ICLG

The International Comparative Legal Guide to:

Insurance & Reinsurance 2014

3rd Edition

A practical cross-border insight into insurance and reinsurance law

Published by Global Legal Group, with contributions from:

AlixPartners
Anderson Mōri & Tomotsune
Attorneys at Law Borenius Ltd
Bedell Cristin
Blaney McMurtry LLP
Cabinet BOPS
Chalfin, Goldberg, Vainboim & Fichtner Advogados Associados
Clyde & Co LLP
Clyde & Co LLP and associate CIS Advocates
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
DAC Beachcroft SLPU
DAC Beachcroft Colombia Abogados SAS
Debarliev, Dameski & Kelesoska Attorneys at Law
Erçin Bilgin Bektaşoğlu Law Firm
gbf Attorneys-at-law
JŠK, advokátní kancelář, s.r.o.
KALO & ASSOCIATES
Morton Fraser LLP
Oppenhoff & Partner Rechtsanwälte Steuerberater mbB
Osterling Abogados
Rose-Marie Lundström Advokat AB
Russell McVeagh
Sahurie & Asociados
Studio Legale Giorgetti
Tuli & Co
Wotton + Kearney

GLG
Global Legal Group

The International Comparative Legal Guide to: Insurance & Reinsurance 2014

GLG
Global Legal Group

Contributing Editors
Jon Turnbull & Geraldine Quirk, Clyde & Co LLP

Account Managers
Edmond Atta, Beth Bassett, Maksim Dolgusev, Dror Levy, Maria Lopez, Florjan Osmani, Oliver Smith, Rory Smith

Sales Support Manager
Toni Wyatt

Sub Editors
Nicholas Catlin
Amy Hirst

Editors
Beatriz Arroyo
Gemma Bridge

Senior Editor
Suzie Kidd

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
February 2014

ISBN 978-1-908070-88-3
ISSN 2048-6871

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

Country Question and Answer Chapters:

Data Risk, Privacy Breach and Insurance Coverage in Canada

Lori D. Mountford

David R. Mackenzie

Blaney McMurtry LLP

Big Data

The advent of cloud computing has meant that the data storage capacity available to businesses and institutions has become limitless. According to a 2011 IBM advertisement, 90 per cent of the data in the world was created in the two years prior. [See Endnote 1.] IBM estimates that 2.5 quintillion bytes of new data are created daily. [See Endnote 2.] Just this year, *The New York Times* reported that commercial rents in areas of New Jersey are reaching $600 or more per square foot because of demand from new data centres. [See Endnote 3.] These data centres, and others like them around the world, are hosting vast data collections, which have been popularly dubbed *Big Data*.

Big Data is the outcome of an electronically interconnected world. Most of us connect with the electronic world frequently each day. We pay with credit cards and debit cards, access online social networks and use search engines. Our activities are recorded by omnipresent cameras, both public and private, and uploaded to the Internet. Our daily lives generate innumerable electronic records. Much of this digital information is open to public or commercial view. When aggregated, such information becomes Big Data.

Big Data is seen as providing new ways of gaining remarkable insights into a vast range of subjects. An article in *Foreign Affairs* magazine explains:

> "Big data starts with the fact that there is a lot more information floating around these days than ever before, and it is being put to extraordinary new uses. Big data is distinct from the Internet, although the Web makes it much easier to collect and share data. Big data is about more than just communication: the idea is that we can learn from a large body of information things that we could not comprehend when we used only smaller amounts." [See Endnote 4.]

Accessible Big Data is changing the manner in which business, research, and even politics are conducted. Increasingly, business, government, educational and medical institutions, as well as individuals, are seeing the benefits of using enormous data pools to better advance their goals. When processed properly, large data collections can reveal trends and patterns that provide in-depth understanding of human behaviour.

The expansion of consumer information available to businesses is perhaps the most notable (and, to many, concerning) of all developments. An article on the American Bar Association's *ABA Journal* site states:

> "… Soon, just as websites recognize an individual and start targeting personalized advertising onscreen, retailers will be able to put a name to a face and take a similar marketing approach by linking information obtained from the Internet to the real-life person. Even social security numbers will likely be part of the mix." [See Endnote 5.]

The author warns that a facial recognition database could include anyone whose picture has been posted online along with their name. The technology necessary to link data from the Internet to the real-life person for marketing purposes does not yet exist, but may well soon for large corporations.

It is not only large business entities, however, that present data risks. While not every business entity and organisation will have pools of information comparable to those collected by large retailers, credit card companies, search engines, and social networks, almost every organisation will store substantial private electronic information. Health networks can aggregate medical information; universities can aggregate student information; banks can aggregate financial information. Even small businesses seek to aggregate as much information about their customers as they can. How often are we asked to provide our telephone number or postal code at the cash register? There is value in developing comprehensive customer profiles. Risks arise out of data pools whether the collection is large or small.

