Canadian Privacy Law and Video Surveillance

David T.S. Fraser and David Graves

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the provincially regulated sector as of January 1, 2004. It is legislation which has as its stated goal the balancing of individual privacy rights with the needs of businesses to collect, use and disclose personal information. It was not written with the insurance industry in mind. The insurance industry is involved in the collection of information to assess claims. Often this is an adversarial process which includes gathering of information for presentation as evidence in Court, often by non-consensual means. Litigants are obliged to disclose personal information about themselves which they would not otherwise have to provide. Information which is relevant and not privileged must be disclosed. While this information is gathered under an implied undertaking of confidentiality, the protection of individual privacy rights is not at the heart of the civil litigation process.

A vexing question is the extent to which the rules set out in PIPEDA apply to the insurance industry and the routine practice of video surveillance.

An argument can be advance that PIPEDA does not apply to the handling of an insurance claim. The Act only applies if an organization collects, uses or discloses personal information "in the course of a commercial activity." The argument runs that

Video Surveillance – Is Consent Required?

Among the fundamental tenets of PIPEDA is consent to the gathering of personal information. Principle 3 of the CSA Model Code, which is Schedule I to PIPEDA, states:

> 4.3 Principle 3 – Consent
>
> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

PIPEDA defines personal information as all "information about an identifiable individual" excluding the name, title and business address or telephone number of an employee of an organization. The Privacy Commissioner has taken the position that video surveillance of an individual is a collection of "personal information." As such, this collection requires the consent of the individual unless one is able to come within one of the exceptions in the Act.

Video Surveillance With Express Consent

First-party insurers can seek consent to investigations when the policy is underwritten or when claims are made. Prudent insurers should consider language in their policies and claim forms that provides consent for the collection, use and disclosure of personal information that is reasonably necessary to investigate and verify all claims, including surveillance. Policy language and claim forms need to be very carefully drafted with assistance of legal counsel experienced with privacy issues in order to cover all anticipated circumstances.

Video Surveillance With Implied Consent

Consent under PIPEDA may take many forms. The commentary to the consent principle states that the form of the consent sought by the organization may vary, depending upon

- the circumstances,
- the type of and sensitivity of the information, and
- the reasonable expectations of the individual.

A position taken by some insurers is that when a claim is presented, the claimant impliedly consents to the investigation and confirmation of the claim, which would include video surveillance. The argument runs that "reasonable expectations" of the parties covers this. However, it remains to be seen whether this position will be accepted by the Privacy Commissioner or by the courts.

Video Surveillance Without Consent

Principle 3 does state that consent is required for the collection, use and disclosure of personal information "except where inappropriate". Unfortunately, the Act in Section 7 prescribes the only circumstances where consent is not required and, therefore, one will have to come within one of the exceptions in Section 7 if video surveillance is conducted without consent, express or implied.

Paragraph 7(1)(b) is seen as the most applicable, which requires all of the following to be present:

1. it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information;

2. the collection is reasonable; and

3. the collection is for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The first condition is easily satisfied. It is unclear what the "laws of Canada or a province" are in order to satisfy the third requirement that the surveillance relate to the investigation of a breach of "the laws of Canada or a province." Some commentators have taken the position that this reference is limited to statutes and regulations and does not extend to common law. Cases of suspected fraud have been considered by the Privacy Commissioner (and an Arbitrator in Ontario) to come within the laws of Canada or a province.

The third requirement to the exception to consent in Section 7(1)(b) is that the collection be reasonable.

A recent decision of an Arbitrator in Ontario, *Ross v. Rosedale Transport*, has applied the reasonableness principle to exclude video surveillance. In that case, the employee was fired from his employment for misrepresenting his injuries to his employer. The employee sustained a low-back injury when moving a pallet from a truck. He was off work and was then put on reduced duties to accommodate his back injury. After some months of reduced duties, the employee went on vacation. On the day before commencing his leave, the employee told his supervisor that he would be moving with his family. The employer hired an investigator who conducted video surveillance which showed the employee carried furniture in the course of moving. The employee was fired for fraud.

The arbitrator, surprisingly, found that the video evidence was not admissible because it was not reasonable for the employer to initiate video surveillance. It was open to the employer to ask for an independent medical examination but ordering video surveillance was not reasonable. While one may choose to disagree with the Arbitrator's definition of reasonableness, this decision demonstrates that if video surveillance is obtained without consent, one must ensure that there is a good reason for proceeding with surveillance in order to satisfy the requirement that the collection be reasonable. The basis for the decision to conduct surveillance should be well documented in the claims file to avoid court challenges to the introduction of surveillance evidence.

Conclusion

It is clear that the advent of PIPEDA will not end the relatively common practice of video surveillance. But PIPEDA does usher in a new era of sensitivity to individual privacy. Insurers can expect that video surveillance will be challenged, both in court and before the office of the Privacy Commissioner. Since the law came into force in the provincially regulated private sector, plaintiffs' counsel have relied on PIPEDA to impede investigation of claims. With respect to surveillance, steps should be taken to increase the likelihood that its use will survive court challenges. All claims staff must know the new rules and, when the rules are unclear, should seek specific advice from counsel who are well-versed in both insurance and privacy law.

The Authors

David T.S. Fraser, is chair of the privacy law practice group of McInnes Cooper, Atlantic Canada's largest single law partnership. He is regularly called upon to advise on matters related to Canadian privacy law and insurance. **David Graves** is a partner with McInnes Cooper practicing insurance litigation.

The McInnes Cooper PIPEDA Team

McInnes Cooper has established a fully-integrated privacy law practice group that draws upon the diverse strengths of the firm from across its many locations. The members of the McInnes Cooper Privacy Law Group regularly assist clients with all aspects of federal and provincial, public and private sector privacy law and freedom of information legislation. Our lawyers have experience providing strategic advice on privacy law compliance and implementing information protection measures for many of Atlantic Canada's largest businesses, institutions and international companies operating in Canada. If you have any questions, please contact any of the following:

David T.S. Fraser 902 424 1347 david.fraser@mcinnescooper.com	David Graves 902 424 1330 david.graves@mcinnescooper.com
Marc-Antoine Chiasson 506 861 1920 marc.chiasson@mcinnescooper.com	Jackie Penney 709 724 8239 jackie.penney@mcinnescooper.com