

Opening the Door for Intrusion upon Seclusion: The Common Law Tort of Invasion of Privacy and what it means for Employers

By Shafik Bhalloo, Alisha Parmar

INTRODUCTION

In today's workplace, privacy is an evolving issue and Canadian privacy law is developing rapidly. Perhaps surprisingly, only a handful of Canadian jurisdictions, (including British Columbia, Saskatchewan, Manitoba and Newfoundland) have privacy legislation that creates a statutory tort or civil right of action for invasion of privacy. Until recently, most Canadian jurisdictions could only rely on legislative schemes that applied in very specific contexts – there was no general remedy for an invasion of privacy, unless the claimant managed to successfully establish the existence of a common law right to bring a civil action.

That changed when the common law tort of invasion of privacy was given teeth by the Ontario Court of Appeal in *Jones v Tsige*, 2012 ONCA 32 (“*Jones*”), wherein the Court definitively recognized the common law cause of action for intrusion upon seclusion. In *Jones*, the tort of intrusion upon seclusion enabled the plaintiff to recover not insignificant damages for the invasion of her privacy where no legislative scheme applied and where she had suffered no pecuniary loss.

But the bite of *Jones* and the tort of intrusion upon seclusion do not stop there. This year, the Ontario Superior Court of Justice relied on *Jones* to certify a class action proceeding against an employer for, *inter alia*, vicarious liability of an employee's tort of intrusion upon seclusion. While the case, *Evans v The Bank of Nova Scotia*, 2014 ONSC 2135 (“*Evans*”), has yet to proceed to trial, the decision is one to watch out for. Whether or not the employer is ultimately found liable for the employee's breach of privacy, *Evans* serves as a reminder that the law around breach of privacy is progressing swiftly and that employers must keep up.

JONES V TSIGE

The Facts

The plaintiff, Ms. Jones, and the defendant, Ms. Tsige, were both employees of the Bank of Montreal (“BMO”). Another coincidental common factor was that Ms. Jones' former husband had formed a common law relationship with Ms. Tsige. However, Ms. Jones and Ms. Tsige did not know each other, and they worked at different branches of the BMO in different positions.

By virtue of her position with the BMO, Ms. Tsige had access to Ms. Jones' personal information, and on at least 174 occasions, using her computer at her workplace, Ms. Tsige did in fact access Ms. Jones' personal information. The information included Ms. Jones' date of birth, marital status, language spoken, residential address, and details of her financial transactions in her personal accounts with the BMO.

The BMO discovered Ms. Tsige's activities and confronted her. Ms. Tsige admitted to the BMO that she had no legitimate reason for accessing Ms. Jones' personal information. Instead, Ms. Tsige explained she had been accessing Ms. Jones' information since she was in a financial dispute with her common law spouse (Ms. Jones' former husband) and wanted to find out if he

KORNFELD LLP

was paying Ms. Jones child support. Notably, Ms. Tsige did not make any copies of or disseminate Ms. Jones' personal information.

The BMO disciplined Ms. Tsige by meting out a five-day suspension and denying her a yearly bonus. The BMO also issued her a warning that future repetition of her conduct would result in termination of her employment. Ms. Tsige was asked to review and discuss the BMO privacy principles and standards.

The Ontario Superior Court

Ms. Jones lodged an action in the Ontario Superior Court of Justice asserting that her privacy interest in her confidential banking information was "irreversibly destroyed" and claimed damages of \$70,000 for invasion of privacy and breach of fiduciary duty, and punitive and exemplary damages of \$20,000 against Ms. Tsige.

The Court held there was no fiduciary duty owed by Ms. Tsige to Ms. Jones and dismissed the breach of fiduciary duty claim, finding there was no fiduciary relationship between them in the traditional or non-traditional sense.

With respect to the invasion of privacy claim, the Court rejected the notion that in Ontario a common law tort of invasion of privacy exists. As a result, the privacy claim was also dismissed. The Court stated that in spite of the dismissal, Ms. Jones was not without remedy because she could bring an action for invasion of privacy under the federal *Personal Information Protection and Electronic Documents Act*, 2000 c. 5 ("PIPEDA").

The Ontario Court of Appeal

Ms. Jones appealed the Superior Court's ruling to the Ontario Court of Appeal only on the ground that Ontario law does not recognize the tort of invasion of privacy. The Court of Appeal reversed the lower Court's decision, recognized the tort of intrusion upon seclusion, and awarded Ms. Jones damages.

In order to come to the conclusion that the tort of intrusion upon seclusion exists in Ontario, the Court of Appeal conducted an extensive review of Canadian, American, and English jurisprudence on the tort of invasion of privacy. The Court found the comments of Professor Prosser particularly compelling, and stated that if Ms. Jones did have a cause of action for the invasion of her privacy, it would fall in Professor Prosser's first category of invasion of privacy, namely intrusion upon seclusion.¹

For her case, Ms. Tsige submitted that the existing Ontario and federal legislative framework addressing privacy is an adequate basis for the Court to refuse to recognize the emerging tort of intrusion upon seclusion. To that end, Ms. Tsige argued that expansion of the law in the area should be left to Parliament and the legislature.

