Blaney McMurtry
BARRISTERS & SOLICITORS LLP

Data Risk, Privacy Breach and Insurance Coverage

David R. Mackenzie
416.597.4890
dmackenzie@blaney.com

The advent of cloud computing has meant that the data storage capacity available to business and institutions has become limitless. IBM has estimated that 90% of the data in the world was created in the last two years.[1] The New York Times reported recently that commercial rents in areas of New Jersey, nearby New York City, are reaching $600 per square foot because of demand from new data centres.[2]

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. Each of us connects with the electronic world frequently each day. We use our credit cards and debit cards, access online social networks and 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, We expose a great deal about ourselves in the digital world. Much of this 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 this month's Foreign Affairs Magazine explains:

---

1 Bringing Smarter Computing to Big Data: http://public.dhe.ibm.com/software/data/sw-library/data/IBM_Smarter_Computing_BIG_DATA.pdf

2 James Glanz, Landlords Double as Energy Brokers, New York Times, May 13, 2013.

> 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.[3]

Accessible Big Data is changing the manner in which business, research and even politics are being conducted. In creating Big Data, new avenues to develop novel approaches, insights and opportunities are opened. Increasingly business, government, educational and medical institutions, and individuals have seen the benefits of using enormous data pools to better advance their goals. When processed properly, large data collections can reveal trends and patterns which provide in-depth understanding of human behaviour. The expansion of consumer information available to business is perhaps the most notable (and to many, concerning) of all developments. A post on the American Bar Association's ABA Journal site reports: "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."[4]

Such technology does not yet exist, but likely soon will for large corporations. But it is not only large business entities which present data risks. While not every business entity and organization will have pools of information comparable to those collected by large retailers, credit card companies, search engines and social networks, almost every organization 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 do we get asked to provide our phone numbers or postal codes at the cash register? There is value in developing comprehensive customer profiles.

---

[3] Kenneth Neil Cukier and Viktor Mayer-Schoenberger: The Rise of Big Data: How Its Changing The Way We Think About The World: Foreign Affairs, May/June 2013.

[4] Martha Neil: Is your photo online? Are you on Facebook? If so, retailers can ID you and your shopping profile: ABA Journal, May 20, 2013.

Of course, information is useless unless it can be analysed. It is important to data owners to get information processed, evaluated and put to use as quickly as possible. This means that data must be stored in an easily accessible form. The result is that very large amounts of data, including commercially sensitive information and private individual information, is stored in places that put it at risk of being lost or stolen: inadequately protected servers, the cloud, laptop computers, iPhones and Blackberries, USB keys and so on.

Many risks arise out of data pools, whether the collection is large or small. According to the Identity Theft Resource Center in 2012 alone more than 17 million confidential records were put at risk through in nearly 450 reported security breaches.[5]

Risks abound. Any organization which stores large amounts of potentially 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 which arise out of their electronic data collections: first party costs arising out of data breach, third party liability for privacy breach relating to loss of personal identifiable information, and third party liability for electronic breach of privacy interests.

These are insurable risks. Every time an organization is hacked, or an employee loses their iPhone or blackberry, or a USB key, or a 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, but may require investigation into the cause and extent of the data breach, data recovery expenses, notification to affected individuals, monitoring costs, fines and penalties , and potentially interruption of the policyholder's operations.[6]

---

[5] http://www.idtheftcenter.org/ITRC%20Breach%20Report%202012.pdf.

[6] Tech//404 has a very interesting data breach cost calculator on its website: 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 135,000 and 200,000 to rectify, including investigation costs, notification and crisis management costs, and regulatory compliance costs.

Additionally, if the lost data includes private information about customers or other individuals, or commercially sensitive information of others, the loss may be actionable. If lost data is misused, plaintiffs will sue seeking damage 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 - - particularly after last year's decision of the Ontario Court of Appeal in *Jones v. Tsige,*[7] which strongly suggested that "public disclosure of embarrassing facts about the plaintiff" was a cause of action, even in the absence of demonstrable economic or physical loss. Those torts are compensable injuries on their own.

