Guild Yule LLP

Coverage for Cyber-Liability Under the CGL Policy

March 2015

Adam Howden-Duke

This paper is intended to give general information about legal topics and is not a compete statement of the law. It is not intended to be relied upon in the absence of specific legal advice on particular circumstances. Accordingly we do not accept any liability for any loss which may result from reliance upon this publication or the information it contains. Any opinions expressed herein are those of the author and may not represent the views of Guild Yule LLP.

1. Introduction[1]:

Risks falling under the general term "cyber liability" can give rise to both first party and third party losses. For example, a company subject to a cyber-hacking event may have coverage under a property policy in respect of damage to its own hardware and software. A cyber liability event may also give rise to a claim in negligence to which an Errors and Omissions policy, or possibly a claim to which a Directors' and Officers' policy may respond.

There are many potential facets to liability arising out of a cyber-related event beyond the release of private information examples commonly seen in papers on this topic. Take as one example, the hacking of a company's website and placement therein of pages associated with a phishing scheme.

This is a scheme where e-mails are sent out purporting to be from a financial institution (usually a bank), with a request for the recipient, as a customer of that institution, to confirm their account details. The e-mail contains a link to a webpage that purports to be of that financial institution, but is in fact a fraud, set up by the hackers. To prevent (or perhaps delay) detection, that page may be hidden in a legitimate website – the owners of that domain unaware it rests there. The unsuspecting recipient enters their account details, which are now in the possession of the hackers, who use that information to syphon the account.

It is at least possible that those who fell victim to the phishing scheme may assert a cause of action as against the company in whose website the fraudulent pages had been inserted (they being an easier target to identify than the hackers) alleging negligence in respect of the existence of security flaws in their website. Such action may well be launched as a class action and result in significant defence costs. It may well be commenced in another jurisdiction, which may or may not fall within coverage.

The website may include a client portal, raising the possibility of unauthorized access to personal information; in turn giving rise to other claims and notification costs. First party losses could include the need to build a new website, possible corrupted hardware and software, and associated business interruption.

This paper does not intend to try and tackle the myriad claims & coverage considerations possible in this area, but instead concentrates on a discussion of coverage for liabilities arising out of "cyber" risks under the CGL policy. The most common circumstance, as is evident from the few cases in this area, involve data breach; either unauthorized access to, or loss of, personal or confidential data.

What follows is a discussion of coverage under part A of the CGL, and the change in definition of "*property damage*" relevant to that. Then, a consideration of the concept of "compensation: in "*compensable damages*", in particular as that pertains to the Canada anti-spam legislation ("CASL").

[1] This is an updated version of a paper delivered at the CLEBC Insurance Law Conference, September 19, 2014, Vancouver, B.C. The author acknowledges the assistance of Mary Nguyen & Lindsay McGivern (articled student) in that updating.

Most of this paper is devoted to coverage under part B and in particular, personal and advertising injury as "*oral or written publication, in any manner, of material that violates a person's right of privacy*". Most of the (sparse) caselaw in this area focuses on this aspect of coverage under the CGL policy. The issues revolve around what amounts to "publication" in the context of a hacking event and whether the publication must be by or on behalf of the insured.

2. Part A – Bodily Injury and Property Damage Liability:

Coverage A provides that the insurer "*will pay those sums that the insured becomes legally obligated to pay as "compensatory damages" because of ... "property damage" to which this insurance applies*".

The typical CGL (IBC model wording) policy also provides that coverage is only provided for property damage where that is caused by an "*occurrence*" that takes place in the "*coverage territory*" and where the property damage occurs during the policy period. Those terms may well limit coverage in cases of cyber liability, where the insured is pursued for damage to property outside of the coverage territory, which is often limited to the country in which the insured carries on business.

