The International Comparative Legal Guide to:

Insurance & Reinsurance 2019

8th Edition

A practical cross-border insight into insurance and reinsurance law

Published by Global Legal Group, with contributions from:

Advokatfirman Vinge KB
Arthur Cox
Bae, Kim & Lee LLC
Bech-Bruun Law Firm P/S
BLACK SEA LAW COMPANY
Blaney McMurtry LLP
BSA Ahmad Bin Hezeem & Associates LLP
Camilleri Preziosi Advocates
Christos Chrissanthis & Partners
Chuo Sogo Law Office, P.C.
CIS Risk Consultant Company (insurance brokers) LLP (CIS)
Clyde & Co (Deutschland) LLP
Clyde & Co LLP
Cordero & Cordero Abogados
Creel, Garcia - Cuellar, Aiza y Enríquez, S.C.
DAC Beachcroft Colombia Abogados SAS
DAC Beachcroft LLP
Dirkzwager legal & tax
DLA Piper Norway DA
Esenyel|Partners Lawyers & Consultants
ESTUDIO ARCA & PAOLI, Abogados S.A.C.
Eversheds Sutherland Ltd.
GPA –Gouveia Pereira, Costa Freitas & Associados
Gross Orad Schlimoff & Co.
Hamdan AlShamsi Lawyers and Legal Consultants
Jurinflot International Law Firm
Kennedys Chudleigh Ltd.
Lee & Li, Attorneys-At-Law
Legance – Avvocati Associati
Matheson
McMillan LLP
MinterEllison
Norton Rose Fulbright
Paul, Weiss, Rifkind, Wharton & Garrison LLP
Railas Attorneys Ltd.
RCD
R&T Asia (Thailand) Co., Ltd.
SOW & PARTNERS
Steptoe & Johnson LLP
Tavares Advogados
Tuli & Co
Vavrovsky Heine Marth

INSIGHT CONSENSUS INFLUENCE

glg global legal group

Chapter 2

Cyber Class Action Exposure in Canada

David R. Mackenzie

Dominic T. Clarke

Blaney McMurtry LLP

The Canadian insurance market is awakening to the need for cyber-insurance against data loss and privacy breach events. Although there is clearly room for this market to grow, Canadian insurers are routinely issuing cyber coverage to protect against these risks. While insurers have developed loss-experience with first party data breach expense, ransomware and business interruption claims in recent years, knowledge and understanding of third-party risks caused by covered breaches remains limited. This article reviews the status of emerging third-party claim experience.

Class actions seeking damages arising out of data loss and privacy breaches are becoming increasingly common. However, all of the actions to date either remain at the certification stage or have been resolved through settlements. As a result, we have yet to see judicial analysis at a common issues trial of the causes of action being advanced and a final determination of damages. Nevertheless, three recent cases are instructive about the potential indemnity obligations of Canadian insurers under the cyber policies they have issued: *Condon v. Canada* (*Condon*);[1] *Tucci v. Peoples Trust Company* (*Tucci*);[2] and *Broutzas v. Rouge Valley Health System* (*Broutzas*).[3]

1. Litigation and Causes of Action

The decisions in *Condon, Tucci,* and *Broutzas* provide insight into various potential causes of action, because each arises out of a distinct set of circumstances. *Condon* pertains to the loss of a hard drive on which personal and financial information of hundreds of thousands of Canadian student loan recipients was stored. *Tucci* arose out of the hacking of a bank by a malicious third party. *Broutzas* concerns alleged misappropriation of personal health information by hospital employees and the subsequent sale of that information to vendors of certain financial services (particularly Registered Educational Savings Plans, or "RESPs").

Each of these claims was made the subject of a putative class action (*Broutzas* was the subject of two distinct class actions). As a result, Canadian courts have been asked to certify causes of action in each set of circumstances. *Condon* is the subject of a negotiated settlement, which the Federal Court of Canada has approved. The consideration given to the various causes of action in the course of certification – and in the case of *Condon*, appeal and settlement as well – provides insight into the difficulties that class counsel and defence counsel (together with their instructing insurers) face in prosecuting and defending privacy and data breach class actions.

