

## Ontario Court of Appeal Recognizes Tort of Invasion of Privacy

Jan 23, 2012

By [Jennifer Dolman](#), [Evan Thomas](#), [Lia Bruschetta](#)

On January 18, 2012, the Ontario Court of Appeal recognized a common law tort of “intrusion upon seclusion” in Ontario law in its decision in *Jones v. Tsige*<sup>1</sup>. This decision has potentially significant implications, not just for individuals who may have invaded another person’s private affairs, but for any organization that collects and/or uses personal health, financial and other information. In particular, the decision may increase the reputational and other risks of unauthorized use of personal information and the incidence and risk of privacy class actions.

While the full implications of *Jones v. Tsige* will only be known as the decision is applied in the lower courts, proactive organizations should consider reviewing their collection and/or use of personal information and ensuring the enforcement of privacy and data protection policies.

### ***1. Jones v. Tsige***

Both Jones and Tsige were employees at different branches of the Bank of Montreal. Neither woman knew each other personally, but Tsige had formed a common-law relationship with Jones’ ex-husband. In 2009, Jones discovered that Tsige had accessed Jones’ banking records at least 174 times over the course of four years. The information accessed included transaction details, as well as personal information such as Jones’ date of birth, marital status, and address.

Jones sued Tsige, claiming \$70,000 for invasion of privacy and breach of fiduciary duty. A motions judge dismissed Jones’ claims in March 2011 after concluding there was no cause of action for invasion of privacy in Ontario<sup>2</sup>. Jones appealed. The Court of Appeal unanimously concluded that Ontario common law did recognize a cause of action for “intrusion upon seclusion” and reversed the lower court’s decision. The Court placed the case at the mid-point of the range of damages it identified as appropriate for this cause of action and awarded Jones damages of \$10,000.

In reaching its decision, the Court stated that the tort was both a necessary and welcome “incremental step” consistent with developing the common law to the changing needs of society. The Court noted the importance of privacy interests in traditional causes of action, such as trespass, and under the *Charter of Rights and Freedoms*.

The Court of Appeal held that to succeed in a claim for intrusion upon seclusion, a plaintiff must prove the following elements, which the Court adopted from the U.S. *Restatement (Second) of Torts* (2010):

1. The defendant's conduct was intentional (which includes reckless conduct);
2. The defendant invaded, without lawful justification, the plaintiff's private affairs or concerns; and
3. A reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish.

The Court made it clear that proof of actual loss is *not* an element of the cause of action, and so a plaintiff does not have to show an actual economic loss to succeed.

However, the Court of Appeal placed clear limits on the new tort:

1. **Claims can arise only for *deliberate and significant* invasions of personal privacy.** As the intrusion must be "highly offensive" to a reasonable person, only intrusions into matters such as personal financial or health records, sexual practices and orientation, employment, diary or private correspondence will be actionable.
2. **The right of privacy is not absolute.** The Court expressly noted that, in the right circumstances, competing claims for freedom of expression and freedom of the press will need to be reconciled with the right to privacy. The Court did not provide any guidance on how these competing claims should be balanced.
3. **"Symbolic" or "moral" damages will rarely be more than \$20,000.** The Court found that damages for "inclusion upon seclusion" were properly considered "symbolic" or "moral" damages. The Court suggested that in all but exceptional circumstances these damages should be in a range up to \$20,000.

The Court neither excluded, nor encouraged, awards of aggravated or punitive damages.

## II. Risks and Mitigation

In light of the widespread availability, collection and use of personal financial, health and other information by businesses and other organizations, the recognition of a tort of intrusion upon seclusion may create new risks for these organizations:

1. **Class Actions** – Certain features of the new tort - including the objective standard for determining whether the conduct is "highly offensive", the fact that the requisite "intentional" element of the tort includes reckless behaviour (which could be very far-reaching), the absence of a requirement for actual economic loss, and the ability of a court to award "symbolic" or "moral" damages - may make it easier for Ontario courts to certify class actions against organizations that collect and/or use personal information in a manner that is alleged to be an invasion of privacy. If each individual affected by a data breach, for example, may be entitled to damages of up to \$20,000 for invasion of their privacy, an organization may be exposed to a very substantial lawsuit, depending on the number of customers or other persons affected.
2. **Other Business Impact of Privacy Litigation** - Although the primary remedy sought in the *Jones* case was damages, it is not inconceivable that a future plaintiff could seek an interlocutory injunction to restrain an organization's collection and/or use of personal information pending a trial. Such an injunction could have a significant business impact on the organization, even if the organization's collection and/or use was ultimately found to be lawful.
3. **Reputational Damage** – Although the monetary risk of individual litigation is low given that damages will usually be limited to "moral" damages, claims for intrusion upon seclusion based on an organization's collection and/or use of

financial, health or other personal information may have a serious impact on the organization's reputation and relationship with customers. Further, as the facts of the *Jones v. Tsige* case demonstrated, organizations face reputational risks from unauthorized misuse of personal information by "rogue" employees, even if the organization is not named as a party in litigation.

Proactive organizations that collect and/or use personal information in their activities and that wish to mitigate the potential risks in the wake of this decision should consider the following:

1. **Obtaining Consent** - As the new cause of action requires an *unlawful* invasion of private affairs, evidence that shows that a plaintiff claiming damages for invasion of privacy expressly consented to the collection and/or use of his or her personal information could provide a strong defence to the claim.
2. **Data Protection and Privacy Policies** – This case, and particularly the fact that the unauthorized misuse of information continued for four years, reinforces the need for organizations that collect, use and/or disclose personal information to not only enact sufficient privacy and data protection policies but to also ensure that these policies are adequately enforced.

1 2012 ONCA 32. The case may yet be appealed to the Supreme Court of Canada.

2 2011 ONSC 1475 (reasons delivered by Whitaker J.).