Of course, information is useless unless it is capable of analysis in a timely fashion. It is important to data owners to get information processed, evaluated, and put to use as quickly as possible. It follows that data must be stored in an easily accessible form. The result is large amounts of data, including commercially sensitive information and private individual information, stored in places which put it at risk of being lost or stolen. Examples include inadequately protected servers, the cloud, laptop computers, iPhones and BlackBerries, USB keys, and so on.

According to the Identity Theft Resource Center, in 2012 alone, more than 17 million confidential records were put at risk through 470 reported security breaches in the US. [See Endnote 6.] A breach is defined in the report as "an event in which an individual's name plus Social Security Number (SSN), driver's license number, medical record, or a financial record/credit/debit card is potentially put at risk - either in electronic or paper format". Almost 85 per cent of the breaches reported and more than 99 per cent of the records put at risk were in respect of electronic as opposed to paper data breaches. [See Endnote 7.]

The Risks

Risks abound. Any organisation that stores large amounts of sensitive information faces many hazards and potential liabilities. Policyholders are increasingly looking to their insurers to indemnify them against the world of cyber-risk. Particularly, they are seeking protection against three specific risks that arise out of their electronic data collections: first-party costs arising out of data

breach; third-party liability for loss of personal information; and third-party electronic breach of privacy interests.

These are insurable risks. Each time an organisation's network is hacked or an employee loses his or her work iPhone, BlackBerry, USB key, or laptop, a data breach has occurred.

The owner of the data will incur first-party loss, as some response must be undertaken. The degree of such response will depend upon the information lost. It may include an investigation into the cause and extent of the data breach, data recovery, notification of affected individuals, monitoring costs, fines and penalties, and, potentially, interruption of the policyholder's operations, all at significant expense to the organisation. [See Endnote 8.]

If the lost data includes private information or commercially sensitive information of others, for example, that of customers, the loss may be actionable. If the information is used, customers whose information was lost, for example, will sue seeking damages awards in compensation for any resulting losses. Even where data is not misused, the breach of individual privacy may give rise to an award of damages. This is particularly so in Ontario after last year's decision of the Ontario Court of Appeal in *Jones v Tsige*. [See Endnote 9.] Although, on its facts, the case dealt with intrusion upon seclusion, the decision suggests that public disclosure of embarrassing private facts may also give rise to a cause of action at common law, compensable even in the absence of pecuniary loss. *Jones* has been used to support recognition of this additional invasion of privacy tort in at least one subsequent Ontario case, albeit one decided at the Small Claims Court level. [See Endnote 10.]

Finally, the expansion of the digital world has increased the number of points of electronic contact between the individual and the world at large. Each additional point of contact increases the likelihood that an individual's privacy will be intruded upon. The electronic intrusion of individual interlopers and commercial interests into individual privacy is increasingly recognised as being actionable.

The Regulation of Electronic Spam and Data Breach in Canada

Adding to the challenge facing policyholders and insurers is the fact that the Canadian regulatory environment has not kept pace with the scope of the risks.

In respect of privacy rights, the federal anti-spam legislation ("Bill C-28") received Royal Assent on 15 December 2010. [See Endnote 11.]

The legislation sets up a regulatory scheme to deal, amongst other things, with unsolicited, commercial electronic contact or spam. As presently drafted, the legislation includes fines or "an administrative monetary penalty" (the purpose of which is to promote compliance with the Act) of up to $10,000,000.00 per contravention for businesses. It also grants a private right of action to those targeted for compensation "in an amount equal to the actual loss or damage suffered or expenses incurred by the applicant" plus up to $200.00 per contravention of the spam section to a maximum of $1,000,000.00 for each day on which a contravention occurred. The stated purpose of the additional statutory sum is to promote compliance with the relevant legislation. [See Endnote 12.]

Despite being passed almost three years ago, Bill C-28 has not yet come into force. Regulations under the Act are still being worked out. Canada will be the last G8 country to introduce specific anti-spam legislation. [See Endnote 13.]

In respect of data breach, the legal requirements imposed on an entity suffering the breach are uncertain at best. Unlike other countries around the world, including many in which Canadian businesses operate, Canada has yet to pass comprehensive laws and regulations that broadly mandate responses to data breaches. [See Endnote 14.] Elsewhere, laws require that when a data breach involving private information occurs: those affected must be notified; responsible parties must take steps to ensure that the scope of the breach is limited; negative outcomes from the breach must be prevented; and regulators must be informed.

In Canada, the federal government has introduced a bill proposing to amend the *Personal Information Protection and Electronic Documents Act*. [See Endnote 15.] Bill C-12 is drafted to provide much of the regulatory structure outlined above. [See Endnote 16.] Under this Bill, in the event of a "material breach" of security surrounding personal information, the organisation must notify the Office of the Privacy Commissioner of Canada ("the Commissioner"). The organisation must also notify the individuals involved where it is "reasonable" to "believe that the breach creates a real risk of significant harm to the individual". "Significant harm" is defined to include "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property".