Property damage is defined as follows:

> *"a. Physical injury to **tangible** property, including all resulting loss of use of that property; or*
>
> *b. Loss of use of **tangible** property that is not physically injured."* [our emphasis]

The circumstances of a data breach may not fall in neatly into either category. As has previously been commented: "*a data breach from a hacking incident or errant e-mail does not involve tangible property. Nor does "careless erasure of a hard drive" necessarily constitute physical injury*."[2]

Nonetheless, as has also been commented[3], there is conflicting US case authority denying and accepting coverage for data breach claims under the property damage provisions of a CGL policy. For example, in ***America Online Inc. v. St. Paul Mercury Insurance Company***,[4] AOL had been sued by a group of disgruntled users who claimed that AOL 5.0 damaged their computer systems. AOL commenced this action against its insurer to force it to defend AOL under their CGL policy. The policy defined "property damage," as:

> "*physical damage to **tangible** property of others, including all resulting loss of use of that property; or loss of use of tangible property of others that isn't physically damaged*." [our emphasis]

---

[2] Gordon Hilliker; "***Cyber Risks and Liability Insurance***", the Lawyer's Weekly (August 19, 2011)
[3] Jennifer Biernaskie; "***CGL coverage for cyber risks***", Canadian Defence Lawyers CLE, 2014
[4] 207 F.Supp.2d 459 (E.D. Va. 2002)

In the underlying action, it was alleged that AOL 5.0, inter alia, "*damaged their* [consumers'] *software, damaged their data, damaged their computers' operating system, and caused the loss of data and the loss of use of the computers*." AOL contended that computer data, software and systems were tangible property. Its insurer, St. Paul argued that computer data and the like are not tangible property because "*they constitute property that one cannot touch*."

The Virginia District Court agreed with the insurer and found that none of these things were "tangible" property. However, the Court went on to hold that "loss of use" of the claimants' computers constituted a loss of use of tangible property and was, thus, compensable under AOL's CGL policy.

On a not dissimilar fact pattern, a Kansas District Court held this did not amount to a loss of use of tangible property sufficient to trigger a duty to defend. There it appears the allegations against the defendant in the underlying litigation were slightly different in that the court found there was no allegation the computer hardware was useless, damaged or sat idle as a result of defective software.[5]

Returning to Canada, the Insurance Bureau of Canada model wordings, have likely put pay to a court finding coverage for these risks under part A of the CGL policy by virtue of 2 changes brought about by the 2005 model wording.

Firstly, the "property damage" definition was amended to include:

> *"For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and application software, hard or floppy disks, CD ROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."*

The IBC 2011 advisory model wording maintains the same definition.

Secondly, the 2005 model policy wording included an exclusion for electronic data (exclusion "l") which excludes from coverage:

> *""compensatory damages" arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."*

That would seem to close the door to coverage under part A in respect of cyber liability.

A case with facts relevant to consideration of coverage under part A is ***Recall Total Information Management Inc. et al. v. Federal Insurance Company et al.*** [6] This was a 2014 Connecticut Appellate Court decision.

---

[5] ***Cincinnati Insurance Company v Professional Data Services Inc et al*** (2003 U.S. Dist. LEXIS 15859)
[6] 147 Conn. App. 450; 83 A. 3d 664; 2014 Conn. App. Lexis 6

In this case, Recall Total Information Management had entered into an agreement with IBM to transport and store various electronic media belonging to IBM. During transport, a cart containing computer tapes of IBM fell out of the back of a van and approximately 130 of them were removed from the roadside by a person or persons unknown, and were never recovered. Because the tapes contained personal information of some 500,000 past and present employees of IBM, it took steps to protect the affected employees against identity theft at a cost of more than $6 million. It made demand of Recall Total for the costs it had incurred.

The Appellate decision considers whether there was coverage under part B of the CGL. However, it also notes the trial Court addressed whether the loss was covered under the property damage provision of the policy. It is noted that the lower court determined that the data loss constituted intangible property which was expressly excluded from coverage. The issue being that it was the loss of data on the tapes which gave rise to the claim by IBM for compensatory damages rather than loss of the tapes per se.

3. "Compensatory damages":

The first party costs flowing from a data breach may include store credits and similar voluntary payments. Both Part A & Part B provide coverage for sums an insured becomes legally obligated to pay as "*compensatory damages*". The IBC model wording[7] defines these as:

"*means damages due or awarded in payment for actual injury or economic loss*"

It is possible that certain types of third party losses and claims flowing from a data breach may not fall within this definition. Examples include privacy legislation such as PIPEDA which may require restorative steps, notification steps, or preventative costs.