The putative class actions advanced many theories of liability: negligence; breach of contract; Intrusion upon Seclusion; Breach of Confidence; waiver of tort/unjust enrichment; and statutory theories of liability. Only three of these, however, have met with a measure of success at the certification stage: negligence; breach of contract; and intrusion upon seclusion.

In Canada, in order for certification to be granted, it must merely not be "plain and obvious that the cause of action will fail".[4] Provided that there is "some basis in fact" for the existence of a common issue to be tried on behalf of all class members, the action can proceed as a class action.[5] These are low threshold standards. Judicial consideration of each of these at the certification stage, however, has highlighted potential weaknesses in each theory and given rise to cautions from the bench with regard to their relative chances of success at trial. This article focuses on the strengths and weaknesses of each of these causes of action.

Review of these decisions also highlights the increased importance of "nominal damages" in the context of data/privacy breach class actions. As is outlined below, it is apparent that class counsel will in many, but not all, cases have difficulty in proving class-wide compensatory damages. While success at trial is far from assured, certain causes of action, if proved, can result in awards of nominal damages even in the absence of proven compensable injury. To better understand the exposure facing defendants and their insurers, we will also examine the meaning of "nominal damages" in the Canadian context.

2. Negligence

In each of the proceedings the putative class alleged that the defendants were negligent, arguing that they owed a duty of care to class members and failed to meet that duty by falling below the standard of care owed. More particularly, they failed to have adequate safeguards in place to protect the information of class members. Each of the actions asserted that the class members had suffered actual damages as a result.

There are three primary pitfalls with respect to the allegations advanced. First, the theory of liability being advanced against many defendants is novel, in that it is not well established in Canada that a plaintiff can sue many defendants for what amounts to pure economic loss in the circumstances of a data/privacy breach. Second, proving actual damages on a class wide basis, as is required in negligence, may be an insurmountable challenge, particularly where the risks involved are primarily prospective identity theft. Finally, even if a negligence cause of action is certified, class counsel must still prove the claim.

In *Broutzas*, the RESP dealer defendants were allegedly negligent for not properly supervising their employees who were allegedly buying confidential personal information of new mothers from hospital

employees. That information was used to market RESP investments to those mothers. While the hospital acknowledged that it was in a relationship of proximity to its patients, the RESP dealers argued that the relationship between them and the class members was not sufficiently proximate to give rise to a duty of care. Perell J. characterised that element of the claim as novel and undertook the three-step analysis established in *Anns v. Merton London Borough Council*[6] – foreseeability, proximity, and policy considerations. He determined that there was no duty of care on the part of the RESP defendants as the privacy breach was perpetrated by hospital employees. In the Court's view it was nonsensical to suggest that the RESP dealers could have supervised hospital employees.

While commenting primarily on the breach of contract claim, Perrell J. also expressed concerns that the negligence cause of action as proposed, merely mirrored existing statutory obligations and the emerging tort of intrusion on seclusion. He was reluctant to certify any novel negligence action in circumstances where a statute already spoke to the issue. He also expressed concern that the negligence theory was being used as a "backstop" to the intrusion on seclusion claim that was also being advanced. He refused to certify the negligence claim against the RESP dealers and their employees and, as seen below, the entirety of the claim.

Standing in contrast to that analysis is the decision in *Tucci*. There, the defendants provided financial services to members of the putative class and required those members to provide sensitive personal and financial information. The information at issue could clearly be used to harm the class members if lost (foreseeability) and those people were in a direct commercial relationship with the defendants (proximity). Masuhara J. did express concerns regarding the public policy stage of the *Anns* test, providing: 1) negligence ought not to step in where statutes already govern; and 2) a duty of care should not be imposed that creates indeterminate liability. He found that the theory of liability advanced did not arise because of statutory obligations but out of privacy and security policies the defendant itself had created. Similarly, liability was not indeterminate because it could only be owned to those who were customers of the Defendant and whose information was stolen. This latter conclusion appears controversial, as liability could still be regarded as temporally indeterminate, in that damages for the future risk of identity theft clearly seek to compensate for an indeterminate period of time and amount. While this risk may be real, the law of negligence has rarely been used to impose damages for a potentially perpetual risk.

