l'Association canadienne du droit
des technologies de l'information

January 25, 2012

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Robert Currie and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School, and David Fraser.

Les auteurs du présent bulletin sont les professeurs Robert Currie et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie, et David Fraser.

Tort of Invasion of Privacy

The Ontario Court of Appeal has found that the tort of invasion of privacy exists with its decision in *Jones v. Tsige*. Jones and Tsige both worked at the Bank of Montreal (BMO), though they were employed in different branches and did not know each other. Jones also maintained her primary bank account at the BMO. Tsige became involved in a relationship with Jones' former husband and over a period of roughly four years Tsige used her workplace computer to access Jones' personal BMO bank accounts. She did so at least 174 times, gaining access to transaction details and personal information such as date of birth, marital status and address.

Jones eventually became suspicious that Tsige was accessing her information and reported those suspicions to BMO. When BMO investigated Tsige admitted what she had been doing and acknowledged that it was a breach of BMO's Code of Business Conduct and Ethics. She was disciplined by being suspended without pay for a week and denied a bonus, and Jones brought an action against her. In that action Jones claimed $70,000 in damages for invasion of privacy and breach of fiduciary duty and $20,000 in punitive damages. The motion judge (on an application for summary judgment) found that Tsige did not owe Jones any fiduciary duty, and also found that the tort of invasion of privacy did not exist: he concluded that any expansion of privacy rights should take place through statute, not by the common law. Jones did not appeal the finding with regard to fiduciary duty, but did appeal the tort of privacy ruling. The Ontario Court of Appeal overturned the lower court decision, holding that the tort did exist and that Tsige had committed that tort in regard to Jones.

The Court of Appeal noted that there had been discussion of a potential tort of invasion of privacy for over a century, and that in particular the *United States Restatement (Second) of Torts* (2010) had accepted it. The Restatement broke the invasion of privacy down into four potential torts:

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.

The Court of Appeal accepted that these four interests were different and worth distinguishing. They also noted that Jones' complaint in this case concerned the first category, intrusion upon the plaintiff's seclusion, and accordingly it was only that potential aspect of the tort which they were considering in their decision.

The court noted that case law on the subject had not foreclosed the tort of intrusion upon seclusion, and remained at least open to the possibility. They also noted that *Charter* case law had recognised the importance of privacy, breaking it into the three categories of personal, territorial and informational privacy: Tsige's actions in this case of using her computer to gain access to Jones banking records infringed her informational privacy as that concept had been elaborated by the Supreme Court. They noted as well that international law also contains guarantees of privacy. Though none of this directly meant that a tort of privacy existed, the Court of Appeal noted that the common law ought to develop in a manner consistent with *Charter* values.

The Ontario Court of Appeal also looked at legislation relating to privacy: PIPEDA, legislation in other provinces creating a tort of invasion of privacy, and other jurisdictions. Although PIPEDA would be applicable to these circumstances, the court held, it was not a substitute for a tort action. If she acted under PIPEDA Jones would actually have to lay a complaint about BMO (her own employer) rather than about Tsige, and the fact that Tsige was acting entirely without authority might mean the complaint would fail. In any event Jones could not receive damages if she succeeded under PIPEDA, so it was no substitute for a tort action. On the other hand the fact that some provinces *had*, by statute, created a tort of invasion of privacy did not lead the Court of Appeal to think that they could not act unless the legislature in Ontario did so first. The court noted that the legislation in other provinces created a right of action without defining the right, leaving that task to the courts. They saw no reason, therefore, that they could not simply extend the common law.

Finally, the Court of Appeal noted that the pace of technological change made it particularly important to extend privacy protection:

> [67] 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. Legal scholars such as Peter Burns have written of "the pressing need to preserve 'privacy' which is being threatened by science and technology to the point of surrender": "The Law and Privacy: the Canadian Experience" at p. 1. See also Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967). The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic data bases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled, and the nature of our communications by cell phone, e-mail or text message.
>
> [68] 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.

