

FTR Now

How the New Privacy Tort Will Affect Employers

Date: January 23, 2012

On January 18th, 2012, the Court of Appeal for Ontario in [Jones v. Tsige](#) recognized a new “intrusion upon seclusion” civil cause of action. In this *FTR Now*, we describe the new cause of action (or “tort”) and identify its significance to employers.

THE INTRUSION UPON SECLUSION TORT

Under Ontario law it is now clear that individuals can sue for breach of privacy based on proof of:

If these elements are proven, harms that justify an award of moral damages will be presumed. Such damages will be awarded “to mark the wrong that has been done” in an amount that does not ordinarily exceed \$20,000, with an amount being set based on:

1. an intentional unauthorized intrusion;
2. which is an intrusion upon private affairs or concerns (i.e. that breaches a reasonable expectation of privacy); and
3. that is made in circumstances that are highly offensive to the reasonable person, causing distress, humiliation or anguish.

If these elements are proven, harms that justify an award of moral damages will be presumed. Such damages will be awarded “to mark the wrong that has been done” in an amount that does not ordinarily exceed \$20,000, with an amount being set based on:

1. the nature, incidence and occasion of the defendant’s wrongful act;
 2. the effect of the wrong on the plaintiff’s health, welfare, social, business or financial position;
 3. any relationship, whether domestic or otherwise, between the parties;
- any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and
 - the conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.

The Court stressed that valid claims for intrusion upon seclusion will only arise “for deliberate and significant invasions of privacy” and also said that the law will develop affirmative defences based

on countervailing claims for the protection of freedom of expression and freedom of the press.

Courts outside of Ontario are not bound by an Ontario judgment, but courts in provinces outside of Ontario have not disclaimed the intrusion upon seclusion tort and are likely to be influenced by the Court of Appeal for Ontario's pronouncement. Moreover, four provinces already have statutory privacy torts that could be revitalized based on the new attention bound to be given to privacy actions. This is therefore a development with significance to employers across Canada.

TWO OUT OF FOUR OF THE WARREN AND BRANDEIS TORTS AND COUNTING

The intrusion upon seclusion tort has a long history in American law, first proposed in 1890 by American lawyers Samuel Warren and Louis Brandeis. (Brandeis later became a renowned United States Supreme Court justice.) It was one of four privacy-protecting torts that they proposed – protecting against physical intrusion into private spaces and the *collection* of private information. Warren and Brandeis also proposed a tort to protect against the unauthorized exploitation of one's identity or personality that is also recognized in our law.

The Court of Appeal did not recognize the Warren and Brandeis tort that protects against the *disclosure* of embarrassing private facts nor did it recognize the Warren and Brandeis "false light" tort. There are greater policy questions raised by these two torts given they have the potential to upset the existing policy embedded in our defamation law. Notably, the four privacy torts created by statute in British Columbia, Saskatchewan, Manitoba and Newfoundland expressly contemplate claims for intrusions and claims for misappropriation of personality, but do not expressly contemplate disclosure-based claims. Plaintiff counsel may raise disclosure-based privacy claims now that the Court of Appeal for Ontario has expressed such openness to the Warren and Brandeis framework, but their recognition is not a forgone conclusion.

IMPACT ON EMPLOYERS

Privacy in the workplace

The new tort is not likely to create a significant barrier to managing employees, but employers should re-visit all work policies that authorize and govern the collection of employee personal information, especially their computer use policies.

The tort rests on an unauthorized "intrusion" that affects a "reasonable expectation of privacy" in a manner that is "highly offensive." These elements have proven to immunize American employers from a wide range of claims based on the collection of information inside the workplace. Notable exceptions include cases in which employers were found liable for conducting video surveillance inside of bathrooms and locker rooms.

Regardless of the latitude that is likely to be shown to employers by Canadian courts, Canadian employers should provide employees with clear notice of any practices that might be construed as “surveillance.” Policies governing time and attendance monitoring, social network monitoring, GPS and Radio Frequency Identification (RFID) technology use, physical searches, locker searches, telephone and voicemail monitoring, video surveillance and computer system use should all be reviewed.

Of all policies to review, employers should give special attention to their computer use policies in light of a decision of the Court of Appeal for Ontario last year that recognized that an employee had a reasonable expectation of privacy arising out of his personal use of his work laptop. His employer did not have a clear and unambiguous policy that set out a broad right of access to personal communications and files, which was one of the factors that weighed heavily on the Court. An appeal of this decision (*R. v. Cole*) will be heard by the Supreme Court of Canada in the next year and will be of critical interest to employers across Canada.

Privacy outside the workplace

The risks of investigating off-duty conduct (including through video surveillance) are likely to increase based on the tort, though employers should not be liable if the investigation techniques they employ are reasonable and if such techniques are employed based on reasonable grounds.

Employers have a great interest in having a continued ability to use surreptitious video surveillance to combat sick leave and disability benefit abuse. Most of the time this surveillance is conducted of activity available to public view, now likely a requirement. There is certainly a more limited expectation of privacy in public, though former Supreme Court of Canada Justice Gérard LaForest has suggested that it is “too facile” to rule out a protectable privacy interest in one’s public activity. Regardless, there is likely to be some theory for justifying this very common kind of surveillance when it is conducted reasonably and based on reasonable grounds, perhaps by using the “highly offensive” element of the new tort to dismiss claims. Most employers will wish to continue to use outside investigations as required, but all should proceed with a new degree of caution. Retainer agreements with private investigators should impose new requirements to ensure that investigations are conducted reasonably and, in general, employers should exercise greater control over their private investigators.

Data breaches

The new tort is not likely to give rise to significant new data breach liability.

Employers who take custody of others’ personal information have a duty to take care of that information. This duty is imposed through privacy legislation to the extent it applies. There is also good reason to believe that an employer who takes custody of others’ personal information owes individuals a duty of care that is enforceable (in court) through the negligence cause of action. A

negligence claim requires proof of damage, which is a significant limitation for those who wish to sue following a data breach.

The intrusion upon seclusion tort is not likely to give rise to new significant data breach liability because it is a tort that governs the *collection* of information and not the *disclosure* of information. Unauthorized access to personal information by employees is an all too common phenomenon, but the reason to establish controls to prevent unauthorized access already exist. Vicarious liability claims for employee intrusions upon seclusion are a possibility, but should be defensible if proper controls are in place.

Employers as plaintiffs

It is questionable whether the tort will be of use to employers who are the subject of industrial espionage. The tort is of interest because a breach of confidence claim can only apply to information that has been provided to another in confidence. There are times when information is simply taken by an arm's length party, and property-based claims are not a perfect fit for dealing with such a scenario. Some employers will attempt to use the intrusion from seclusion tort to seek a remedy for theft of corporate information by a person who is at arm's length, though the application of the tort to corporations may be questioned. In the United States, corporations cannot make such claims.

CONCLUSION

Yes, it is a brave new world. The new intrusion upon seclusion tort is a significant development for employers. We have made some prescriptions here, the most important of which is that employers immediately revisit their computer use policies. In support of that activity, we have published a guide entitled [Ten Questions and Answers About Computer Use Policies](#).

We would be pleased to look at your computer use policy and provide any guidance related to this important development. For more information, please contact [Paul E. Broad](#) at 519.931.5604 or any other member of our firm's [Information and Privacy Group](#).

The articles in this Client Update provide general information and should not be relied on as legal advice or opinion. This publication is copyrighted by Hicks Morley Hamilton Stewart Storie LLP and may not be photocopied or reproduced in any form, in whole or in part, without the express permission of Hicks Morley Hamilton Stewart Storie LLP. ©