Internet and E-Commerce Law in Canada

Editor-in-Chief: Professor Michael A. Geist, Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law

VOLUME 16, NUMBER 11 Cited as (2015–16) 16 I.E.C.L.C. MARCH 2016

• CAN YOU KEEP A SECRET? THE COURTS RECOGNIZE A NEW TORT FOR PUBLIC DISCLOSURE OF PRIVATE FACTS •

Lyndsay Wasser and Mitch Koczerginski
McMillan LLP

The common law related to privacy rights continues to evolve in Canada. Just a few weeks ago, the Ontario Superior Court of Justice recognized a novel common law tort applicable to violations of privacy rights. This is the second new tort recognized by an Ontario court in approximately four years. In the earlier case, *Jones v. Tsige* [*Jones*],[1] the Ontario Court of Appeal recognized the tort of "intrusion upon seclusion", which had a significant impact on privacy litigation in Canada, including providing grounds for numerous class action lawsuits related to privacy and data security breaches.[2] *Jones* also laid the groundwork for the recent case of *Jane Doe 464533 v. ND* [*Doe*],[3] which will likely now be the seminal case for the tort of "public disclosure of private facts" in Canada.

• In This Issue •

LexisNexis

The Facts

The plaintiff and defendant were in a romantic relationship during their final year of high school. The couple broke up before the plaintiff moved to another city to attend university, but continued to communicate regularly. The defendant asked the plaintiff to make a sexually explicit video of herself to send to him. At first, the plaintiff refused. The defendant persisted for several months and reassured the plaintiff that no one else would ever see the video. When the plaintiff eventually sent a video to the defendant, he posted it online and shared it with several of his friends almost immediately. The video was online for three weeks before it was eventually removed.

INTERNET AND E-COMMERCE LAW IN CANADA

Internet and E-Commerce Law in Canada is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto, Ontario M2H 3R1

ISBN: 0-433-42472-9 **ISSN 1494-4146**
ISBN: 0-433-44385-5 (print & PDF)
ISBN: 0-433-44674-9 (PDF)

Subscription rates: $250 per year (print or PDF)
$370 per year (print & PDF)

Please address all editorial inquiries to:

Boris Roginsky, Journals Editor
LexisNexis Canada Inc.
Tel. (905) 479-2665; Toll-Free Tel. 1-800-668-6481
Fax (905) 479-2826; Toll-Free Fax 1-800-461-3275
Internet e-mail: ieclc@lexisnexis.ca.

When the plaintiff learned that the video had been posted and that several members of her own community had viewed it, she became mentally distraught. The plaintiff was unable to sleep, lost her appetite, could not focus on school, and was eventually checked into a crisis intervention center at a hospital. For over a year after the video was posted, the plaintiff experienced serious depression and suffered from occasional panic attacks. The plaintiff gave evidence that she remains concerned that the video may impact her future employment and relationships.

Recognition of Liability for Public Disclosure of Private Facts

The Court acknowledged that the current state of technology enables predators and bullies to victimize others on a much larger scale than in the past.[4] It also noted that society is scrambling to catch up to the problem and that the law is only beginning to respond. While the Court found that the facts supported liability for both breach of confidence[5] and intentional infliction of emotional distress,[6] it noted that the unique harm caused by the publication of an intimate video requires its own civil remedy.[7]

Just four years earlier, in *Jones*, the Ontario Court of Appeal found that the defendant committed an invasion of privacy when she used her position as a bank employee to access the banking records of her husband's ex-wife. While the Court in *Doe* conceded that *Jones* is factually distinct from the present case, it considered the following passage regarding the recognition of new causes of action relating to invasion of privacy:

> [t]he question of whether the common law should recognize a cause of action in tort for invasion of privacy has been debated for the past one hundred and twenty years. Aspects of privacy have long been protected by causes of action such as breach of confidence, defamation, breach of copyright, nuisance and various property rights. Although the individual's privacy interest is a fundamental value underlying such claims, the recognition of a distinct right of action for breach of privacy remains uncertain.[8]

Like in *Jones*, the Court in *Doe* found that it was presented "with facts that cry out for a remedy".[9]

Upon review of Canadian and American case law and commentary, the Court in *Doe* recognized a cause of action for invasion of privacy on the basis of "publically disclosing the private facts of another". The elements of the new tort were stated as follows:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of the other's privacy, if the matter publicized or the act of the publication (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[10]