There is a paucity of case law dealing with the concept of what constitutes "compensatory damages" in cyber liability. The point does not appear to have been argued in ***Recall Total Management Inc.***,[8] despite the nature of the costs which IBM were seeking repayment of.

A Canadian case considering what constituted compensatory damages under a liability policy is ***Brockton Municipality v. Frank Cowan Company***[9]. Residents of Walkerton commenced a class action lawsuit against the municipality for damages arising out of E. coli contamination of the public water supply. This litigation concerned Brockton's application for determination of its rights under two insurance policies. Those included whether there was a duty to defend.

The municipality sought coverage for all of its costs including;

- legal fees for the compensatory damages claims,
- legal fees for responses to regulatory and investigative authorities including the OPP, the Coroner and the Ministry of Environment,
- engineering expenses to respond to the Ministry of Environment field order,

[7] 2005 & 2011
[8] This was not addressed in the Appellate decision; the author has not reviewed the trial decision
[9] 2000 O.J. No. 4455; [affirmed on appeal: (2002) O.J. No. 20 (Ont. C.A.)]

- public relations expenses, and
- remediation expenses.

Caswell, J. commenced with noting:

> *"Traditionally the legal costs associated with the defence of damage claims have been covered by the liability insurance policy. Canadian cases tend to take a more conservative view of the insurer's obligation to pay additional costs, but the American authorities can be quite instructive on this issue."*[10]

While he went on to note that some American and Canadian authorities have held the cost of remedial measures taken by an insured in response to the directive of an administrative agency, may fall within the coverage ordinarily provided by a liability insurance policy:

> *"It is my view, however, that the expenses incurred by Brockton with respect to the MOE and OPP investigations, the engineering reports, remediation work, the public relations expenses and the public inquiry are simply too remote and are not covered by their liability policy".*[11]

(a) Compensatory damages & CASL:

While not likely to fall under the GCL policy, a current talking point in this area of the debate are how damages under the CASL are to be viewed.

Technology has dramatically changed the day-to-day operations of most organizations. Businesses and institutions are seeing the benefits of using large pools of data to advance their marketing objectives. The easy collection and storage of consumer information has enabled organizations to promote their products and services by inundating the inboxes of hundreds and thousands of existing as well as prospective consumers. However, the arrival of CASL has put businesses at risk of contravening the legislation and potentially hefty fines.

CASL's main objective is to prohibit the sending of commercial electronic messages (CEMs) to recipients in Canada whose express consent has not been obtained. Subject to limited exceptions, organizations will generally have to obtain the express consent of the prospective clients before transmitting messages of a commercial nature.

Organizations that find themselves in violation of CASL can face serious consequences. In addition to significant administrative penalties of up to $1 million per violation for individuals and $10 million per violation for organizations, CASL also creates a private right of action, permitting any person affected by the CASL violation to sue for actual as well as statutory damages. When the provisions creating private right of actions come into effect on July 1, 2017, persons receiving electronic spam will be able to assert fixed damages of $200 per statutory contravention up to a maximum of $1 million. The legislation also opens the door for anti-spam class action lawsuits.

[10] Ibid, para. 78
[11] Ibid, para. 81

In time, it is anticipated that organizations will transition into specialized forms of insurance coverage that provides for wider scope of electronic and data coverage and even specific coverage for CASL-related actions. However, in the near future, one of the key concerns arising out of CASL is whether organizations can look to their insurers to defend and indemnify them for costs and damages arising from non-compliance with the legislation. Put differently, ought CASL-related losses fall within the scope of traditional liability policies?

From the insurer's perspective, the issue of whether CASL-related damages will be covered will likely depend on whether such damages are "compensatory" as that term is generally used in policy wordings.

On its face, there is presently nothing in CASL that specifically states whether damages under the regime are compensatory or punitive. Conventional wisdom suggests that courts will likely look to the purpose of the statute when determining the nature of the damages. The general principle is that if there is a compensatory element to the award, then the award is compensatory. Conversely, if the goal of the award is to deter and punish, then the award is not compensatory and hence, not covered under traditional coverage.[12]

Whether damages under CASL fall under the current rubric of "compensatory damages" remains a question to be decided in Canada. To this end, we turn to the US for guidance. There have been several American authorities that have considered the issue of whether liquidated damages, that are more than the amount of actual harm sustained by the injured party, were penal and therefore not covered.

