A New Approach to Data Security Breaches

Gideon Emcee Christian*

INTRODUCTION

Identity theft, or fraud, has become a serious cause for concern in the information technology world. It is quickly gaining notoriety as one of the fastest growing crimes, and its growth has been attributed to the ever-increasing rate of data security breaches, which have continued to dominate the news as well as the courts.[1] The judiciary and the legislature, in various legal jurisdictions, have made several efforts to deal with the ever-increasing cases of data security breaches. In the case of the judiciary, it has sought (with great difficulty) to stretch or over-stretch existing laws, which have been formulated when the information technology world had not been conceived. The legislature, on the other hand, has been more concerned with formulating new laws to comprehensively deal with the situation.

This article examines the problems associated with data security breaches from two different, but not mutually exclusive, perspectives. The first part of the article examines the need for notification in the event of a data security breach and proposes an amendment of the *Personal Information Protection and Electronic Document Act*[2] (PIPEDA) to create a legal, or statutory, obligation in Canada to compel disclosure or notification of data security breaches. My recommendations are based on the examination of legislation from other legal jurisdictions, highlighting, where necessary, the shortcomings of the legislation, which ought to be taken into consideration in amending PIPEDA or in drafting a model data security breach notification legislation in Canada.

The second part of the article examines the resort to the common law tort of negligence by victims of data security breaches in seeking legal remedy from individuals or organizations whose negligent act(s) resulted in a data spill. While acknowledging that data security breach is a new phenomenon, not yet adequately addressed in common law, I shall go further to show the difficulty in attempts to redress much of the legal claims that come with data security breaches in common law.

---

* LL.M (Law and Technology), Researcher, International Development Research Centre (IDRC). gchristian@ldrc.ca. The author is grateful to Prof. Jennifer Chandler for supervising this research, and to Mr. Isa Alade for taking time to proof read the original draft.

1 Amanda Draper, "Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law" (2007) 40 John Marshall Law Review 681 at 685.

2 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

I. A NEW APPROACH TO DATA SECURITY BREACH NOTIFICATION

The year 2005 witnessed an unprecedented number of disclosures of data security breaches.[3] In the United States, there were approximately 130 reported cases of data security breaches that year, involving the personal information of more than 55 million individuals.[4] A superficial look at these statistics will tend to give the deceptive impression that there were no serious cases of data security breaches before then. However, many such incidents, which occurred prior to 2005, went undisclosed due to the absence of any legal obligation on the part of data brokers or custodians to disclose their data "spill." Such incidents were surreptitiously shielded from the public, as well as the victims, whose personal information was spilled, leaving the latter at the risk of identity theft and fraud.

A new California state law prompted the turning point in 2005. It imposed an obligation on a person, business, or state agency that conducts business in the state of California and that owns or licenses computerized data that includes personal information, to disclose any breach of the security of the data of any resident of California, whose unencrypted personal information was, or is reasonably believed to have been acquired by an unauthorized person.[5] A leading case of data security breach that was disclosed because of this legislation was the notorious Choicepoint security breach in the United States in 2005.[6]

One may wonder why a legislative intervention is necessary to impose an obligation on data possessors or custodians to disclose incidents of data security breaches. This query finds response in the fact that, in the absence of such legal obligation, organizations, data brokers and corporate entities have no incentive to voluntarily disclose such security breaches. If the market gives companies the requisite incentives to notify their clients that personal information has been breached, so that they can take the necessary steps to mitigate damage or risks that may arise from the misappropriation of their personal information, legislative intervention might not be necessary. However, this is not the case.

There are many reasons why an organization or corporate body, in the absence of any legal obligation to the contrary, will prefer not to disclose its data security breaches. First, such notification could have an adverse effect on the company's reputation and business, especially where the company trades in a very competitive

---

3 An updated chronology of data security breaches in the United States can be found online: Privacy Right Clearing House <http://www.privacyrights.org/ar/chrondatabreaches.htm>.

4 See David G. Ries, "Information Security Law An Overview" *ISACA* (February 2007), online: ISACA <http://www.isacapgh.org/SecurityLaw.pdf>.

5 S.B. 1386, codified at *California Civil Code* ss. 1798.29, 1798.82, online: California State Senate <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html>.

6 The data broker singled out only residents of California for notification despite the fact that more than 100,000 other people in the United States were affected by the breach.

market or is a public company.[7] In addition to being embarrassing, notification or disclosure will also send an ugly message to the public, conveying the company's lack of adequate security for its clients' personal information, thus affecting the company's future business.[8] The latter case applies to companies whose business model involves the collection of their customers' personal information as opposed to that of data brokers.

Secondly, security breach notification or disclosure could open a floodgate of civil litigation (individual or class) against the company. In addition, depending on the legal jurisdiction, the Attorney-General could also bring an enforcement action.[9] The financial costs from this myriad of litigations might as well far exceed the cost of non-disclosure from the company's perspective, thus providing adequate incentive for the company to lean on the side of non-disclosure in the absence of any legal obligation to the contrary.[10]

---

7 In 2005, a poll by Ponemon Institute revealed that one in five Americans surveyed immediately terminated their business with organizations that lost their personal information. Another 40% of the respondents polled by the organization's *National Survey on Data Security Breach Notification* considered taking their business to some other organization following their receipt of data breach notifications. See Ponemon Institute LLC, Survey, "National Survey on Data Security Breach Notification" (26 September 2005), online: RSA Conference <http://www.rsaconference.com/uploadedFiles/RSA365/ESAF/2006_Archives/Sept2005_Security_Breach_Survey_Ponemon.pdf>. *ChoicePoint*, for example, at a particular point in time, experienced more than a 20 per cent decline in its stock price that followed its February 2005 disclosure of a serious security breach. See Thomas J. Smedinghoff, "The Challenge of Electronic Data: Corporate Legal Obligations to Provide Information Security" (2006) 10:3 Wall Street Lawyer 1 at 6, online: Baker&McKenzie <http://www.bakernet.com/ecommerce/wallstreetlawyerarticle.pdf>.

8 The annual Computer Security Institute and FBI Computer Crime and Security Survey for 2005 reported that only 20 per cent of respondents who suffered serious computer security breaches reported the incident to law enforcement. According to the survey, the key reason companies do not report intrusions to law enforcement is the concern for negative publicity. See full report, online: i.cmpnet.com <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf>.

9 Political & Economic Research Council, Michael Turner, "Towards a Rational Personal Data Breach Notification Regime" *Information Policy Institute* (June 2006) at 14, online: Political&Economic Research Council <http://www.infopolicy.org/pdf/data-breach.pdf>.

10 In the case of *ChoicePoint*, earlier mentioned, the company, in addition to being sued by its customers, was fined US$10 million and US$5million for civil penalties and consumer redress respectively, by the Federal Trade Commission. See U.S., Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (FTC File No. 052-3069) (26 January 2006), online: Federal Trade Commission <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>.

It suffices to reiterate that data brokers and custodians, whether government, business, etc., apparently have no incentive to disclose incidents of data security breaches in the absence of any legal obligation. Resultantly, there arises the need for legal intervention in this area because, when an incident of data security breach is concealed, affected individuals are exposed to risks, of which they are completely unaware and, more so, have no reasonable opportunity to remedy the situation or take precautionary measures.

