CANADIAN LITIGATION COUNSEL

# Canadian Litigation Counsel Seminar:

## October 6, 2016

# Insurance Coverage for Data Breach and Cyber Liability Claims

Prepared by John Vamplew & Cameron Kennedy, Whitelaw Twining Law Corporation

*Presented by John Vamplew, Whitelaw Twining Law Corporation*

WHITELAW TWINING LAW CORPORATION

**www.whitelawtwining.com**

The proliferation of people using the internet to socialize, shop, and attend to their finances has led to a complacent attitude among many consumers regarding their personal information. People provide private details to companies in exchange for easy access to their services. When this private data falls into the wrong hands, the public's complacent attitude becomes litigious. A 2015 Verizon study found that a data breach involving stolen records will cost a company an average of $5,320,000. What obligation does a company have when it accepts private information from the public, and what liability does a company have to those consumers if the company fails to protect that data?

Increasingly, companies will look to their liability insurers seeking coverage for defence and indemnity under their Commercial General Liability policies, Directors and Officers policies, or policies specifically tailored for cyber-liability risks. Despite several recent high profile data breach cases, the legal system in Canada has yet to provide a clear answer in response to coverage issues under these various liability insurance policies.

Increasing the risk: Statutory Obligations

The increasing liability exposure that companies face to data breach claims arises in part from federal and provincial legislation enacted in recent years to protect the privacy interests of individuals.

In 2000, the Government of Canada passed the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*"PIPEDA"*) to protect the public's private data. More recently, the Government of Canada introduced the *Digital Privacy Act (Bill S4)* to strengthen the protections *PIPEDA* was intended to provide. The *Digital Privacy Act* received Royal Assent on June 18, 2015 and most of its provisions are now in force, or are expected to come into force soon.

Under the newly amended *PIPEDA*, if the Privacy Commissioner finds that a company has obstructed his investigation, or contravened the *PIPEDA* requirements to report security breaches, the company may be fined a maximum of $100,000. Under *PIPEDA,* a company is obliged to notify individuals whose information has been breached, as well as the office of the Privacy Commissioner, "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual". A breach report to a victim must include enough information

so the person can understand the significance of the breach and how to act to mitigate any potential damage. This report must be conspicuous, given directly to the individual, and made as soon as is feasible, barring a criminal investigation. A company is also obligated to notify any organization or government institution capable of mitigating the harm created by the data breach. Companies are obliged to keep and maintain records of every breach involving security safeguards under their control, and provide those to the Privacy Commissioner upon request.

The Office of the Privacy Commissioner has the power to make regulations respecting data breach reports. *PIPEDA* does not specify the speed or level of detail required when a company is reporting a data breach. What constitutes a "real risk of significant harm to an individual" has not yet been defined. This triggers a company's requirement to file a report. Should the harm be considered in strictly economic terms, such as loss of employment or damage to reputation? Or is the potential humiliation and damage to relationships alone sufficient to force a company to expend the considerable costs required to notify its customers? The answers to these questions remain to be resolved through regulation by the Privacy Commissioner's Office, and through developments in the case law.

Provincial governments have been slower to enact legislation that addresses data breach scenarios. While many provinces have a form of privacy legislation, this typically does not impose mandatory reporting requirements. For instance, British Columbia's *Privacy Act*, R.S.B.C. 1996, c. 373, s. 1(1) sets out that, "It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another." However, this Act is silent on what obligations exist when a person's privacy is violated. Further, B.C.'s *Personal Information Protection Act,* S.B.C. 2003, c. 63, sets out requirements in relation to the collection, use and disclosure of personal information by organizations but does not set out mandatory reporting procedures for instances of data breach.

Increasing the Risk: Common Law Privacy Rights

Developments in the common law have also led to increased liability exposure for companies arising from instances of data breach.

In *Jones v Tsige,* 2012 ONCA 32, the Ontario Court of Appeal recognized the right to bring a civil action for damages for the invasion of personal privacy. In that case, the plaintiff and the defendant were unacquainted co-workers. The defendant began a relationship with the plaintiff's ex-husband, and over the course of four years, frequently used her work computer to access personal information about the plaintiff. The plaintiff could not demonstrate economic loss, but sued under the American tort of intrusion upon seclusion. The action was summarily dismissed at trial, but the Court of Appeal ruled that if a defendant has intentionally or recklessly invaded the plaintiff's private affairs or concerns, and a reasonable person would consider the invasion as highly offensive, causing distress, humiliation, or anguish, damages may be awarded.

In *Condon v Canada,* 2015 FCA 159, the Federal Court of Appeal recently upheld the trial court's certification of a class action where the plaintiffs did not claim economic loss, proceeding on the tort of intrusion upon seclusion. Damages awarded for this tort have been up to a maximum of $20,000. When this figure is multiplied by thousands or millions of people whose personal information has not been properly protected by a company, as has been the case in some recent high profile data breach incidents, a company can quickly be driven towards bankruptcy, thus highlighting the significance of the company's need to seek defence and indemnity coverage from its liability insurers.