Finally, development of "Big Data" has only occurred because of the growth in the electronic interconnections in people's lives. 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 recognized as being actionable.

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 risk. In respect of privacy rights, the Federal Government has failed to date to pass its anti-spam legislation. In respect of data breach, the legal requirements imposed on an entity suffering a data breach are uncertain at best. Unlike other governments around the world, including many in which Canadian businesses operate, Canada has yet to pass comprehensive laws and regulations which broadly mandate response to data breach. Elsewhere, laws require that when a data breach occurs involving private information, 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 are prevented, and regulators must be notified.

The Federal Government has introduced legislation to amend the Personal Information Protection and Electronic Documents Act (PIPEDA) in Bill C-12. Bill C-12 is drafted to provide much of the regulatory structure outlined above. However, that Bill has been before

[7] 2012 ONCA 32

Parliament since 2011, and follows on Bill C-29 which was not passed by Parliament in 2010. Bill C-12 has not been passed, much less put into force. The result is that when Canadian organizations face data breaches, there is little in the way of law they can turn to determine their responsibilities and obligations. One example which highlights the problem is found in a story the Globe and Mail has been reporting on involving the Investment Industry Association of Canada. An Association laptop which stored private information of 52,000 individuals was lost. The Association waited two months before publicly disclosing the data breach. The risk to the 52,000 individuals seems apparent. However, the best response regulators could muster under the present legal regime amounted to a scolding from Ontario's Privacy Commissioner. She is reported to have called the Association to tell them she was "appalled", and to suggest that in future they follow the Commissioner's "best practices".[8] The legal requirements required of entities suffering data breaches are far from clear. We are not well-served by the lack of formal regulation in the data breach area.

Cover for First and Third Party Cyber-Loss

Comprehensive coverage against first and third party cyber-risks is available in the Canadian marketplace. However, such coverage is relatively new in this country. Cyber-cover has started to make in-roads in the Canadian market, and will continue to do so. However, such coverage is far from universal.

It is to be expected, then, that policyholders facing first and/or third party data or privacy breach liabilities will seek coverage under their existing policies - - General Liability, Property, Errors & Omissions and/or Directors & Officers forms. These claims will pose challenges for policyholders and insurers. The standard forms setting the terms of these 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.

[8] Canada's brokers demand answers on missing financial data: The Globe and Mail, Apr. 19 2013; IIROC broke own rules by losing private data — can we believe its explanation?: National Post, April 30, 2013.

As is discussed further below, policyholders have sometimes succeeded in defeating insurers' efforts to limit the scope of the coverage provided in their traditional "bricks and mortar" policies. As exposures increase, the challenges to exclusions and other limiting clauses in policy wordings will become more frequent. Virtually every Canadian business and organization faces some form of cyber-risk. Those not carrying cyber-risk coverage are potentially facing large uninsured losses. As time goes on, it is to be expected that more and more businesses will transition into coverage with providing greater and greater electronic and data cover.

However, as the Canadian insurance market moves to reflect data breach and privacy risks, insurers are almost certain to face claims from their policyholders for cyber losses under non-cyber forms. For the near future, the question policyholders and insurers will be most likely to face will not be whether a cyber-risk policy covers a loss or not, but whether or not traditional insurance forms exclude them. Given that carriers now expect to cover many risks their policyholders face through cyber-risk insurance, rather than other commercial forms, efforts by policyholders to fit loss or damage arising out of the loss of electronic information or privacy breaches into their commercial policies are likely to be met with coverage denials and litigation.

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 CGL and property forms. Ultimately, however, insurers who expected different results will better define the scope of the risk they intend to cover. Policy wording which is found to be successful in defining the intended scope of risk will be widely adopted, while faulty policy wording will be jettisoned

Many interesting challenges are posed by wordings of new cyber-forms. However, until cyber-risk policies have achieved greater market penetration (as they certainly will do), it is important to evaluate cyber-risk coverage in light of standard form liability and first party policies.

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 such 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 which require physical damage 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 v. Lombard*, the wording of the insurance contract is paramount. Policy language will govern.

Most first and third party forms have existed in their present form for decades. 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 dogged reliance on the scope of coverage grants and development of exclusions.