Bill C-12 has been before Parliament since 2011 and appears to have stalled. It has not been passed, much less put into force. In fact, Bill C-12 was a reintroduction of Bill C-29, an earlier bill introduced, but not passed, in tandem with the anti-spam legislation (Bill C-28) already discussed. [See Endnote 17.]

In February 2013, yet another bill, Bill C-475, was introduced proposing to amend *PIPEDA* to include mandatory security breach disclosure requirements. [See Endnote 18.] An organisation's obligations under this private member's bill are more likely to be triggered than those under Bill C-12. Bill C-475 includes mandatory reporting to the Commissioner "where a reasonable person would conclude that there exists a possible risk of harm to an individual" as a result of "any incident involving the loss or disclosure of, or unauthorized access to, personal information". The organisation would be ordered to notify affected individuals where the Commissioner determines the loss of, disclosure of, or unauthorised access to personal information "is likely to result in an appreciable risk of harm" to them. It remains to be seen what will become of this bill, if anything.

The result is that when Canadian organisations face data breaches, there is presently little in the way of law they can turn to in order to determine their responsibilities and obligations. [See Endnote 19.]

Cover for First- and Third-Party Cyber-loss

Coverage against first- and third-party cyber-risks is available in the Canadian marketplace. However, such coverage is relatively new in this country. It is far from universal. On the other hand, virtually every Canadian business and organisation faces some form of cyber-risk. In such circumstances, the potential for large uninsured losses exists. It is to be expected that policyholders facing first-party data loss and/or third-party data or privacy breach liabilities will seek coverage under their existing policies: General Liability; Property; Errors & Omissions; and Directors & Officers forms.

These claims will pose challenges for policyholders and insurers alike. The standard forms setting the terms of these traditional policies were drafted before data breach and electronic privacy invasions had developed as significant policyholder risks. While insurers have sought to draft new exclusions and endorsements to limit the scope of such exposure, success has not been universal. As exposures increase, the challenges to exclusions and other limiting clauses in policy wordings will become more frequent.

Ultimately, it is to be expected that more and more businesses will transition into specialised coverage providing greater and greater electronic and data cover. For the near future, however, the question policyholders and insurers in Canada are most likely to face will not be whether a cyber-risk policy covers a loss but whether or not traditional insurance forms exclude it. Until cyber-risk policies have achieved greater market penetration, it is important to evaluate cyber-risk coverage in light of standard form liability and first-party policies.

There is reason to believe, at least in the short term, that policyholders may succeed in some of their claims. A review of US law shows that policyholders have, in some circumstances, found cover for cyber-risks under commercial general liability ("CGL") and property forms.

Policy Provisions Excluding Data Losses from Coverage

Insurers' first reaction to data breach claims will almost certainly be that the claims are not covered by CGL and commercial property policies. Data cannot suffer "physical loss". Data is not "tangible property". Data loss does not, therefore, fall within the scope of cover provided by policies that require physical damage to, or loss of use of, a tangible thing.

However, insurers must tread carefully and assess the strength of their policy wording. As the Supreme Court of Canada reminded us again in *Progressive Homes Ltd v Lombard General Insurance Co of Canada*, the wording of the insurance contract is paramount. [See Endnote 20.] Policy language will govern.

Most first- and third-party forms have existed in their present form for years. Change has been slow and incremental. Insuring agreements were not drafted in contemplation of data losses. As data losses have come into greater focus, insurers have sought to clarify coverage through reliance on the scope of coverage grants and development of exclusions.

Standard form property coverage requires that the insured suffer some form of physical loss. [See Endnote 21.] Insurers take the position that data is intangible property that cannot suffer physical damage and have sought to define it as such. Similarly, standard form CGL policies provide protection against physical injury to tangible property or loss of use thereof. [See Endnote 22.] Carriers argue that data is not "tangible property" and that damage to data cannot fall within the insuring agreement. Buttressing insurers' arguments are a range of exclusions. In one form or another, these exclusions seek to remove coverage for damages arising out of the loss of, loss of use of, damage to, corruption of, and inability to access or manipulate electronic data. [See Endnote 23.]

While insurers have found frequent success, they have not always prevailed.

In the first-party context, the US Fourth Circuit, along with a court in Arizona, has found that lost programming information and erasure of data constitute "physical damage" or "physical loss". [See Endnote 24.] More recently, albeit under an Information Systems Coverage Form as opposed to more traditional property cover, a Louisiana court found that electronic data is physical in nature and, therefore, capable of "direct, physical 'loss or damage'". [See Endnote 25.] The court reasoned that, while not tangible, the chemical analysis data stored on the insured's hard disk storage system which suffered corruption is physical. The data can be observed, takes up space on the disk and can be altered through human action, making physical things happen.

