itworldcanada.com

Understanding Canadian cybersecurity laws: Peer-to-peer privacy protection — 'Intrusion upon seclusion' and the protection of intimate images (Article 6)

Melissa Lukings and Arash Habibi Lashkari

19-23 minutes

Introduction

The prevalence of digital communication has created nearly limitless possibilities for the rapid, large-scale sharing of private communications, intimate images, and personal information. Through the use of online tools and social media applications, access to the internet can be used to turn a small threat within an interpersonal dispute into a viral media publication; downloaded, viewed, and retransmitted to millions of people around the world. In the modern age of high-speed information sharing, privacy and the ability to control the information which is publicly shared about yourself has become increasingly imperative. Not only can the intrusion upon your personal information feel harmful and disruptive to your personal and professional reputation, but the use of visual recordings of intimate images has also been weaponized

as a tool for criminal acts of extortion and cyberbullying, and has quickly become a contributing factor to an increase of suicides and suicide attempts amongst our young Canadians.

In our previous articles, we have discussed the foundations of Canadian laws and the specific legislations which apply to government, commercial enterprises, and some peer-to-peer cyber-specific criminal activities.

Related:

- Understanding Canadian Cybersecurity Laws: The Foundations (Article 1)
- Understanding Canadian Cybersecurity Laws: Privacy and Access to Information — the Acts (Article 2)
- Understanding Canadian Cybersecurity Laws: Privacy Protection in the Modern Marketplace — PIPEDA (Article 3)
- Understanding Canadian Cybersecurity Laws: Interpersonal Privacy and Cybercrime — Criminal Code of Canada (Article 4)
- Understanding Canadian Cybersecurity Laws: “Insert Something Clever Here” — Canada’s Anti-Spam Legislation (Article 5)

In this article, the sixth in our Understanding Canadian Cybersecurity Laws series, we will highlight the common law tort of intrusion upon seclusion and the relatively new criminal offences pertaining to cyberbullying and the sharing of intimate images. Cyberbullying is the use of technology (like the internet, social media, text messaging, etc.) to harass, threaten, intimidate, embarrass or otherwise harmfully target another person.

Sexual cybercrime and cyberbullying involving the distribution or

sharing of intimate images, videos, or any visual recording, can result in very serious criminal and civil consequences in Canadian law. Not only can an invasion of privacy of this nature result in jail time and a criminal record, but the perpetrator may also be hit with a costly civil lawsuit on top of the criminal charges. A civil lawsuit of this nature can be based on the common law tort of "intrusion upon seclusion", which we can see clearly illustrated in the Ontario Court of Appeal in the 2012 case of *Jones v Tsige,* 2012 ONCA 32*.*

Invasion of privacy as "intrusion upon seclusion"

In January 2012, the case of *Jones v. Tsige (*2012 ONCA 32) became a landmark case in the Ontario Court of Appeal for recognizing the "new" privacy tort of "intrusion upon seclusion", which allows victims of such privacy breaches to have the right to sue the privacy breacher in civil court for invasion of privacy. In this case, the Ontario Court of Appeal found that the Canadian common law was required to evolve in order to effectively respond to more modern privacy issues. This includes those which have arisen from technological changes and the constantly evolving need to reassess how personal information is collected, stored, protected, and made accessible in electronic form. The case has had huge privacy and liability implications for employers, which we will outline below.

The *Jones v. Tsige* case involved a bank employee who accessed and reviewed another employee's personal bank accounts on 174 occasions over a four-year period. When the victim became aware of the unauthorized access to her accounts, she

understandably sued the defendant. The victim claimed that by improperly accessing and reviewing her bank accounts the defendant committed the tort of invasion of privacy. In response, the defendant argued that Ontario does not recognize the invasion of privacy as a tort.