In applying these elements to the present case, the Court found that (1) the defendant made public an aspect of the plaintiff's private life; (2) a reasonable person would find the act of publication to be highly offensive; and (3) there was no legitimate public concern justifying publication of the matter.[11]

Damages

Unlike in *Jones*, the Court in *Doe* did not seem concerned about imposing strict limits upon non-pecuniary damages. In *Jones*, the Court awarded $10,000 for a fairly significant intrusion into sensitive personal information (*i.e.*, the plaintiff's financial and banking records), and placed a cap on non-pecuniary damages of $20,000. The present case was distinguished from *Jones* in that it involved something much more sensitive than an invasion of informational privacy.[12]

The Court found that the facts of this case presented a novel situation that is unprecedented by earlier privacy decisions. It was clear from the reasoning in the case that the Court was particularly offended by the defendant's conduct when committing the offence, and afterwards, which the Court describes as: "invasive", "degrading", "a breach of trust", and having been carried out with "malice".

In total, the plaintiff was awarded $100,000 (plus costs), which was the maximum allowable because the claim had been brought under Simplified Procedure. Although it is not possible to know for certain, the Court may have been prepared to award even greater damages in this case if it had been able to do so. More specifically, the Court awarded the plaintiff $50,000 in non-pecuniary damages, $25,000 in aggravated damages, $25,000 in punitive damages and costs on a full indemnity basis of over $36,000.[13]

In coming to this damage award, the Court sought guidance from cases dealing with sexual assaults. The Court reasoned that despite the fact that the present case does not involve physical touching, the injuries to the plaintiff's dignity and personal autonomy were tantamount to the harms that follow sexual assault. The purposes for the damage awards in this case included "vindication" of "fundamental, although intangible, rights which have been violated by the offender", as well as deterrence, "to dissuade others from engaging in similar harmful misconduct".[14]

Significance of Decision to the Development of Privacy Law

As with *Jones*, the Court's decision in *Doe* will likely have significant implications for privacy litigation in Canada. In particular, the plaintiffs in some class action lawsuits have already alleged something similar to "public disclosure of private facts", including the claim that has been filed in connection with the mailing to participants in the Marihuana Medical Access Program, which identified the program on the outside of the envelope. The confirmation that this is a recognized cause of action in Canada will likely impact the negotiations between the parties in this and other cases.

However, it will be interesting to see how the reasoning in *Doe*, and particularly the principles related to determining damages, will be applied in future cases. In particular, the reference to damages in sexual assault cases would seem to only be relevant to publicity of sexually explicit material.

What is clear is that the common law of privacy has once again been expanded in Canada. Where *Jones* previously introduced a cause of action for invasion of privacy on the basis of *intrusion* into one's private life, *Doe* has now

introduced another cause of action on the basis of *disclosure* of one's private life.

The Courts in both *Jones* and *Doe* recognized that technological developments in recent years create the potential for significant privacy violations, and accordingly, the Courts found it necessary for the law to evolve in order to provide recourses to victims.[15] Furthermore, in both cases, the Courts found that sufficient recourse could not be found in applicable legislation. In *Jones*, the Court recognized that the *Personal Information Protection and Electronic Documents Act*[16] applies to commercial activities, and therefore, did not apply to the defendant's actions (which were purely personal), and therefore the plaintiff would have no recourse in the absence of a civil remedy. In *Doe*, the Court noted that the *Criminal Code* provision prohibiting publication of an intimate image without consent[17] was not in force at the time that the defendant published the video of the plaintiff. Only Manitoba has specific legislation applicable to the conduct at issue in this case.[18]

Organizations would be well advised to consider *Doe*, going forward, when engaging in activities that could impact the privacy of individuals. This case is a further example of the quickly evolving privacy landscape in Canada and globally. Organizations that take steps now to implement best practices with respect to handling personal information will be best positioned to meet these evolving legal obligations.

[*Editor's note*: **Lyndsay Wasser** is a Certified Information Privacy Professional/Canada and the Co-chair of McMillan's Privacy Group. She regularly advises and assists clients on a broad range of privacy issues, including advising on access requests, privacy breaches, workplace privacy issues (*e.g.*, background checks, computer/video/phone monitoring, GPS tracking, drug and alcohol testing), handling personal health information, transferring personal information across borders, and CASL compliance, as well as helping organizations to develop privacy compliance programs, privacy and social media policies, data protection agreements and consent forms. Lyndsay regularly writes and speaks on privacy-related topics, and is the co-author of *Privacy in the Workplace*, 3rd ed. and the Privacy chapter in the *Ultimate Corporate Counsel Guide*.