The issue before the Illinois Supreme Court in ***Standard Mutual Insurance Co v Lay***[13], was whether damages awarded under the *Telephone Consumer Protection Act*, 47 USC §227(b) ("TCPA") was covered under the a CGL policy or a liability policy. Briefly, TCPA prohibits a number of advertising practices including the use of automated telephone dialing systems to parties without their consent as well as the transmission of unsolicited fax advertisements. The underlying case involved Lay, a real estate agency that had contracted with a Business to Business (BTB), "blast fax" service, to send advertisements to 5,000 Illinois residents. B2B falsely represented to Lay that it had obtained the consent of the fax recipients when it had in fact, not. The recipients brought a class action against Lay, alleging violations of the TCPA and claiming the statutory damages of $500 per violation.

Lay tendered the TCPA class action to its insurer, Standard Mutual, which undertook the defence but reserved the right to deny coverage on a number of grounds. Standard Mutual sought, among other things, a declaration that the statutory damages under the TCPA were punitive and therefore, excluded from coverage.

The circuit court who found in favour of the insurer. The decision was affirmed by the appellate court which agreed with Standard Mutual that damages pursuant to the TCPA were punitive and

[12] Heather Sanderson: *"The CGL-Policy & Privacy Breach- What's Covered and What's Not?"*, Canadian Defence Lawyers CLE, February 2015
[13] 2013 IL 114617.

uninsurable. The Illinois Supreme Court reversed the lower courts' decisions, finding that the "*manifest purpose of the TCPA is remedial and not penal*". The court noted that the liquidated damages of $500 per violation under the TCPA could be viewed as compensation for the annoyance and inconvenience of receiving the unsolicited fax as well as an incentive for the aggrieved consumers to enforce the state. In short, the $500 liquidated damages served "*additional goals than deterrence and punishment*" and was therefore, compensatory for the purposes of coverage.

4. Part B – Personal and Advertising Injury Liability:

Part B coverage provides (in part):

> *"We will pay those sums that the insured becomes legally obligated to pay as "compensatory damages" because of "personal and advertising injury" to which this insurance applies..."*

Personal and advertising injury is defined exclusively from a list of offences. Relevant to cyber liability is:

> *"e. Oral or written publication, in any manner, of material that violates a person's right of privacy;"*

As is mentioned above, the typical cyber liability exposure follows the release of, or unauthorized access to, personal and/or confidential data. There is no available caselaw in Canada directly on the issue of coverage under a CGL policy for data breach that the author has been able to locate. We therefore consider US case law. These cases focus on the meaning of "*publication*" & "*in any manner*".

Defender Security Company v. First Mercury Insurance Company[14]was a motion by Defender Security, for a declaration that it was owed a defence. The underlying facts involved a class action arising from the allegedly unauthorized recording of customer calls into Defender security. The class action asserted that Defender's acts violated the California Penal Code which prohibits the recording of confidential communications made by telephone without the consent of all parties to the communication.

Defender Security sought coverage under part B and in particular, personal and advertising injury. The application before the Court was that of the insurer seeking dismissal of the action. Accordingly, the matter proceeded upon the face of the pleadings in the underlying class action. It was noted that the underlying action did not contain any allegations of "*publication*" of the recorded conversations. The Court records:

> *"Here, the only dispute between the parties is whether Ms. Brown's allegation that Defender recorded her telephone conversation in which she revealed*

[14] Dist. Ct. Southern District of Indiana, Mar. 14, 2014

> *personal information and then stored that recorded information, constitutes 'publication' under the terms of policy. We are not persuaded that it does."*[15]

The Court considered that the insured's argument that the fact that the Brown complaint alleges that Defender stores the recordings "*for various business purposes*" implied that a third party would be listening to the recordings and that they are thus being produced for distribution to at least one person as "… *at best a strained interpretation* [of the term] *publication"*[16]

This case illustrates that in most cases of data breach, the insured may well fail in proving the "*publication*" requirement under the definition of "*personal and advertising injury*" in cases of data breach.