The duty to disclose breaches of data security is comparable to the common law "duty to warn" of dangers. This is premised on the principle that a party with superior knowledge of a danger of injury or damage to another, which is posed by a specific hazard, must warn those who lack such knowledge, especially when a special relationship exists between the parties. The existing data security breach notification statutes have been driven by concerns relating to identity theft and fraud, thus compelling disclosure of breaches affecting personal information as a way of protecting individuals who might be at risk without such notification. Schwartz and Janger identified an important function of data breach notification laws as the mitigation of harm after a data leak.[11] These statutes seek to provide such individuals with opportunity to take preventive measures.[12] Hence, it has been argued that the only way to ensure true accountability is to impose a legal obligation on organizations to disclose their data security breaches.[13]

On the other hand, critics of security breach notification laws argue that such legislative efforts seek to impose unnecessary and burdensome costs, in terms of time and money, on both organizations, as well as clients who may take no necessary steps to protect themselves notwithstanding such notification. They argue that the chance of breached personal information being misappropriated for identity theft or fraud is negligible — a one per cent to five per cent chance. Hence, imposing an obligation for disclosure or notification may result in over-notification in most cases and cause unnecessary alarm on the part of the majority of those notified.[14]

Such over-notification will have some negative implications. First, it may have the tendency to erode the confidence of consumers, not only in the company or organization, but also in the online transaction system, which has contributed positively to a vibrant world economy — notwithstanding the fact that such breaches only account for a negligible share of fraud cases.[15] Second, it may result

---

11 Schwartz and Janger, "Notification and Data Security Breaches" (2007) 105 Michigan Law Review 913 at 918.

12 Smedinghoff, *supra* note 7 at 12.

13 See Public Interest Advocacies Centre, *Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics Considering the 2006 Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)*, (23 October 2006), online: CIPPIC <http://www.cippic.ca/en/projects-cases/privacy/submissions/PIACSubmissiontoETHI.pdf>.

14 Turner, *supra* note 9 at 28.

15 *Ibid.* at 30.

in notification desensitization. Consumers may become so accustomed to receiving breach notifications that they may ignore them without taking any steps to protect themselves. This argument seems to find support in a theory by the information theorist Herbert Simon, who was of the view that the problem associated with being over-informed, lies in how to allocate our limited attention span to the ever-expanding sources of information. According to him, attention is a scarce resource and, in a world of expanding information, more information can be a problem; rather than an automatic solution to the dilemma of ignorance, information can turn individuals "off" to important messages that they otherwise would have noticed.[16]

One of the primary opponents of data security breach notification legislation in Canada is the Canadian Chamber of Commerce. The Chairman of the Canadian Chamber of Commerce, in his oral submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics with consideration of the Review of the *Personal Information Protection and Electronic Documents Act*, noted:

> The Canadian Chamber does not believe that mandatory breach notification is necessary in the legislation. We would encourage businesses to continue to work closely with the Privacy Commissioner's office in order to identify breaches and to notify those who could be affected by a possible breach in privacy. This flexibility enables notice where appropriate in the circumstances, with no adverse impact on consumers. I'd also like to note that it would be beneficial for the Canadian Chamber and other business associations to develop a best practices set of guidelines that could be used when breaches in privacy occur.[17]

A study finds that the adoption of data breach disclosure laws by some states in the U.S., between 2002 and 2007, had a marginal effect on the incidence of identity theft and reduced the rate by just two per cent, on the average. The study further acknowledges that, notwithstanding the marginal effect, reducing identity theft is only one means by which data breach disclosure laws can be evaluated. The laws may have other important benefits, such as reducing the average victim's losses or improving a firm's security and operational practices.[18]

---

16 Herbert A. Simon, "Designing Organizations for an Information-Rich World" in M. Greenberger, ed., *Computers, Communications, and the Public Interest* (Baltimore: John Hopkins Press, 1971) 38, cited after reprint in: H.A. Simon, *Models of Bounded Rationality, Volume 2: Behavioral Economics and Business Organization* (Cambridge, Mass.: MIT Press, 1982) at 40.

17 See Parliament, "Statutory Review of the *Personal Information Protection and Electronic Document Act (PIPEDA)*" by Tom Wappel, M.P. Chairman, Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, 39th Parl. 1st Sess., online: Government of Canada <http://cmte.parl.gc.ca/Content/HOC/ committee/391/ethi/reports/rp2891060/ethirp04-e.html>.

18 Sasha Romanosky, Rahul Telang & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?" (16 September 2008), (SSRN), online: SSRN <http://ssrn.com/abstract=1268926>.

Some critics of breach notification laws argue that, if for any reason data breach notification legislation is necessary, such legislation should leave it open to the discretion of the data broker or organization involved in the breach to determine if the breach is of such a nature as to warrant disclosure.[19] This, they argue, will check the problems associated with over-notification. This argument seems to find expression in the data security breaches notification law of the state of Arkansas.[20] The legislation provides for exemption for notification "if after a reasonable investigation the person or the business determines that there is no reasonable likelihood of harm to customers."[21] There are, however, many reasons to oppose this approach.

Granted, over-notification could lead to desensitization, but leaving it to the discretion of data brokers or organizations to determine whether to notify their clients of a security breach or not, will not be in the best interest of the individual whose personal information is at risk. The reason for this is that, in the exercise of such discretion, the organizations involved will tend to put their business interests or corporate image ahead of the personal interests of the clients. Such a company will become the judge in its own case, and it is hard to imagine that such discretion will be exercised judiciously in most cases. As I shall argue later, the discretion to determine whether a disclosure or notification should be made would be best exercised by a third party who has no personal interest in the matter.

As the number and size of personal information, or data banks, continues to rise in response to modern business needs, incidents of data security breach will continue to rise correlatively, along with incidental identity theft and fraud. Unless an organization notifies individuals that their personal information is at risk, such individuals may eventually become the unwitting victims of potentially devastating identity theft and fraud. Whatever argument may be proffered by the anti-notifica-

---

19 In late April 2008, Canwest News Service reported on a leaked draft review of PIPEDA. The report reveals that the "federal government is proposing to leave it up to companies to decide when to tell customers of a loss of personal information and only in cases where businesses determine there is a 'high risk of significant harm' from the security breach." The report went further to state that "factors to be considered by companies in determining whether a security breach meets the threshold include the sensitivity of information, nature and number of data elements, whether the information is unreadable or unusable, probability that the information could be misused for harmful purposes, and other 'contextual and situational factors.'" See Sarah Schmidt, "Feds to Leave Disclosure of Data Security Breaches to Businesses: Legislative Plan" *Canada.com* (24 April 2008), online: Canada.com <http://www.canada.com/topics/news/national/story.html?id=b1e17cf1-bbba-46e6-acdc-a9650682d6a9&k=1253>.

20 U.S., Bill S. 1167, 86th General Assembly, Ar. (2005) *An Act to Provide Notice to Consumers of the Disclosure of Their Personal Information*, online: Arkansas 86th General Assembly <http://www.arkleg.state.ar.us/ftproot/bills/2005/public/SB1167.pdf>.

21 *Ibid.* at s. 4-110-105(d). See also the position in the State of Kansas, U.S., Bill S. 196, Kan. (2006) ss. 4(1), 149, online: Kansas Legislature <http://www.kslegislature.org/bills/2006/196.pdf>.

tion school of thought, I am of the view that the benefits of well-designed notification regimes far outweigh the costs. I shall further analyze existing data security breach notification statutes in the United States and Canada. In the course of the analysis, I shall proffer recommendations, where necessary, for a well-designed data security breach notification law in Canada, taking into consideration the criticisms hitherto highlighted.