An example where policy language did not achieve insurer intentions is the *Retail Ventures, Inc v National Union Fire Ins. Co of Pittsburgh, PA* decision of the US Court of Appeals, Sixth Circuit. [See Endnote 26.] At issue was the coverage provided by a first-party commercial crime policy. Effectively, the policy was found to protect the insured against third-party liability.

The policyholder was a discount shoe retail chain. Hackers used a local wireless network in one of its stores to steal customers' credit card and chequing account information. The stolen data was subsequently used in fraudulent transactions. Amongst other losses, the policyholder paid substantial costs to rectify the credit card breaches including costs associated with charge backs, costs of card reissuance, account monitoring, and Visa and MasterCard fines.

The policyholder sought coverage for its costs under the computer fraud rider of its Blanket Crime Policy. The policy only covered the insured's "direct" losses, namely, "[l]oss which the Insured shall sustain resulting directly from: A. The theft of any Insured property by Computer Fraud; … ". Given that the losses were incurred by credit card companies and/or customers, who then passed them along to the insured, the insurer expected that there would be no coverage under its policy. The insurer was mistaken.

The insurer did not contest that the unauthorised access to, and copying of, the credit card data constituted "theft of any Insured property by Computer Fraud". Rather, the insurer argued that the loss claimed was not the "direct" result of the breach. The insurer maintained that the theft of property by computer fraud was not the sole and immediate cause of the insured's loss as required by the phrase "resulting directly from". The coverage here was intended to be first-party, not third-party – in essence, a fidelity bond. The losses were those of the credit card companies and/or customers for which the insured was liable.

The court rejected the insurer's argument. The court ruled, at best, the phrase "resulting directly from" was ambiguous in the circumstances. "Direct" cause need not be the immediately preceding cause of a loss. Instead, a proximate cause standard was adopted. The theft of customer information data was the proximate (and, therefore, "direct") cause of the policyholder's credit card-related expenses. The insurer owed coverage.

Similarly, insurers' efforts to insulate their third-party forms against data risks have also met with their share of failure. A Minnesota court held data on a lost tape was "tangible property" within the meaning of "property damage" under general liability coverage. [See Endnote 27.]

The 2010 decision of the US Court of Appeals, Eighth Circuit in *Eyeblaster, Inc v Federal Ins. Co* is an example where liability policy wording did not successfully exclude a cyber-claim. [See Endnote 28.]

The policyholder was the provider of online services including delivery and management of interactive advertising campaigns. Eyeblaster was sued by a computer user who alleged, amongst other things, that his computer had been infected with spyware by Eyeblaster, causing it to freeze up and lose data. Once again operational, the plaintiff's computer received pop-up advertisements, experienced a hijacked browser and was slow.

The insurer succeeded in its denial of a defence at the lower court level. It argued that the complaint did not allege "property damage" within the meaning of the General Liability policy. "Property damage" was defined so as to restrict coverage to "tangible property". "Tangible property" was defined to exclude "any software, data or other information that is in electronic form". The insurer maintained that the claim only pertained to software on the plaintiff's computer and, therefore, did not allege damage to tangible property.

The Court of Appeals reversed, finding a duty to defend Eyeblaster.

It reasoned that the plaintiff was, in fact, seeking damages for the loss of use of the computer. The computer itself was "tangible property". Coverage for such a claim was available under the general liability form which defined "property damage" to also include loss of use of tangible property that is not physically injured. [See Endnote 29.]

Privacy Claims and CGL Cover

The Ontario Court of Appeal's decision in *Jones* acknowledged four distinct forms of invasion of privacy, as outlined in the 1960s by American professor, William Prosser:

> "1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> 2. Public disclosure of embarrassing private facts about the plaintiff.
>
> 3. Publicity which places the plaintiff in a false light in the public eye.
>
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness."

The appellate court explicitly confirmed the existence of a common law right of action for intrusion upon seclusion in Ontario. The rationale of the decision, however, also supports recognition of a right of action for public disclosure of embarrassing private facts. R.J. Sharpe J.A. stated:

> "… The internet and digital technology have brought an enormous change in the way we communicate and in our capacity to capture, store and retrieve information. As the facts of this case indicate, routinely kept electronic data bases render our most personal financial information vulnerable. Sensitive information as to our health is similarly available, as are records of the books we have borrowed or bought, the movies we have rented or downloaded, where we have shopped, where we have travelled, and the nature of our communications by cell phone, e-mail or text message.
>
> It is within the capacity of the common law to evolve to respond to the problem posed by the routine collection and aggregation of highly personal information that is readily accessible in electronic form. Technological change poses a novel threat to a right of privacy that has been protected for hundreds of years by the common law under various guises and that, since 1982 and the Charter, has been recognized as a right that is integral to our social and political order." [See Endnote 30.]