The novel nature of the negligence claims is not the only issue standing in the way of succeeding on a negligence claim. A plaintiff must prove actual loss resulting from the negligence of the defendant. The fact that the claim is being advanced through a class action only complicates matters, as actual damage must be demonstrated on a class-wide basis.

Tucci and *Condon* considered the loss of control over financial information, not personal health information as was the case in *Broutzas*. This is a critical distinction. In *Tucci*, it was not plain and obvious that damage to credit reputation cannot constitute a compensable harm. Similarly, out of pocket expenses including credit monitoring and wasted time and inconvenience related to preventing identity theft could constitute a class-wide harm.

These concerns were raised at the certification stage in *Condon*. There the court acknowledged that the allegations advanced against the government could support findings of a duty of care and of a breach of the standard of care, but questioned whether claims for compensable damages were advanced. It concluded they were not:[7]

> … The Plaintiffs have not been victims of fraud or identity theft, they have spent at most some four hours over the phone seeking status updates from the Minister, they have not availed themselves of any credit monitoring services offered by the credit monitoring agencies nor have they availed themselves of the Credit Flag service offered by the Defendant.

The certification court held that damages cannot be awarded for merely speculative injuries and declined to certify the negligence issue for trial. Class counsel appealed that decision and it was overturned by the Federal Court of Appeal on the basis that "costs incurred in preventing identity theft" and "out of pocket expenses" could satisfy the damages requirement. While such damages may be capable of proof, actually marshalling this evidence on a class-wide basis appears to require judicial approval of some form of aggregate model. Whether this is possible or will be accepted by the courts is unclear.

Finally, in many circumstances, actually proving negligence may be difficult. Attacks by hackers, theft of large amounts of data by employees, and even lost laptops are relatively new phenomena. The fact that courts are still grappling with the law of negligence in this context is not surprising. When a person slips and falls, when one car hits another or when professional services fall below the expected standard, the act, error or omission is relatively straightforward and the resulting damages are reasonably identifiable. In data breach cases, numerous questions arise that are not so easily answered. If an organisation has handling and security protocols and an employee breaches those protocols, has the organisation fallen below the required standard? If that same organisation suffers a criminal attack that defeats the cyber-security in place, has it failed to fulfil its obligations? If a stolen laptop is password protected and the data encrypted, has the organisation been negligent? These are all considerable hurdles.

3. Breach of Contract

Breach of Contract allegations have met with some success, being certified in both *Condon* and *Tucci*. *Condon* involved contracts in the form of Student Loan Agreements. Multiple sections expressly pertained to the Minister's collection, protection and use of the information provided. The certification court acknowledged that these terms could potentially be relied upon to establish a breach of contract such that it was not plain and obvious that the claim would fail.

Similarly, in *Tucci* there were express contractual terms between the bank and its customers. The exact terms of the contract, however, needed to be determined, as the pleadings asserted that the contract included the defendant's "Website Terms & Conditions" and other terms. Those included statements that the defendant would comply with Federal and provincial privacy legislation, as well as express or implied terms that the defendant would keep information confidential and secure from loss and theft and would not use it except for purposes expressly authorised.

The defendant disputed that the contract included all such terms. It further argued that there was no allegation that those terms had been breached; it had promised to take reasonable steps to protect the information and had done so. The fact that a security breach had occurred did not mean that reasonable steps to protect the information had not been taken. Masuhara J. acknowledged these arguments but held that they should be determined at trial. The Court did not accept the defendant's argument that all forms of damages claimed were too remote, on the basis that, even if no actual damages were proved, nominal damages could be awarded if a breach of contract had occurred.

An interesting discussion pertained to a limitation of liability clause which the defendant said precluded the claim. The Court found that the limitation of liability clause did not preclude the claims *per se*; and that its effect was an issue for trial.

In *Broutzas*, the court refused to certify the breach of contract claims advanced. They were premised on the existence of a contract between the patients and the hospitals, which allegedly included terms governing the protection and use of personal information and promising peace of mind. Perell J. ruled that it was "plain and obvious that the putative Class Members [did] not have a claim for breach of contract and warranty". The judge agreed with Rouge Valley's submission that this claim was an artifice by which to sue for breach of statutory obligations. The pleadings simply alleged the duties that the hospitals owed under the *Personal Health Information Protection Act, 2004*.[8] Moreover, the admission forms and information forms provided to the incoming patients were not contractual in nature, and there was no bargaining between patients and the hospital about preserving the confidentiality and privacy of patient information, which the hospitals were statutorily obliged to do. In short, there was no contract into which terms could be implied and if there had been, those terms were already the subject of non-contractual legal duties.

Where a commercial relationship is present, any contract is likely to either be silent on privacy issues or to favour the corporate entity. Commercial contracts, particularly consumer contracts, increasingly feature arbitration, venue and jurisdiction clauses that may restrict the ability of individuals to bring claims before Canadian courts – especially those claims seeking to enforce express or implied terms of the contract itself. While the Supreme Court of Canada, together with lower courts, has questioned the validity of onerous terms (see *Douez v. Facebook*[9] and *Heller v. Uber Technologies Inc.*[10]), reasonable terms may still be enforced. Where that existing contract considers the gathering of information by the organisation, a contract claim will likely be easier to have certified than a negligence claim because there is no requirement to show actual damages. A breach alone should be sufficient to result in nominal damages at minimum. However, a breach of contractual terms must still be shown, and those terms will not necessarily create an obligation to prevent security breaches or misuse of information altogether. As the Defendant in *Tucci* pointed out, the fact that a security breach has occurred does not mean that reasonable steps to protect the information have not been taken.

Like potential class members, organisations that have been hacked are victims of a crime. The standard likely to be imposed by contract is not strict liability. If express contractual terms drafted by the organisation set the standard, that standard is not likely to be high. Again, certification is a low bar, but proving contractual terms existed and were breached may be a significant challenge. On the other hand, there is arguably an important benefit to breach of contract claims: they can result in an award of nominal damages even if no actual loss is proved. However, a passage in *Condon* suggests the availability of an award of nominal damages may not be a certainty in the class action context:[11]

> [The Defendant] further argues that nominal damages should never be awarded in a class action as it would not favour the plaintiffs but rather their counsel, since the latter would be the only ones effectively standing to benefit financially from the outcome.
>
> The Defendant advances an interesting and strong argument on this point but the Plaintiffs' position, although novel in the context of a class proceeding is supported by sufficient authorities that this cause of action should be considered on the merit of the action. In other words, it is not plain and obvious that the cause of action in contract would fail. As to any disproportionate advantages in favour of the Plaintiffs' counsel, the Court will also be better positioned to rule on that issue when it hears it on the merit.

Although it must be acknowledged that the court in *Tucci* certified the question as to whether wasted time could be the basis for awarding aggregate damages, it is open to question whether such damages are "nominal" in nature, or simply a form of compensatory damages arising out of economic loss. In short, like negligence claims, it is not clear that breach of contract claims offer a direct path to recovery for class members in the data and privacy breach context.

4. Intrusion Upon Seclusion

Certification courts have expressed uncertainty about the role of the developing intrusion upon seclusion tort in data breach and privacy cases where information was lost or stolen rather than having been intentionally misused. While intrusion upon seclusion was certified in both *Condon* and *Tucci*, both Courts expressed concerns in respect of the viability of the cause of action should the matter be tried. In *Broutzas*, Perell J. declined to certify, questioning the viability of the claim in the circumstances of that case.

