Guild Yule LLP

Coverage for Cyber-Liability Under Existing Policies

September 19, 2014

Adam Howden-Duke

1. Introduction:

Despite the width of the title to this paper, it concentrates upon coverage under the commercial general liability ("CGL") policy.

Risks falling under the general term "cyber liability" can give rise to both first party and third party losses. For example, a firm subject to a cyber-hacking event may have coverage under a property policy in respect of damage 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. Take as one example, the hacking of an entity'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.

Without commenting on the merits of such an action, it is at least feasible that those who fell victim to the phishing scheme may assert a cause of action against the firm 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.

However, we turn back to the purpose of this paper and 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.

We will discuss coverage under side A of the CGL, and the change in definition of "*property damage*" relevant to that. We will also discuss briefly a recent US case relevant in this area.

Most of this paper is devoted to coverage under side B and in particular, coverage for "*personal and advertising injury*" as "*oral or written publication, in any manner, of material that violates a person's right of privacy*". This is because most of the (sparse) caselaw in this area focuses on this.

Within this area, we consider what losses may fall within the definition of "*compensatory damages*" under a CGL policy, noting one Canadian case on the issue. Following this, we will discuss 4 recent US cases that consider coverage under this part of the policy.

2. Coverage 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*."[1]

Nonetheless, as has also been commented[2], 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***,[3] 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]

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*."

---

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

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.

Returning to Canada, the Insurance Bureau of Canada, has likely put pay to a court finding coverage for these risks under side 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.*** [4] This was a Connecticut Appellate Court decision of January this year.

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 side 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

[4] 147 Conn. App. 450; 83 A. 3d 664; 2014 Conn. App. Lexis 6

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. Coverage B – Personal and Advertising Injury Liability:

Side 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 in the outset of this paper, the typical cyber liability exposure follows the release of , or unauthorized access to, personal and/or confidential data.

(a) "Compensatory damages":

Before discussing coverage under clause "e" of the personal and advertising liability definition, we will consider the concept of what damages may attract coverage.

The first party costs flowing from a data breach may include store credits and similar voluntary payments. When considering third party liability claims, a question arises as to whether all damages claimed are "*compensatory damages*". The IBC model wording[5] defines these as: "*means damages due or awarded in payment for actual injury or economic loss*"

It is possible that certain types of claims flowing from a data breach may not fall within the definition of compensatory damages. 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.***,[6] despite the nature of the costs which IBM were seeking repayment of.

However, of potential relevance are those cases dealing with environmental damage claims where those statutes have a variety of relief measures. As regards responsive costs, as noted by Snowden and Lichty[7], a CGL policy responds only to claims for damages.

---

[5] 2005 & 2011
[6] This was not addressed in the Appellate decision; the author has not reviewed the trial decision
[7] Annotated CGL policy 8:20.7

In ***Energy North Natural Gas Inc. v. Century Indemnity Co.***[8], a distinction was made between responsive costs which were strictly preventative versus those which were remedial in nature. That case concerned environmental cleanup costs of land which had housed a former gas plant. The insurer had denied coverage on the basis the cleanup costs were at least partly preventative and therefore outside of coverage. The Appeals Court affirmed the lower court decision that the response (cleanup) costs were remedial in nature and therefore covered under the policy.

In ***Cinergy Corp. v. Associated Electric and Gas Insurance Co.***[9], the Supreme Court of Indiana denied the policyholder's request that its insurer defend the insured energy company in an underlying action commenced by the US federal government, arising out of an alleged failure to comply with the *Clean Air Act*. The Court held that CGL insurers do not owe a duty to defend claims that call for the installation of government mandated equipment which reduces emissions and pollution.

Although preventative expenditures need to be distinguished from abatement expenditures, where there is present damage, the costs of remediating and preventing further harm are generally categorized as damages. For example, and ***N.L. Industries Inc. v. Commercial Union Insurance Co.***[10], the District Court of New Jersey dealt with a claim by a lead paint manufacturer for indemnity. An action had been commenced against a public Housing Authority arising out of the presence of lead paint in a housing project. The Housing Authority joined the paint manufacturer as a party to the action. The insurer argued that the costs incurred to remove or prevent the chipping and decomposition of the lead paint were purely preventative and they were neither "damages" nor "property damage". The Court disagreed, holding that there was ongoing damage which could result in lead poisoning. "*In the circumstances, the case was one of abatement rather than one of prevention*."[11]

A Canadian case considering what constituted compensatory damages under a Liability policy is ***Brockton Municipality v. Frank Cowan Company***[12]. 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,
- public relations expenses, and
- remediation expenses.