As previously noted, public disclosure of embarrassing private facts was explicitly accepted as an actionable invasion of privacy tort in the subsequent Ontario lower court decision in *Action Auto Leasing*. [See Endnote 31.]

In the context of data breach and electronic privacy, claims will very likely fall within the first two forms enumerated by Prosser.

The first type of claim will arise out of inadequate protections for private information and will likely allege that private information about an individual plaintiff has not been protected and has become available to others not authorised to access it. When private records are lost or stolen, the possibility exists that embarrassing or disconcerting information will be made available to the public.

The second type will involve a claim that the defendant's conduct has breached the plaintiff's right of seclusion and solitude by electronic means. In *Jones*, the defendant bank employee repeatedly accessed the plaintiff's personal banking records using a workplace computer. If Canadian courts follow a broad line of American reasoning, unwanted electronic intrusion into people's homes or private computers could also form the basis of an intrusion upon seclusion claim. Individuals who have not consented to receive commercial faxes and emails may be able to sue in tort (although the federal government's anti-spam legislation may create a statutory basis for this claim should it come into force).

Policyholders are most likely to seek coverage for these claims in the Personal Injury section of their CGL policies. Standard wording extends coverage to claims for the publication of material that violates a person's right to privacy. [See Endnote 32.]

It is little wonder that one of the most hotly contested areas of insurance coverage litigation in the US presently centres on the meaning of the term "publication" and the scope of an individual's "right to privacy". US experience demonstrates that claims alleging private information about plaintiffs was made publicly available may be covered by Part B (Personal and Advertising Injury Liability). [See Endnote 33.] If litigated to judgment, the *Sony PlayStation* coverage litigation will provide considerable insight into the coverage obligations of insurers in respect of policyholders who fail to adequately protect their customers' information. [See Endnote 34.]

American blastfax and spam insurance cases may also be particularly instructive in respect of what Canadian insurers should expect in relation to coverage for intrusion on seclusion and solitude claims. [See Endnote 35.] US experience demonstrates that claims involving unpermitted electronic intrusion into private homes and business may be covered by Part B of a CGL policy.

Damage awards may not be insignificant, particularly if claims are aggregated in class actions. The *Jones* decision states that damages for intrusion upon seclusion where no pecuniary loss is suffered should be modest. The Ontario Court of Appeal fixed the top end of the range as $20,000.00. Although "modest" on a per claimant basis, the sums at issue could be extraordinary when one considers the number of records (and, therefore, affected persons) involved in some data breach litigation or the number of unwelcome commercial messages sent by some businesses.

Canadian insurers facing such claims on their liability policies will be forced to consider the scope of the privacy cover they intend to provide. Some Canadian CGL forms already seek to limit the scope of personal injury coverage against electronic privacy claims. Conversely, policyholders may want to consider whether they wish to obtain broader coverage in their liability and property forms.

Conclusion

Big Data will only get bigger. The electronic world will increasingly infiltrate private spheres. It is to be expected that controls on data collection will not always be as strong or effective as one might wish. It is also to be expected that people will become increasingly vigilant about protecting their privacy. On both counts, data breach claims and privacy claims are almost certain to become far more frequent in the coming years. The insurance industry has begun to provide products that respond to these risks. However, the Canadian insurance market has yet to fully embrace new cyber-risk products. For the foreseeable future, many policyholders will be inadequately protected against data and privacy risks. When faced with claims, they will turn to their first- and third-party insurance carriers for protection. Insurance coverage for such claims is far from certain.

Acknowledgment

Special thanks are reserved for Mark G. Lichty, whose assistance was invaluable in drafting this chapter.

Endnotes

1 http://www.ibm.com/smarterplanet/global/files/us__en_us__smarter_computing__ibm_data_final.pdf.

2 http://www.ibm.com/smarterplanet/global/files/ca__en_us__overview__changing_conventions_overarching_op_ad_9_3_final.pdf.

3 James Glanz, "Landlords Double as Energy Brokers", *The New York Times*, 13 May 2013, http://www.nytimes.com/2013/05/14/technology/north-jersey-data-center-industry-blurs-utility-real-estate-boundaries.html?pagewanted=all&_r=0.

4 Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think about the World", *Foreign Affairs*, May/June 2013, http://www.foreignaffairs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data.

5 Martha Neil, "Is your photo online? Are you on Facebook? If so, retailers can ID you and your shopping profile", *ABA Journal*, 20 May 2013, http://www.abajournal.com/mobile/article/is_your_photo_online_are_you_on_facebook_if_so_retailers_can_id_you_an/?utm_source=feedburner&utm_medium=feed&utm_campaign+ABA+Journal+Top+Storiesy.