(a) An Analysis of Data Security Breach Notification Legislation

(i) United States

Although there is a profusion of data security breach notification statutes in the United States, none of them seems to be of general application. More than half of the states have enacted their own data security breach notification legislation. An attempt to introduce similar legislation at the federal level has remained in a stalemate. Hence, what is obtainable in the United States today is a labyrinth of sectoral and issue-specific state legislation. One cannot but warn of the conflicts of laws situations probably to arise from such a proliferation of state legislation, especially considering the ease of data transferability across state boundaries.

(A) Federal Legislation

In 1999, the U.S. Congress introduced the *Gramm-Leach-Bliley Act* (GLBA). Section 501(b) of the Act mandated each agency or authority mentioned in section 505(a) of the Act[22] to establish an appropriate standard for financial institutions under their jurisdiction "to protect against unauthorized *access to* or *use* of such records or information which could result in substantial harm or inconvenience to any customer."[23] The fact that the statute required a regulatory standard that will prevent the "use" of personal information obtained through such unauthorized access could imply, among others, a response program that will ensure notification to individuals whose personal information has been breached. Such a response program is the best way to give the affected individuals the opportunity to take preventive measures to forestall the *use* of breached personal information.[24]

---

22 Such agencies include Office of the Comptroller of the Currency, Treasury (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision, Treasury (OTS) and National Credit Union Administration (NCUA).

23 Emphasis added. See generally s. 505 *Gramm-Leach-Bliley Act*, 15 USCS ss. 6801–6809, *et seq.* 106 P.L. 102, 113 Stat. 1338, 1999 Enacted S. 900; 106 Enacted S. 900 [GLBA].

24 It could also imply notification to credit card companies, credit monitoring agencies or other third parties who may be instrumental in forestalling the unauthorized use of such personal information.

In response to this mandate, the Federal Financial Institution Examination Council (FFIEC) agencies[25] jointly issued interpretative guidance for financial institutions.[26] The Interagency Guidance, among others, requires financial institutions to "develop and implement a response program designed to address incidents of unauthorized access to customer information maintained by the financial institution or its service provider."[27] Such a response program should contain, among other things, procedures for assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information has been accessed or misused. It should also contain procedures for notifying customers, when warranted, in a manner designed to ensure that customers will be able to reasonably receive the news.[28] Such notification should include, *inter alia*,

1) a description of the incident,
2) the type of information subject to unauthorized access,
3) measures taken by the institution to protect customers from further unauthorized access,
4) a telephone number customers can call for information and assistance,
5) a reminder to the customers to remain vigilant over the next twelve to 24 months and to report suspected identity theft incidents to the institution.[29]

Although the Interagency Guidance obligates notification for security breaches when warranted, it suffices to state that it is neither a piece of legislation nor part of the GLBA. It can be considered as a directive made by a regulatory body, pursuant to powers conferred on it by law, the breach or non-compliance of which may result in administrative sanctions by the regulatory body.[30]

(B) State Legislation

The state of California was the first jurisdiction in the United States to introduce a data security breach notification law. The Bill, which came into effect in

---

25 GLBA, *supra* note 23.

26 See "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice." 70:59 Fed, Reg, 15636 (2005).

27 *Ibid.* at 15737.

28 Customer notification is warranted where the financial institution becomes aware of a breach of "sensitive customer information", unless the institution after adequate investigation, "reasonably concludes that misuse of the information is unlikely to occur". Notwithstanding, it must take appropriate steps to protect the interest of the affected customers including, but not limited to, monitoring the affected customers' account. See Interagency Guidance, *supra* note 26 at 15743.

29 *Ibid.* at 15746.

30 See *Guin v. Brazos Higher Education Service Corp. Inc.*, 2006 U.S. Dist. LEXIS 4846 (D. Minn., 2006), [*Brazos*]. Where the court said that GLBA did not impose an obligation on financial institution to encrypt data.

July 2003, was incorporated into the *California Civil Code*[31] and applies to government agencies[32] as well as any person or business[33] doing business in California, irrespective of whether such a person or business resides in, or is based in California. The mere fact that such a person or business carries on business in California, whether online or offline, brings it within the long arm of the California law. Therefore, it is suggested that a Canadian merchant, who transacts business with a Californian resident online, is bound to give notice to the latter in the event of a data security breach involving his personal information. Curiously, under the current state of Canadian law, the merchant is not under any legal obligation to give the same kind of notice to Canadian residents who transact business with him.

The California law requires notification to be made with regard to *any* security breach involving unencrypted personal information. Personal information is defined to mean "an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number, driver's license number or California Identification Card number, account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account."[34] Therefore, it logically follows that the requirement for notification under this law will not apply if the data security breach involves encrypted data.[35]

The problem with this limitation of notification to unencrypted data lies in the fact that, with development in information technology, certain levels of encryption, hitherto considered secure, may subsequently become less secure and hence, lend themselves to being cracked without much difficulty. What we have today is a continuous increase in levels of encryption; the higher the level, the more secure the encrypted data. A data breach with a very low level of encryption will not require notification under the California law — this notwithstanding the fact that the personal information stands the risk of being deciphered and misappropriated. In view of this, the Federal Interagency Guidance, issued under the authority of the GLBA, rejects blanket exclusion for encrypted information because, "there are many levels of encryption, some of which do not effectively protect customer information".[36]

Considering the dynamic nature of information technology, it is recommended that comprehensive data security breaches notification legislation should be flexible

---

31 *California Civil Code*, supra note 5.

32 *Ibid.* at s. 1798.29.

33 *Ibid.* at ss. 1798.82 to 1798.84.

34 *Ibid.* at s. 1798.29(e). The definition excludes "publicly available information that is lawfully made available to the general public from federal, state, or local government records." See also s. 1798.29(f).

35 Some other states exempt the requirement for notification not only for encrypted data, but also where redaction or other methods are used to render the data "unreadable or unusable". These states include Colorado, Illinois, Indiana, Kansas, Louisiana, Maine, Nebraska, Pennsylvania and Vermont.

36 See *Interagency Guidance*, *supra* note 26 at 15745.

and dynamic to keep pace with the dynamic world of information technology. In addition (though the legislation was silent on this), where the security of encrypted data is breached and the breach also results in the acquisition of the private key for the encrypted data, such data stands in the same position as unencrypted data, hence, the requirement of notification under the law should also apply. The New York data security breach notification law filled this gap by requiring the notification of breaches involving encrypted data along with the encryption key.[37]

In view of the foregoing, it is recommended that Canadian breach notification legislation should expressly require that notification be made in the following cases:

1) when there is a breach of encrypted data of which the level of encryption does not provide adequate or sufficient security, judging from the level or standard of technology in place at the time of the breach,
2) when there is a breach of encrypted data resulting in the acquisition of the private key.

Another point to highlight from the California law is that it does not leave it to the discretion of the data broker or organization involved in security breaches to determine whether the breach is of such a serious nature as to require notification. Once the breach relates to unencrypted personal information, there is no discretion in the matter. Disclosure or notification must be made in the most expeditious time possible and without unreasonable delay. Delay is only permissible where it is consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system, or where it is consistent with the legitimate needs of law enforcement, e.g. where immediate disclosure or notification will jeopardize the activities of law enforcement agents.[38]

This presents a vicious dilemma. If organizations are required to notify clients in the event of any security breach of unencrypted data (even where the breach may not be of a serious nature), it may result in over-notification along with the consequential effects hitherto highlighted. On the other hand, if organizations are given the leeway to determine which security breach to report or notify clients about,

---

37 New York, *Information Security Breach and Notification Act*, 2005 N.Y. LAWS 442, s. 899-AA, online: Cyber Security&Critical Infrastructure Coordination <http://www.cscic.state.ny.us/lib/laws/documents/899-aa.pdf> [*New York Breach Notification Act*].