Lyndsay also regularly provides advice and assistance to vendors and purchasers with respect to the privacy aspects of corporate transactions, including negotiating the privacy terms of purchase agreements.

You can reach her at (416) 865-7083 or <lyndsay.wasser@mcmillan.ca>.

Mitch Koczerginski is an associate in the Advocacy and Litigation Group. He is developing a broad practice in corporate and commercial litigation and privacy law.

Mitch earned a designation in law and technology from University of Ottawa and completed an externship with the Canadian Internet Policy and Public Interest Clinic. Mitch has written on various issues at the cross-section of privacy law and technology.

You can reach him at (416) 865-7262 or <mitch.koczerginski@mcmillan.ca>.]

---

1 *Jones*, [2012] O.J. No. 148, 2012 ONCA 32.
2 *Ibid*.
3 *Doe*, [2016] O.J. No. 382, 2016 ONSC 541.
4 *Ibid*. at para. 16.
5 *Ibid*. at para. 25.
6 *Ibid*. at para. 33.
7 *Ibid*. at para. 45.
8 *Ibid*. at para. 35.
9 *Ibid*. at para. 39.
10 *Ibid*. at para. 46.
11 *Ibid*. at para. 47.
12 *Ibid*. at para. 52.
13 *Ibid*. at para. 69.
14 *Ibid*. at paras. 56 and 62.
15 *Ibid*. at para. 16; *Jones,* supra *note 1* at para. 67.
16 S.C. 2000, c. 5.
17 *Criminal Code*, R.S.C., 1985, c. C-46.
18 *The Intimate Image Protection Act*, C.C.S.M. c. 187, s. 11.

• INTERNET OF THINGS: OFFICE OF PRIVACY COMMISSIONER OF CANADA PUBLISHES RESEARCH PAPER ON PRIVACY AND SECURITY RISKS ASSOCIATED WITH RETAIL AND HOME ENVIRONMENTS •

Roberto Ghignone
Borden Ladner Gervais LLP

The Office of the Privacy Commissioner of Canada (the "OPC") published a new research paper on the Internet of Things.[1] The paper focuses, in particular, on issues of privacy and security in retail and home environments.

The Internet of Things is the generic description given to the ability of everyday objects to connect to the internet and/or communicate with other devices or objects. For example, radio-frequency identification (RFID) chips imbedded into goods or objects permit real-time tracking of the objects to which they are attached. Devices and/or objects can also transfer small amounts of data quickly and imperceptibly through near-field communications (NFC) or communicate directly with each other or larger systems.

While interconnected devices and systems are not new, technological advancements such as smartphones and the development of low-cost sensors and wireless networks have significantly increased the ability to monitor, gather, and communicate information about the devices themselves and their environment. It is possible to gather extensive data about the habits and patterns of individuals, based on the uniquely identified mobile devices they carry with them. The amount of data as well as its quality and precision will increase in the future.

The OPC cites forecasts that predict exponential growth: for example, ABI Research predicts that the number of connected devices will increase from 10 billion to 30 billion by 2020, while Cisco Systems forecasts that there will be 50 billion devices connected by that same year.

Internet of Things in the Retail Sector

The prevalence of smartphones and other connected devices in conjunction with the spread of wireless hotspots, Bluetooth, and other networks in public spaces has dramatically increased the amount of information that can be gathered both visibly, such as through smartphone applications associated with loyalty programs, and invisibly, such as data gathered from interactions with a device's radio interfaces (*i.e.*, Bluetooth or WiFi). Retailers can use this data to improve efficiency, through better inventory management and store layouts, or to direct promotions to customers who are in and around their store.

The OPC focused on the issues associated on the invisible collection of information: where small amounts of data, including a device's unique identifier and general location, can be collected without the device connecting to a network. The placement of networks of sensors or beacons in public spaces and retail stores can make it possible to track the movement of electronic devices, and the individuals carrying them, across a large geographical area. These same networks could also be used to send targeted messages or promotions to those devices.