[8] 452 F. 3d 44 (1st CIR (N.H.) 2006)
[9] 865 N.E. 2d 571 (Ind. Sup. Ct. 2007)
[10] 926 F. Supp. 446, 1996 U.S. Dist.
[11] Supra note 7 8:20.9; p. 8-32
[12] 2000 O.J. No. 4455; [affirmed on appeal: (2002) O.J. No. 20 (Ont. C.A.)]

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."*[13]

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".*[14]

(b) Recent caselaw:

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.

We consider three cases on analogous issues in considering whether there is coverage for claims for compensatory damages arising from "*Oral or written publication, in any manner, of material that violates a person's right of privacy"* following a cyber-liability event / data breach, and one (much anticipated) decision considering coverage for a hacking incident under coverage B of the CGL.

Defender Security Company v. First Mercury Insurance Company[15]

This 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 side B and 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:

[13] Ibid, para. 78
[14] Ibid, para. 81
[15] Dist. Ct. Southern District of Indiana, Mar. 14, 2014

> *"Here, the only dispute between the parties is whether Ms. Brown's allegation that Defender recorded her telephone conversation in which she revealed personal information and then stored that recorded information, constitutes 'publication' under the terms of policy. We are not persuaded that it does."*[16]

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*" implies that a third party will 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"*[17]

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*".

An opposite result was arrived at in ***Encore Receivable Management Inc. v. ACE Property and Casualty Insurance***[18].

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***."[19]

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".*

In Canada, 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

[16] Ibid at p. 8 of the judgment
[17] Ibid at p. 9 of the judgment
[18] Dist. Ct. Southern District of Ohio, July 3, 2013
[19] Supra, note 16 at p. 12 of the judgment
[20] (1994) 18 Alta. L.R. (3d) 270
[21] This was based on earlier IBC wording – 1987.

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.

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***[23], perhaps one of the most keenly anticipated decisions in the area of cyber liability[24].

---

[22] [1999] BCJ No. 2794 (reversed on other grounds; [2001] BCJ No. 697 (BCCA))
[23] NY State Supreme Court, Mar. 3, 2014
[24] See e.g. Randy Maniloff: "***coverage opinions***" vol. 3, issue no. 6, April 1, 2014 (www.coverageopinions.info)

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 side B of the CGL policy, which was argued in March this year - although it appears the motion was within a wider set of proceedings between various Sony entities and insurers.

Firstly, the Court considered the insurer's position that exclusion J applied:

> *"This insurance does not apply to:*
> *…*
> ***j. Insureds In Media and Internet Type Businesses***
> *"Personal and advertising injury" committed by an insured whose business is:*
> *(1) Advertising, broadcasting, publishing or telecasting;*
> *(2) Designing or determining content of web-sites for others; or*
> *(3) An Internet search, access, content or service provider."*

It was the insurer's argument that Sony fell within the 3rd element that of this exclusion; that by virtue of the PSP's internet capability and the operation of qriocity, Sony was "*an Internet search, access, content or service provider*". It was admitted that this was not all Sony did; the insurer's argued that it was sufficient to fall within the exclusion, that it was a principal or central party of Sony's business. The Judge summed up the insurer's argument as:

> "… *You're asking me to read this your way of saying that, well, it doesn't mean that's exclusively what they have to do, but principally what they have to do.*
> *There is no such wording in here that says, either principally or exclusively.*
> *But, you're asking me to read it this way.*"[25]

[25] Supra note 23, @p. 19 line 22 to p. 20 line 2 (transcript of proceedings)

Aligned with this argument, was one with regard to which Sony entity was bringing the motion (different entities apparently playing different roles in the provision of the totality of the services). Indeed, counsel for Sony admits that "*we brought this motion on behalf of two companies that we thought under no possible conception should be within the internet business exclusion*."[26] The court went on to find that there was no qualifying language in the exclusion to support the insurer's position and that on the facts before the court, Sony Computer Entertainment America Inc, being the entity at issue, did not fall within the language of the exclusion.[27]

Next, the Court considered the insurer's argument that the matter fell within an exclusion applying to distribution of material or information in violation of statute. The Court found that that did not apply.

We wish to 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*."[28]

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 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*"[29]

[26] Supra note 23, @p. 21, lines 13-15
[27] Supra note 23, @p. 24, line 6 to p25, line 21
[28] Supra note 23, @p. 32, lines 21 - 23
[29] Supra, note 23 @p. 55, lines 18-21

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*".[30]

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.[31] 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*".[32] 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."*[33]

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. We understand this judgment is under appeal, the hearing is set to occur in December.

4. Conclusion

The current state of the law (at least in the short term) therefore 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.

[30] Supra, note 23, @p. 75, lines 9 - 12
[31] Supra, note 23, @p. 76
[32] Supra, note 23, @p. 37, lines 22-25
[33] Supra, note 23, @p. 76, line 24 to p. 77, line 8