38 *California Civil Code*, *supra* note 5 at s. 1798.82(a). The current practice in Canada is for organizations to notify the Office of the Privacy Commissioner when they experience incidents of security breach to client's personal information and the Privacy Commissioner may then initiate an investigation into the matter. It does not seem that there is a legal obligation on their part to do this under the PIPEDA. See Office of the Privacy Commissioner of Canada, News Release, "Privacy Commissioner Launches Investigation of CIBC Breach of Talvest Customers' Personal Information" (18 January 2007), online: News Release: Privacy Commissioner <http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070118_e.asp>.

such freedom will not be exercised in the best interest of the clients whose personal information has been breached. It may also result in outright concealment.

Hence, to deal with the issue of over-notification versus outright or partial concealment of breach, it is recommended that a typical Canadian data security breach notification law should require that, in the event of a security breach, the organization involved should immediately, upon becoming aware of the breach, notify the Office of the Privacy Commissioner (in addition to the law enforcement agency) who shall, without delay, investigate the nature or seriousness of the breach to determine if notification should be made.[39] The position of the Privacy Commissioner, as an unbiased third party, will serve to adequately represent the interest of the organization involved, the clients whose personal information has been breached, and the public.

An apparent problem with the California legislation is its definition of data security breach or, to use the exact wording in the legislation, "breach of the security of the system."[40] It is defined as "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[41] The use of the word "computerized" raises a problem with that definition.[42] Data is said to be computerized when it exists in electronic or digital format.[43] The definition tends to imply that a data security breach could only occur when there has been unauthorized acquisition of personal information existing in digital or electronic format.

The problem with the use of the word "computerized" becomes obvious when we consider some data spill incidents, such as those in 2001 and 2002, when a Canadian bank mistakenly faxed documents containing its customers' personal information to an unwilling and unauthorized third party.[44] In this case, although the personal information was transferred electronically — by fax — there was no unauthorized acquisition until the documents were printed from the recipients' fax ma-

---

39 This was also the position adopted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics Considering the 2006 Review of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

40 *California Civil Code*, *supra* note 5 at s. 1798.82(d).

41 *Ibid.* [emphasis added].

42 Connecticut version of the legislation uses the phrase "unauthorized access to or acquisition of *electronic* files, media, databases or *computerized data*" [emphasis added]. See U.S., S.B. 650, *An Act Requiring Consumer Credit Bureaus To Offer Security Freezes*, 2005, Reg. Sess., C.T. 2005.

43 "Computerized" is defined as "to control, perform, process, or store (a system, operation, or information) by means of or in an electronic computer or computers." See *Dictionary.com, s.v.* "computerized", online: Dictionary.com <http://dictionary.reference.com/browse/computerized>.

44 See *Speevak v. Canadian Imperial Bank of Commerce*, Claim No. 05-CV-283484CP, online: Girard Law Office <http://www.cacounsel.com/CIBC%20Class%20Action%20Claim.pdf>.

chine. Thereafter, the documents existed in paper form as opposed to computerized form.

In another case involving a Canadian collection agency, Nor-Don Collection Network Inc,[45] documents containing debtors' names and personal information were recovered from a vacant building. The personal information contained in the documents included phone numbers, social insurance numbers, addresses, dates of birth, occupations, bank names, branches, account numbers, account balances, etc; this information was more than sufficient to perpetrate identity fraud.[46]

Hence, the use of the word "computerized" in the definition of data security breach under the California law would imply that situations, like the ones above, cannot be classified as security breaches simply because the personal information involved was not in computerized form, even though the same result is generated in cases of unauthorized acquisition of computerized data. In light of the problem that may arise from this definition, the State of Indiana Legislature, in enacting its data security breach notification legislation, opted for a more comprehensive and unambiguous definition, viz:

> unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.[47]

In light of the foregoing, it is recommended that any Canadian data security breach notification legislation should, for the purpose of clarity and the avoidance of any ambiguity, adopt a definition styled along the lines of the Indiana legislation: "an unauthorized acquisition or access to data or *documents* that compromises the security, confidentiality, or integrity of personal information maintained by a person, business or agency".

With respect to notification, there are three acceptable forms of notification under the California legislation, namely, a written notice, an electronic notice[48] and

---

45 Alberta, Office of the Information and Privacy Commissioner, Nor-Don Collection Network Inc. Investigation P2005-IR-002, "Report on an Investigation into the Security of Customer Information" by Jill Clayton, Portfolio Officer (31 January 2005), online: Information and Privacy Commissioner of Alberta <http://www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf>.

46 See also *Giordano v. Wachovia Securities LLC et al*, 2006 U.S. Dist. LEXIS 52266 (D. NJ, 2006) which involved the loss of a printed report containing financial information of the plaintiffs and tens of other customers of the defendant financial institution.

47 *Indiana Code*, s. 24-4.9-2-2, online: State of Indiana <http://www.in.gov/legislative/ic/code/title24/ar4.9/ch2.html>.

48 The electronic notice must conform to provisions regarding records and signatures set forth in s. 7001 of Title 15 of the *United States Code*, which provides, inter alia, that where a law requires information relating to a transaction(s) to be in writing, such requirement is satisfied by the use of an electronic record to provide the information if

a substitute notice.[49] Although written notices and electronic notices are the primary means of notification under the legislation, substitute notices, where permissible, shall consist of *all* of the following: an email notice, a conspicuous posting on the organization's website (if it has one), and a publication in statewide media.[50] It is necessary to note that the three methods under substitute notice are all cumulative, i.e., the notice must be sent through all the methods (where applicable) and not either of them.[51]

A substitute notice is permissible "if the person or business demonstrates that the cost of providing such notice would exceed two hundred and fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information."[52] However, the legislation fell short of specifically stating to *whom* these facts must be proved or demonstrated before a substitute means of notification could be authorized. It is suggested that under the Canadian model legislation or amendment, which is being proposed, the facts should have to be proved to the federal Privacy Commissioner, who may then authorize the issuance of substitute notice.

Whatever form the notification takes, the ultimate priority should be to convey a comprehensive notice to the affected individuals. Such notice should provide detailed information as to the nature and extent of the breach, addressing: the type of personal information that was involved, the steps the organization has taken since it discovered the breach, the steps the individuals should take to protect themselves, and a contact person or persons within the organization to call for further information.

(ii) Canada

A bold legislative attempt towards notification of breach of personal information in Canada, emerged with the enactment of the provincial *Personal Health Information Protection Act, 2004* by the Ontario legislature.[53] The purpose of the

---

the consumer has affirmatively consented to receiving the information via electronic means and has not withdrawn the consent at the time of the information being sent. See 15 U.S.C. s. 7001.

49 Some states, such as Arizona, Colorado, Connecticut, Hawaii, Idaho, Michigan, among others, provide for telephonic notice.

50 *California Civil Code*, *supra* note 5 at s. 1798.82(g)(3). Provision is also made for organizations to utilize their own notification procedure where it is in compliance with the notification requirement under the legislation. See also s. 1798.82(g)(3).

51 The only exception being, where the subject person does not have an email contact or, where the organization does not own a website.

52 *California Civil Code*, *supra* note 5 at s. 1798.29(g)(3).

53 *Personal Health and Information protection Act*, 2004, S.O. 2004, c. 3, Sched. A., online: Service Ontario e-Laws <http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm>.

