and *R. v. Jones*, a pair of decisions issued in December, the Supreme Court addressed the circumstances in which the unreasonable search and seizure protections of the *Charter* apply to text messages held by third parties. In *Marakah*, the majority determined that the defendant had a reasonable expectation of privacy in the text messages found on the iPhone of his accomplice (recovered at the accomplice's home), excluded the evidence and acquitted the defendant. Similarly, in *Jones*, the court found that the defendant had a reasonable expectation of privacy in the text messages, sent to his co-accused, that were stored by the accused's mobile service provider. However, as the court found that the seizure

was made pursuant to a valid production order under the *Criminal Code*, the defendant's *Charter* rights were found not to have been breached.

4. **CASL survives first constitutional challenge**
In 2015, staff of the Canadian Radio-television and Telecommunications Commission (CRTC) fined CompuFinder $1.1 million for breaches of CASL. Exercising its right to make submissions to the appointed members of the CRTC, CompuFinder challenged CASL as an unconstitutional exercise of federal authority and an unjustifiable breach of *Charter* protections, including freedom of expression. The CRTC rejected these claims, finding that CASL was a valid exercise of Parliament's general trade and commerce powers, and that the limitations on freedom of expression were justified by the legislative goals of regulating spam and other electronic threats. It remains to be seen whether the case will be further appealed to the Federal Court of Appeal.

5. **An expanding tort of intrusion upon seclusion?**
In 2012, the Ontario Court of Appeal in *Jones v. Tsige* recognized the tort of intrusion upon seclusion, a privacy tort that allows recovery for the intentional and "highly offensive" invasion of privacy. In *Vanderveen v Waterbridge Media Inc.*, the Ontario small claims court found that a promotional video produced for the defendant real estate developer, which contained a two second clip of the plaintiff jogging on a public walking trail, was a "significant" privacy breach. The court awarded the plaintiff $4,000 for breach of privacy and $100 for appropriation of personality. Although it was a small claims decision, the judgement is noteworthy as previously, courts in the common law provinces have generally rejected "misappropriation of personality" common law tort claims by non-celebrities.

6. **Privacy and competition law meet in *TREB* case**
In *Toronto Real Estate Board v. Commissioner of Competition*, TREB argued that the allegedly anti-competitive policies that restricted the distribution of certain data to brokers arose from privacy obligations under *PIPEDA*. The Federal Court of Appeal disagreed, finding that the listing agreements between selling homeowners and brokers contained sufficient consents under *PIPEDA* to permit disclosure of the personal information in the data feed. Citing the Supreme Court's 2016 decision in *Royal Bank of Canada v. Trang*, which found a reduced expectation of privacy in mortgage statement information, the court also noted that the privacy interests involved in the *TREB* case were less sensitive because home selling prices were publicly available pursuant to land registry legislation.

7. **BC Privacy Commissioner rules against "Creep Catchers"**
Surrey Creep Catchers was a vigilante organization that impersonated minors online in order to lure potential child predators to a live meeting, at which the organization confronted the alleged predators, video-recording the confrontation and subsequently posting their interactions on social media. Two targets of the organization complained to the Office of the Information & Privacy Commissioner of British Columbia (BC OIPC). The BC OIPC determined that the organization collected, used and disclosed a range of personal information without consent, and ordered the organization to stop, rejecting the contention that the organization was conducting an "investigation" or carrying out a journalistic purpose.

8. **Eyes on Europe's GDPR**
Businesses around the world are readying themselves for Europe's *General Data Protection Regulation*, which goes into effect in May 2018. The regulations make significant changes to the previous 1995 directive, including higher penalties (up to 4% of global turnover), stricter consent provisions and a formalized "Right to be Forgotten". The law purports to have

extra-territorial effect on online businesses dealing with European residents, leaving many Canadian companies with websites, or who might otherwise do incidental business with European residents, to wonder how the law might apply to them. Moreover, while the European Commission has long considered Canada's privacy legislation to be "adequate" to allow personal data to flow between Canada and the EU without additional safeguards, it is not clear, in light of the pending GDPR, whether that status may change, or whether Canada will be required to makes changes to its own privacy laws in order to maintain its adequacy status.

9. ***PIPEDA Breach of Security Safeguards Regulations* tabled**
In 2015, the *Digital Privacy Act* amended *PIPEDA* to establish data breach reporting requirements, including notifying affected individuals of a "real risk of significant harm" and reporting the breach to the Privacy Commissioner of Canada (OPC). While those amendments are not yet in force, in September 2017 the government inched closer to implementation by unveiling proposed regulations that provide more specifics on the obligations. The draft regulations come amid a year of several highly publicized data breaches globally and in Canada, including Equifax, Uber, and the Canadian government.

10. **Company held responsible for privacy breaches of rogue sales representative**
A sales representative of Global RESP Corporation inappropriately obtained access to personal information of maternity patients of the Rouge River Hospital, which the representative used as leads to sell Registered Education Savings Plans to the parents of newborns. The representative, who had purchased the personal information from hospital employees, claimed to be acting alone.

    Following an investigation, the OPC concluded in a decision summary published in 2017 that the RESP company was nonetheless accountable under PIPEDA for the actions of its salesperson. The OPC also found that the company had breached its obligations under the law, as it had no reliable system to document how personal information was obtained and used by sales representatives, and no policies, procedures or training in place to ensure compliance with PIPEDA. The Commissioner made recommendations to the company about compliance, which the company accepted and implemented.

    In a widely reported decision, the Ontario Information and Privacy Commissioner had already found in 2014 that the hospital had failed to comply with its obligations under the *Personal Health Information Protection Act* to adequately protect personal health information. The hospital employee and the sales representative also pled guilty in 2016 to criminal charges stemming from the incident, and a class action against the hospital is still pending.