In this regard, standard form property coverage requires that the insured suffer some form of "physical loss". 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". Carriers argue that data is not "tangible property", and 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, destruction of, misappropriation of, corruption of, erasure of, errors in, and inability to access or manipulate electronic data.

While insurers have found frequent success, that view has not always prevailed. In the first party context the U.S. 4th Circuit along with courts in Minnesota and Arizona have found that corrupted data does suffer "physical injury".[9] Recently, American courts have denied summary judgment applications brought by property insurers in situations where data loss occurred after hackers took over a company's servers.[10] Coverage was also available where a company's data had become corrupted.[11]

---

[9] *Retail Systems, Inc. v. CNA Insurance Co* 469 N.W.2d 735 (Minn. Ct. App. 1991; *American Guarantee & Liability Insurance Co. v. Ingram Micro, Inc* 2000 WL 726789 (D. Ariz. Apr. 18, 2000); *NMS Services Inc. v. The Hartford* 62 F. App'x 511 (4th Cir. 2003)

[10] *Vonage Holdings Cor. V. Hartford Fire Ins. Co.* 2012 U.S. Dist. LEXIS 44401 (New Jersey)

[11] *Landmark Amer. Ins. Co., v. Gulf Coast Analytical Labs* 2012 U.S. Dist LEXIS 45184 (Louisiana)

Another prime example of policy language not achieving insurer intentions is the *Retail Ventures Inc. v. National Union Fire*[12] decision of the US Sixth Circuit. In issue was the coverage provided by a first party commercial crime policy. In the result, that policy was found to protect the policyholder 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 policyholder was required to pay substantial costs to rectify the credit card breaches, including costs of card reissuance, account monitoring, and Visa and MasterCard fines.

The policyholder sought coverage for its costs under its Blanket Crime Policy. The policy only covered the insured's "direct" losses. Given that the losses here were incurred by credit card companies, 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 theft of credit card data was "insured property" under the policy. The argument advanced, rather, was that the loss claimed was not the "direct" result of the breach. The losses, the insurer argued, were not "direct" but were actually the losses of the credit card companies for which the insured was liable. The coverage here was intended to be first party, not third party - - in essence a fidelity bond.

The court rejected the insurer's argument that the losses were not "direct" losses. At best, the Court ruled, the word "direct" was ambiguous in the circumstances. "Direct" did not need to be the immediate preceding cause of a loss. The theft of customer information data was the proximate (and therefore "direct") cause of the policyholders 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. An example is the 2010 decision of the US 8th Circuit in *Eyeblaster, Inc. v. Federal Insurance Co*[13]. is an example of policy wording not successfully excluding a cyber-claim. The policyholder was the provider of certain online advertising services to a

[12] 691 F.3d 821 (6th Cir. 2012)
[13] 613 F.3d 797 (8th Cir. 2010).

customer. Eyeblaster was sued by a plaintiff who alleged, amongst other things, that his computer had been infected with spyware through Eyeblaster's negligence. The computer continually received pop-up advertisements and would freeze up. When the claim was submitted to Eyeblaster's third party insurer, the claim was denied on the basis that the policy covered only "tangible property", and excluded loss arising out of "software, data or other information that it in electronic form". The insurer argued that the claim only pertained to software on the plaintiff's computer, and did not allege damage to tangible property.

The court disagreed finding that the plaintiff was in fact seeking damages for the loss of use of the computer. The computer itself was "tangible property", and was alleged to be lost to use. Coverage for such a claim was available under Eyeblaster's general liability form. What appeared on its face to be a clear-cut cyber-risk claim was found to be a claim for "physical loss".

Privacy Claims and CGL Cover

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

> (i) intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
>
> (ii) public disclosure of embarrassing private facts about the plaintiff;
>
> (iii)publicity which places the plaintiff in a false light in the public eye; and
>
> (iv) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

In the contexts of data breach and electronic privacy, claims will very likely fall within one of two forms. The first type of claim will arise out of inadequate protections for private information, and will likely allege that private information about individual plaintiffs has not been protected, and has become available to people not authorized 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 form of claim includes claims that the defendants conduct has breached the plaintiffs rights of seclusion and solitude through electronic means. The *Tsige* decision itself is one example of how such intrusion may occur. If Canadian courts follow a broad line of American reasoning, unwanted electronic intrusions into people's homes or private computers could form the basis an "intrusion upon seclusion" claim. Individuals who have not consented to receive commercial faxes and email may be able to sue in tort (though the Federal Government's anti-spam legislation may create a statutory basis for this claim, should it ever come into force).

Policyholders are most likely to find coverage against these claims, in the Part B (Personal Injury) sections of their CGL policies. Standard wording extends coverage to claims for the publication of material which violates a person's right to privacy. It is little wonder that one of the most hotly contested areas of insurance coverage litigation in the United States presently centres on the meaning of the term "publication", and the scope of an individual's "right to privacy".[14] US experience demonstrates that making private information about plaintiffs publicly available, and claims involving unpermitted electronic intrusion into private homes and businesses may be claims covered by Part B.

American experience will clearly be informative. If litigated to judgment, the Sony PlayStation coverage litigation will provide considerable insights into the coverage obligations of insurers in respect of policyholders who fail to adequately protect their customers' information.[15] The

[14] See *Netscape v. Fed. Ins. Co.* 343 F.App'x. 271 (9th Cir. 2009) wherein Netscape was found to be entitled to coverage in circumstances where it had not disseminated private information publicly, but had allowed its own employees to have access to said information in potential violation of the privacy rights of Netscape users. Netscape's personal injury coverage grant included coverage for "making known" information which violates a person's right of privacy.

[15] 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 has 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

blastfax and spam insurance cases may be particularly instructive in respect of what Canadian insurers should expect in respect of intrusions on seclusion and solitude.[16] If the American experience is reflective of what occurs here, many electronic privacy claims may fall within the personal injury coverage grant.

New types of large loss scenarios are not hard to imagine in the Big Data era. One only needs to review headlines in the newspapers. There is considerable controversy in British Columbia in respect of the firing of a number of scientists formerly employed at the Ministry of Health's Therapeutics Initiative. While disputed, the basis of their termination appears to have been failure to follow privacy protocols protecting personal patient information. Where an owner of sensitive data does not put proper protocols into place, or those protocols are not followed, a claim can arise if unauthorized individuals access private information. Protection of private information is only effective if adequate protocols are in place and followed.

Damage awards may not be insignificant, particularly if claims are aggregated in class actions. While only dealing with the "intrusion on seclusion" tort, the *Tsige* decision ruled that such privacy breaches may be compensable at a rate of up to $20,000 per claimant. When one

---

allegations for "bodily injury", "property damage", "advertising injury" or "personal injury". Zurich also relies on certain non - described exclusions.

[16] See for e.g. *Owners Ins. Co. v. European Auto Works, Inc.*, 2012 WL 4052406 (8th Cir. Sept. 17, 2012) concerned a car repair shop that sent unsolicited faxes that were received by 3,903 recipients. The sender faced $1.9 million in liability under US Federal privacy legislation. The claim was tendered to the insurer under personal injury coverage which insured against publication of material that violated a person's right to privacy.

The insurer argued that the receipt of a fax did not violate anyone's right to privacy. It is an annoyance, but not a privacy invasion. Privacy was, in essence, limited to personal secrets. There is a body of case law which supported the insurer's argument. However, the 8th Circuit took a broader view of privacy than 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 [Telephone Consumer Protection Act]. 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 recognized 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.

considers the example of the numbers of records involved in some data breach litigation, or the number of unwelcome commercial messages sent by some businesses, the sums potentially in question are extraordinary.

Canadian insurers facing such claims on their liability policies will be forced to consider whether they wish to consider the scope of the privacy cover they wish to provide. Some Canadian CGL forms already seek to limit the scope of personal injury coverage against electronic privacy claims. Interestingly, in the United States, ISO has just released a new endorsement to remove privacy claims from the scope of coverage in American liability policies.

Conversely policyholders may wish to consider whether they wish to obtain broader coverage in desirable 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 collections 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 which 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 will be far from certain.