CARTERS
BARRISTERS
SOLICITORS
TRADEMARK AGENTS

CHARITY & NFP LAW BULLETIN NO. 463

FEBRUARY 27, 2020

EDITOR: TERRANCE S. CARTER
ASSISTANT EDITORS: NANCY E. CLARIDGE,
RYAN M. PRENDERGAST AND ADRIEL N. CLAYTON

RECENT ISSUES IN PRIVACY: CASE LAW UPDATE

By Esther Shainblum*

A. INTRODUCTION

Three recent court decisions illustrate the rapid pace of change in the Canadian privacy landscape and the uncertainty in predicting the parameters of individual privacy rights. These cases, discussed below, are (i) the Ontario Superior Court of Justice's decision in *Yenovkian v Gulian*,[1] in which the court recognized the new privacy tort of "publicity placing a person in a false light"; (ii) the Ontario Superior Court of Justice's decision in *Stewart v Demme*,[2] in which a class action was certified for a privacy breach claim, apparently narrowing a previous, inconsistent decision of the court; and (iii) the Court of Queen's Bench of Alberta's decision in *R v Bykovets*,[3] in which it was held that there is no reasonable expectation of privacy in IP addresses. This *Bulletin* provides brief summaries of these decisions, all of which will have application to charities and not-for-profits in a privacy context.

B. YENOVKIAN v GULIAN

On December 17, 2019, Justice Kristjanson of the Ontario Superior Court of Justice recognized a new privacy tort of "publicity placing person in false light" in the case of *Yenovkian v Gulian*. This case adds a fourth cause of action to the three invasion of privacy torts previously recognized in Ontario: intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; public disclosure of embarrassing

* Esther Shainblum, B.A., LL.B., LL.M., CRM, practices in the areas of charity and not-for-profit law, privacy law and health law with the Carters Ottawa office. The author would like to thank Urshita Grover, H.B.Sc., J.D., Student-at-Law for her assistance in preparing this Bulletin.
[1] 2019 ONSC 7279 ["*Yenovkian*"].
[2] 2020 ONSC 83 ["*Stewart*"].
[3] 2020 ABQB 70 ["*Bykovets*"].

private facts about the plaintiff; and appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

This case arose from an egregious divorce and custody battle in which the father, Mr. Yenovkian, had engaged in a lengthy campaign of cyberbullying, attacks and intimidation of his two children, their mother ("Ms. Gulian"), and her parents over the course of years. This conduct included publicly posting significant personal information of the children on the internet; posting edited and labelled pictures and videos of the children, including critical comments about them; creating a website focused on Ms. Gulian, her parents, and their family business; making serious allegations about Ms. Gulian and her family, including that she is a kidnapper, that she drugs and abuses the children, that she forges documents, and that she defrauds governments; making multiple false complaints to various authorities, including the police and child welfare authorities; starting a GoFundMe campaign and an online petition against Ms. Gulian "to save an abducted autistic girl from captivity"; inviting the public to engage in cyberbullying of Ms. Gulian; putting up posters of Ms. Gulian and her parents across London, England, where she resides; and distributing flyers containing these allegations to members of her community, her church and her co-workers.[4] These actions led to Ms. Gulian to fear for her and her family's safety – both physical and psychological – in addition to having an impact on her mental health.

The tort of "publicity placing a person in a false light" was the last item in the "four-tort catalogue" of causes of action for invasion of privacy described by the Ontario Court of Appeal in *Jones v. Tsige*.[5] The court determined that "this [was] the case in which this cause of action should be recognized," and adopted the following statement concerning the elements of the tort: "(a) the false light in which the person was placed would be highly offensive to a reasonable person and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed."[6] The court noted that defamation is not required and that it is enough for the plaintiff to show that a reasonable person would find it highly offensive to be publicly misrepresented as they have been. The wrong is in publicly representing someone, not as worse than they are, but as other than they are. It noted