An opposite result was arrived at in ***Encore Receivable Management Inc. v. ACE Property and Casualty Insurance***[17].

This case also concerned a duty to defend in an underlying action arising from unauthorized recording of customer calls. There were two underlying actions that were commenced. In one, it was alleged that not only were the calls recorded without consent, they were "*then distributed internally within Encore for training and quality control purposes*". However, while that would distinguish the facts from ***Defender Security***, it does not appear to be the basis upon which the Court came to the opposite finding here than the Indiana District Court had in that case. The Court held:

> "*this Court need not find that the communications were actually disseminated to third parties because the initial dissemination of the conversation constitutes publication at the* ***very moment that the conversation*** *is disseminated or* ***transmitted to the recording device***."[18]

This decision predated that in ***Defender Security***, and the Indiana Court does record as a footnote to its judgment being apprised of the decision in ***Encore.*** However, it chose not to follow it. Judge Sarah Evans-Barker noting:

> *"we are not bound by this District Court decision, and because we find its analysis to be contrary to the manner in which we believe Indiana Courts would decide this issue, we do not apply its reasoning here".*

The difficulty insureds face in proving the publication requirement was highlighted more recently in the Pennsylvania Federal court decision of ***OneBeacon America v Urban Outfitters Inc et al.***[19] In the underlying action, Urban Outfitters and Anthropology faced multiple class actions related to the collection of customer information at the point of sale. The allegations were generally that the retailers were collecting customer information to create a database which they

[15] Ibid at p. 8 of the judgment
[16] Ibid at p. 9 of the judgment
[17] Dist. Ct. Southern District of Ohio, July 3, 2013
[18] Ibid at p. 12 of the judgment
[19] Dist. Ct. Eastern Pennsylvania, May 15, 2014)

could then potentially sell to other businesses, in violation of various privacy-related statutes in each of the states where the actions were commenced.

OneBeacon filed a suit seeking a declaration that it was not obligated to defend or indemnify the retailers in the underlying actions where violations of state statutes and common law privacy rights were being alleged. OneBeacon had issued the retailers CGL and umbrella policies that defined "*personal and advertising injury*" in part as "*injury arising out of* [o]*ral or written publication of material that violates a person's right to privacy*". OneBeacon took the position that no coverage was triggered as the allegations did not make out a "publication" as required by language of the policy.

The court agreed with OneBeacon, stating that although the term "publication" was not defined in the policy, a plain dictionary definition of the word required the material in question to be promulgated "*to the public, even to a limited number of people*" such that the matter can be regarded as substantially certain to become one of public knowledge. In essence, the fact that the database *could* be sold by the retailers to a third party did not constitute publication triggering coverage.

In Canada, the word "*publication*" as used in the standard IBC GCL coverage grant, has yet to be tested. That said, what constitutes "*publication*" was considered by the Alberta Court of Queen's Bench in ***PCS Investments Ltd. v. Dominion of Canada General Insurance Co.***[20] The policy there afforded coverage for personal injury "*excluding advertising, publishing, broadcasting or telecasting*"[21]. The plaintiff sought coverage for the defence of an action alleging that it mailed a defamatory letter to 130 members of the insurance industry. The Court held distribution to 130 persons was not a widespread or public distribution to a broad audience and therefore not a "*publication*".

In a more recent decision from B.C. – ***Reform Party of Canada v Western Union Insurance Company***[22] it was held that posting on the internet met the definition of "*publication*". The Court noted that dictionary definitions of "*publish*" and "*broadcast*" required activity that is accessible and available to the public. There were 738 'hits' to the website. The court commented that the number of hits was not relevant; unlike in ***PCS***, the audience was not restricted.

While some of the earlier mentioned examples would appear to suggest that the publication requirement can sometimes be difficult for insureds to meet, it is important to remember that in cases where there are ambiguities as to whether there has been a "publication", Canadian courts will be likely interpret the term broadly and in favour of coverage. This broad approach is highlighted in ***Conservation Council of New Brunswick v Encon Group Inc***.[23] The underlying defamation action involved allegations that two of the Conservation Council's officials defamed a corporation by making oral and written statements to several newspapers that got published by the newspapers.