Privacy Concerns

The OPC identified a number of privacy concerns associated with the invisible collection of information about electronic devices. First, even though the data is linked to a uniquely identified device, rather than an individual, the OPC and other entities consider the information collected to be personal information. The reason is that the amount and quality of the data gathered on electronic devices makes it possible to identify individuals and reveal their habits or preferences when this is combined with other publicly available information.

Another privacy concern identified by the OPC is that individuals are generally unaware that this information is being collected and, as such, are not able to consent to its collection. The OPC was of the view that the existing consent

model, which involves a one-size fits all consent, is inadequate and a more nuanced approach is required where consent can be time or location limited. Possible approaches identified by the OPC include creating rules for machine-based decision making or allowing the devices to "learn" what is acceptable behaviour.

A further issue identified by the OPC is that it will be extremely difficult for individuals whose data has been collected to ensure the accuracy of the collected data and to determine which entity to hold accountable.

Security Concerns

The interconnectivity of the devices that make up the Internet of Things will also increase the privacy and security risks faced by organizations and individuals. The large amounts of information that is gathered, or the information-gathering devices themselves, will be vulnerable to attack and/or the theft of data. Similarly, the linking of smart appliances, such as remote power outlets, door locks, televisions, and webcams as well as security systems that are controlled from smartphones with in-home networks will increase the vulnerability of these networks.

One of the primary sources of risk is that the sensors and simple Internet-enabled devices that make up much of the Internet of Things tend to have low security and/or weak encryption capabilities due to "limitations on power, computing capacity, and other factors". This means that firewalls and other security features are unavailable or ineffective. New security solutions or network controls will be required.

Conclusion

The importance and reach of the Internet of Things is expected to increase exponentially in the next few years. As this occurs, privacy and security risks will likely continue to increase. Further research and development will be required to unlock the benefits from the collection of this additional information as well as to mitigate the new privacy and security risks. We may also see governments explore new ways to address consent to the collection, use, and disclosure of information about electronic devices.

[*Editor's note*: **Roberto Ghignone** is an associate in the Ottawa office of Borden Ladner Gervais LLP who specializes in privacy law. Roberto also regularly represents clients in litigation matters in the areas of health law and insurance law. You may contact him at (613) 369-4791 or <RGhignone@blg.com>.]

[1] *The Internet of Things: an Introduction to Privacy Issues with a Focus on the Retail and Home Environments*.

• NOVA SCOTIA COURT STRIKES DOWN CYBER-BULLYING LEGISLATION •

Bethan Dinning
Borden Ladner Gervais LLP

In 2013, Nova Scotia became the first jurisdiction in Canada to implement legislation aimed at protecting victims of online harassment or "cyber-bullying". On December 11, 2015, the Supreme Court of Nova Scotia struck down the *Cyber Safety Act* (the "Act") in *Crouch v. Snell*[1] [*Crouch*], stating that it was contrary to the *Canadian Charter of Rights and Freedoms* (the "Charter") and calling the legislation a "colossal failure".

Legislative Context

The Act was proclaimed on August 6, 2013. It was drafted under heightened public scrutiny and in the months following the death of 17-year-old high school student Rehtaeh Parsons who was bullied, attempted suicide, and subsequently died on April 4, 2013.

The Act was a multi-faceted attempt by the Government of Nova Scotia to make it easier for individuals to report bullying and to give the

courts increased authority to protect victims of cyber-bullying. The main provisions of the Act are as follows:

- Greater powers and responsibilities to principals and school boards through amendments to the *Education Act*;
- Parental responsibility for cyber-bullying in some circumstances;
- Creation of a cyber-investigative unit;
- Victims of cyber-bullying may apply for a protection order from the court, and
- New statutory tort of cyber-bullying, which permits individuals to sue for damages or obtain an injunction.

In addition, the Act provided a broad definition of cyber-bullying that included both adults and minors (under 19 years of age). The Act defined cyber-bullying as

> [A]ny electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way.

Background

Giles Crouch and Robert Snell were former business partners. Their business relationship ended in late 2013 when Mr. Crouch resigned from the company and forfeited half of his shares in the venture amid allegations by both parties of unprofessionalism and misappropriation of funds. The business relationship ended tumultuously. Mr. Crouch and Mr. Snell were both avid users of social media, and Mr. Crouch alleged that in the months following his resignation, Mr. Snell began a "smear campaign" against him on social media.