Ontario Court of Appeal Justice Sharpe started by conducting a thorough review of the case law and previous legal commentary related to the tort of invasion of privacy. Following his review of the case law, Justice Sharpe concluded that "Ontario has already accepted the existence of a tort claim for the appropriation of personality and, at the very least, remains open to the proposition that a tort action will lie for an intrusion upon seclusion."

The *Charter* protects the right to privacy under s.8. Although the *Charter* cannot apply in a civil case, the Court noted that in developing common law, it makes sense to develop it in the direction which Charter values suggest. Justice Sharpe noted that the existing case law establishes that personal privacy is worthy of constitutional protection and that it is integral to the relationship between individuals and the rest of society. He then combined this explicit *Charter* recognition with the idea that the common law should evolve and develop consistently with *Charter* values in order to be most effective in our modern circumstances. In Justice Sharpe's view, there was already ample support to recognize a civil action for damages (aka: a lawsuit) for "intrusion upon seclusion" as a tort. He described it as follows:

"…the tort includes physical intrusions into private places as well as listening or looking, with or without mechanical aids, into the plaintiff's private affairs. Of particular relevance to this appeal, is the observation that other non-physical forms of investigation or

examination into private concerns may be actionable. These include opening private and personal mail or examining a private bank account."

— ONCA Justice Sharpe

In his decision, Justice Sharpe explained the elements of the newly-recognized tort as:

(1) The defendant's conduct must be intentional or reckless;

(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 theory behind the third element (the "reasonable person" part) was that it would operate to prevent a metaphorical tsunami of future and retroactive privacy tort claims, since the third element establishes that the intrusion must be highly offensive on a "reasonable person" standard.

It is very interesting to note that, in the view of the Court, harm to an economic interest was not a fourth element of the cause of action for this tort, however financial harm can be a factor in determining the amount of monetary damages to be paid by the defendant. While the court said that economic harm need not be shown, only "intrusion upon seclusion" claims which demonstrate **deliberate** and **significant** invasions of personal privacy are to be recognized under this tort. Examples may include invasion of privacy relating to financial or health records, sexual practices and orientation, employment, or private correspondence.

Justice Sharpe stated that "given the intangible nature of the

interest protected" damages would ordinarily be measured by "a modest conventional sum." In cases where the plaintiff had not suffered financial loss, the damages should be modest but sufficient to address the intrusion. He fixed the upper limit for such damages at $20,000. While Justice Sharpe did not exclude the possibility that aggravated and/or punitive damages might also be awarded in "exceptional" cases, he was reluctant to encourage awarding such damages, noting the value of consistency and predictability in the court. Unless there are extreme or exceptional circumstances, the upper limit on awards for damages should be no more than $20,000. It should be noted, however, that this upper limit does not rule out significant damage awards where an intentional or reckless invasion of privacy involves a large number of victims.

The following factors were provided as a guide to assist the court in determining where the damages should fall in the within the range:

(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;

(4) Any distress, annoyance or embarrassment suffered by the plaintiff arising from the wrong; and

(5) The conduct of the parties, both before and after the wrong, including any apology or offer of amends made by the defendant.

In the case of the bank employee in *Jones v. Tsige (*2012 ONCA 32), the Ontario Court of Appeal found that the defendant had committed the tort of "intrusion upon seclusion" when she repeatedly accessed the plaintiff's private banking records because the following elements were met:

(1) The intrusion was intentional;

(2) It amounted to an unlawful invasion of the plaintiff's private affairs;

(3) It would be viewed as highly offensive to a reasonable person; and

(4) It caused distress, humiliation or anguish.

In determining the damages, Justice Sharpe placed this particular case at the mid-point of the severity range. His reasoning was that although the defendant's actions were deliberate, repetitive and caused emotional distress, the plaintiff suffered no public embarrassment or harm to her health or financial interests. In addition, the defendant had apologized and made genuine attempts to make amends. In light of these factors, the damages were set at $10,000. It should be noted that, based on the novel issue raised by the case, the Court held that the parties should bear their own costs at both levels of court.