---

[20] (1994) 18 Alta. L.R. (3d) 270
[21] This was based on earlier IBC wording – 1987.
[22] [1999] BCJ No. 2794 (reversed on other grounds; [2001] BCJ No. 697 (BCCA))
[23] 2006 NBCA 51, as summarized by Sanderson, *supra*., note 12

The insured brought a petition for coverage. Co-operators denied coverage on the basis that defamation coverage under the policy required the insured to have published the defamatory material itself. In this case, the statements were published by third parties. Alternatively, Cooperators argued that if the allegations triggered coverage, they were squarely excluded by the exclusion against claims for "*advertising, publishing or telecasting done by or for* [the insured]".

Given Co-operator's alternative arguments, the court was forced to determine what the terms "*publication*" and "*publishing*" meant as the terms were used in the coverage grant and in the exclusion. The court noted that the two words could not mean the same thing because everything that would fall within coverage would then be excluded by the exclusion, resulting in a "*nonsensical interpretation*" nullifying reasonable expectations of coverage. In face of the ambiguity, the court found a duty to defend.

The New Brunswick Court of Appeal dismissed the insurer's appeal, holding that since it was not clear that the statement of claim fell outside the insuring agreement, there was a possibility of coverage and the insurer was therefore compelled to defend the claim.

The definition of "*advertisement*" in the 2005 and 2011 IBC model wording now includes, explicitly, a notice published "*to the general public or specific market segments*".

It also holds:

> *"For the purposes of this definition:*
>
> *A. Notices that are published include material placed on the Internet or on similar electronic means of communication;..."*

Returning to ***Recall Total Information Management v. Federal insurance Co.***, in addition to seeking coverage under the property damage side of its CGL policy, Recall Total also sought coverage under personal and advertising liability.

Recall Total alleged that the data on the stolen tapes had been "*published*" to the thief and/or other persons unknown. The Court adopted the definition of publication set forth in Webster's Third New International Dictionary which defines publication as the "*communication (as of news or information) to the public*". As the parties agreed that no identity theft incident could be traced to the loss of the IBM tapes, there was no allegation in the underlying action of publication. The Court noted that Recall Total did not allege that the information contained in the tapes was ever accessed and there was no evidence as of the date of the lower court decision - noted to be some four years after the incident - that any person had suffered any identity theft.

In ***Recall Total***, the data on the tapes was encrypted, but what if the data had in fact been accessed and there was evidence of that? Would that have been publication by Recall Total, or by the unidentified hackers within the definition in the policy? Does the policy require the publication to be by the policy holders, or can it apply to publication by others? These issues, amongst others were considered by the Supreme Court of the State of New York in ***Zurich***

American Insurance Co. v. Sony Corporation of America[24], perhaps one of the most keenly anticipated decisions in the area of cyber liability[25].

This was an application for a declaration of a duty to defend Sony Corp. as a result of a large scale data breach. The background circumstances are as follows.

Sony develops and markets PlayStation portable handheld devices (known as PSP's) which allow users to play games. However the device can also connect to the internet, and access "*qriocity*". Through all of this, account holders are able to engage in on-line games, play other account holders through the internet, and purchase and download content from the internet including games, movies and similar entertainment. Users can also access other prepaid third party internet services such as Netflix.

The facts of this case centered on the user account data given to Sony; users are required to provide Sony with personal identification information including the names, mailing addresses, e-mail address, birthdate, credit and debit card information in order to open an account through the PlayStation console. That system was hacked into and that information stolen. Sony then faced a number of actions; some alleging that it disclosed private information to unauthorized parties, and another alleging that it had breached its duty of care to protect personal information from being disclosed to unauthorized parties, and placed sensitive information in the hands of cyber hackers.

The proceedings were a summary judgment application seeking a duty to defend under part B of the CGL policy, which was argued in March of last year - although it appears the motion was within a wider set of proceedings between various Sony entities and insurers. We focus on the Court's determination of whether the data breach constituted personal and advertising injury as "*oral or written publication, in any manner, of material that violates a person's right of privacy*".