Act, among others, was to establish rules, for the collection, use and disclosure of personal health information about individuals, that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care.[54]

The Act imposes an obligation on health information custodians, who have custody or control of personal health information about an individual, to notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.[55] For the purpose of clarity, the Act went further to define personal health information as well as the health information custodian. Personal health information was defined by the Act to include information about an individual in *oral or recorded* form, relating to the physical or mental health of the individual, and including information that consists of the health history of the individual's family, the provision of health care to the individual, the individual's eligibility for health care, and health number, among others.[56]

"Health information custodian" was defined to include persons or organizations that have custody or control of personal health information as a result of, or in connection with, the performance of the person's or organization's powers or duties.[57] This definition would, no doubt, include health care practitioners and providers, pharmacies, a health or medical laboratory, nursing homes, as well as health insurance companies, to mention a few.

Although this Act introduced the recommended approach of imposing statutory obligation to raise notification for a data security breach, it suffices to state that it did not deal with the issue of notification in broad detail. For example, the Act was silent as to the form which notification should take. There was also a complete absence of any statutory penalty or remedy for failure to comply with the requirement of notification under s. 12 of the Act. In addition, the Act only governs personal health information and, more so, it is a provincial legislation applicable only within the province of Ontario. Notwithstanding, the novel move by Ontario toward statutory imposition of a duty to notify in the event of a breach of data security, is a step in the right direction. This may as well pave the way for Canadian breach of data security notification legislation that would fill the current gap created by the absence of legislation to that effect, as well as the uncertainties in common law with regard to a duty to notify for data security breaches.

Where there has been a security breach, accompanied by notification to the individuals involved, in most cases, the usual response on the part of the affected individuals is to take preventive measures to forestall damages or future harm that may arise from the use of their personal information. This will normally involve expenditure in terms of time and monetary resources. In some cases, the victims may resort to litigation to recover damages for these preventive costs. In the next

54 *Ibid.* at s. 1.

55 *Ibid.* at s. 12(1).

56 *Ibid.* at s. 4(1).

57 *Ibid.* at s. 3(1).

part of this article, I shall examine the inadequacy of common law in providing remedies to victims of data security breaches.

II. COMMON LAW AND DATA SECURITY BREACH

Development in the field of information technology has continued at an unprecedented speed, bringing with it greater benefits to humanity, as well as exposing us to the risk of injuries. Some of these injuries are novel and, in most cases, fall outside the scope of legal remedies provided by existing laws.

Information technology is creating "novel" relationships as well as injuries that are not analogous to any that have come before.[58] Some legal jurisdictions have resorted to the promulgation of statutory laws to provide remedies for victims of these "novel" injuries, which include data security breaches. In some other jurisdictions, where such statutory remedies are not yet in place, the recourse for legal redress has often been founded in antiquated and inadequate common law remedies such as negligence, breach of contract or breach of fiduciary duty, etc.[59] This development has posed a challenge to existing rules of common law as is rightly observed by Currie:

> The common law, with its tradition of conservatism and incremental change, is confronted with developments that do not lend themselves readily to the application of precedent and analogy.[60]

Currie also examines the capacity of the common law tort of negligence to adequately handle "tech torts". He acknowledges that technological expansion has resulted in new forces producing new relationships, as well as new kinds of injuries, which need to be compensated. However, he is reluctant to concede the inability of common law to continue its "mostly proud tradition" of compensating the injured and providing education and deterrence in relation to tech torts.[61] De Villiers also argues that a victim of a data security breach could litigate, under a negligence theory, against anyone who contributed to the risk associated with the breach, including those who failed in their duty to reduce or eliminate the risk.[62]

Generally, in an action for negligence in common law, the plaintiff has the burden of proof. The plaintiff must prove that the defendant owed him a duty of care, that the defendant was in breach of the duty, and that the breach of duty re-

---

58 Robert J Currie, "Of Neighbours and Netizens, or, Duty of Care in the Tech Age: A Comment on *Cooper v. Hobart*" (2004) 3:2 Canadian Journal of Law and Technology 81 at 83.

59 This research paper focuses on the common law tort of negligence.

60 Currie, *supra* note 58 at 81.

61 *Ibid.* at 87.

62 Meiring De Villiers, "Reasonable Foreseeability in the Information Security Law: A Forensic Analysis" (2008) 30:3 Hastings Communications and Entertainment Law Journal 419.

sulted in legal injury to the plaintiff.[63] It must also be shown that the defendant's act or omission was the proximate cause of the plaintiff's injury.[64]

When the tort of negligence was enunciated in the famous case of *Donoghue v. Stevenson*,[65] it was applied with reference to a manufacturer of a drink. Over time, the tort of negligence was extended to other contexts. Recent attempts to extend same to cases of data security breaches have been, in most cases, met with judicial disapproval. Although judicial decisions in this area of information technology law in Canada are now emerging, I shall examine the judicial approach to the issue from the United States, where this area of law has received considerable judicial attention. I shall also examine Canadian tort laws relating to recovery of damages for economic loss. It is my argument that the economic loss rule in Canadian tort law should undergo further judicial reform to enable recovery for out-of-pocket expenses resulting from data security breaches.

(a) Proof of Negligence in Data Security Breach Litigation

Data security breaches vary in nature, ranging from the theft or loss of data tapes or computers,[66] the hacking of computer networks and databases, the disposal of computer systems or mediums containing personal information,[67] and the theft of customer personal information by employees. Other forms include wrongful or mistaken transfer of clients' personal information to third parties,[68] as well as other forms of unlawful or unauthorized access to databases containing confidential personal information.[69] Whatever form it takes, a breach of data security could result in identity theft, credit fraud, or account takeovers. In the latter case, the identity thief takes over the financial account of the victim.[70] Some cases of data security

---

63 See *Donoghue v. Stevenson*, [1932] A.C. 562 (U.K. H.L.).

64 *Derksen v. 539938 Ontario Ltd.*, [2001] 3 S.C.R. 398 (S.C.C.).

65 *Donoghue*, *supra* note 63.

66 *Brazos*, *supra* note 30.

67 See e.g. B.C., Office of the Information and Privacy Commissioner, Investigation Report F06-01, "Sale of Provincial Government Computer Tapes Containing Personal Information" (2006) B.C.I.PC.D. No. 7, online: <http://www.oipc.bc.ca/orders/ investigation_reports/InvestigationReportF06-01.pdf>.

68 See *Speevak*, *supra* note 44.

69 It should be noted that the Office of the Privacy Commissioner of Canada has on many occasions launched investigations into cases of data security breaches, especially those cases involving breaches of the provisions of the PIPEDA. For comprehensive lists of these reports, see Office of the Privacy Commissioner of Canada, "Commissioner's Findings: Summaries of Incidents under the *Personal Information Protection and Electronic Documents Act*", online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/incidents/index_e.asp>.

70 If the identity thief opens a new bank or credit account in the victims name, this is referred to as true name fraud. See Anthony E. White, "The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who is Going to Pay for It?" (2005) 88 Marq. L. Rev. 847 at 851.

breach have been the results of the negligent act of the organizations, or their agents, in custody of the breached data. For example, in *Forbes v. Wells Fargo Bank*,[71] a laptop containing unencrypted personal information of the defendant bank's customers was negligently left unattended in a rental car, parked at a gas station with the ignition key switched on, while the defendant bank's employees were off to a convenience store located within the gas station. A car thief made away with the car as well as the laptop. The latter was never recovered.

The security breach in the above case resulted in a class action against the bank for the negligence of its employees.[72] In their complaint, the plaintiffs claimed they suffered fear, anxiety and worry. Although there was no record of any fraudulent use of the plaintiffs' personal information at the time of the proceeding, the plaintiffs expressed the fear, anxiety and worry as to the possibility of their becoming victims of identity theft or credit fraud sometime in the future. To forestall this, the plaintiffs expended time and money to monitor their credit for any fraudulent use of their personal information.