Intrusion upon seclusion, like negligence and breach of contract, appears to be problematic in the data/privacy breach context in Canada for a number of reasons. First, the tort does not exist in British Columbia, and likely in other Canadian jurisdictions with privacy legislation similar to British Columbia's *Privacy Act*. There are other concerns.

As Perell J. stated in *Broutzas*, the tort is not simply a backstop for negligence; it has its own distinct elements. Unlike negligence, intrusion upon seclusion is an intentional tort and requires intentional or reckless conduct on the part of the defendant. As Masuhara J. noted in *Tucci*, it is one thing to plead recklessness, but another thing to prove it in the commercial context. To date, there has been no judgment establishing what "reckless" means in the context of a data or privacy breach.

The standard further requires that the defendant invade the plaintiff's private affairs or concerns without lawful justification. In breach scenarios involving a third party, such as a hacker, this element will be difficult to prove. Similarly, where a laptop or hard drive is lost, the risk created is that unknown third parties, not the defendant, will intrude the plaintiff's privacy. It may also be difficult to prove that intrusion did in fact occur. As the Court in *Condon* noted in approving the settlement, "[b]efore there can be an award of damages, however, the onus remains on the plaintiffs to establish first that an intrusion actually occurred".[12] The risk of future harm in the form of a prospective privacy breach that has not yet occurred can almost certainly not be the basis for an intrusion upon seclusion claim.

There are, however, indications from Canadian courts that in circumstances where an employee is caught snooping, the claim may be easier to advance. In *Oliveira v. Aviva Canada Inc.*, the Ontario Court of Appeal considered a case in which a nurse and her hospital employer were sued for snooping into patient records, and sought insurance coverage against the claim. The policy provided coverage to hospital employees "while acting under the direction of the named insured".[13] The insurer denied coverage because the nurse was acting outside of the course and scope of her employment in her unauthorised review of the plaintiff's medical records. The Court disagreed and ordered the insurer to defend:[14]

> … In our view this is precisely the sort of conduct the policy was intended to respond to. The applicant was employed by the hospital as a nurse and while on duty, in the course of the hospital's operations, to use the language of the policy (which would include the maintenance of patient's health records), she accessed the records that she had apparently no business doing because she was not involved in J.L.'s care. The applicant was employed by the hospital, (she was essentially an employee 24/7) but was only acting under the direction of the hospital when she was on duty as such.

> In our view the common sense interpretation of the language can only have this meaning. To hold as the appellant argues that unauthorized access to medical records does not arise out of the hospital's operations, or under the direction of the hospital because it would never direct such conduct, would negate the coverage intended. It is plain that the policy, in covering invasion of privacy, is intended to cover the type of conduct that is alleged in the Statement of Claim.

There are obviously differences between the standard applied to the duty to defend under an insurance policy and the intentional tort of intrusion upon seclusion. However, the decision suggests a willingness to hold organisations liable for the privacy breaches of their employees, even if such actions occur outside the course and scope of employment. As such, the tort element requiring that the invasion of the plaintiff's privacy by the defendant may not be as significant a hurdle where the intrusion is the intentional act of an employee.

The third requirement of the tort was critical in the *Broutzas* decision. In order to succeed, a plaintiff must demonstrate that a reasonable person would regard the invasion as highly offensive and causing distress, humiliation and anguish. In *Broutzas*, the Defendants argued that there may had been intrusion, but no seclusion. The Court agreed. There was no seclusion because the contact information that was the objective of the intrusion was not private. The disclosure of mere contact information did not intrude on the class members' significant private affairs and concerns and the disclosure would not be highly offensive to a reasonable person nor cause her distress, humiliation and anguish. This finding provides guidance about the kinds of information that must be in issue for an intrusion upon seclusion claim to succeed. The Court listed "medical, financial, or sensitive information" as sufficient to found a claim. What the court meant by "sensitive information" is less clear. However, mere contact information will not fall within that category. The Court went on to note that "Generally speaking, there is no privacy in information in the public domain".