The Court of Appeal considered and rejected this argument, pointing out the various deficiencies in the legislative framework with respect to Ms. Jones' case. Namely, the legislation that Ms. Jones could use, *PIPEDA*, only deals with "organizations" that are within federal jurisdiction and does not address the existence of a civil cause of action for invasion of privacy within provincial jurisdiction. In addition, Ms. Jones would only be able to use *PIPEDA* to lodge an action against the BMO, not Ms. Tsige, and the statute would not permit her to recover damages. Further, the Court of Appeal identified that existing Ontario legislation does not provide for a private cause of action between individuals; it merely addresses individual privacy rights in the context of governmental and other public institutions.

KORNFELD LLP

The Court of Appeal then confirmed the existence of a right of action for intrusion upon seclusion, reasoning as follows:

Recognition of such a cause of action would amount to an incremental step that is consistent with the role of this court to develop the common law in a manner consistent with the changing needs of society.

For over one hundred years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially...

It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the *Charter*, has been recognized as a right that is integral to our social and political order.

The Legal Elements of Intrusion upon Seclusion

The Ontario Court of Appeal expressly adopted the key features of intrusion upon seclusion as delineated in the *Restatement (Second) of Torts* (2010). The legal elements are that:

1. The defendant's conduct must be intentional, which includes reckless conduct;
2. The defendant must have 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 of Appeal opined that recognizing intrusion upon seclusion as a cause of action does not pose a serious risk of opening the proverbial "floodgates". The Court stated only "deliberate and significant invasions of personal privacy" are caught by the tort and not *de minimus* cases:

Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.

Nonetheless, the Court indicated that a plaintiff is not required to establish actual loss or damages as part of the cause of action. In this respect, the tort of intrusion upon seclusion is similar to the statutory causes of action for invasion of privacy which exist under the legislative schemes implemented in the four provinces, including British Columbia.

Having said this, the Court stated that where the plaintiff has suffered no pecuniary loss, only "symbolic" or "moral" damages are appropriate to acknowledge the wrong done. After considering Ontario case law and the Manitoba *Privacy Act*, the Court of Appeal established the upper range for damages where no pecuniary loss is suffered at \$20,000. The Court then awarded Ms. Jones \$10,000, the mid-point of the range, stating that Ms. Tsige's conduct was "highly offensive to the reasonable person and caused humiliation, distress and anguish", but that it did not qualify as "exceptional circumstances" meriting an award of punitive or exemplary damages – those awards were to be left for "truly exceptional circumstances".

EVANS V THE BANK OF NOVA SCOTIA

The Facts

Evans also involves another major bank, the Bank of Nova Scotia ("BNS"), where an employee illegitimately accessed customer information. The employee, Mr. Wilson was a mortgage

KORNFELD LLP

administration officer for the BNS, and as such had access to highly confidential customer information.

Over the course of approximately one year, Mr. Wilson accessed the files of 643 customers of the BNS and forwarded private information to his girlfriend. His girlfriend then distributed the information to individuals who used it to commit identity theft and other fraud. Unlike *Jones*, it was law enforcement and not the bank that uncovered the scheme. The arrangement and Mr. Wilson's involvement was exposed by the Calgary Police in the course of executing a search warrant against individuals who were attempting to use the information to perpetrate fraud in Alberta. Mr. Wilson was confronted and confessed to improperly printing and accessing customer profiles for individuals who had applied for mortgages.

The BNS gave notice to the 643 individuals whose profiles had been accessed by Mr. Wilson (the "Notice Group"). Over 130 individuals from the Notice Group have since informed the BNS that they have been victims of identity theft or fraud. The BNS compensated those individuals for their financial losses and offered each individual in the Notice Group a complimentary subscription to credit monitoring and identity-theft protection service.

In spite of these efforts, the BNS, in addition to Mr. Wilson, was named as a defendant in a class action, with the class being the entire Notice Group. The Ontario Superior Court certified the Notice Group's class action for, *inter alia*, the BNS' vicarious liability for intrusion upon seclusion.

Vicarious Liability and Intrusion Upon Seclusion

The Ontario Superior Court relied on the Supreme Court of Canada's decision *Bazley v Curry*, [1999] SCR 534 ("*Bazley*") for the rationale to impose vicarious liability on an employer. In *Bazley*, McLaughlin J (as she then was) stated:

The fundamental question is whether the wrongful act is sufficiently related to conduct authorized by the employer to justify the imposition of vicarious liability...

In determining the sufficiency of the connection between the employer's creation or enhancement of the risk and the wrong complained of, subsidiary factors may be considered. These may vary with the nature of the case. When related to intentional torts, the relevant factors may include, but are not limited to, the following:

- (a) the opportunity that the enterprise afforded the employee to abuse his or her power;
- (b) the extent to which the wrongful act may have furthered the employer's aims (and hence be more likely to have been committed by the employee);
- (c) the extent to which the wrongful act was related to friction, confrontation or intimacy inherent in the employer's enterprise;
- (d) the extent of power conferred on the employee in relation to the victim;
- (e) the vulnerability of potential victims to wrongful exercise of the employee's power.