6 http://www.idtheftcenter.org/images/breach/_Breach_Report_2012.pdf.

7 http://idtheftcenter.org/images/breach/Paper_vs_Electronic_w_Category__Summary_2012.pdf.

8 Allied World Assurance Company has a very interesting data breach cost calculator available online in connection with its Tech//404 specialty liability insurance coverage for technology-dependent organisations and providers, http://www.tech-404.com/calculator.html. By way of an example, the calculator estimates that a data breach involving 1,000 records will cost between approximately $133,000.00 and $200,000.00 to rectify, including investigation costs, notification/crisis management costs, and regulatory compliance costs (were the incident to result in a class action claim).

9 *Jones v Tsige*, 2012 ONCA 32, 108 OR (3d) 241, [2012] OJ no 148 (QL) [*Jones*].

10 *Action Auto Leasing & Gallery Inc v Gray*, [2013] OJ no 898 (QL) [*Action Auto Leasing*].

11 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SO 2010, c 23.

12 See sections 6, 20, 47 and 51.

13 Erin Virgint and Terrence J Thomas, "Legislative Summary of Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities", *Library of Parliament Research Publications*, 28 May 2010, revised on 15 November 2012, http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_Is.asp?source=library_prb&Is+C28&Parl=40&Ses=3&Language=E&Mode=1.

14 At least Alberta, however, has data breach response obligations regarding notice and reporting built into their provincial, personal information protection legislation. *Personal Information Protection Act*, SA 2003 c P-6.5. See sections 34.1 and 37.1.

15 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]. *PIPEDA* came into force in parts beginning in 2000. Amongst other things, the Act governs the collection, use and disclosure of personal information in the course of commercial activities by private sector organisations. Organisations and activities in provinces with substantially similar legislation may be exempted. See sections 3, 4 and 26(2)(b).

16 Dara Lithwick, "Legislative Summary of Bill C-12: An Act to amend the Personal Information Protection and Electronic Documents Act", *Library of Parliament Research Publications*, 19 October 2011, http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_Is.asp?Is=cl2&Parl=41&Ses=1.

17 *Ibid*.

18 *Bill C-475: An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power)*, First reading in the House of Commons of Canada, 26 February 2013, http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6000116.

19 Organisations can reference the office of the Ontario privacy commissioner's guide to "best practices". Information and Privacy Commissioner Ontario, Canada, "Privacy Breach Protocol Guidelines for Government Organizations", 1 December 2006, revised in March 2012, http://www.ipc.on.ca/English/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Profesional-Guidelines-Summary/?id=292.

20 2010 SCC 33, [2010] 2 SCR 245, [2010] SCJ no 33 (QL). Rothstein J. wrote, "[t]he primary interpretive principle is that when the language of the policy is unambiguous, the court should give effect to clear language, reading the contract as a whole (*Scalera*, at para. 71)". Put simply, "[t]he focus of insurance policy interpretation should first and foremost be on the language of the policy at issue". Policy terms are accorded their "plain" meaning. The particular policy wording trumps general principles of law.

21 In the United States, the Insurance Services Office (the "ISO") oversees standard form insurance contracts. In Canada, the Insurance Bureau of Canada (the "IBC") provides model policy and endorsement wordings. The IBC was founded in 1964. It is a national industry association representing Canadian home, car and business insurers. While the IBC wordings discussed herein serve as benchmarks for the industry, their adoption or modification is discretionary.

The 1 June 2008 edition of the Commercial Property (Broad Form) IBC form 4037 provides, in part:

"Indemnity Agreement

1. In the event that any of the insured property is lost or damaged during the policy period by an insured peril, the Insurer will indemnify the Insured against the direct loss or damage so caused to an amount not exceeding whichever is the least of:

(a) the value of the lost or damaged property as determined in Clause 15;

(b) the interest of the Insured in the property;

(c) the amount of insurance specified on the "Declarations Page" for the lost or damaged property.

[…]

Insured Perils

5. This form, except as otherwise provided, insures against all risks of direct physical loss of or damage to the insured property."

22 The 1 October 2011 edition of the Commercial General Liability Policy (Occurrence Form) IBC form 2100 states, in part:

"SECTION I - Coverages

Coverage A. Bodily Injury and Property Damage Liability

1. Insuring Agreement

a. We will pay those sums that the insured becomes legally obligated to pay as "compensatory damages" because of "bodily injury" or "property damage" to which this insurance applies. We will have the right and duty to defend the insured against any "action" seeking those "compensatory damages". However, we will have no duty to defend the insured against any "action" seeking "compensatory damages" for "bodily injury" or "property damage" to which this insurance does not apply. […]."