Recommendations for employers

Employers should prepare and enforce reasonable and effective employee privacy policies and consider bulking up their computer-use policies so that there is no "reasonable expectation of privacy" regardless of whether the computer is used for work or personal purposes and subject to monitoring without notice.

While computer monitoring does tend to be the focal point for employee privacy concerns, there are additional privacy considerations to consider with regard to bag checks, locker searches, desk searches, the use of GPS on employee vehicles, and private investigations conducted outside the workplace — such as with the hiring of private investigators to look into the external actions of employees who are suspected of insurance, or other, fraud.

As “intrusion upon seclusion” is a relatively new tort with a very recent precedent, we have yet to see what the full impact of this tort will have on employers, their relationship with regard to employees, and employer liability on behalf of those whom they employ. As the common law continues to develop over the next few years and with more of these cases being tried, further clarification will gradually become available to the public. As that unfolds, it will be necessary for employers to stay up to date with the evolving common law to prevent any liability claims which could have been avoidable with proper awareness and the implementation of precautionary measures.

Voyeurism and sextortion

In Canada, it is a crime for a person to share another person’s intimate image even if the intimate image came from the subject itself. The subject holds a “reasonable expectation of privacy” on the intimate image regardless of whether the subject was a willing participant in creating it, as may be the case for recorded materials in an intimate relationship.

In December 2014, the Canadian federal government criminalized

the unauthorized distribution of intimate images and videos in the wake of the high-profile suicide deaths of Rehtaeh Parsons and Amanda Todd. Both girls suicided after being subjected to extremely cruel cyber-bullying and harassment following the widespread distribution of their intimate images, and in the case of Parsons, an explicit photo of an alleged gang rape. Since then, Canada has enacted offences to criminalize the distribution of "intimate" or "invasive" images without the consent of those depicted in those images. This can be found in the Criminal Code of Canada, s. 162.1 (1).

162.1 (1) *Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty*

(a) *of an indictable offence and liable to imprisonment for a term of not more than five years; or*

(b) *of an offence punishable on summary conviction.*

"Intimate image", is defined in s. 162.1(2) of the Criminal Code of Canada as:

162.1 (2) *In this section, intimate image means a visual recording of a person made by any means including a photographic, film or video recording,*

(a) *in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;*

(b) *in respect of which, at the time of the recording, there were*

circumstances that gave rise to a reasonable expectation of privacy; and

***(c)** in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.*

"Visual recording", is also defined in the Criminal Code of Canada as:

***162 (2)** In this section, visual recording includes a photographic, film or video recording made by any means.*

"Private act" includes images taken in which a person has a "reasonable expectation of privacy". This is not limited to images depicting sexual activity or nudity. While nudity is not required, however, it may be considered as an aggravating factor during sentencing.

"Non-consensual pornography", also known as "revenge porn" is when intimate images, which are taken consensually, are then uploaded to the internet or otherwise distributed.

"Surveillance", as a form of voyeurism, is defined under s. 264(2)(c) of the Criminal Code of Canada as "besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be." This would suggest that the offender must have the victim under physical surveillance and leaves a potential gap where the offender may be monitoring the victim remotely. This provision is not easily applied to other forms of surveillance like monitoring emails, text messages, and other communications.

