Durham Community Legal Clinic
& Access to Justice Hub

10/16/2020

Ontario Private Sector Privacy Reform

Proposal:20-MGCS015

About the Durham Community Legal Clinic

The **Durham Community Legal Clinic** (DCLC) is a community legal clinic, primarily funded by Legal Aid Ontario (LAO). It was founded in 1985, and provides legal services, information, education, and representation for historically marginalized and low-income residents of Durham Region. DCLC also engages in advocacy and law reform activities, in particular to ensure that our laws properly consider the perspectives of historically marginalized and low-income Ontarians.

In early 2019, DCLC established the **Durham Access to Justice Hub**® (the "Hub) with the assistance of LAO. This inter-agency and inter-disciplinary initiative intended to provide legal services beyond the income thresholds and subject matter of LAO, and other social, financial, and psychological services. These cooperative relationships seek to foster better client-centered services, reduce administrative barriers and silos, and improve efficiency of services that are funded or subsidized by taxpayer dollars. Some techniques used to achieve these goals include recruitment of volunteers to contribute towards improving access to justice, and by embedding students into workflows and innovative projects through experiential education.

About the Author

Omar Ha-Redeye is the Executive Director of the Durham Community Legal Clinic, a Community Legal Clinic funded primarily by Legal Aid Ontario that provides legal information, services, advocacy, and law reform efforts on behalf of low-income Ontarians. He holds a JD from Western University, and an LLM from Osgoode Hall. He has received numerous recognitions and awards for advocacy and law reform efforts, especially on behalf of historically marginalized and low-income populations.

Omar is a part-time professor at Ryerson University, where he teaches LAW 723 – Issues in Information Technology Law, in the School of Law & Business, which covers the right to be forgotten, data portability, deidentified data, and using data for innovation. He also teaches JUR - 102 Tort Law in the new Faculty of Law, which includes a review of privacy torts.

About the Researchers

Jessica Barbosa is a first-year law student at Ryerson's Faculty of Law, and a volunteer with the Durham Community Legal Clinic. She is a graduate of the University of Guelph, with a Bachelor of Arts Degree in Criminal Justice & Public Policy and Political Science, as well as a Masters Degree in Criminology and Criminal Justice Policy.

Jessica has participated in two community-based research projects; The 2016-2017 Femicide Report with OAITH, and Safety Planning Guidelines for Victim Services Guelph-Wellington in 2017-2018. Jessica is passionate about helping her communities, and hopes to use her education and research skills to help expand access to justice for Ontarians.

Page MacRae is a first-year law student at Ryerson's Faculty of Law, and a volunteer with the Durham Community Legal Clinic. She completed her Honours Bachelor of Arts at Queen's University with a major in Health Studies and a double minor in Commerce and Employment Relations. Unlike many other law programs, Ryerson University appealed to Page because of their progressive and forward-looking approach to the study of law.

Kevin Zhou is a first-year law student at Ryerson's Faculty of Law, and a volunteer with the Durham Community Legal Clinic. He graduated from McGill University in 2020 with a BA, double majoring in Economics and Political Science with a minor in East Asian Cultural Studies.

Introduction

1. Privacy law, as we currently understand it, is a relatively new concept. It has developed and has been informed by advances in technology, and the reality that so much of our lives that used to be private is now acquired, stored, and shared electronically.
2. Notions of privacy in the common law, which were very much limited to personal physical spaces like the home and the activities that might occur within the home, as contrasted with activities that occur in public, fail to properly encapsulate the privacy concerns of modern living.
3. As contemporary notions of privacy could never have been envisioned at the time of Confederation, the area of privacy is of overlapping and sometimes concurrent jurisdiction under the constitution. This makes the development of statutes in this area challenging at times, especially if there is concern of potential overlap. However, the needs of the public, including the need for government to utilize digital innovation to improve its services, requires further actions.
4. This submission to the Ministry of Government and Consumer Services (MGCS) will attempt to address some of the gaps of the legislative framework for privacy in Ontario, with a particular focus on the needs of historically marginalized and low-income populations. We believe that an equity-oriented lens to regulatory reform in the area of privacy will also help nurture innovation in Ontario in an inclusive manner, which is always better for our local businesses, associations, and other organizations.
5. Included in these submissions are themes of how Ontarians should access or have control over their own data when they interact with business and organizations in the private sector.

In order to do this, Ontarians need to be fully informed about how personal information is used, be able to withdraw consent when necessary, and be provided statutory monetary remedies if these private entities fail to fulfill their obligations.

6. An enhanced provincial statutory framework providing these obligations and remedies will provide greater clarity in the law, which is the best way to ensure that any unnecessary burdens are not imposed on businesses, and to promote the growth and prosperity of innovation in Ontario. In doing so, we will refer to a 2015 journal article on privacy law class actions to provide an overview of the current legislative schemes in place,[1] attached as Appendix "A," and provide some updates of the law since that time. We will then explain why these privacy issues need to be codified into statute.
7. The current patchwork of ever-changing privacy protections in the common law is unclear and confusing for consumers and businesses alike, and a provincial privacy statute should streamline these interest and expectations.

Current Privacy Law Scheme

8. Canada's earliest responses to privacy concerns and data protection was through privacy specific legislation introduced in 1985 under the *Privacy Act*.[2] This act also created the Privacy Commissioner of Canada, who operates as an ombudsman and to audit the federal government. However, the *Privacy Act* alone proved "woefully inadequate" in a digital era, prompting Parliament to introduce new legislation in 1999.

[1] Omar Ha-Redeye, "Class Action Intrusions: A Development In Privacy Rights or an Indeterminate Liability?," *The Western Journal of Legal Studies 6:1* (2015) ["*Class Action Intrusions*"], available at: <https://ojs.lib.uwo.ca/index.php/uwojls/article/view/5637>; Appendix "A."
[2] RSC 1985, c P-21.

9. The concepts of privacy found in *PIPEDA* can be traced the academic commentary of American jurists over a century ago.[3] International law instruments in the modern era have highlighted the need to protect privacy, and also informed the creation of *PIPEDA*.[4]
10. PIPEDA potentially applies to all private-sector organizations in Canada that collect, use or disclose personal information for commercial purposes. It covers all federally regulated organizations that conduct business in Canada, as well as provincially regulated organizations where the province does not have a substantially similar provincial privacy law, or where the provincial privacy law does not cover an area that is covered by *PIPEDA*.
11. Other organizations or activities that are not covered by *PIPEDA* is personal information covered by federal organizations that are included in the *Privacy Act*, provincial governments or their agents, business contact information, or information collected exclusively for journalistic, artistic or literary purposes.[5]
12. Periodic reviews of *PIPEDA* are contemplated in s. 29 of the Act, and some changes have occurred over the years. Although changes were proposed to *PIPEDA* under Bill C-29 (40-3), *An Act to amend the Personal Information Protection and Electronic Documents Act* in 2010, it died on the order paper. It was re-introduced in 2011 under Bill C-12 (41-1), *Safeguarding Canadians' Personal Information Act*, but this was not implemented either. A Senate Bill S-4, *Digital Privacy Act* did receive Royal Assent in

[3] https://www.priv.gc.ca/en/opc-news/speeches/archive/02_05_a_000128/
[4] Instruments of international law prompting these changes include: *Universal Declaration of Human Rights*, GA Res 217A (III), UNGAOR, 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71; *International Covenant on Civil and Political Rights* (ICCPR), December 19, 1966, [1976] Can TS No 47; *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221, Eur. T.S. 5 ("European Convention on Human Rights"); *American Convention on Human Rights, adopted at the Inter-American Specialized Conference on Human Rights*, San José, Costa Rica, 22 November 1969, OASTS No 36; 1144 UNTS 123.
[5] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

June 2015, changing elements of valid consent, the Commissioner's powers, exceptions to consent, and other matters.

13. Almost 20 years after the inception of *PIPEDA*, the federal government launched a discussion paper in 2019[6] on creating a "Digital Charter."[7] This discussion is still underway, but is likely to result in further amendments to the act.

Privacy Torts

14. The emergency of privacy law torts in Ontario occurred specifically because of legislative gaps in the privacy law statutory scheme, specifically due to the lack of private action against an individual. Justice Sharpe in *Jones v. Tsige,*[8] canvassed the existing legislation at the time, found it to be insufficient, before creating Ontario's first privacy tort of intrusion upon seclusion.

15. Since that time, two new torts have been added in Ontario; public disclosure of private facts,[9] and publicity placing a person in a false light.[10] However, the former has had some significant issues around enforcement, with an outcome that likely diminishes any deterrent effects this tort may have.[11] The latter emerged in the family law context, and may not be as applicable at this time in the private law or commercial contexts.

---

[6] Government of Canada, "Strengthening Privacy for the Digital Age," May 21, 2019, available at: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html>.
[7] Government of Canada, "Canada's Digital Charter in Action: A Plan by Canadians, for Canadians," Oct. 23, 2019, available at: <https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html>.
[8] 2012 ONCA 32.
[9] *Doe 464533 v N.D.*, 2016 ONSC 541; 2017 ONSC 127; *Jane Doe 725111 v Morgan*, 2018 ONSC 6607.
[10] *Yenovkian v. Gulian*, 2019 ONSC 7279.
[11] Omar Ha-Redeye, "The Uncertain Future of Public Disclosure of Private Facts," Slaw, Jan. 22, 2017, available at: <http://www.slaw.ca/2017/01/22/the-uncertain-future-of-public-disclosure-of-private-facts/>. See, however, its use in a subsequent case, *Jane Doe 725111 v Morgan*, 2018 ONSC 6607; Omar Ha-Redeye, "Public Disclosure of Private Facts – Redux," Slaw, Nov. 11, 2018, available at: <http://www.slaw.ca/2018/11/11/public-disclosure-of-private-facts-redux/>.

16. What is clear is that privacy issues are important and pressing ones facing the public, and that there will continue to be litigation in these areas in the years to come. A statutory right of action for this privacy interests would streamline these claims, and reduce uncertainty and risk around privacy considerations. This would assist historically marginalized and low-income Ontarians specifically, as they would not have the same access to the common law as the rest of the population, whereas a statutory right is typically more accessible. Low-income Ontarians are also less likely to provide informed and meaningful consent for the disclosure of private information, meaning there are particular vulnerabilities that need to be addressed.

17. The need for a statutory right for privacy torts can also be found in the context of privacy class actions.[12] Bill 161, *Smarter and Stronger Justice Act, 2020* amended various class action procedures, largely out of a concern that these actions were generally becoming costly and taking up valuable court resources. The inadvertent affect of this though might be a diminished ability to utilize privacy torts in this way.[13]

18. Codifying these privacy torts into statute will invariably create more predictability and stability in the area of privacy law, rather than leaving this area to be developed further by the common law. Clarity around the expectations of businesses therefore reduces the risk around data use and respect for individual privacy, and is more likely to spurn innovation and allow businesses in this sector to grow.

[12] Although *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A was amended most recently in 2019 under Bill 119, *Health Information Protection Act, 2016*, it's still uncertain whether it will be effective in addressing the concerns outlined in Appendix "A."

[13] Omar Ha-Redeye, "Class Proceedings Changes Proclaimed in Ontario," Sept. 20, 2020, available at: <http://www.slaw.ca/2020/09/20/class-proceedings-proclaimed-in-ontario/>.

International Considerations

19. Ontario increasingly is engaged in trade beyond its provincial boarders, and even abroad. The estimated trade between Ontario and the European Union has been steadily increasing over the past years, with the EU comprising 10.19% of all global goods exports from Ontario in 2019, and 9.58% of all goods imports in 2019.[14]
20. The European Commission introduced the General Data Protection Regulation (GDPR) in 2018, which set greater requirements for anyone doing trade with the EU to privacy interests. GDPR also introduced a right for individuals to have personal data erased under Art. 17, also known as a right to be forgotten.[15]
21. Also in 2018, the Office of the Privacy Commissioner of Canada indicated an interest in gleaning a right to be forgotten in *PIPEDA*, even filing a court application in the process.[16] These proceedings are still ongoing, meaning that there is not clarity on the applicability of these principles in Ontario yet, but any privacy law initiatives in the province may need to anticipate or be responsive to any court decision that may give effect to these interests or rights.[17]
22. The other critical aspect of GDPR that does not yet exist in Ontario is data portability. Data portability is generally the idea that you can request and access your information in portable standardized formats to take to and from service providers.

---

[14] https://www.sourcefromontario.com/tradefactsheet/en/page/tradefactsheet.php?countryid=all&type=EU
[15] Omar Ha-Redeye, "Regulating the Future Flows of Big Data Overseas," Slaw, Aug. 27, 2017, available at: <http://www.slaw.ca/2017/08/27/regulating-the-future-flows-of-big-data-overseas/>.
[16] Omar Ha-Redeye, "Challenges Around the Right to Be Forgotten in Canada," Slaw, Jan. 28, 2018, available at: <http://www.slaw.ca/2018/01/28/challenges-around-the-right-to-be-forgotten-in-canada/>; Omar Ha-Redeye, "Right to Be Forgotten Referred to Federal Court," Slaw, Oct. 14, 2018, available at: <http://www.slaw.ca/2018/10/14/right-to-be-forgotten-referred-to-federal-court/>.
[17] Additional concerns are raised in light of the Supreme Court of Canada's decision in *R. v. Vice Media Canada Inc.*, 2018 SCC 53 (CanLII), [2018] 3 SCR 374. See Omar Ha-Redeye, "Need for Greater Protections of Investigative Journalism," Slaw, available at: <http://www.slaw.ca/2018/12/02/need-for-greater-protections-of-investigative-journalism/>.

23. The ease of duplication for data poses a significant barrier to data portability. Standardized formats or partitioned "data cards" would necessarily rely on the "right to be forgotten" to be effective in a rights-based approach.
24. Any relevant changes to *PIPEDA* or other privacy statutes that seeks to unify itself with GDPR would have to address the extinguishment of data under personal and state, to promote these ideas of data erasure and data portability.

Conclusions

25. Privacy law in Ontario is rapidly changing, due to an increased interest by the public in greater protections, an increased emphasis by businesses and industries to utilize data, and regulatory changes in jurisdictions where Ontario maintains significant trade ties.
26. Ontario should draft and introduce legislation for debate before the legislature, and further submissions at committee, to properly address the needs and interests of the public, and the growing requirements for certainty in this sector. Of particular interest would be a statutory basis for privacy torts, and greater development of common standards across shared markets.
27. DCLC would be interested in providing further comment on this legislation, with a particular emphasis on historically marginalized and low-income populations, and in light of the social and economic needs and interests of these populations.

Appendix “A”

Western Journal of Legal Studies

Volume 6 |

Issue 1 *Law: Helping Hand or Iron Fist?* Article 1

2015

Class Action Intrusions: A Development In Privacy Rights or an Indeterminate Liability?

Omar Ha-Redeye
Fleet Street Law, omar@fleetstreetlaw.com

Class Action Intrusions: A Development In Privacy Rights or an Indeterminate Liability?

Abstract
Since its inception in *Jones v Tsige*, legal practitioners have struggled with the tort of intrusion upon seclusion. The limited damages awarded in that case, and what the court indicated would be reasonable for privacy breaches, suggested that the tort would have limited utility as a stand-alone cause of action, and may only arise in in conjunction with other claims. However, the tort has recently been used successfully, at least at the summary judgment level, particularly in the class actions context where the aggregate claims make it more feasible to rely on the tort exclusively. In the wake of The Ontario Court of Appeal's decision in *Hopkins v Kay*, this paper examines intrusion upon seclusion in the context of privacy breaches in the healthcare sector. This work purports to show that although a statutory regime exists to govern healthcare privacy breaches in Ontario and other provinces in Canada, intrusion upon seclusion is the best method for addressing privacy breaches in this context.

Keywords
class actions, intrusion upon seclusion, jones v tsige, civil litigation, hopkins v kay, healthcare law, tort law, privacy law

CLASS ACTION INTRUSIONS: A DEVELOPMENT IN PRIVACY RIGHTS OR AN INDETERMINATE LIABILITY?

OMAR HA- REDEYE*

INTRODUCTION

In 2012 the Ontario Court of Appeal created the tort of intrusion upon seclusion in *Jones v Tsige*.[1] In that case, the defendant bank employee accessed the plaintiff's private financial information 174 times.[2] Adopting the American definition, the court defined the tort of intrusion upon seclusion as follows:

> 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.[3]

In other words, the tort is aimed at defendants who intentionally violate the privacy of a plaintiff in a highly offensive way. The court reviewed the existing legislative regime and concluded that the remedies available to the plaintiff were insufficient: a common law privacy remedy was needed.

The Ontario Court of Appeal indicated that damages for breaches of intrusion upon seclusion would be modest, raising concern about the tort's practical significance in litigation.[4] However, the use of this tort in class actions[5] has largely put this concern to rest.[6] Since class actions allow for the aggregation of cases and the accumulation of sizable awards, it may increase the financial feasibility of intrusion upon seclusion litigation.

Condon v Canada[7] was the first intrusion upon seclusion claim to be certified as a class action in Canada. The representative plaintiff was successful in

---

* Omar Ha-Redeye, AAS, BHA (Hons), PGCert, JD, LLM, CNMT, RT(N)(ARRT) Principal, Fleet Street Law. Adjunct Faculty at Ryerson University, Seneca College and Centennial College. Special thanks to Kaleigh Hawkins-Schulz of Western Law (2018), and Desron Harry, Rohini Talwar, and Matthew Gyimadu of the Centennial College Paralegal Program (2015) for their assistance with this paper.

[1] *Jones v Tsige*, 2012 ONCA 32 [*Jones*]; Omar Ha-Redeye, "New Tort of Intrusion Upon Seclusion and Electronic Health Records" (Paper delivered at Lorman Educational Services Live Seminar, 4 December 2014) [unpublished, archived at <http://ssrn.com/abstract=2533987>].

[2] *Ibid* at para 2.

[3] *Ibid* at para 19.

[4] Glenn Kauth, "Legal aid employee to pay $7,500 for intrusion upon seclusion", Canadian Lawyer Magazine (10 November 2014), online: <http://www.canadianlawyermag.com/legalfeeds/2373/legal-aid-employee-to-pay-7-500-for-intrusion-upon-seclusion.html>.

[5] This paper uses the terms class actions and class proceedings interchangeably.

[6] Arshy Mann, "Focus: Privacy class actions on the rise", *Law Times* (1 September 2014), online: <http://lawtimesnews.com/201409014155/focus-on/privacy-class-actions-on-the-rise>.

[7] 2014 FC 250.

demonstrating a common issue, despite differences in the circumstances of each breach, for a class of Canadians who allegedly had their privacy breached when an external hard drive of the Federal Minister of Human Resources and Skills Development was lost. While the first of these cases mainly dealt with the disclosure of confidential financial information for fraudulent and improper purposes,[8] the tort has evolved since *Jones*, and has been used as a claim in various other contexts.[9]

Notably, in *Hopkins v Kay*,[10] the Ontario Court of Appeal held that an intrusion upon seclusion claim could be brought by the plaintiff despite the existence of a statutory regime governing privacy breaches in the health sector. In expanding the common law remedy to the health care sector, *Hopkins* highlighted several issues including: (1) the potential increased liability faced by health institutions for privacy breaches; (2) the possible strengthening of individual privacy rights in the health care sector given new initiatives to minimize this potential liability; and (3) the usurping by the courts of statutory enforcement mechanisms, which have proved ineffective in preventing privacy breaches. These observations indicate that intrusion upon seclusion claims may play a central role in enhancing patient privacy in the future.

This paper will examine the practical purposes of class action litigation paying particular attention to how class actions may be used with intrusion upon seclusion claims. Further, the paper will review how *Jones* has been used in subsequent cases. I will argue that class action intrusion upon seclusion claims, despite the existence of statutory mechanisms, may be the most viable means to foster individual privacy rights in the health care sector. Part One will provide a brief background of class actions in Canada and explore this unique procedure's relationship with intrusion upon seclusion generally. Part Two will focus specifically on health information class action intrusions. The class actions procedure will be compared with other mechanisms, such as the current Ontario legislative framework, for fostering greater individual privacy protections in Canada. The article will conclude with a discussion of alternatives to vicarious liability for intrusion upon seclusion claims, including regulatory colleges and vicarious liability. I will argue that these methods alone are insufficient for fostering a robust privacy regime. Indeed, given the other mechanisms available, tort law may be the best incentive for advancing protections and controls of sensitive patient information in the health sector rather than being overkill in liability.

[8] See for example, *Rosati v Cornelio,* 2013 ONSC 6461; *Alberta v Alberta Union of Provincial Employees (Privacy Rights Grievance)* (2012), 221 LAC (4th) 104 (Alb Grievance Arb).

[9] See for example, *Trout Point Lodge Ltd v Handshoe*, 2012 NSSC 245 [*Trout Point Lodge*]; *Leung v Shanks*, 2013 ONSC 4943 [*Leung*] (where intrusion upon seclusion claim that defendant used plaintiff's personal information disclosed to a fertility clinic was dismissed).

[10] 2014 ONCA 112 [*Hopkins* CA].

I. OVERVIEW OF CLASS ACTIONS IN CANADA

A. Background and Benefits of Class Actions in Canada

While Québec has had class action legislation since 1978,[11] Ontario did not enact similar legislation until 1992 with the *Class Proceedings Act, 1992*.[12] British Columbia,[13] Saskatchewan,[14] Newfoundland,[15] Manitoba,[16] and Alberta[17] passed similar statutes by 2003. Nova Scotia[18] and New Brunswick[19] passed their respective class actions legislation in 2007 and 2011. Prior to the enactment of the *Class Proceedings Act, 1992*, Rule 75 of the *Rules of Civil Procedure*[20] governed class proceedings in Ontario, which effectively made class actions in Ontario a common law proceeding. Rule 75 was a deficient method to bring a class action because it permitted the representative plaintiff to bind the class without the knowledge or consent of its members, which resulted in inadequate judicial oversight to ensure that the interests of the class members were properly represented.[21]

The Ontario *Class Proceedings Act, 1992* identifies the goals of class actions as (1) improving access to justice; (2) increasing the efficiency and efficacy of managing complex cases; and (3) coercing behavioural "modification through public accountability."[22] First, class actions aim to improve access to justice by reducing the cost of litigation. Class proceedings are typically commenced on a contingency-fee basis, where the cost of litigation is frequently borne by the law firm commencing the claim. When a law firm cannot fund a claim, third-party commercial funding[23] or disbursements from the Class Proceedings Fund[24] are available. Second, the judicial efficiency and efficacy are improved because courts can address similar claims together, rather than hearing separate claims from each individual plaintiff. As class actions many have hundreds of plaintiffs, this can be a substantial change, which saves scarce court resources and avoids the use of several judges on the same issue. Third, class proceedings foster behaviour modification,

---

[11] *An Act Respecting the Class Action*, CQLR c R-2.1.
[12] SO 1992, c 19.
[13] *Class Proceedings Act*, RSBC 1996, c 50.
[14] *The Class Actions Act*, SS 2001, c C-12.01.
[15] *Class Actions Act*, SNL 2001, c C-18.1.
[16] *Class Proceedings Act*, CCSM, c C130.
[17] *Class Proceedings Act*, SA 2003, c C-16.5.
[18] *Class Proceedings Act*, SNS 2007, c 28.
[19] *Class Proceedings Act*, RSNB 2011, c 125.
[20] RRO 1990, Reg 194 [*Rules of Civil Procedure*].
[21] Law Commission of Ontario, *Review of Class Actions in Ontario: Issues to be Considered* (Toronto: Law Commission of Ontario, November 2013) at 1 [LCO Report].
[22] *Ibid* at 1; see also *Western Canadian Shopping Centres Inc v Dutton*, 2001 SCC 46.
[23] Aaron Dantowitz, "Commercial Third Party Funding of Class Actions in Ontario: Eight Early Lessons" (Paper delivered at the Second Annual Securities Litigation Practice Group Symposium, 13 September 2012) [unpublished, archived at <http://www.stockwoods.ca/wp-content/uploads/2012/01/Third_Party_Funding-Final.pdf>].
[24] *Law Society Act*, RSO 1990, c L8, s 59.1.

since they aim to deter potential defendants by ensuring compliance with the law and the proper provision of goods and services to the market.[25]

Where the privacy breach by a potential defendant is borne by many plaintiffs, class proceedings are the preferable means to advance intrusion upon seclusion claims. Importantly, limited damages are available for such breaches with individual claimants: damages for intrusion upon seclusion are capped at $20,000.[26] The size of these awards would normally place individual plaintiffs in the Small Claims Court's jurisdiction in Ontario.[27] However, given the extensive rules for discovery and productions available to trial courts class proceedings arguably allow for a more rigorous examination of the evidence and a more thorough investigation of the claims being made. Moreover, the threat of intrusion upon seclusion class actions should encourage potential defendants to take measures to prevent these breaches. The heightened sensitivity to privacy breaches and importance of individual privacy in today's society[28] enables this threat of liability to incentivize institutions to develop proactive measures to prevent these breaches. In turn, this may encourage broader societal change towards stronger privacy protections, which is necessary given the outdated privacy law regime.[29]

B. Intrusion Upon Seclusion In Its Infancy

Use Of The Tort

Early intrusion upon seclusion cases frequently used the tort to supplement other claims[30] because the corresponding modest damages did not justify using the tort alone in litigation commenced by individuals. To date, *Jones* has been referenced in nearly fifty cases but only a small number of decisions make a finding on the tort. Many of these reported decisions have stalled on interlocutory judgment, summary judgment motions, or on a certification motion for class proceedings.[31] Likely, in certification motions for class actions, a similar stall will emerge in the form of not disclosing a reasonable cause of action. However, the reasonable cause of action test is a low threshold. The substantive merits of a claim are not evaluated beyond the pleadings standard under Rule 21 of the *Rules of Civil Procedure*.[32] As

[25] *Hollick v Toronto (City)*, 2001 SCC 68 at para 34 [*Hollick*].
[26] *Jones*, *supra* note 1 at para 87.
[27] *Vertolli v YouTube LLC*, 2012 CanLII 99832 (ON SCSM); *Luu v O'Sullivan*, 2012 CanLII 98396 (Ont Sm Cl Ct).
[28] Michael Geist, "Surveillance Laws Can't Handle Modern Snooping Technologies", *Toronto Star* (14 June 2013), online: <http://www.thestar.com/business/2013/06/14/surveillance_laws_cant_handle_modern_snooping_technologies.html>.
[29] *Ibid*.
[30] See e.g. *Leung*, *supra* note 9.
[31] See e.g. *Ari v Insurance Corp. of British Columbia*, 2013 BCSC 1308; *Ladas v Apple Inc*, 2014 BCSC 1821.
[32] *Rules of Civil Procedure*, *supra* note 20, ss 21.1–21.03.

such, the full scope of intrusion upon seclusion claims, and its impact on tort law generally, has yet to be determined.

Where an intrusion claim has been advanced as the sole head of damages, the damages have been modest. In *McIntosh v Legal Aid Ontario*,[33] the plaintiff was awarded damages for a privacy breach against the defendant who worked at Legal Aid Ontario. The defendant accessed the Children's Aid information of the plaintiff, the defendant's current boyfriend's ex-girlfriend. The boyfriend disclosed this breach to the ex-girlfriend, who threatened to use this information to take away the plaintiff's children. As a result, the plaintiff claimed she suffered "substantial anxiety, emotion [*sic*] upset, depression, significant stress, embarrassment, weight loss, insomnia, isolation, and an inability to concentrate at work."[34] While the judge found that the elements of the tort were met, he only awarded the plaintiff $10,000 in damages. Given the arguably serious nature of the breach, it is not clear whether the court would have awarded more damages if the cap was not set so low.

In some stand-alone intrusion upon seclusion claims, courts have rejected or limited the applicability of the tort, thereby demonstrating the potential limits of the use of this claim for a breach of privacy. For example, in *Complex Services Inc v Ontario Public Service Employees Union Local 278*,[35] the arbitrator dismissed an intrusion upon seclusion claim in the context of a disclosure of medical information. The arbitrator determined that *Jones* should not be interpreted as establishing an absolute right to privacy for employees and that case did not alter the right of the employer to manage the workplace in a reasonable manner.[36] In *Ludmer v Ludmer*,[37] the applicant pleaded intrusion upon seclusion based on allegations of intercepted email and fax communication in a matrimonial proceeding. The Ontario Court of Appeal upheld the trial court's decision that there was no evidence of the email interception, and that the act of putting documents in a fax machine to the applicant's lawyer was not in itself sufficient for an invasion of privacy claim.[38] Despite the test in *Jones* not being met, the Ontario Court of Appeal upheld the Trial Court's award of damages.[39]

Scope Of The Tort

Despite the potential limits of the tort, Canadian jurisprudence has recognized its arguably broad applicability. For example, in *Trout Point Lodge Ltd v Handshoe*,[40] the plaintiffs relied on *Jones* to make an invasion of privacy claim coupled with a defamation claim. While they failed to establish the elements of

[33] 2014 ONSC 6136.
[34] *Ibid*, at para 8.
[35] 2012 CanLII 8645 (Ont LA).
[36] *Ibid* at para 93.
[37] 2014 ONCA 827 [*Ludmer* ONCA].
[38] *Ibid* at para 70; *Ludmer v Ludmer*, 2013 ONSC 784 at para 313 [*Ludmer* ONSC].
[39] *Ibid*; Ludmer ONCA, *supra* note 37 at paras 47-50.
[40] 2012 NSSC 245.

intrusion upon seclusion, the motions judge affirmed the applicability of the tort in the province by stating, "I am satisfied that in an appropriate case in Nova Scotia there can be an award for invasion of privacy or as the Ontario Court of Appeal called it, 'the intrusion upon seclusion.'"[41] The decision suggests that intrusion upon seclusion claims—and its use in health records class actions—can be used outside of Ontario.

A more extensive analysis of the tort occurred in *Re Alberta and AUPE (Privacy Rights Grievance)*.[42] In this case, twenty-six government employees brought a labour grievance based on access of their private information during a series of unjustified credit checks by a peace officer. The arbitrator distinguished the case from *Jones* because the activity in *Jones* emerged in a commercial, rather than an employment, relationship.[43] The arbitrator also found "the conduct and the harm in this case to be considerably less egregious and damaging" than in *Jones*.[44] While the intrusion claim failed, this case suggests that sensitivities surrounding private information, and the nature of the privacy breach, will play a significant role in how courts apply the tort. In a health care context, it is likely that inappropriate access or disclosure of this information will meet this threshold.

II. CLASS ACTION INTRUSIONS

A. Class Actions for Health Records

Summary of Hopkins

In 2015, the Ontario Court of Appeal released *Hopkins*, a landmark decision that is perhaps the most unanticipated use of the tort of intrusion upon seclusion to date. Specifically, *Hopkins* demonstrated that the tort could be applied not only to the financial sector, as was the case in *Jones*, but also to the health care industry.[45] Like financial institutions, health care organizations collect, store, and use large quantities of private information on a daily basis. Intrusion upon seclusion is particularly relevant in the health care context because of the potential distress and humiliation that individuals may experience if health records are disclosed to the public or to third parties. Historically, Ontario has addressed medical privacy breaches through the *Personal Health Information Protection Act* (*PHIPA*).[46] While *PHIPA* was intended to be comprehensive by covering all aspects of medical data,[47]

[41] *Ibid* at para 55.
[42] [2012] AGAA No 23.
[43] *Ibid* at para 20.
[44] *Ibid* at para 33.
[45] *Hopkins* CA, *supra* note 10 at para 73.
[46] SO 2004, c 3, Schedule A [*PHIPA*].
[47] *Re Hamilton Health Sciences and Ontario Nurses' Association,* 2007 CanLII 73923, 167 LAC (4th) 122 (Arbitrator Surdykowski) at para 20.

Hopkins established that the statute does not preclude the use of a common law claim through intrusion upon seclusion.[48]

In *Hopkins*, the defendant hospital sought to strike the plaintiffs' statement of claim as disclosing no reasonable cause of action, stating that *PHIPA* provided a comprehensive code that precluded a civil action.[49] The defendant's argument was based on two cases from outside of Ontario:[50] *Facilities Subsector Bargaining Association v British Columbia Nurses' Union*[51] and *Martin v General Teamsters*.[52] In both of these cases, the courts found that the statutory schemes in their respective jurisdictions prohibited the use of intrusion upon seclusion as a common law mechanism of privacy enforcement.[53] The defendant in *Hopkins* thus claimed that *PHIPA* was similarly structured in Ontario.

Under *PHIPA*, the mechanism for enforcement in cases of a suspected breach is a complaint to the Information and Privacy Commissioner (IPC),[54] who has discretion to investigate complaints [55] and commence investigations independently.[56] The IPC's powers of investigation are broad, including the power to inspect and to produce records without a warrant.[57] The IPC also requires a health information custodian to change their practices for the use, collection, or disclosure of personal health information. [58] Given this arguably expansive statute, the defendant took the position in *Hopkins* that recognizing a common law cause of action for private health information would usurp the role of the legislature, which intended *PHIPA* to comprehensively govern this area.[59] The trial judge rejected this argument, noting significant differences in the remedies provided by the tort and *PHIPA*, as well as differences in limitations.[60] In *obiter dicta*, the trial judge stated that the explicit reference to *PHIPA* in *Jones* indicated that both the trial judge and the Ontario Court of Appeal were fully aware of the existing statutory regimes in this area.[61] He further noted that both courts in *Jones* conducted an extensive review and were aware of the rulings in other jurisdictions when they chose not to adopt the same reasoning.[62] Ultimately, the judge concluded that intrusion upon seclusion did in fact apply to claims otherwise covered by *PHIPA*.

---

[48] *Hopkins* CA, supra note 10 at para 3.
[49] *Ibid* at para 11.
[50] *Hopkins v Kay*, 2014 ONSC 321 at paras 16–17 [*Hopkins* ONSC].
[51] 2009 BCSC 1562 [*Facilities*].
[52] 2011 ABQB 41 [*Martin*].
[53] *Facilities*, *supra* note 53 at para 77; *Martin*, *supra* note 54 at para 47.
[54] *PHIPA*, *supra* note 48 s 56(1).
[55] *Ibid* s 57(1-4).
[56] *Ibid* ss 58 and 60.
[57] *Ibid* s 60.
[58] *Hopkins* ONSC, s*upra* note 52 at paras 10–11.
[59] *Ibid* at para 19.
[60] *Ibid* at para 14.
[61] *Ibid* at para 27.
[62] *Ibid* at para 30.

Implications and Scope of Hopkins

While the applicability of intrusion upon seclusion in the health context was not a guarantee, in rendering its judgment in *Jones*, the Ontario Court of Appeal explicitly included health information as the type of issue that would attract an interest in privacy:

> As the facts of this case indicate, routinely kept electronic databases 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 cellphone, email or text message. [63]

Therefore, following *Hopkins*, the broader applicability of intrusion upon seclusion in the health care sector will have a significant impact on the regulation of privacy breaches.

As seen in *Trout Point Lodge*, the implications of *Hopkins* have already been felt outside of Ontario. For example, in *Grant v Winnipeg Regional Health Authority*,[64] the Manitoba Court of Appeal considered the high-profile case of Brian Sinclair, a 45-year-old double amputee who died while awaiting treatment in a hospital emergency room for thirty-four hours. As part of the reaction to criticism against the hospital, information about Mr. Sinclair's medical history and medical condition at the time of his death was released to the media. Mr. Sinclair's estate sought damages for the negligent disclosure and alleged misuse of his personal medical information by hospital officials after his death. On appeal, Justice Monnin referred to *Hopkins* and noted that Manitoba's health privacy legislation, the *Personal Health Information Act*,[65] was substantially similar to Ontario's *PHIPA*.[66] He stated that it was too early to dismiss the possibility that the family members of Mr. Sinclair had sufficient proximity in tort to make a claim as the result of a privacy breach of a family member.[67] Justice Monnin stated that the genetic nature of many medical conditions, and the sensitive nature of inheritable traits and diseases, may in fact open up intrusion upon seclusion claims to a much larger plaintiff base and even to a broader class than what was observed in *Hopkins*.[68]

[63] *Jones*, *supra* note 1 at para 67.
[64] 2015 MBCA 44 [*Grant*].
[65] *Personal Health Information Act*, CCSM 1997, c P33.5.
[66] *Grant*, *supra* note 64 at para 125.
[67] *Ibid* at para 127.
[68] *Ibid* at paras 125-128.

B. Use of *PHIPA* for Protecting Privacy

As stated in *Hopkins*, since privacy legislation is comprehensive, bringing an intrusion upon seclusion claim may be redundant when trying to address an alleged privacy breach. Under *PHIPA*, for example, an individual may be guilty of an offence and liable for a fine of up to $50,000 if he or she intentionally collects, uses, or discloses personal health information, while organizations may be liable to a fine of up to $250,000.[69]

However, this section of *PHIPA* is misleading. Although these penalties do exist under *PHIPA*, the statute has not been effectively applied in this manner. For example, there has been only one prosecution for an offence under *PHIPA* to date, and it did not result in a conviction.[70] In *North Bay Health Centre v Ontario Nurses' Assn (McLellan Grievance)*,[71] a nurse allegedly accessed the personal health information of 5,800 patients without a legitimate reason. She faced nine charges[72] under *PHIPA*. While this suggested some promise for the enforcement mechanisms of the statute, the charges were ultimately dropped due to a sixteen-month delay and no fines were imposed on the nurse.[73]

Arguably, *PHIPA* has been ineffective in addressing privacy breaches by health information custodians and in providing a proper deterrence mechanism for privacy breaches of health records. These deficiencies were highlighted by the Ontario Information and Privacy Commissioner (IPC), who stated the following:

> The fact that charges may be laid will be an effective deterrent only to the extent that custodians and their agents believe that such measures are going to be used in appropriate circumstances. Given the current pervasiveness of the problem of unauthorized access, it may be necessary to increase the number of prosecutions to warn custodians and their agents that unauthorized access is not acceptable and will not be tolerated.[74]

---

[69] Information and Privacy Commissioner of Ontario, *Detecting and Deterring Unauthorized Access to Personal Health Information* (Toronto: Information and Privacy Commissioner of Ontario, 2015), online: <https://www.ipc.on.ca/images/Resources/Detect_Deter.pdf> at 8 [IPCO Report].
[70] Olivia Carville, "Ontario's sole health privacy prosecution quietly dismissed", *The Toronto Star* (30 March 2015), online: <http://www.thestar.com/life/health_wellness/2015/03/30/ontarios-sole-health-privacy-prosecution-quietly-dismissed.html>.
[71] *Ibid*; [2012] OLAA No 11 216 [*North Bay*].
[72] Maria Calabrese, "Hospital Ordered to Disclose Records", *North Bay Nugget* (5 July 2015), online: <http://www.nugget.ca/2013/07/05/hospital-ordered-to-disclose-record>.
[73] Theresa Boyle, "Public Should be Barred from Hearing into Alleged Snooping by Nurse: Lawyer", *Toronto Star* (29 April 2015), online: <http://www.thestar.com/life/health_wellness/2015/04/29/public-should-be-barred-from-hearing-into-alleged-snooping-by-nurse-lawyer.html>.
[74] IPCO Report, *supra* note 71 at 9.

Despite the Ontario IPC receiving over 400 complaints of privacy breaches a year, the IPC has been unable to effectively investigate and prosecute breaches, as evidenced by the lack of prosecutions.[75]

It is perhaps not surprising that Ontario has been less successful in prosecuting the unauthorized access of personal health information than other jurisdictions in Canada.[76] This may be the result of statutory regimes or ineffective regulatory enforcement mechanisms. However, as seen in the above cases, Canadian prosecutions have generally tended to focus on the health information custodian and not on the organization itself. This creates little incentive or motivation for health institutions to place proper checks and balances on their employees in order to deter privacy breaches within their organizations.

The types of damages awarded under *PHIPA* also differ from intrusion upon seclusion, as noted in *Hopkins*. For example, if an individual or an organization is convicted under *PHIPA*, potential plaintiffs affected by an order or the conduct leading to the conviction may initiate court proceedings for damages for any actual harm suffered: *PHIPA* specifically permits courts to award up to $10,000 for mental anguish in cases where a defendant's wilful or reckless conduct causes actual harm to a plaintiff.[77] However, proof of harm is not a required element for intrusion upon seclusion, which is particularly important given the nature of privacy breaches.[78] While privacy breaches are themselves harmful, it is very difficult to demonstrate actual harm unless the information is used inappropriately, as was the case in *Evans v The Bank of Nova Scotia*.[79]

The high threshold for obtaining damages under *PHIPA* suggests that it will be even less likely to secure a successful conviction. This threshold also shifts the focus away from preventing the actual breach and, instead, prioritizes harm prevention with respect to the use of the inappropriately collected information, which is ineffective as a practical deterrent. In contrast, the modest damages threshold established in *Jones* would be appropriately increased under the intrusion upon seclusion framework if actual harm is established. [80]

A further advantage to intrusion upon seclusion claims when compared to *PHIPA* regulation is that, rather than strengthening privacy rights through taxpayer funding or extended investigation periods for the IPC, the common law mechanism would effectively shift the costs of privacy enforcement from the public sector to private parties. While courts are strained for resources, the judicial economy of class actions makes the large number of these breaches a more effective means to address them, rather than on a case-by-case basis.

---

[75] Information and Privacy Commissioner of Ontario, *2014 Annual Report: Charting a Course for the Future* (Toronto: Information and Privacy Commissioner of Ontario, 2015) at 18 [IPCO Annual Report].
[76] IPCO Report, *supra* note 71 at 9-10.
[77] *PHIPA*, *supra* note 48 at s 65(3).
[78] *Jones*, *supra* note 1 at para 74.
[79] 2014 ONSC 2135 at para 52.
[80] *Jones*, *supra* note 1 at para 83.

C. Other Methods of Privacy Disincentives and Enforcement

Professional Discipline as a Disincentive to Breach

Another enforcement mechanism against the unauthorized access of health information is direct disciplinary action against the health information custodian. For example, the Professional Standards for the College of Nurses of Ontario states that "[n]urses are responsible for their actions and the consequences of those actions,"[81] and are "accountable for conducting themselves in ways that promote respect for the profession."[82]

While the college disciplines its members for accessing health information without authorization, this method is ultimately ineffective in preventing privacy breaches. For example, the college suspended a nurse for three months for accessing the personal health information of 338 hospital patients without authorization.[83] Although the employer terminated the nurse, the official term was changed to a resignation for the purposes of her employment record. Consequently, following a three-month suspension, the nurse had no record of professional misconduct.[84] A similar penalty was used in *College of Nurses of Ontario v Smith*,[85] despite the nurse having already been disciplined for accessing and disclosing a patient's medical record multiple times without consent. The Discipline Committee of the college explained the rationale behind the nurse's punishment as follows:

> [T]he three-month suspension is a clear message to the Member and the membership that clients' health information must be protected. Because of the ease of access to electronic health records, there is greater onus on the membership to access information only when appropriate and for professional use. The public has every right to expect that nurses will safeguard their health information.[86]

Sanction by the College of Nurses of Ontario is often even less condemning than the above two cases. For example, in *College of Nurses of Ontario v Hooker*,[87] a nurse

[81] College of Nurses of Ontario, *Professional Standards*, *Revised 2002* (Toronto: College of Nurses of Ontario, 2009) at 4, online: <https://www.cno.org/Global/docs/prac/41006_ProfStds.pdf>.
[82] *Ibid*.
[83] Theresa Boyle, "Nurse Suspended for Snooping into Patient Files", *Toronto Star* (5 May 2015), online: <http://www.thestar.com/life/health_wellness/2015/05/05/nurse-suspended-for-snooping-into-patient-files.html>.
[84] *Ibid*.
[85] (15 April 2009), online: Discipline Committee of the Ontario College of Nurses <http://www.cno.org/Global/2-HowWeProtectThePublic/ih/decisions/fulltext/pdf/2009/Kerry%20Smith,%20HB00883,%20July%2010,%202008.pdf>.
[86] *Ibid*.
[87] (29 August 2006), online: Discipline Committee of the Ontario College of Nurses <http://www.cno.org/Global/2-

accessed electronic records of two physicians, who were also patients, at a mental health facility that had recently transitioned to electronic records. The nurse accessed this information solely because she knew both of the physicians and was curious. Despite being warned that any subsequent misconduct could result in termination of her employment, less than six months later she accessed the files of several other patients for whom she was never clinically responsible.[88] Upon termination, the college determined that based on the nurse's acceptance of responsibility and the fact that this was her first instance of discipline, a suspension of thirty days and a fine of $3,500 was both reasonable and in the public interest.[89]

While some professional bodies have elected to uphold the termination of employees who accessed patients' health information without authorization, this situation is not common. For example, in *Timmins & District Hospital v Ontario Nurses' Assn (Peever Grievance)*,[90] an employee accessed a former spouse and mother of the spouse's grandchild's health information with whom the nurse had no clinical relationships. In this case, the dismissal was upheld despite the nurse's twenty-two years of service and no previous disciplinary infractions. The Discipline Committee held that the violation of the patient's trust, the disregard for employer policies and professional ethics, and the *PHIPA* breach all meant that the discipline was not excessive.[91] Similarly, in *North Bay*,[92] a nurse inappropriately accessed personal health information from 5,800 patients on more than 12,000 occasions over seven years. While the nurse claimed she had right to access this information for educational purposes, based on section 37(1)(d) of *PHIPA*, the arbitrator rejected this claim.[93] Evidently, the current statutory regime and the professional regulations have been ineffective in preventing and in disciplining privacy breaches.

Vicarious Liability and the Health Care Institution

A health care institution may also take disciplinary action against its employees in order to avoid becoming vicariously liable for their actions. In *Bazley v Curry*,[94] the Supreme Court of Canada declared that the extent of power that employers have over their employees is a significant factor when determining whether an organization should be held vicariously liable for torts committed by its employees. The court noted that the vulnerability of victims to the wrongful exercise of employer power—in this case, the collection or disclosure of private health data—would further indicate that the organization should be held vicariously liable

HowWeProtectThePublic/ih/decisions/fulltext/pdf/2007/Catherine%20Hooker,%207908734,%20August%2029,%202006.pdf> [*Hooker*].
[88] *Ibid*.
[89] *Ibid*.
[90] [2011] OLAA No. 222.
[91] *Ibid* at para 72.
[92] *Supra* note 73.
[93] *Ibid* at paras 45–46.
[94] [1999] 2 SCR 534 at para 41.

for such abuses of power.[95] This risk is potentially heightened where these patients have a disability, as in a mental health institution. Health care institutions have a variety of strategies available to limit potential breaches and vicarious liability, including technology audits (such as those performed in *Hooker*), zero-tolerance policies for confidentiality or privacy breaches, and direct disciplinary actions against employees. These strategies may have prevented the widespread breach of privacy seen in *North Bay*. The risk of vicarious liability, coupled with the threat of intrusion upon seclusion class actions, may be one of the best ways to enhance privacy protections in the health sector.

While regulatory colleges may be inclined to protect the identities of the nurses it oversees, the publicity of a court case may not lead to the same concern for the defendant's privacy. As a result intrusion upon seclusion class actions may ultimately result in widespread identification of the employees involved in a particular breach, which may provide the incentive needed for organizations as well as individual custodians to adhere to *PHIPA* and other policies.

Outside Regulated Professions

Professional regulation is also insufficient to prevent privacy breaches given that health-related breaches occur outside of the self-regulated professions. For example, the Ontario Human Rights Tribunal reviewed a summary hearing in *Fallico v St Joseph's Health Centre*,[96] where a chaplain in a Roman Catholic community teaching hospital disclosed information about a patient's desire to end his life. The chaplain was ultimately terminated for this disclosure. The patient had also expressed this desire to individuals outside his circle of care. While both parties conceded that the hospital was a health information custodian under *PHIPA* and that the chaplain was an agent of the hospital,[97] the disagreement was about whether *PHIPA* or the hospital's policies prohibited this disclosure, since the information had already been provided to third parties.

The adjudicator found that there was nothing under either the regulatory or the statutory regime that prevented the chaplain from disclosing this information, and he was therefore able to follow his religious beliefs.[98] Nevertheless, the adjudicator held that the termination of applicant was based on his violation of company policies, not his religion, and violating company policies is not a protected ground under the *Code*.[99] Although the chaplain's application was unsuccessful, the ruling demonstrates the limited recourse available to health institutions to enforce privacy policies, which is often limited to termination of employment. Health care settings often involve several different types of employees, including many who are

[95] *Ibid.*
[96] 2013 HRTO 1192 (CanLII).
[97] *Ibid* at para 12.
[98] *Ibid* at para 21.
[99] *Ibid*.

not subject to discipline by a regulatory college. Therefore, as a privacy enforcement mechanism, regulatory discipline alone is unlikely to be effective.

CONCLUSION

While *PHIPA* was intended to be a comprehensive and thorough regulatory regime to address privacy interests in the health sector, there is a noticeable regulatory gap in the way this act functions. The threat of prosecution under *PHIPA* has not adequately deterred health information custodians, or others who may have access to medical records, from committing privacy breaches. To address this issue and update the legislation for modern technology, Ontario Health Minister Dr. Eric Hoskins introduced new measures on June 10, 2015 that aim to protect patient privacy and strengthen accountability in the health care system. The new amendments are expected to increase fines and make the prosecution of *PHIPA* offences less cumbersome.[100] However, even if the amendments are passed, it is uncertain whether they will provide a sufficient deterrent to individuals and organizations involved in privacy breaches.

After two decades of class proceedings legislation in Ontario, class actions are under review by the Law Commission of Ontario. The review is being conducted because of criticism of the settlement funds received per class member after legal fees and the ample costs imposed in unsuccessful actions.[101] Nonetheless, there appears to be even greater shortcomings in other deterrent mechanisms, such as *PHIPA* and the discipline of professional colleges. For example, several hospital workers were charged under *PHIPA* for accessing the medical records of Rob Ford, the former mayor of Toronto, without authorization during his 2015 cancer treatments.[102] However, this was only the second instance of the IPC reporting offenders of *PHIPA* to the Ministry of the Attorney General for prosecution. Evidently, for the health sector in particular, the risk of widespread liability in class action litigation is more likely to motivate health institutions to strengthen their privacy protections and impose harsher disciplinary measures than the current statutory regime.

Neither *PHIPA* nor regulatory bodies have been successfully employed in a consistent manner for privacy breaches and they have not been useful in directly imposing financial penalties on the parties involved. In contrast, class actions are effective in deterring conduct in potential defendants and have the ability to encourage change. Society may eventually be forced to choose between two

[100] Ministry of Health and Long-Term Care, News Release, "Ontario to Introduce New Measures to Protect Patient Privacy" (10 June 2015), online: <http://news.ontario.ca/mohltc/en/2015/06/ontario-to-introduce-new-measures-to-protect-patient-privacy.html>.
[101] LCO Report, *supra* note 21 at 9–11.
[102] Olivia Carville, "Govt. prosecutes health workers for snooping into Rob Ford's medical records", (8 July 2015), *Toronto Star*, online: <http://www.thestar.com/life/health_wellness/2015/07/08/govt-prosecutes-health-workers-for-snooping-into-rob-fords-medical-records.html>.

alternatives: either invest and strengthen the statutory regime or provide more resources to assist in processing class action cases.

Currently, there are enhancements being made to the statutory regime. [103] For example, the sharing of electronic health records (EHRs), results in all participants becoming custodians of the shared and collected information.[104] As a result, the IPC has urged providers that share EHRs to establish a governance framework that would clearly show providers how to comply with *PHIPA* and create preventive measures that reduce privacy breaches. [105] Nevertheless, as with other IPC mechanisms, there is little enforcement or likelihood of prosecution to ensure compliance with these guidelines. These changes could improve the statutory regime by making reporting to the IPC mandatory and by doubling the fines where an investigation is pursued.[106] However, the lack of successful prosecutions in the past decade of *PHIPA* illustrates that these changes alone are unlikely to foster improved privacy protections.

Class actions thus remain the preferable option for privacy enforcement. As noted by Chief Justice McLachlin in *Hollick*, "judicial economy, access to justice, and behaviour modification" are distinct advantages of class actions. [107] Intrusion upon seclusion and its use in class proceedings is still new in Ontario, so the influence of these legal developments has yet to be fully realized. The tort was created in Ontario because of inaction by the legislature in properly addressing privacy breaches and because of the corresponding rise of public concern over privacy interests. Therefore, the ineffectiveness of the IPC, or the inability of the statutory regime to properly protect privacy rights in the health sector, may also give rise to a greater use of the court system to enforce these interests. Given the pressure that Ontario courts are already under, this may not be an ideal shift. However, it may be one that becomes necessary until alternative enforcement mechanisms or adequate deterrents are in place to protect the privacy interests of Canadians, especially within the health sector.

---

[103] Provinces and Territories, Bill 78, *Electronic Personal Health Information Protection Act, 2014*, 2nd session, 41st Parl, Ontario, 2013.
[104] IPCO Annual Report, *supra* note 71 at 13.
[105] *Ibid.*
[106] Kathy O'Brien, "Bill 78: How Ontario's proposed regime for the sharing of electronic personal health information will impact your organization", (13 January 2014), *DDO Health Law*, online: <http://ddohealthlaw.com/477>.
[107] *Hollick*, *supra* note 25 at 159-160.