Under IBC form 2200, 1 October 2008 edition, "property damage" is defined, in part, as:

"a. Physical injury to tangible property including all resulting loss of use of that property. […]

b. Loss of use of tangible property that is not physically injured. […]

[…]"

23 Within IBC form 2100, the exclusion is as follows:

"This insurance does not apply to:

[…]

l. Electronic Data

"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."

In addition, the IBC CGL policy form expressly states that electronic data is not tangible property within the definition of "property damage". Under IBC form 2200, the definition of "property damage" quoted in endnote 22 continues:

"[…]

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 applications software, hard or floppy discs, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

With respect to the property coverage, IBC form 4037 contains the following exclusion:

"6.D. DATA EXCLUSION

(1) This form does not insure "data".

(2) This form does not insure loss or damage caused directly or indirectly by a "data problem". This exclusion (2) does not apply to loss or damage caused directly by resultant fire, explosion, smoke or leakage from "fire protective equipment", all as described in Clause 18(m);".

The form continues:

"Definitions

18. Wherever used in this form:

[…]

(f) "Data" means representations of information or concepts, in any form.

(g) "Data problem" means:

(i) erasure, destruction, corruption, misappropriation, misinterpretation of "data";

(ii) error in creating, amending, entering, deleting or using "data"; or

(iii) inability to receive, transmit or use "data"."

24 Erasure, by a former employee/hacker, of computer files and databases necessary for the operation of software development computer systems constituted 'direct physical loss of or damage to property' under a property policy in *NMS Services Inc v Hartford*, 62 Fed Appx 511 (4th Cir (Va) 2003); mainframe computers and matrix switch which lost all programming information from their random access memory in a power outage and required reprogramming to restore operation amounted to "physical damage" under a property policy insuring against business/service interruption in *American Guarantee & Liability Ins. Co v Ingram Micro, Inc*, 2000 WL 726789 (D Ariz 2000).

25 *Landmark American Ins. Co v Gulf Coast Analytical Laboratories, Inc*, 2012 WL 1094761 (MD La 2012).

26 691 F3d 821 (6th Cir (Ohio) 2012).

27 In *Retail Systems, Inc v CAN Ins. Companies*, 469 NW2d 735 (Minn Ct App 1991), a customer's computer tape containing data was held to be "tangible property" and defence was owed under the data processing consultant's general liability coverage when the tape and data were lost.

28 613 F3d 797 (8th Cir (Minn) 2010).

29 One judge dissented, finding no duty to defend under the general liability form on the basis of application of a property not physically injured exclusion.

30 *Jones*, *supra* Endnote 9.

31 *Action Auto Leasing*, *supra* note 10. It should be noted that some other common law provinces in Canada have established a right of action for invasion of privacy by statute. These include: *Privacy Act*, RSBC 1996 c 373; *Privacy Act*, RSM 1987 c P125; *Privacy Act*, RSS 1978 c P-24; and P*rivacy Act,* RSN 1990, c P-22.

32 The 1 October 2011 edition of the Commercial General Liability Policy (Occurrence Form) IBC form 2100 states, in part:

"SECTION I - Coverages

Coverage B. Personal and Advertising Injury Liability

1. Insuring Agreement

a. 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. We will have the right and duty to defend the insured against any "action" seeking those "compensatory damages". However, we will have no duty to defend the insured against any "action" seeking "compensatory damages" for "personal and advertising injury" to which this insurance does not apply. […]."

Under IBC form 2200, 1 October 2008 edition, "personal and advertising injury" is defined, in part, as:

"injury, including consequential "bodily injury", arising out of one or more of the following offenses:

[…]

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

It should be noted that IBC form 2100 contains an exclusion regarding insureds in media and internet-type businesses.

33 See *Netscape Communications Corp v Federal Ins. Co*, 343 Fed Appx 271 (9th Cir (Cal) 2009) wherein the insureds, American Online and its subsidiary, Netscape, were found to be entitled to defence in circumstances where Netscape had not publicly disseminated information of users' internet activities obtained in connection with its software programme but where its employees had circulated the information internally as well as made it known to the parent company in potential violation of the privacy rights of Netscape users. Netscape's personal injury coverage grant included coverage for "[m]aking known to any person or organization" material that violates a person's right of privacy.

See also *Hartford Casualty Ins. Co v Corcino & Associates*, CV 13-03728-GAF (CD Cal Oct 7, 2013) [*Corcino*], not reported on Westlaw at the time of writing of this chapter, but discussed in an online summary authored by Hunton & Williams LLP, dated 14 October 2013, titled "Insurance policy's statutory rights exclusion does not apply to data breach claims". In *Corcino*, a general liability insurer was held to owe defence under the privacy and advertising injury coverage for a claim arising out of alleged posting of private information and medical records of patients on a public website by a job applicant of the insured without the plaintiffs' consent. The court reportedly rejected application of exclusions for violation of statutorily created rights and for statutory penalties. According to another online comment on the case by Judy Selby of Baker & Hostetler LLP, dated 16 October 2013, titled "California court finds advertising injury coverage is triggered by medical information data breach", the personal and advertising injury coverage grant at issue included "electronic publication of material that violates a person's right of privacy".