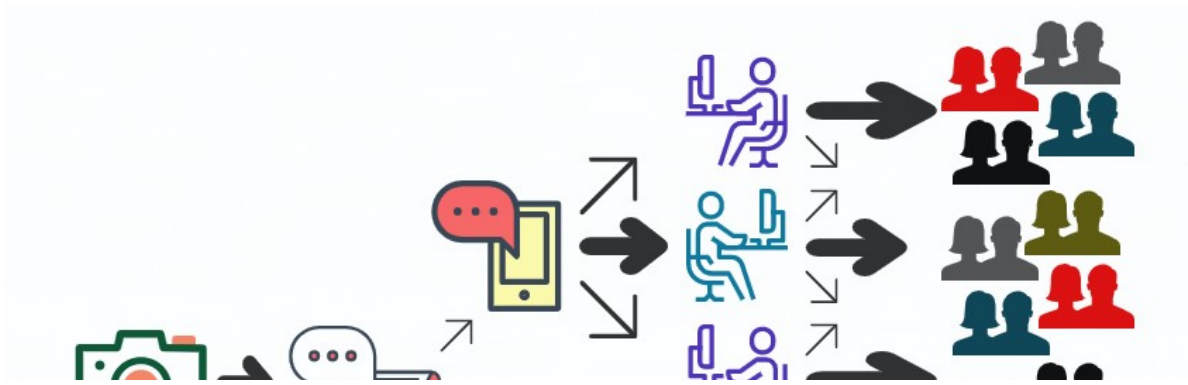
"Digital surveillance" is a subset of surveillance which is based on the idea that a person should have some control over the

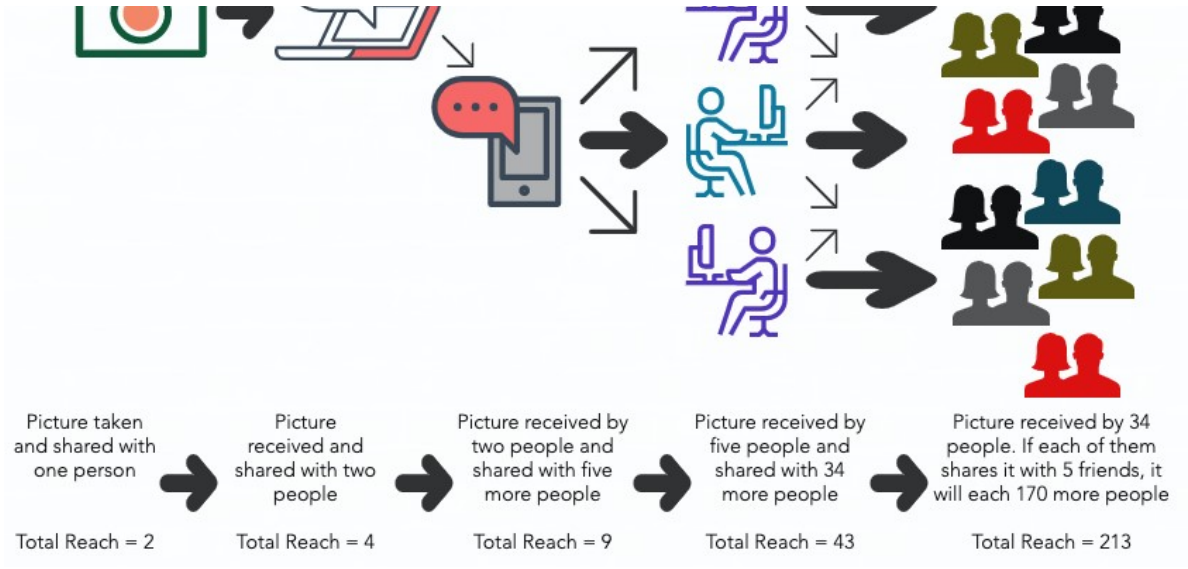
personal information which is shared and made publicly available about them and the right to restrict access to one's personal information, including that which is collected and / or stored digitally.

One of the challenges in enforcing this law is the difficulty for general duty officers in learning how to investigate the electronic footprint of these crimes and deal with internet service providers. For this reason, police forces may have experts available to assist.

Over the last 5 years, with regard to revenge porn and "sexting" related crimes, Canada has seen more than 5,000 cases reported to police. Of the cases reported to police, approximately 20% of those result in criminal charges. This problem has intensified in recent years, with police reportedly handling more than 1,500 cases per year for each of the past three years. While this may seem low, the prospect of convictions with revenge porn and "sextortion" crimes is actually higher than in some sexual assault cases because there is more likely to be a trail of evidence when dealing with revenge porn. When you have images, then there is something evidentiary to work with, whereas in a sexual assault case, there is not always material evidence available.