While intrusion upon seclusion claims have been certified in both *Condon* and *Tucci*, both Courts expressed significant concerns as to the likely success of the claims if they proceeded to trial on the merits. This underscores the reluctance that courts have expressed generally about the tort of intrusion upon seclusion. In creating the tort in the first place, the Ontario Court of Appeal sought to make clear that it should be rarely used, and even more rarely successful:[15]

> These elements make it clear that recognizing this cause of action will not open the floodgates. A claim for intrusion upon seclusion will arise only for deliberate and significant invasions of personal privacy. Claims from individuals who are sensitive or unusually concerned about their privacy are excluded: it is only intrusions into matters such as one's financial or health records, sexual practices and orientation, employment, diary or private correspondence that, viewed objectively on the reasonable person standard, can be described as highly offensive.

In the rare instances where this tort claim is successful, class counsel will be able to seek actual, general or nominal damages. Proof of damage, particularly in the absence of significant psychological harm or damage to reputation and embarrassment, may be difficult to prove. In many scenarios, nominal damages may be the ultimate award. However, class member and counsel may be disappointed in what they can actually recover in the way of nominal damages.

5. Nominal Damages

As discussed above, proof of actual damages on a class-wide basis may be difficult in the data/privacy breach context. To overcome this problem, class counsel have been asserting a right to nominal damages in respect of proved breach of contract and intrusion upon seclusion claims. A settlement in which the damages paid were characterised as "nominal" was approved in *Condon*. That settlement was premised on evidence that individuals had spent up to four hours dealing with the data breach that had occurred and, on an assigned rate of $15 per hour of time spent, each class member was entitled to a $60 recovery.[16]

Is "nominal" a misnomer in that situation? This is important because, in breach of data or privacy class actions, class counsel will face considerable difficulty in proving actual damages on the part of individuals, and even more in proving damages class-wide. The apparent availability of nominal damages in compensation for breach of contract and inclusion upon seclusion means that those damages may be the most likely avenue of recovery for class members. Policyholders and insurers will need to understand the nature of nominal damages in order properly to assess the risk they face. As is set out below, nominal damages are not intended to compensate for a loss, but to act as an acknowledgment of a wrong suffered by a plaintiff. In the authors' view, the award in *Condon* was not nominal in nature, but compensatory. As such, that decision does not set a precedent for the value of nominal awards. Nominal damages are available when the plaintiff has proved a cause of action but not a right to compensatory damages. They may be awarded in all cases of breach of contract and in torts actionable *per se*.[17] They are not awarded by way of compensation, but in recognition of the existence of some legal right vested in the plaintiff and violated by the defendant. In contrast, real damages are those which are assessed and awarded as compensation for damage actually suffered.[18] The practical significance of a judgment for nominal damages is that the plaintiff establishes a legal right, which may deter future infringements or enable the plaintiff to obtain an injunction to prevent a repetition of the wrong.[19] It is also a way to record the defendant's liability[20] and to vindicate the plaintiff's rights even when no compensation is necessary.[21] In many cases, it will also entitle a plaintiff to costs.

Because of their non-compensatory nature, nominal damages are meant to be "a sum of money that may be spoken of, but that has no existence in point of quantity", and are damages in the name only. Although nominal awards in Canada do not have a standard size, it appears early Canadian cases assumed that the proper amount was $1, an amount which is still being awarded. However, in recent years some courts have granted significantly larger awards[22]; this is controversial. In cases where larger sums have been referred to as "nominal damages", there is often evidence, as in *Condon*, that what the court is really doing is providing compensation for a loss that it has found difficult to quantify. In *The Law of Damages*, Professor Waddams submits that courts should re-establish a conventional figure of $1 for nominal damages. Although in inflationary times it might be argued that the amount should perpetually increase, this ignores the nature of nominal damages, which is to mark symbolically the infringement of a right. An amount of $1 is not so low as to be confused with contemptuous damages and appears to be the figure having most authoritative support in Canadian cases.[23] In short, nominal damages are not simply small damages awards; they are qualitatively different from other types of damages because they are not meant to compensate a loss but to symbolically recognise that a plaintiff has been wronged.