34 Following commencement of class actions arising out of a hack in which information was stolen from 75 million PlayStation accounts (including some credit card information), Sony sought coverage under a number of Zurich liability policies. Zurich seeks a declaration of no coverage (interestingly, Sony of Canada is included as a defendant in respect of policies issued by Zurich in Canada). Zurich asserts that none of the claims advance allegations for "bodily injury", "property damage", "advertising injury", or "personal injury". Zurich also relies on certain non-described exclusions.

35 See *Hooters of Augusta, Inc v American Global Ins. Co*, 157 Fed Appx 201 (11th Cir (CA) 2005) wherein a claim for violation of the Telephone Consumer Protection Act ("TCPA") by purchase of advertising space on flyers faxed to businesses in Augusta, Georgia was held to fall within the advertising injury coverage grant in respect of "[o]ral or written publication of material that violates a person's right to privacy". It appears from the reasons that the court would agree the "right to privacy" includes 'the right to be let alone' or 'the right to seclusion or solitude'. "Publication" was interpreted broadly to include "to place before the public: disseminate".

See also *Owners Ins. Co v European Auto Works, Inc*, 695 F3d 814 (8th Cir (Minn) 2012). It concerned a car repair shop that sent unsolicited fax advertisements received by 3,903 persons. The sender faced $1.9 million in liability under the TCPA. The claim was tendered to the insurers under advertising injury coverage which insured against "oral or written publication of material that violates a person's right to privacy".

The CGL and commercial umbrella policy insurers argued that the receipt of a fax did not violate anyone's right to privacy. Privacy was submitted, in essence, to be limited to personal secrets. There is a body of case law that supported the insurers' argument. However, the Eighth Circuit took a broader view of privacy, namely, that privacy includes the right to seclusion:

"We conclude that the ordinary meaning of the term "right of privacy" easily includes violations of the type of privacy interest protected by the TCPA. Our court has previously stated that violations of the TCPA are "'invasions of privacy' under [the] ordinary, lay meaning [ ] of the [ ] phrase [ ]."… Other courts have recognised that "an unexpected fax, like a jangling telephone or a knock on the door, can disrupt a householder's peace and quiet" and that the TCPA promotes this "interest in seclusion, as it also keeps telephone lines from being tied up and avoids consumption of the recipients' ink and paper." … Percic's complaint alleged that Autopia violated the TCPA by sending unsolicited faxes which "unlawfully interrupted Plaintiff's and the other class members' privacy interests in being left alone." We conclude that the policies' phrase "violat[ing] a … right of privacy" encompasses violations of privacy rights protected by the TCPA."

The term "publication" was also interpreted broadly. It was held to include communicating information generally. The dissemination of fax advertisements was a form of "publication".

Coverage was afforded to the insured.

Lori D. Mountford

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

Tel: +1 416 596 2889
Fax: +1 416 593 5437
Email: lmountford@blaney.com
URL: www.blaney.com

Lori Mountford is a senior associate at Blaney McMurtry LLP and a member of the firm's Insurance Coverage Counsel and Insurance Litigation Groups.
Lori obtained her LL.B. at the University of Toronto in 1998 and was admitted to the Ontario Bar in 2000. She also holds an Honours B.A. in philosophy.
Lori's focus at Blaney McMurtry is insurance coverage. Her practice encompasses opinion work, research, drafting, negotiation and litigation involving a range of policy coverages. These include commercial general liability, commercial property, homeowners insurance, builders risk, errors and omissions and directors and officers liability.
Lori is an experienced litigator and has appeared before the Ontario Superior Court of Justice, the Financial Services Commission of Ontario and private arbitrators. She has also participated in numerous mediations in an advocacy role.

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 5092
Email: dmackenzie@blaney.com
URL: www.blaney.com

David is a partner in Blaney McMurtry LLP's insurance group. His practice focuses on insurance coverage and reinsurance matters, and complex multi-party disputes. He is called to the Bar in Ontario, British Columbia and Washington State.

Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Blaney McMurtry LLP is a multi-service firm, helping clients overcome challenges and seize opportunities for more than fifty years, with a comprehensive yet personalised, approach to advice and representation.

In particular, the firm has a wealth of depth and experience in serving the insurance industry in both coverage and defence of a broad range of claims, and is recognised as one of the leading insurance law practices in Canada.

Blaney McMurtry is a member of the Risk Management Counsel of Canada, a national association of law firms providing services to the risk management industry. The firm is also a member of TAGLaw, one of the world's largest legal networks.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Corporate Governance
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

GLG
Global Legal Group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk