PALLETT VALO LLP
Lawyers & Trade-Mark Agents

Your Authority For:
Business Law • Commercial Litigation • Commercial Real Estate
Construction • Insolvency and Corporate Restructuring
Labour and Employment • Wills, Estates & Trusts

www.pallettvalo.com

# Privacy Law

February 2012

## Ontario's Top Court Recognizes the Tort of Invasion of Privacy

A person can now commence litigation seeking a monetary award for invasion of privacy. The Ontario Court of Appeal has adopted American jurisprudence in ruling that a person can sue for "intrusion upon their seclusion."

### *Jones v. Tsige* Breaks New Ground

In a recent decision, *Jones v. Tsige*, Sandra Jones discovered that Winnie Tsige, a fellow bank employee, had accessed Jones' bank records 174 times over a four-year period. Tsige claimed she was looking to see if Jones' ex-husband (who had since become Tsige's common-law partner) was paying Jones child support as he had claimed to Tsige.

Pointing to years of precedent that held that privacy trespass is only actionable by statute (such as the federal *Personal Information Protection and Electronic Documents Act*, also known as PIPEDA, for example). Tsige asked the court to dismiss Jones' action. The lower court did so, stating there is no tort of breach of privacy in Ontario. Jones appealed to the Court of Appeal.

The Court adopted a US description of the tort of intrusion upon seclusion as intentional intrusion, physically or otherwise (non-physical intrusion would include listening or looking), on the seclusion of another person or on his or her private affairs or concerns if the invasion would be highly offensive to a reasonable person. The Court made it clear that a person does not need to prove monetary loss to succeed. Where no monetary loss can be proven, a court may award "symbolic" or "moral" damages, which the Court capped at $20,000. Awards above that range may be available where the wrong-doer's conduct is especially egregious or where the victim can show actual financial loss.

Applying these elements to the case, the Court concluded that although the intrusion was deliberate and shocking, the plaintiff suffered no public embarrassment or physical or economic harm. An award of damages of $10,000 was found to be appropriate under these circumstances.

### What does it mean for business?

Where the victim can only show little or no financial losses as a result of the breach, the costs of litigation will likely cause most individual plaintiffs to hesitate before bringing a claim of intrusion upon seclusion to court. It may be, however, that the Court has opened the door to class action litigation of breaches of privacy. Organizations that collect personal information will now want to be extra careful in avoiding breaches of privacy – especially where the breach arises from the way personal information is collected and used consistently throughout the organization.

Following *Jones v. Tsige*, the best practice is to revisit your organization's privacy, data collection and computer use policies. As it is only unlawful invasion of privacy that can give rise to a lawsuit, try to build into your collection practices the consent of the persons whose information you are collecting. You will also want to ensure that your policies are adequate and enforced.

### What does it mean for employers?

Although the *Jones v. Tsige* decision involved a dispute between two employees in the workplace, the reasoning of the Court applies equally to the employer-employee relationship.

In an era driven by technology and productivity, companies now frequently provide their employees with company-paid laptops and handheld devices. Employees are regularly provided access to company servers and corporate email accounts, and are granted access to or possession of a great deal of their employer's confidential or proprietary information.

Employers have a genuine interest in protecting their property and reputation, as well as ensuring workplace productivity. They increasingly resort to monitoring the activities of their employees, using GPS technology or video-surveillance, auditing employees' computer or email usage, searching employee lockers, or retaining private investigators to investigate concerns, such as the abuse of sick leave, disability or WSIB benefits.

It is, however, becoming more common for employees to raise claims of breach of their individual privacy rights upon finding out their employer has secretly engaged in monitoring activity.

Employers who don't overtly communicate their privacy expectations to their employees run the risk that an employee will make allegations of invasion of privacy based on the new tort of intrusion upon seclusion. Management employees who misuse the personal information they discover in the course of monitoring activity, such as spreading gossip or publicly embarrassing other workers, potentially expose their employers to awards of damages at the highest end of the range.

We strongly recommend that employers implement (or re-examine existing) formal written policies to ensure they use the appropriate language in communicating privacy expectations in the workplace. In particular, employers should implement and enforce a computer use policy which warns employees that the employer always reserves the right to monitor computer or email usage at any time. The computer use policy should also set out all of the reasonable purposes for which the employer may collect, access and use information stored on its system, including preventing misconduct or illegal activity.

Prudent employers who properly inform their workers about the reasonable limits on privacy expectations in the workplace will greatly reduce the chance of a successful claim of invasion of privacy by their employees.

## Pallett Valo LLP Privacy Law Group

Pallett Valo LLP's Privacy Law Group advises and supports private sector organizations to comply with their obligations under the Personal Information Protection and Electronic Documents Act. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation. We are also experienced in advising clients regarding the Freedom of Information Act and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act.

Greg Azeff

**Greg Azeff** gazeff@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 264

Andy Balaura

**Andy Balaura** abalaura@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 225

Catherine Phillips

**Catherine Phillips** cphillips@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 203

This article provides information of a general nature only and should not be relied upon as professional advice in any particular context. For more information about Privacy Law, contact a member of our **Privacy Law Group** at **905.273.3300**.

If you would prefer to receive your bulletins by email, visit www.pallettvalo.com/signup or send an email to marketing@pallettvalo.com.