6. What Does this Mean for Insurers and Policyholders?

As noted at the outset, while loss history is developing for first party claims in the cyber-insurance context, the scope of third-party liability remains opaque. Some class actions that have been

commenced have succeeded in having certain causes of action certified for trial: primarily negligence; breach of contract; and intrusion upon seclusion. While more exotic theories of liability have been advanced, they have either been abandoned prior to certification or have not succeeded in meeting even the very low bar applied to certification in Canada. There is no clear cause of action which will result in recovery for class members in all, or even most, cases of data/privacy breach.

With this in mind, absent unique facts which may support one or more of those "exotic" theories, at present class action claims in Canada for data/privacy breach should be evaluated primarily on the basis of whether or not they pose viable negligence, breach of contract or intrusion upon seclusion claims. It seems inevitable that one or more of the ongoing privacy class actions in Canada will proceed to trial and judgment. While defence of class action claims, particularly ones in which there are novel theories of liability, can be eye-wateringly expensive, some classes are sufficiently large to warrant such expenditure. Based on the *Condon, Tucci* and *Broutzas* decisions, it is class counsel, not defence counsel that are likely to have the more difficult time in making their case.

Were they to prove their case, the matter of damages remains thorny. In the likely event that genuine losses cannot be proved on a class-wide basis, it remains uncertain as to whether nominal damages can be awarded in the class action context. Some doubt was expressed about this prospect in *Condon*. Should nominal damages be awarded, the *Condon* decision is not precedent for the basis of such awards, as the settlement was worked out between the parties and merely approved (as opposed to awarded) by the Court. It seems more likely to the authors that a nominal award will be more in line with the discussion in this article (i.e. a token amount whether it is one dollar, ten dollars, or some other amount).

In short, while third-party data/privacy breach claims are beginning to take form, there is little in the way of certainty and predictability in respect of actual monetary exposure that can yet be discerned. The arguments available to class counsel appear poorly designed for the purpose they are presently being advanced to serve. Policyholders, insurers and their defence counsel have numerous defences that may yet succeed notwithstanding recent certification decisions. At present, and absent legislation that creates a cause of action designed and intended to address data/privacy breach liability and damages issues, it appears that the defence has the upper hand.

Endnotes

1. *Condon v. Canada*, 2014 FC 250.
2. *Tucci v. Peoples Trust Company*, 2017 BCSC 1525.
3. *Broutzas v. Rouge Valley Health System*, 2018 ONSC 6315.
4. *R v. Imperial Tobacco Canada*, 2011 SCC 42 at 17.
5. *Fehr v. Sun Life Assurance Co of Canada*, 2018 ONCA 718 at 85.
6. *Anns v. Merton London Borough Council*, [1978] AC 728 (HL).
7. *Condon* at 68.
8. *Broutzas* at 216–217.
9. *Douez v. Facebook, Inc*, 2017 SCC 33.
10. *Heller v. Uber Technologies Inc*, 2019 ONCA 1.
11. *Condon* at 50–51.
12. *Condon Settlement*, 28.
13. *Oliveira v. Aviva Canada Inc*, 2018 ONCA 321.
14. *Oliveira* at 3–4.
15. *Jones v. Tsige*, 2012 ONCA 32 at 72.
16. *Condon Settlement* at 9, 23.
17. Harvey McGregor, *McGregor on Damages*, 17th ed (London, UK: Sweet & Maxwell, 2003) at 10-001 to 10-002 [*McGregor*].
18. *Messer v. J Clark & Son Ltd*, 27 DLR (2d) 766, 1961 CarswellNB 18 (N-B Sup Ct) at 12 [*Messer*].
19. SM Waddams, *The Law of Damages* (Toronto, ON: Canada Law Book, 1991) (loose-leaf revision: 2017) at 10.10 [*Waddams*].
20. Ken Cooper-Stephenson and Elizabeth Adjin-Tettey, *Personal Injury Damages in Canada*, 3rd ed (Toronto, ON: Thomson Reuters, 2018) at 141[*Cooper-Stephenson*].
21. Jamie Cassels and Elizabeth Adjin-Tettey, *Remedies: The Law of Damages*, 2nd ed (Toronto, ON: Irwin Law, 2008) at 310 [*Cassels*].
22. Lewis N Klar, Allen M. Linden, Earl A. Cherniak & Peter W. Kryworuk, *Remedies in Tort* (Toronto, ON: Thomson Reuters, 1987) (loose-leaf revision: 2018-10) at §5.
23. *Waddams* at 10.30.