From a layman's perspective, the conduct of the defendants' employees in this case was, no doubt, negligent. However, it suffices to state that in the tort of negligence, merely acting negligently does not give rise to a cause for action. A special relationship must exist between the parties (at the time of the negligent act) giving rise to a duty of care, which must have been breached, thus resulting not just in injury or damage, but rather resulting in the kind of injury or damage recognized by law.[73]

Arising from the relationship between a bank and its customer is a responsibility on the part of the bank to safeguard its clients' personal information.[74] Failure to do this might give rise to an action for breach of fiduciary duty.[75] The customer has a right to expect that personal information divulged in confidence, in a business or similar transaction, will be guarded with the utmost care. In addition, looking at the issue from a control standpoint, the organization in custody of the personal information is in the best position to protect such information from unauthorized access.[76] Hence, it is not in dispute that the defendant bank in this case owed the

---

71 *Forbes v. Wells Fargo Bank, N.A.*, 420 F.Supp.2d 1018 (D. Minn., 2006), [*Wells Fargo*].

72 In Canada, U.S. and Puerto Rico, a similar class action was commenced in 2007, following breaches of data security at TJX Companies Inc., owners of Winners and HomeSense. The class action was terminated following an out-of-court settlement reached between the plaintiffs and TJX Companies. Under the terms of the settlement, TJX agreed to provide among others for credit monitoring as well as reimbursement for out-of-pocket costs or personal lost time incurred by affected victims.

73 See *Priestman v. Colangelo*, [1959] S.C.R. 615 (S.C.C.).

74 See *Daly v. Metropolitan Life Ins. Co.*, 4 Misc. 3d 887, 782 N.Y.S.2d 530, 532 (N.Y. Sup., 2004).

75 See *Jones v. Commerce Bank*, 06 Civ. 835 (U.S. Dist. 2007) [RNF].

76 *Bell v. Michigan Council 25*, 2005 Mich. App. LEXIS 353 (Mich. C.A., 2005).

plaintiffs a legal duty to protect their personal information while in the possession or custody of the bank.

In the context of negligence, a legal duty has been defined as an obligation under the law, of a party to conform to a particular standard of conduct towards another party.[77] The standard for ordinary negligence is the traditional standard of the reasonable man of ordinary prudence.[78] Proceeding from this premise, there should not be much difficulty in asserting that the defendants' employees, by leaving the said laptop in an unlocked and unattended car, with the ignition key turned on, acted negligently. Such a negligent act was in breach of the duty of care, which the defendant bank owed the affected customers.

However, it is curious that the application of the common law tort of negligence to cases of data security breaches is not as easy as presented in the hypothesis above. The difficulty lies in that, considering the nature of data security breaches,[79] the damage resulting from the breach (which is an essential element of negligence) may not become immediately evident, as the data thief has in his possession a vast stock of personal information. He may not be able to utilize this large amount of information immediately. This being the case, the only prudent course of action for victims of data security breaches would be to expend time and money in running and reviewing their credit checks, setting up credit fraud alerts, obtaining new credit and debit cards, closing old, and opening new bank accounts, and taking other precautionary measures to forestall future harm likely to arise from the fraudulent use of such personal information.

This gives rise to some difficult questions, to which the judicial answers will essentially highlight the adequacy or inadequacy of the common law tort of negligence to cases of data security breaches. First, in an action for negligence arising from a data security breach, can a victim of the breach recover damages for a threat of future harm that has not yet crystallized or, in other words, if the plaintiff has not suffered a present harm, could the possibility of a future harm satisfy the third element of the tort of negligence? Secondly, where the plaintiff expends time and resources in taking precautionary measures to prevent the threat of future harm from arising due to the breach, are such expenditures or damages recoverable in an action for negligence arising from the breach? Where the breach results in actual or immediate damage, how does the plaintiff prove the element of causation — that the personal information used to perpetrate fraud in his name — was actually obtained from the breach incident and not from other sources? The question relating to recovery of damages also relates to lost time and opportunities arising from the breach. To what extent are lost time and opportunities recoverable, if at all?

As I commence to examine these issues in light of decided cases, I must enter an early caveat to the effect that many of the judicial answers to these questions

---

77 See *Minneapolis Employees Retirement Fund v. Allison-Williams Co.*, 519 N.W.2d 176, 182 (Minn., 1994).

78 *Queen v. Cognos Inc.*, [1993] 1 S.C.R. 87 (S.C.C.).

79 Typically, data security breaches usually result in unauthorized access to the personal information of a large number of persons.

have been met with the utmost dissatisfaction from many victims of data security breaches. This dissatisfaction serves to substantiate the need for judicial reform through case law as well as statutory intervention.

In the *Wells Fargo* case mentioned earlier,[80] the plaintiffs claimed that the time and money they spent monitoring their credit report suffices to establish the essential element of damage in an action for negligence. The Court disagreed with them, holding that a plaintiff can only recover damages for loss of time in terms of earning capacity or wages. More so, the loss must result from the present injury and not from anticipation of future injury. Accordingly, the Court ruled that:

> the plaintiffs' injuries are solely the result of a perceived risk of future harm. Plaintiffs have shown no present injury or reasonably certain future injury to support damages for any alleged increased risk of harm. For these reasons, plaintiffs have failed to establish the essential element of damages.[81]

Here, the court seems to follow the decision in the earlier case of *Guin v. Brazos Higher Education Service Corp. Inc.*,[82] in which facts were similar to those in the *Wells Fargo* case. In *Brazos*, the defendant corporation kept some of their customers' personal information in an unencrypted format in a laptop computer that was subsequently stolen from an employee's home during a burglary. The plaintiff, on being notified of the incident, ordered and reviewed copies of his credit report from three credit agencies. Although the credit report did not indicate that the plaintiff's personal information had been accessed or misappropriated, the plaintiff still commenced an action for negligence against the defendants, seeking to recover for out-of-pocket loss, emotional distress, fear and anxiety, as well as consequential and incidental damages. In refusing the claim, the Court held that the threat of a future harm, which has not yet crystallized, will not satisfy the damage requirement in an action for negligence.[83] Of all the cases of data security breaches that have come before the court so far, the court has not considered the risk of future harm as sufficient damage.[84]

---

80 *Wells Fargo*, *supra* note 71.

81 *Ibid.* at 1021.

82 *Brazos*, *supra* note 30.

83 See *Reliance Ins. Co. v. Arneson*, 322 N.W.2d 604, 607 (Minn., 1982); *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 U.S. Dist. LEXIS 41054, 1 (D. Ariz., 2005); *Randolph et al. v. ING Life Insurance and Annuity Co.*, 2007 U.S. Dist. LEXIS 11523 (D. D.C., 2007).

84 *Walters v. DHL Exp.*, 2006 U.S. Dist. LEXIS 29057 (D. Ill., 2006) (the court was of the view that such risk amounts to mere speculation as opposed to actual damage); *Hendricks v. DSW Shoe Warehouse Inc.*, 2006 U.S. Dist. LEXIS 51235 (W.D. Mich., 2006) (the court characterized the plaintiff's claim as an action to "to buy peace of mind, or to help her determine if and when a claim accrues through actual loss").