[4] *Yenovkian*, *supra* note 1, paras 19-26.
[5] 2012 ONCA 32 ["*Jones*"]. For further information on this case, see Barry W Kwasniewski, *Charity & NFP Law Bulletin No. 277*, "'Intrusion Upon Seclusion' New Tort from Ontario Court of Appeal" online: Carters Professional Corporation <http://www.carters.ca/pub/bulletin/charity/2012/chylb277.pdf>.
[6] *Yenovkian*, *supra* note 1, para 170.

that the value at stake is respect of a person's privacy right to control the way they present themselves to the world.[7]

The court noted that this tort is similar to the tort of "public disclosure of private facts" in that both share common elements of (1) publicity that is (2) highly offensive to a reasonable person. However, in "public disclosure of private facts" true facts are disclosed in a situation in which there is no legitimate public concern justifying the disclosure, while the "false light" tort involves false or misleading claims that are made by a defendant who knows or is reckless to the falsity of the information. The court stated that one who subjects another to highly offensive publicity should be held responsible whether the publicity is true or false, which is why the "false light" tort should be recognized.[8] The court found that Mr. Yenovkian had committed both "false light" as well as "public disclosure of private facts" torts and awarded damages of $100,000 for the invasion of privacy torts, noting the increased potential for harm given that the publicity is by way of the internet. The court also awarded damages of $50,000 for intentional infliction of mental suffering and punitive damages of $150,000 due to Mr. Yenovkian's outrageous, egregious and reprehensible conduct.[9]

The new "false light" tort is a significant risk exposure to charities and not-for-profits if their employees and volunteers post information on the Internet that could place a person in a false light. Charities and not-for-profits should have robust "appropriate use of technology" and "social media policies" in place to minimize the risk of liability.

C. STEWART v DEMME

On January 6, 2020, Justice Morgan of the Ontario Superior Court of Justice certified a class action in *Stewart v Demme*, a case arising from a nurse's improper access to individual patient health records at the William Osler Heath System ("Hospital"). Over a nearly ten-year period, the nurse had briefly but improperly accessed the records of nearly 12 thousand hospital patients in order to illegally obtain narcotic drugs. The nurse accessed each patient's file for a minute or so, viewing their name, patient identification number, hospital unit location and any applicable allergy information, in order to obtain the drugs.[10] The

[7] *Ibid*, para 171.
[8] *Ibid*, paras 172-173.
[9] *Ibid*, paras 192-193.
[10] *Stewart*, *supra* note 2, paras 8, 12.

plaintiffs sought certification as a class action on the basis that, *inter alia*, the defendants were liable under the tort of "intrusion upon seclusion" as a result of the nurse's improper access to patient health records. The tort of "intrusion upon seclusion" is made out where a person intentionally intrudes on the seclusion of another or his private concerns and the invasion would be "highly offensive to a reasonable person."[11]

In certifying the class action, the court rejected the defendants' argument that these infringements were too trivial to constitute "intrusion upon seclusion", stating that an infringement of privacy can be "highly offensive" without leading to substantial damages. It also rejected an overemphasis on the "fleeting" nature of the nurse's access to each class member's data as this would "unduly minimize the intrusion".[12]

In arriving at its decision, the court also distinguished this case from the rather perplexing decision of the Ontario Superior Court of Justice in *Broutzas v Rouge Valley Health System*,[13] which had found that the tort of "intrusion upon seclusion" was not made out in a case in which hospital patient contact information had been used to sell RESPs to the parents of newborns. While the facts of the two cases were similar in that the health records of hospital patients were improperly accessed, the court found that the two cases could be distinguished on the basis of their differing contexts. In *Broutzas*, the patients seeking certification were in the hospital for birth of their babies and had made announcements about the births on social media, making the expectation of privacy "negligible". In contrast, the claimants in the case at hand were in the Hospital for various procedures that would not ordinarily be publicly broadcast. As stated by the court "Indeed, merely learning that a patient was in the Hospital could be an invasive acquisition of private health information" and the "Hospital is a uniquely private and confidential institution" with a mandate to keep health records private and safe.[14]

Arguably more aligned with Ontario's *Personal Health Information Protection Act* and with fundamental privacy law principles than *Broutzas*, the decision in *Stewart v Demme* may be a welcome narrowing of *Broutzas* and reflects the continuing unpredictability of privacy law in Canada at this time.

[11] *Jones*, *supra* note 5, para 19.
[12] *Ibid*, paras 67, 79.
[13] 2018 ONSC 6315 ["*Broutzas*"].
[14] *Jones*, *supra* note 5, paras 44, 66.

D. R v BYKOVETS

On January 29, 2020, the Court of Queen's Bench of Alberta released *R v Bykovets*, a decision that adds to the uncertainty around the parameters of individual privacy rights in Canada. The accused in this case was facing charges relating to the possession and use of third parties' credit cards and personal identification documents. Defence counsel brought an application alleging, *inter alia*, that the accused's right to be secure against unreasonable search and seizure under section 8 of the *Canadian Charter of Rights and Freedoms* ("*Charter*") had been violated because the Calgary Polices Service ("CPS") obtained his and his father's Internet Protocol ("IP") addresses from a third party without judicial authorization. CPS then applied for and obtained a production order for the subscriber information associated with the IP addresses, followed by a search warrant to search the homes of the subscribers.

In order to determine whether the accused's section 8 Charter rights had been violated, the court had to consider whether the accused had a reasonable expectation of privacy in his IP address. Applying the tests set out by the Supreme Court of Canada ("SCC") in *R* v *Spencer*[15] and in *R v. Marakah*,[16] the court concluded that it is not objectively reasonable to recognize a subjective expectation of privacy in an IP address used by an individual.[17] The court felt that IP addresses do not, on their face, appear to reveal intimate details about the lifestyle and personal choices of individuals, and rejected the defence's argument that, in a free and democratic society, one would not expect a company to turn over information to the police without some form of judicial authorization. Instead, the court found that an IP address does not reveal information about a subscriber that should be protected in a free and democratic society.[18]

The court distinguished the facts of this case from previous cases that had found that there was a reasonable expectation of privacy in international mobile subscriber identity ("IMSI") and international mobile equipment identity ("IMEI") numbers, stating that, while significant amount of personal information could be gleaned about a particular individual through IMSI and IMEI numbers, the nature, quantity and quality of personal information gleaned from an IP address is limited and that there is a significant difference between the nature of the information or what may be inferred when the police obtain an IP address as

[15] 2014 SCC 43.
[16] 2017 SCC 59.
[17] *Bykovets*, *supra* note 3, para 61.
[18] *Ibid*, paras 62-65.

compared to an IMEI or IMSI number.[19] The court acknowledged that the police might be able to obtain information about a user's identity from an IP address, but that there are significant limitations on this. The court went on to say that "obtaining an IP address is an important investigative step for police, but privacy interests are not triggered by mere police investigation."[20]

It is difficult to reconcile the court's acknowledgement that obtaining IP addresses is an important investigative step for police and that the police might be able to obtain user information from them, with its ultimate finding that there is no reasonable expectation of privacy in IP addresses. It is to be hoped that future decisions will clarify this issue.

E. CONCLUSION

Privacy continues to be a volatile area of the law. Charities and not-for-profits should keep abreast of new developments, including evolving case law as reported upon above, to ensure that they are aware of changes and can better manage their privacy and data security risk exposures.

CARTERS

Carters Professional Corporation / Société professionnelle Carters
Barristers · Solicitors · Trademark Agents / Avocats et agents de marques de commerce Toronto · Ottawa · Orangeville
www.carters.ca www.charitylaw.ca www.antiterrorismlaw.ca **Toll Free: 1-877-942-0001**

00449703.DOCX

[19] *Ibid*, paras 40,41.
[20] *Ibid*, para 62.