Mr. Crouch filed an application for a Protection Order under the Act, and it was granted by a Justice of the Peace on December 11, 2014 (the "Protection Order"). The Protection Order was granted on an *ex parte* basis, without notice to Mr. Snell. However, Mr. Snell was later served a copy of the Protection Order, which included the following prohibitions:

- The respondent [Mr. Snell] be prohibited from engaging in cyberbullying of the subject.
- The respondent be restricted (or prohibited) from directly or indirectly communicating with the subject.
- The respondent be restricted (or prohibited) from, directly or indirectly, communicating about the subject.
- Any comments on any social media sites whereby the respondent has made reference to the applicant, either directly or indirectly, are to be removed. Further, any comments on any social media sites directed toward an unnamed or unspecified person(s) are to be removed.

The Court's Decision

In *Crouch*, the court was asked to consider (1) whether to re-confirm the Protection Order under the Act, and (2) whether the Act violates the Charter by infringing on an individual's freedom of expression or by violating an individual's right to life, liberty, and security of the person.

First, the court confirmed that assuming the Act to be Charter compliant, Mr. Snell had engaged in cyberbullying of Mr. Crouch as that term is defined in the Act, and that the behaviour was likely to continue. Therefore, the Protection Order was upheld by the court under the Act, with certain minor modifications. The court also reviewed the broad definition of cyber-bullying under the Act and stated that it does not require "malice" on the part of the person posting comments to social media or elsewhere online.

Second, the court held that the Act violated both ss. 2 and 7 of the Charter guaranteeing freedom of expression and an individual's right to life, liberty, and security of the person. The court concluded that the purpose of the Act was to control or restrict expression. Specifically, the court stated that "prevention of cyberbullying is a purpose that aims to restrict the content of

expression by singling out particular meanings that are not to be conveyed, i.e. communication that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional well-being, self-esteem or reputation".[2] Furthermore, the court concluded that the Act does not provide sufficiently clear standards to avoid arbitrary and discriminatory applications. Rather, the legislature has given a plenary discretion to Justices of the Peace to do whatever seems best in a wide set of circumstances. This was also unsatisfactory under the Charter.

In light of the punishments available under the Act, including fines of up to $5,000 or imprisonment for a term up to six months, the court further held that the Act infringed on an individual's right to life, liberty, and security of the person. In addition, the court concluded that the Act was arbitrary, overbroad (in particular, its definition of cyber-bullying) and not procedurally fair. Therefore, the infringements on an individual's right to life, liberty, and security of the person could not be justified under the Charter.

In light of the above, the court concluded that "The act must be struck down in its entirety. […] To temporarily suspend the declaration of validity would be to condone further infringements of charter-protected rights and freedoms".[3] As such, the *Act* was struck down in its entirety and the Protection Order was declared void and of no effect.

Conclusion

In light of the decision, the Government of Nova Scotia has not announced how it plans to respond. Nova Scotia Justice Minister Diana Whalen has confirmed that the department is considering whether to appeal the decision, rewrite the law, or draft new legislation from scratch.[4] In the meantime and as emphasized by the court in its decision, individuals who are confronted with cyber-bullying will have to seek redress through traditional avenues—namely, civil remedies for causes of action, such as defamation or applicable criminal charges.

The decision in *Crouch* will likely serve as a caution for other provinces looking to introduce legislation intended to protect individuals, in particular children, from online harassment and cyber-bullying. This decision makes clear that courts will not uphold legislation that is far-reaching and overly broad, but rather will uphold the protections for freedom of expression and life, liberty, and security of the person afforded to individuals under the Charter.

[*Editor's note*: **Bethan Dinning** is an associate in the Labour and Employment Group at the Toronto office of Borden Ladner Gervais LLP. She advises employers on a wide range of issues, including employment standards, policies and contracts, wrongful dismissal claims, health and safety, and human rights issues. Bethan has published and presented on a variety of topics, including video surveillance in the workplace and cyber-bullying. You can reach her at (416) 367-6226 or <bdinning@blg.com>.]

---

1 *Crouch*, [2015] N.S.J. No. 536, 2015 NSSC 340.

2 *Ibid*. at para. 112.

3 *Ibid*. at para. 220.

4 Brett Ruskin, "Court Strikes Down Anti-cyberbullying Law Created after Rehtaeh Parsons's Death", *CBC News* (December 11, 2015), <http://www.cbc.ca/beta/news/canada/nova-scotia/cyberbullying-law-struck-down-1.3360612>.