(i) The "Medical Monitoring" Analogy

One of the seemingly insurmountable hurdles in litigation resulting from data security breaches has always been the courts' insistence that the threat of future harm does not justify a cause of action. Chandler has identified this as one of the basic problems posed for plaintiffs in negligence claims for harms flowing from breaches of data security.[85]

To overcome this hurdle, plaintiffs have often attempted to draw a similarity between their situations and those of plaintiffs in toxic exposure cases. When a person has been exposed to toxins or harmful substances, or uses a product later found to have adverse side effects that are likely to result in a health hazard sometime in the future, some courts have allowed such individuals to recover expenses for medical monitoring usually undertaken to prevent or check the development of the future hazard arising from such exposure.[86]

Hence, the argument is this; if plaintiffs in toxic exposure cases, which are likely to result in harm to health sometime in the future (but have not actually resulted in any immediate harm), are entitled to recover damages for medical monitoring, it should follow that plaintiffs in data security breaches litigation, who are exposed to the threat of future harm (but have not suffered any immediate harm), should equally be entitled to recover damages for expenditures incurred in credit monitoring as well as other expenditures incurred in forestalling future injury likely to arise from the breach.

Logical as this analogy may seem, it has been rebuffed by the courts. The position of the Court seems to be that in toxic exposure cases, there is usually direct evidence to show that there was *actual* exposure to the harmful substances. This direct evidence entitles the plaintiff in such cases to recover the cost of medical monitoring, notwithstanding that the hazard has not yet arisen. However, in cases of data security breaches, the court seems to have always emphasized the absence of any direct evidence of exposure of the personal information of the plaintiff. In *Stollenwerk*,[87] where unidentified persons burgled the defendants' facility and stole computer hard drives containing the plaintiffs' personal information, the Trial Court was very reluctant to accept the "medical monitoring" analogy on the ground that there was no evidence of exposure of the plaintiffs personal information. According to the Court,

> Plaintiffs have not brought forward evidence that the personal information on the stolen computers was ever exposed to the thieves involved . . . there is nothing in the record here to suggest that the data, rather than the hardware on which the data was stored, formed the thieves' target. Absent evidence that the data was targeted or actually accessed, there is no basis for a

---

85 Jennifer A. Chandler, "The Epidemic of Lost and Stolen Data: Are Custodians of Data Liable in Negligence for Breaches of Data Security" *Techlaw Magazine* 5.1:23 (January 2008) 23.

86 *Wilson v. Servier Canada Inc.* (2005), 252 D.L.R. (4th) 742 (Ont S.C.J.); additional reasons at (2005), 2005 CarswellOnt 6622 (Ont. S.C.J.).

87 *Ibid.* at 83.

> reasonable jury to determine that sensitive personal information was significantly exposed.[88]

Unfortunately, even where there is evidence that the personal information was the target of the data thief, and that such personal information was indeed "exposed" or accessed, the court continues to raise the hurdle for the plaintiff by curiously insisting that the plaintiff must go further to prove that the data thief intends to make unlawful use of the personal information.[89] However, it has been argued that where there is evidence to indicate that the data has been targeted or, even more compelling, a proportion of the data has been used in identity fraud, the analogy between medical monitoring and data security breach cases is more persuasive.[90]

Other reasons for the courts' refusal to adopt the "medical monitoring" analogy to cases of data security breaches are based on public policy, which has been accepted by the courts (in toxic tort cases) as justifying the departure from the general rule that future risk of injury, without more, cannot form the basis for negligence action.[91] Hence, the public policy interest in preserving public health, which may justify an award for "medical monitoring", may not be sufficiently elastic to extend to claims for credit monitoring arising from data security breaches.

In cases of toxic exposure or unsafe product liability, the likelihood of developing a health condition is, to some extent, scientifically ascertainable with a degree of accuracy, and tort law has always insisted on proof of damages, on the balance of probabilities, as opposed to mere speculation. However, in cases of data security breaches, there is no scientific means of proving that the breached data will be used to perpetrate fraud. In fact, available statistics seem to suggest that the probability that the breached data will be used to perpetrate fraud is quite low.[92]

---

88 *Ibid.* at 5. When this case went on appeal, the appellate court disagreed with this assertion. According to the court, "As a matter of twenty-first century common knowledge . . . the theft of a computer hard drive certainly can result in an attempt by a thief to access the contents for purposes of identity fraud, and such an attempt can succeed." See *Stollenwerk*, *supra* note 83 at 10.

89 *Tracy L. Key v. DSW, Inc.*, 2006 U.S. Dist. LEXIS 69887 (S.D. Ohio, 2006), at p.17; *Kahle v. Litton Loan Servicing*, 2007 U.S. Dist. LEXIS 35845 (U.S. Dist., 3007) [RNF].

90 Jennifer A. Chandler, "Negligence Liability for Breaches of Data Security" (2008) 23 Banking & Finance Law Review 223.

91 See *Stollenwerk*, *supra* note 83; *Amfac Distrib. Corp. v. Miller*, 138 Ariz. 152, 673 P.2d 792, 793-94 (Ariz. App. 1983).

92 Turner, *supra* note 9 at 5. It should be noted that the reason why this probability is low is that a single successful act of data security breach by a data thief would usually involve large amounts of personal information sometimes running into tens of thousands or millions. The data thief may only succeed in using a meagre quantity of the personal information at his disposal.

Although, this does not suggest that the negligent exposure of personal information via data security breaches is entirely dissimilar from negligent exposure to a health hazard via toxins or unsafe products. In fact, there is a great deal of similarity between the two. Whereas exposure to toxins or unsafe products may result in harm to health, fraud and identity theft resulting from a data security breach may also result in psychological or emotional distress.[93] More so, the Trial Court in *Stollenwerk* noted that:

> [in] both circumstances the individual may manifest more obvious injury, such as identity fraud or disease, after some period of time, and in neither instance is the later manifestation of patent injury guaranteed, although the certainty with which such a development may be anticipated may be greater for toxic torts.[94]

In view of these similarities, the Trial Court in *Stollenwerk* was of the opinion that the "medical monitoring" analogy can only be applied to credit monitoring in data security breaches if the plaintiff could establish, at a minimum, "(1) significant exposure of sensitive personal information; (2) a significantly increased risk of identity fraud as a result of that exposure; and (3) the necessity and effectiveness of credit monitoring in detecting, treating, and/or preventing identity fraud."[95]

(b) Proof of Causation

So far, we have dealt with situations of data security breaches in which the plaintiffs did not suffer any immediate injury or loss, except for emotional and psychological distress and the incurrence of costs associated with taking preventive measures (which the U.S. courts have consistently maintained will not sustain a cause of action). Subsequently, to illustrate the hardship of the applicability of common law rules to data security breach litigation, I shall examine situations in which the plaintiffs had suffered actual and immediate damage in the form of identity theft or fraud following the breach incident. It may be surprising to observe that even in such situations, recovery of damage remains problematic because of the difficulty in proof of causation. The doctrine of causation requires that the plaintiff must prove that the defendant's act or omission was the proximate cause of his injury — that the act or omission continued "in a natural and continuous sequence, unbroken by any efficient intervening cause", thus, resulting in the injury, and without which the injury would not have occurred.[96]

The problem with proof of causation in litigation resulting from data security breaches lies in the fact that, in the ordinary course of events, an individual's personal information is hardly in the sole custody of just one organization or company. Considering the ease of the flow of information between related organizations, or

---

93 *Stollenwerk*, *supra* note 83. However, this may not be the primary injury.

94 *Ibid.* at 9.

95 *Ibid.* at 13.

96 *Robertson v. Sixpence Inns of America, Inc.*, 789 P.2d 1040, 1047, 163 Ariz. 539 (Ariz., 1990).

government agencies and departments, such information may be held by more institutions than the individual would have originally expected.