[Emphasis in original]

KORNFELD LLP

The Ontario Superior Court further specified that “vicarious liability ‘is strict, and does not require any misconduct on the part of the person who is subject to it’: *Straus Estate v Decaire*, 2011 ONSC 1157, 84 C.C.L.T. (3d) 141 at para. 49.”

Applying this legal test to the conduct of the BNS, the Court found that, at least to the extent required to certify the class action, the BNS had enabled Mr. Wilson to commit the tort of intrusion upon seclusion:

[BNS] created the opportunity for Wilson to abuse his power by allowing him to have unsupervised access to customer’s private information without installing any monitoring system... Wilson was given complete power in relation to the victims’ (customers) confidential information, because of his unsupervised access to their confidential information. Bank customers are entirely vulnerable to an employee releasing their confidential information. Finally, there is a significant connection between the risk created by the employer in this situation and the wrongful conduct of the employee.

Furthermore, the Court’s decision to certify the class action for the tort of intrusion upon seclusion was not influenced by the BNS’ admission of responsibility to compensate the Notice Group for any financial losses. The BNS submitted that it accepted liability for the pecuniary losses of the individuals, as evidenced by the BNS’ willingness to financially compensate the members of the Notice Group that came forward as being victims of fraud. The Court refused to accept the BNS’ argument that it was not liable for further damages through vicarious liability for the tort of intrusion upon seclusion. Conversely, the Court distinguished the two types of damages and stated that the BNS’ “admission of responsibility to pay for the pecuniary damages suffered is a different situation from the absence of claim for compensatory damages”.

COMMENTS

Jones and *Evans* raise a number of thought-provoking issues for employers to consider, and the ramifications of the two cases extend well beyond Ontario.

Though it has yet to proceed to trial, *Evans* clearly brings to light the necessity of employers to keep up with the demands of privacy law. Employers who are neglectful in this regard may be held liable for not only the pecuniary damages associated with illegitimate access or use of private information, but also the moral or compensatory damages that may flow from a successful claim of vicariously liability for intrusion upon seclusion or applicable statutory causes of action for invasion of privacy.

In an increasingly technological world, employers have the responsibility to adequately supervise employees in their access to confidential or private information when such access is granted by virtue of employment. To this end, employers should have up-to-date privacy policies in place and ensure that employees are aware of what constitutes unauthorized access or use of private information. Employers should take active measures to ensure that these policies are implemented and followed, and it is recommended that the policies include mechanisms to monitor employee access to private information in order to identify potential abuse. Being proactive and having effective policies in place may assist employers in decreasing liability in the event that a claim of vicarious liability for an invasion of privacy is brought against the employer, or, in any event, may reduce the number and severity of potential claims by exposing unauthorized access sooner rather than later.

In addition, while the courts in British Columbia are not bound by the decisions of Ontario courts, the decision of the Ontario Court of Appeal in *Jones* and that of the Ontario Superior Court in *Evans* may still be relied upon as persuasive authority. In particular, the two decisions

KORNFELD LLP

may be used to delineate the scope of privacy protection afforded in other jurisdictions, including provinces with general privacy legislation, since “privacy” is not defined in the statutes.

Moreover, *Jones* is a well-reasoned decision with an extensive overview of the relevant jurisprudence, legislation and authoritative academic literature on the tort of invasion of privacy. The Ontario Court of Appeal took judicial notice of the role of technological change and the growing threat it poses for privacy, making a highly persuasive case for other courts to “develop the common law in a manner consistent with changing society”.

Finally, the tort of intrusion upon seclusion may affect individuals outside of Ontario even before a decision is made to import the new cause of action to other jurisdictions. The Notice Group in *Evans* includes individuals who are residents of British Columbia and New Brunswick. The BNS attempted to argue that as against those 35 individuals, the claim of vicarious liability for intrusion upon seclusion could not disclose a reasonable cause of action, since the two jurisdictions have not yet recognized the tort.

The Ontario Superior Court chose not to preclude these individuals from utilizing the cause of action and instead commented that “[w]hile the Courts in British Columbia and New Brunswick have not as of yet recognized the tort of intrusion upon seclusion, I was not given caselaw to suggest that they have definitively shut the door on this cause of action.” In the end, the courts of British Columbia may decide to open the door to intrusion upon seclusion, and employers should be prepared for if, and when, they do.



Shafik Bhalloo has been a partner of Kornfeld LLP since 2000. His practice is focused on labour and employment law, and on commercial and civil litigation. He is also an Adjudicator on the Employment Standards Tribunal and an Adjunct Professor in the Faculty of Business Administration at Simon Fraser University.

 sbhalloo@kornfeldllp.com

 <http://www.kornfeldllp.com/vcards/sbhalloo.vcf>

 604.331.8308

¹ William Prosser, *Law of Torts*, 4th ed. (West Publishing Company, 1971) at p. 389:

1. Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.