Commercial General Liability (CGL) policies

When the Insurance Bureau of Canada first drafted its model Commercial General Liability Policy, it is safe to say it was not considering point of sale intrusions or internet phishing schemes. Nevertheless, companies have turned to insurers seeking coverage under their CGL policies after incurring costs to remediate a data breach.

In a typical CGL policy, Coverage A insures the policy holder against compensatory damages it is legally obligated to pay because of property damage. Property damage requires that there be damage to tangible property, which is caused by an occurrence in the coverage territory during the period the

policy applies. Most data breach claims do not involve damage to tangible property, and thus such claims typically have not triggered coverage under Coverage A. Nevertheless, to provide added certainty, in 2005, the Insurance Bureau of Canada amended its model CGL policy to specifically exclude electronic data from the definition of property damage. Accordingly, under most modern CGL policies, an insured will have no coverage for a data breach claim under Coverage A.

In a typical CGL policy, Coverage B insures a policy holder against compensatory damages it is obliged to pay as a result of "personal and advertising injury". To attract coverage, an injury requires "oral or written publication, in any manner, of material that violates a person's right of privacy." Compensatory damages are confined to those that are awarded in payment for "actual injury or economic loss". As detailed above, an action alleging the tort of invasion of privacy does not necessarily require a plaintiff to demonstrate economic loss. Companies are more likely to seek coverage under Coverage B, although there are presently no Canadian cases interpreting this issue with respect to data breaches. The American cases have conflicting results defining "publication of material that violates a person's privacy." An Ohio Court[1] found that the moment a conversation is recorded constitutes publication, while an Indiana Court[2] held that a conversation stored on a company's database, potentially to be listened to by a third party, does not constitute publication. The analysis of recorded conversations in those cases may be applied to the collection of any private data.

The most recent and relevant exploration of what constitutes publication in a data breach context arises from the case *Zurich American Insurance Co. v Sony Corporation of America*, NY State Supreme Court, February 24 2014. This case arose out of the Sony PlayStation data breach. In 2011, hackers stole the names, mailing addresses, birthdates, e-mail, and credit card information of ten million people. Zurich Insurance declined to defend Sony in multiple class action lawsuits. Sony sued, arguing there was coverage under Coverage B of its CGL policy and that Zurich had a duty to defend. Zurich argued that the publication of private information which attracts coverage only applied if the insured was responsible for the publication. Unidentified hackers stole and dispersed Sony consumer's private data. The court found that when private information is removed from behind a company's safeguards, that act constitutes publication. The Court held that Coverage B applies to publication by the insured, and not by a third party, therefore Coverage B did not apply.

---

[1] *Encore Receivable Management Inc. v ACE Property and Casualty Insurance,* Dist. Ct. Southern District of Ohio, July 3, 2013.
[2] *Defender Security Company v First Mercury Insurance Company,* Dist. Ct. Southern District of Indiana, Mar. 14, 2014.

Director & Officer liability policies

If the directors and officers of a company fail to ensure their consumers' private data is adequately protected, or fail to disclose cybersecurity risks, it is possible that they may be held personally liable in actions brought by consumers or shareholders. Canadian Courts have yet to deal with a coverage action under a D&O polic in the context of a data breach claim. The bar to hold directors and officers personally liable is high. The Ontario Court of Appeal case *642947 Ontario Ltd. V Fleischer,* [2001] O.J. No. 4771 (ONCA) provides that corporate directors and officers will be found personally liable if "those in control expressly direct a wrongful thing to be done." Recent American jurisprudence indicates that Canadian directors and officers should review their D&O policies carefully.

An American hospitality company was the victim of three data breaches resulting in the theft of 600,000 customers' credit card information. In a New Jersey District Court case[3], a plaintiff filed a derivative action on behalf of the corporation against the board, CEO, and general counsel alleging that they breached their fiduciary duties of care and loyalty to the company. The plaintiff accused them of failing to put a system in place to protect consumer's private data, and concealing the data breaches from investors. American derivative actions require that the board first receive a request to investigate the breaches and sue the responsible employees. The board refused this request, and the plaintiff responded with the lawsuit. Ultimately the lawsuit was dismissed because the New Jersey Court found that the plaintiff failed to plead that the board's refusal of his demand to investigate was made in bad faith. The board had implemented cybersecurity measures previous to the first data breach, and discussed them at multiple meetings. Therefore they could not be found to have been grossly negligent and personally liable for the loss. This presents a relatively low threshold for directors and officers to protect themselves from personal liability. If a company intends to possess consumers' private information, the board must simply ensure that adequate cybersecurity measures are put in place and maintained.