The scope of the problem — hypothetical example





Click to enlarge.

Recommendations for individuals and employers

Like with other sexually motivated crimes, we have all heard the many harmful suggestions given under the guise of protecting oneself against becoming a victim of intimate photo extortion or cyberbullying. Many, if not most, of these “well-intentioned” suggestions, are rooted in an attitude of victim-blaming, which is inherently harmful. As this is 2020, and many of us have presumably moved past the idea that sexual crimes are the result of poor choices made by the victim (e.g. choice of clothing, past sexual history, etc.), the suggestions in this section will instead be directed at individuals who may be unsure as to whether an intimate image or visual recording in their possession is one which can be freely shared with others.

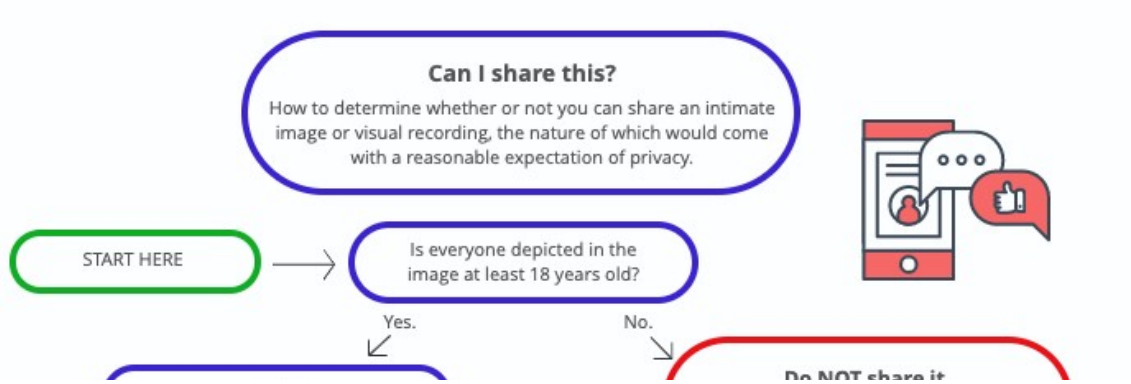
With the crime of illegal distribution of intimate images, there is a reverse onus of proof in the law, which means that the person accused of distributing the image(s) bears the onus to establish that they did indeed have reasonable grounds to believe that