With respect to this, the insurer's first point was that the publication had to be by or on behalf of the insured. As the Court framed the issue: "*but, the question is, does this policy prevent, does this policy provide you coverage for you being the victim rather than the perpetrator*."[26]

It was Sony's position that the words "*in any manner*" meant that publication could either be by or on behalf of the insured, or (as argued in this case) by the cyber hackers. Sony asserted that "*in any manner*" was inconsistent with reading an implied requirement that the publication has to be by the policy holder. Sony went on to note that there are requirements that must be met to fall within coverage for personal and advertising injury liability; namely that the personal and advertising injury must arise out of the insured's business; occur in the coverage territory; and during the policy period. Sony submitted that if the insurer wished to impose the requirement that the publication be by the policyholder, it must express that in the policy.

Relevant to this, the insurer also argued that the policy required purposeful conduct, looking at the definition of "*personal and advertising injury*" (e.g. false arrest, malicious prosecution), and

[24] NY State Supreme Court, Mar. 3, 2014
[25] See e.g. Randy Maniloff: "***coverage opinions***" vol. 3, issue no. 6, April 1, 2014 (www.coverageopinions.info)
[26] Supra note 24, @p. 32, lines 21 - 23

that Sony's contention that the liability arising from this hacking event fell within coverage as "*oral or written publication*" replaces "*publication*" with "*disclosure*" under "e".

As to the "*in any manner*" argument, the insurer replied that that phrase focuses on the mode or method of publication; that "*there are many ways to publicize it. An oral or written publication in any way. It doesn't mean you can replace the word publication with disclosure*"[27]

The Court found that here the information had been stolen and that "*to equate publication with the theft of information is to essentially say, I'm going to ignore the word publication because no definition of publication includes theft*".[28]

It went on to find that coverage was only available when the publication was performed, done or undertaken by the insured or the insured's affiliates, employees and so forth.[29] That is; there is no coverage when the publication is undertaken by someone else.

However, secondly, the Court addressed whether there was in fact "*publication*" of the data in question here. As is noted above, it was the insurer's position that the information had been stolen by the hackers, and to equate publication with those circumstances was to replace the word "*publication*" with "*disclosure of personal information*". It was the insurer's position that publication requires: "… *widespread disclosure to the general public in the sense of a public announcement or a publication of a book or magazine*".[30] I.e. a purposive act.

In this case the underlying complaints did not allege that the hackers had published any of the personal information; they alleged (only) the fear that that may occur.

As to what constituted "publication", the Court held that the mere access to that was sufficient:

> *"So that in the box that is safe and that is secured. Once it is opened, it comes out. And this is where I believe that's where the publication comes in. It's been opened. It comes out. It doesn't matter if it has to be oral or written.*
>
> *We are talking about the internet now. We are talking about the electronic age that we live in. So that in itself, by just merely opening up that safeguard all that safe box where all of the information was, in my mind my finding is that that is publication. It's done."*[31]

However, the court found that the publication was not done or perpetrated by Sony, but by the hackers. The Judge thus denied the motion for a declaration of a duty to defend. The trial judgment was appealed and that appeal was heard in December. The Appeal court's ruling has not yet been handed down.

---

[27] Supra, note 24, @p. 55, lines 18-21
[28] Supra, note 24, @p. 75, lines 9 - 12
[29] Supra, note 24, @p. 76
[30] Supra, note 24, @p. 37, lines 22-25
[31] Supra, note 24, @p. 76, line 24 to p. 77, line 8

5. Conclusion

The current state of the law (at least in the short term) appears to be that the loss of personal or private information as a result of a hacking event, will not be covered under a commercial general liability policy, because "*publication in any manner*" requires the publication be on or behalf of the insured. The effect on Canadian jurisprudence, of the court's finding that mere fact of accessing the information does amount to "*publication*" is unclear, given the existing caselaw suggesting something more active is required.

Following the changes to the IBC model wording, it seems unlikely coverage for first part losses will be found under part A. However experience has taught the industry that it is impossible to dream up every possible claims circumstance that may come before insurers.