In describing the contour of the tort, the Court adopted the wording of the American *Restatement*:

> One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.

The Court of Appeal had no difficulty concluding, of course, that Tsige had committed this tort in relation to Jones and found her liable. As a general rule they concluded that damages for committing this tort should not exceed $20,000: the concluded that this case fell in the mid range and awarded Jones $10,000.

Warrantless Searches and Cell Phones

The issue of the permissible search of cell phones when a person is arrested arose again in *R. v. Cater* (2012 NSPC 2, no hyperlink available). The accused had been arrested on weapons charges and his cell phone had been seized by police at the time: the provincial court judge held that this seizure was part of a search incident to arrest and lawful. The more controversial issue was that the phone was subsequently sent to the Technological Crime Unit for a forensic search without a warrant first being obtained. However, the provincial court judge held that that testing also fell within the "search incident to arrest" power and therefore had been lawfully done without a warrant.

The provincial court judge noted several facts she thought to be relevant. The accused's cell phone was not a smart phone, and so could not be seen as a kind of mini-computer, containing a wealth of

sensitive, personal information. In addition the phone was not password-protected: this did not remove completely any expectation of privacy, the judge held, but it was relevant.

The judge noted that case law suggests that police are entitled to undertake a "cursory search" of a cell phone incident to arrest. In this case the police who arrested the accused seized the phone, removed its battery to prevent further incoming data which might overwrite data already on the phone at the time of the arrest, but then did nothing until the phone was sent for forensic analysis. The judge held that this was the proper course of action: a cursory search, though permitted, would have risked losing or degrading the data on the phone. Indeed she concluded that police ought not to conduct a cursory search incident to arrest unless it is urgent to do so.

In this case, she held, the accused's cell phone was roughly the equivalent of an unlocked briefcase or a logbook which the accused was carrying in his pocket. Police would not require a warrant to examine or photocopy the contents of any such item seized incident to arrest, and so no warrant was required for the forensic analysis in this case.

Privilege Not Waived Over Documents "Stolen" by Computer Tech

In *Pottruff v. Don Berry Holdings Inc.*, Justice Arrell of the Ontario Superior Court heard a motion for the return of documents and a declaration that the documents were subject to solicitor-client privilege. In the underlying action the plaintiff had sued the defendant company for constructive dismissal, arising from a change in her duties at the defendant's Tim Hortons store. Prior to the beginning of the action the principal of the defendant ("Berry") hired a consultant, Beacham, to assist in managing expenses. Beacham arranged for Berry to receive advice from a solicitor about employee matters, and e-mails were exchanged with the solicitor. Berry occasionally asked the plaintiff's husband to help him with his computer, and about one week after the exchange of e-mails Berry asked the husband to train a spam filter on his computer. He did not give the husband open access to the computer or to any documents.

The husband's uncontradicted evidence was that the documents "popped up on his screen." He saw his wife's name on them and made copies. Once the plaintiff's action began the husband showed the documents to other employees, and the defendant demanded their return.

Justice Arrell dismissed the plaintiff's argument that the defendant had waived solicitor-client privilege over the documents, by giving the husband access to the computer and by allowing Beacham, a third party, to be in on the communications. The court held that the husband had stolen the documents from the computer, since he had no right or authority to take them:

> On this basis alone I would conclude that the administration of justice would be brought into disrepute if those who wrongfully and intentionally obtained documents could then use them to their advantage in civil law suits.
>
> This is not a situation where one party's confidential document innocently falls into the hands of the opposing party. This was a deliberate and planned act to remove a document from a person's computer knowing full well it was confidential. [paras. 14-15]

The documents, the court held, were clearly privileged. Giving access to Beacham did not amount to waiver because Beacham was acting as an agent between the defendant and the solicitor and was thus covered by the privilege. Justice Arrell also rejected the plaintiff's argument that the defendant's recklessness in giving the husband access to the computer amounted to waiver of privilege, commenting:

> A person's computer is a highly personal storage instrument. Many cases have concluded that an extremely high level of privacy is expected regarding the contents. There is no evidence in this case that suggests the plaintiff's husband was given access to everything on Mr. Perry's computer. He was asked to train a spam filter and nothing more. He was well aware that he did not have access to the documents he copied and that what he was doing was wrong. I do not find Mr. Perry was reckless in expecting that documents on his computer would not be accessed and

> certainly not copied. Certainly if there was any recklessness it was not sufficient to waive privilege. Clearly, Mr. Perry never intended to waive privilege regarding the documents in question relating to the plaintiff. [para. 24]

The plaintiff was ordered to return the documents and destroy all copies.

How Can I E-Defame Thee? Let Me Count the Ways...

In *Nesbitt v. Neufeld*, the British Columbia Court of Appeal heard an appeal from a finding of defamation and invasion of privacy arising from a family dispute. The parties to the action were embroiled in a contentious marriage breakdown and custody battle that led to a number of extraordinary electronic measures being taken by the husband (Nesbitt) to belittle and criticize the wife (Neufeld). The lower court judge's decision rested upon factual findings of a great deal of misconduct on the part of Nesbitt, who had accessed Neufeld's personal computer in their home on a number of occasions, and had made copies of personal e-mail correspondence between Neufeld and her friend, X.

Edited or altered versions of these e-mails were used by Nesbitt as the basis for a number of communications designed to annoy and embarrass Neufeld, including: faxes to the bank where X worked, containing intimate and embarrassing passages from the e-mails; inclusion of similar passages from the e-mails in letters to Neufeld's Rotary Club; using passages from the e-mails on a website called "Wicked Wendy Neufeld," which had other scandalous information on it; and a letter to the Ministry of Child and Family Health (cc'd to the child's doctor) which made various allegations about Neufeld. Nesbitt also set up a Facebook page called "The Wendy Neufeld Support Group," purporting to have something to do with the death of Neufeld's parents but in fact used as a means of criticizing and embarrassing her. Finally, Nesbitt posted a video on YouTube titled "Wendy Neuffeld [sic] – shirt stuff," which contained a Q&A between Nesbitt and the couple's child in alleged response to an allegation of questionable behaviour toward the child by Nesbitt.

The trial judge found that the initial use of Neufeld's e-mail correspondence amounted to a breach of privacy tort under the B.C. *Privacy Act*, the breach being compounded by the subsequent attachment of the e-mails to various communications made to third parties. He commented:

> I find Ms. Neufeld had a reasonable expectation that her personal information and private correspondence would not be emailed or faxed to third parties or publicly posted on the Internet without her knowledge and consent. Put alternatively, Ms. Neufeld did not consent to Dr. Nesbitt's use of data from her home computer for unlawful purposes. [para. 94]

The trial judge further concluded that one of the Rotary Club e-mails, the website, the Facebook page and the letters to the Ministry and the child's doctor all defamed Neufeld. Neufeld was awarded $40,000 in damages and special costs, the trial judge noting that while internet publication was "to the world," it appeared that any actual damage to Neufeld had been minimal. Writing for the Court of Appeal, Chief Justice Finch declined to interfere with any of the trial judge's findings and upheld the order.

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professor Robert Currie, Director of the Law & Technology Institute, at robert.currie@dal.ca.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Le présent bulletin se veut un outil d'information à l'intention des membres d'IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d'administration de l'Association s'en serviront également pour vous tenir au courant des nouvelles concernant l'Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant le présent bulletin, veuillez communiquer avec le professeur Robert Currie à l'adresse suivante : robert.currie@dal.ca

Avertissement : Le Bulletin IT.Can vise à informer les lecteurs au sujet de récents développements et de certaines questions à portée juridique. Il ne se veut pas un exposé complet de la loi et n'est pas destiné à donner des conseils juridiques. Nul ne devrait donner suite ou se fier aux renseignements figurant dans le Bulletin IT.Can sans avoir consulté au préalable un conseiller juridique.