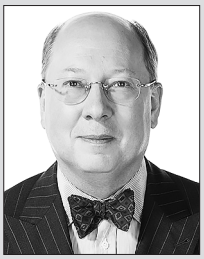
Acknowledgment

The authors would like to acknowledge the assistance of their colleagues Harrison Nemirov and Alex Fernet Brochu in the preparation of this chapter.

David R. Mackenzie
Blaney McMurtry LLP
2 Queen Street East, Suite 1500
Toronto, Ontario M5C 3G5
Canada

Tel: +1 416 597 4890
Fax: +1 416 594 5082
Email: dmackenzie@blaney.com
URL: www.blaney.com

David practises in the area of insurance coverage litigation in respect of commercial liability, technology, information and privacy, professional indemnity and first-party property claims – David has extensive dispute resolution experience both as a litigator in trial and appellate courts as well as in mediation, arbitration and negotiation. David frequently advises insurers on policy-drafting matters, and is often asked to write on insurance coverage matters, particularly involving cyber, technology and information risks. He is the Co-Chair of the Canadian Defence Lawyers Insurance Coverage Symposium, and is regularly invited to speak on insurance coverage issues. David is called to the Bar in Ontario, British Columbia and Washington State, giving him a national and international perspective.



Dominic T. Clarke
Blaney McMurtry LLP
2 Queen Street East, Suite 1500
Toronto, Ontario M5C 3G5
Canada

Tel: +1 416 593 3968
Fax: +1 416 594 2503
Email: dclarke@blaney.com
URL: www.blaney.com

Dominic practises principally in the area of insurance litigation encompassing both coverage and defence matters. He specialises in advising and representing insurers with respect to commercial general liability, directors' and officers' liability and commercial property policies. Dominic has significant experience in the defence of products liability and sexual abuse litigation. He has appeared as counsel in the Ontario Superior Court of Justice and the Ontario Court of Appeal. Dominic is a frequent lecturer to professional bodies, and is "very experienced, very agreeable and highly competent" with respondents drawing praise for his superb litigation practice, especially in coverage disputes, according to *Who's Who Legal*. He has published numerous articles on insurance and is a contributing editor to the leading Canadian insurance text, Annotated Commercial General Liability.

Blaney McMurtry LLP is a prominent, Toronto-based law firm consistently ranked as a top-tier regional firm, delivering top-level expertise in litigation & advocacy, real estate and business law.

Recognised as a leader in providing services to the insurance industry, in both coverage and defence work, many of the firm's insurance clients have worked with them for more than 20 years.

The firm's location in Canada's financial centre positions Blaney McMurtry to handle complex matters that have scope beyond Toronto and the surrounding area. Canadian experience delivered from one office.

Blaney McMurtry is a founding member of Insurance Law Global (ILG), a network of like-minded, independent insurance defence firms committed to providing global service to insurance clients from independent law firms across Europe and North America. In addition, the firm is also a member of the Risk Management Counsel of Canada, a national association of law firms providing services to the risk management industry; and of TAGLaw®, a worldwide network of independent law firms, ranked by *Chambers & Partners* as an "Elite" legal alliance.