Cyber-Liability policies

With the recent publicity regarding large scale data breaches, some insurers have responded by creating new policies specific to risks inherent in safeguarding the public's private information. Their new policies have been specifically structured to address a variety of cyber-risks, including but

[3] *Palkon v Holmes et al,* Dist. Ct. District of New Jersey, October 20, 2014.

not limited to the cost of recovering compromised or destroyed data, the cost of negotiating and paying an extortionist in possession of stolen data, or the cost of investigation, assessment and notification arising from a data breach. These new policies have yet to be interpreted by a Canadian Court.

Many of the cyber-liability risk policies available in the market today do not provide full coverage for companies in relation to data breach claims. For instance, many of these policies do not obligate the insurer to defend, exclude coverage for taxes, fines or penalties imposed on the insured, and do not provide coverage for costs incurred in relation to injunctive relief sought against the insured. Further, many cyber-liability policies do not cover loss of business income resulting from the data breach. Insurers and policy holders should be cautious in this newly developing field. Insurers issuing these policies should do their due diligence to ensure that the insured has adequate cybersecurity measures in place and which are updated appropriately.

High Profile Cases

*Eliot Shore v Avid Life Media Inc and Avid Dating Life Inc.* is a class action lawsuit filed in the Ontario Supreme Court for negligence, breach of contract, breach of the Ontario Consumer Protection Act, and intrusion upon seclusion. This action was brought due to the Ashley Madison hack. Hackers stole and publicly released information sufficient to identify 37,000,000 Ashley Madison users and their history. The site was ostensibly aimed at men and women who were married, and promised to keep their identities a secret. The site also offered a "full delete" service which promised to erase every trace of a user's presence. The hackers cited the falsity of this "full delete" promise as the reason for the exposure and published the information, encouraging swindled customers to take legal action. Eliot Shore obliged, and brought an action seeking damages of $760,000,000. Media reports have suggested that Avid Life has a D&O policy as well as a specific cyber liability policy, but it is not yet publically known if those insurers will provide coverage.

In December 2013, Target reported that hackers had stolen 40 million credit card records. In February of 2015 the company reported that it spent $252,000,000 in gross data breach related expenses. Plaintiff shareholders in a class action lawsuit argue that the 46% drop in profits during the important holiday season of 2013 was due to management's breach of their fiduciary duties to the shareholders, and incompetent cybersecurity measures. Target failed to have a class action

lawsuit filed by credit card issuing financial institutions dismissed. The Minnesota Court was not persuaded by Target's claim that they lacked a contractual relationship with the institutions. In August 2015, Target agreed to pay $67,000,000 to Visa Inc. on behalf of banks and other firms issuing Visa credit cards. Target had a tentative settlement for $19,000,000 with MasterCard, subject to 90% approval by the financial institutions that issued the cards. This deal was rejected by Citigroup, Capital one and J.P. Morgan Chase. They felt the deal was negotiated under a veil of secrecy without adequate legal representation, and "does not begin to cover the costs of issuing new cards and adding call center staff to answer customer questions in response to the data breach".

A class action settlement concerning the previously detailed Sony hack was certified and approved in Ontario in the case *Makisomovic v Sony of Canada Ltd.,* 2013 CanLII 41305. Class members were entitled to be paid out the balance of their funds in cash in unused online accounts, gamers were granted free software, and Sony agreed to pay consumers up to $2,500 if they could demonstrate they were victims of identity theft. Sony Canada spent $265,000 on the plaintiff's legal fees, and paid to notify 3,500,000 consumers of the settlement.

In June of 2013, a Kamloops office of Life Labs, an Ontario and British Columbia company, misplaced a hard drive containing medical information for 16,100 patients. They promptly notified the patients, as required by *PIPEDA*. The RCMP and the Office of the Privacy Commissioner investigated, and were satisfied with the internal steps taken by the company. This case illustrates that it is not only large multi-national corporations that must be vigilant against breaches of consumer privacy. While this appears to be a simple case of lost property, sophisticated hackers may be shifting their focus towards mid-size companies they perceive to be unwilling to spend the money necessary to guard against information thieves.

Conclusion

The recent glut of data breach incidents involving large corporations and millions of dollars of damages has surely drawn the attention of corporate boards and risk managers across the country. Companies who collect personal information as part of their business must be aware of the obligations imposed upon them by federal statute and at common law. They have a duty to their consumers and shareholders to ensure there are adequate cybersecurity measures in place to protect confidential information. Those measures must be fluid and constantly adapting to new threats.

The most expensive system of countermeasures is not a complete defence against a data breach. Corporations should not rely on existing CGL policies if these measures fail. Canadian and American jurisprudence has established that an insurer is likely able to successfully deny coverage for data breach claims under a CGL policy. Savvy corporations with considerable exposure to a data breach will look to a cyber-liability policy for security, however, there have yet to be any reported Canadian cases interpreting such policies.

For more information, please visit our website at www.whitelawtwining.com or contact

John Vamplew
Director
D. (604) 891-7224
E. jvamplew@wt.ca