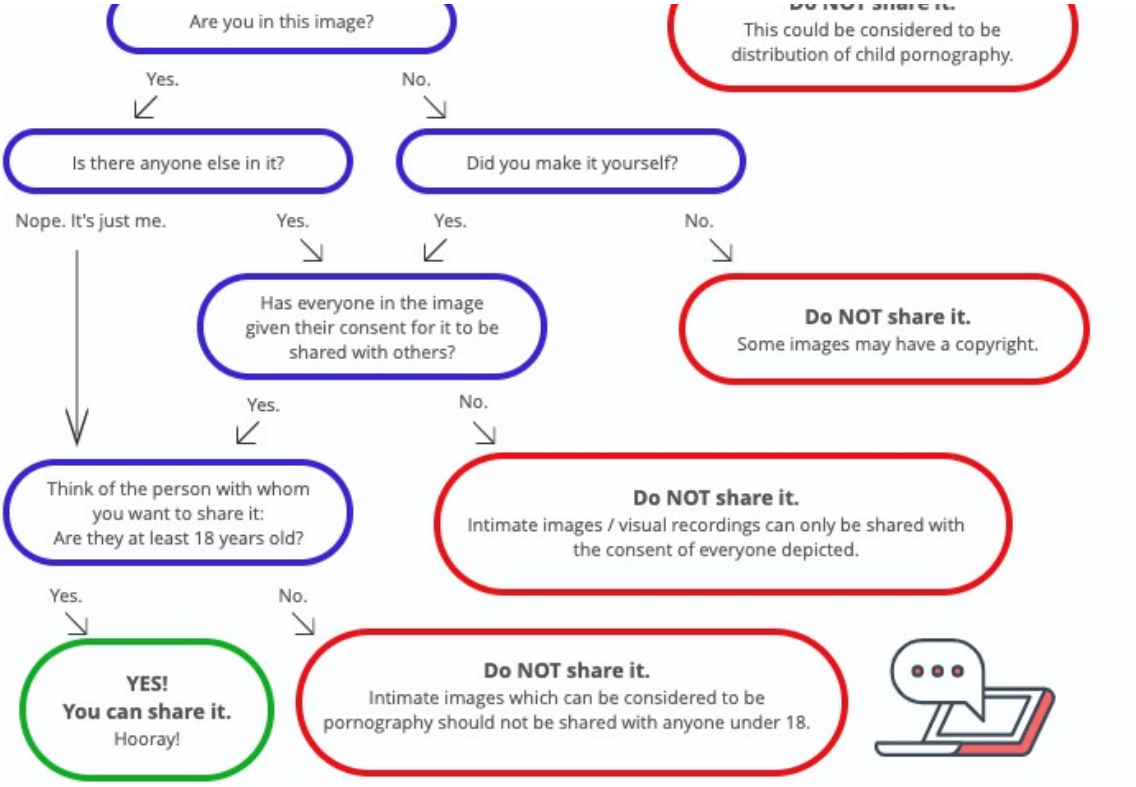
consent to share the image(s) was given. If the accused was unable to prove that they had reasonable grounds to believe that consent had been given, they can be found criminally responsible and face harsh criminal penalties and a criminal record as a result.

As a general rule, if the image or recording has a person in it, that person must give consent for that image to be shared. If you are the only person in the photo, then it is up to you, albeit with some exceptions. It should go without saying (but we will say it anyway) that any image of an intimate or sexual nature that depicts a person who is under the age of 18 is considered to be child pornography. Sharing such an image would constitute the distribution of child pornography. Similarly, sharing or exposing an underage person (under age 18 = child) to pornographic material is also illegal in Canada as a sexual offence. Criminal activities like these can result in much more extreme criminal sentences that carry a high degree of stigma, amongst both the general population and the population of incarcerated individuals.

To assist in clarifying the question of whether or not an intimate image or visual recording can be shared with others, we have created a helpful flowchart, which we have included in the following section below.

The important questions





Click to enlarge.

Conclusion

Sexual cybercrime and cyberbullying through the illegal distribution of intimate images or visual recordings without the consent of those portrayed within the recording can attract serious criminal and civil consequences. The perpetrator could face criminal charges related to revenge porn, voyeurism, and sextortion which attracts jail punishment in Canada if convicted of such crimes. The additional civil tort of “intrusion upon seclusion” has become more relevant as we aim to protect our data at home and while working from home. As our reliance on the internet continues to expand, we must be aware of the limitations of the law and its protections. More and more young people are becoming connected to the web at earlier ages than we have previously seen. For this reason, it is imperative that we provide educational opportunities for increased

awareness of the problem and the repercussions of violating the intimate image distribution law for our youth, as they are highly affected by this and the cost of sexual cyberbullying can be measured in lives lost.

Would you recommend this article?

Thanks for taking the time to let us know what you think of this article!

We'd love to hear your opinion about this or any other story you read in our publication. **Click this link to send me a note →**

Jim Love, Chief Content Officer, IT World Canada

Related Download

Sponsor: **CanadianCIO**

Cybersecurity Conversations with your Board – A Survival Guide

A SURVIVAL GUIDE BY CLAUDIO SILVESTRI, VICE-PRESIDENT AND CIO, NAV CANADA

Download Now