Organizations that may likely have custody or possession of an individual's personal information at any particular point in time include banks, utility companies, insurance companies, telephone service providers, health service providers, government agencies such as the revenue agency, licensing offices, etc. Hence, a negligent act on the part of any of these organizations may result in an incident of security breach, involving the plaintiff's personal information. If the plaintiff subsequently suffers any damage in the form of identity theft or credit fraud as a result of the breach, the doctrine of causation requires that the plaintiff must prove that the personal information used in perpetrating the fraud was obtained from no source other than the defendant. This is particularly difficult to prove because the personal information could have been obtained from any of the organizations associated with the defendant. It is also possible that such information was acquired from the internet using phishing websites, malicious software or spyware, or through an unpublicized breach at some other organization.[97]

Judicial decisions are in unison to the effect that in an action for negligence, arising from a data security breach and resulting in actual or immediate injury to the plaintiff, it is not sufficient for the plaintiff to assert that the injury might have been caused by the defendant's act or omission. He must go further to prove that the injury was indeed caused by the act or omission of the defendant. He must provide sufficient evidence, from which a reasonable jury could conclude, on the balance of probabilities, that the injury resulted from the act or omission of the defendant.[98] Such evidence could be actual or circumstantial.[99] Where circumstantial, it must be strong and cogent to warrant a reasonable inference of causation from the circumstances.[100]

In *Stollenwerk*,[101] one of the plaintiffs contended that the personal information used to open fraudulent credit accounts in his name was identical to the personal information in the custody of the defendant and, more so, the fraudulent accounts were opened six weeks after a security breach that arose from a burglary at the defendant's facility. The Trial Court described the plaintiff's assertion as a "logical fallacy". The Court was of the view that,

> to determine that one event caused another merely because the first preceded the second is a classic example of *post hoc ergo propter hoc* ("af-

97 Chandler, *supra* note 90.

98 *Taft v. Ball, Ball & Brosamer, Inc.*, 169 Ariz. 173, 818 P.2d 158, 162 (Ariz. App., 1991).

99 *Mason v. Arizona Public Service Co.*, 127 Ariz. 546, 622 P.2d 493, 500 (Ariz. App., 1980).

100 *Fontaine v. British Columbia (Official Administrator)*, [1998] 1 S.C.R. 424 (S.C.C.). See also *Sunward Corp v. Dun&Bradstreet, Inc.*, 811 F.2d 511, 521 (C.A.10 (Colo.), 1987); *Dreijer v. Girod Motor Co.*, 294 F.2d 549, 554 (C.A., Miss., 1961).

101 *Stollenwerk*, *supra* note 83.

> ter this, therefore because of this"), a logical fallacy. . . . [E]vidence that the burglary preceded the incidents of identity fraud does not allow a reasonable jury to infer that the burglary caused the incidents of identity fraud. Such a conclusion would be the result of speculation and conjecture, not a reasonable inference.[102]

The Court also observed that the plaintiff in question had also provided similar personal information to individuals and organizations other than the defendants. However, on appeal, the Court of Appeal for the Ninth Circuit disagreed with the views of the Trial Court.[103] The Appellate Court was of the view that the particular victim in question produced sufficient evidence, from which a jury could infer a causal relationship between the theft of the hard drives and the incidents of identity fraud he suffered following the Tri-West burglary. The victim, according to the Appeal Court, need not show that the Tri-West burglary was the sole cause of the identity fraud incidents, only that it was, more likely than not, a "substantial factor in bringing about the result," and a factor "without which the injury would not have occurred."[104]

The Appeal Court identified the primary evidence of causation in this case to include, among others, the fact that, (1) the victim gave Tri-West his personal information, (2) the identity fraud incidents began six weeks after the hard drives containing Tri-West's customers' personal information were stolen, and (3) the victim previously had not suffered any such incidents of identity theft.[105]

(i) The Doctrine of **res ipsa** *loquitor*

Although the general rule in common law is that the plaintiff must plead and prove negligence on the part of the defendant,[106] there are exceptions to this rule wherein the onus of proof is shifted to the defendant. One of the common law doctrines, which enable the invocation of this exceptional rule, is the doctrine of *res ipsa loquitor*.[107] The doctrine is to the effect that, where the actual or specific cause of an accident or injury is unknown, or is within the exclusive knowledge of the defendant, a court or jury "may in certain circumstances infer negligence merely

---

102 *Ibid.* at 20.

103 *Stollenwerk v. Tri-West Healthcare Alliance*, 2007 U.S. App. Lexis 27164 (U.S. App., 2007) [*Stollenwerk Appeal*].

104 *Ibid.* at 8.

105 *Ibid.* at 9.

106 See W. Keeton, *Prosner and Keeton on the Law of Torts*, 5th ed. (St. Paul, Minn.: West Pub. Co., 1984) at 235; J.G. Fleming, *The Law of Torts*, 9th ed. (North Ryde, N.S.W.: LBC Information Services, 1998) at 45.

107 Allen Linden, *Canadian Tort Law*, 8th ed. (Toronto: Butterworths, 2006) at 252. Other examples are found in cases of dangerous products. See *Ives v. Clare Brothers Ltd.* (1970), [1971] 1 O.R. 417 (O.S.C.).

from the happening of an event and the defendant's relation to it."[108] Such an inference automatically shifts the burden to the defendant to disprove negligence.

However, before such an inference can be made by the court or jury, the plaintiff seeking to invoke the doctrine must satisfy three basic conditions: (1) that the event is the kind that ordinarily does not occur in the absence of negligence, (2) that the injury was caused by an agency or instrumentality within the exclusive control of the defendant, (3) that it must not have been due to any voluntary action or contribution on the part of the plaintiff.[109]

In *Jones v. Commerce Bank*,[110] the plaintiff alleged that her personal information was stolen and used to perpetrate a series of frauds in her name, including the opening of a fraudulent bank account and utility accounts, as well as the fraudulent withdrawal of money from her account. This caused payments from her account to return "unpaid" and resulted in damage to her business. The plaintiff asserted that the personal information used to perpetrate the frauds was in the sole custody of the bank. She also drew the Court's attention to a news report describing massive theft of confidential data that resulted in the arrest of four of the defendant's employees. The plaintiff sought to compensate for her lack of evidence of causation by invoking the doctrine of res ipsa loquitor. Rejecting this move, the Court stated that:

> Plaintiff avers, in essence, that [the defendant] must have committed a negligent breach of duty because the combination of personal information used to fraudulently attain a check from Plaintiff's insurance company was only possessed by Commerce, and no other institutions or entities. However, it cannot be said that the identity theft here is an event that "ordinarily does not occur in the absence of someone's negligence," just as it cannot be generally said that criminal activity requires some prior negligence to succeed. The thieves might well have stolen Plaintiff's information without any negligence on the part of [the defendant]. Additionally, it does not appear that the information that allegedly establishes *res ipsa loquitor* was in the exclusive control of [the defendant].[111]

The Court was, therefore, of the view that the facts of the case were not sufficient to warrant the invocation of *res ipsa loquitor*. As a result, the plaintiff was unable to avoid the problem posed by the absence of proof of causation. If the court is right in its assertion that identity fraud, which may result from data security breaches, is not an event that "ordinarily does not occur in the absence of someone's negligence," it is doubtful if the doctrine of *res ipsa loquitor* can be conveniently invoked in an action for data security breach so as to remedy the difficulty associated with proof of causation.

---

108 *Kambat v. St. Francis Hosp.*, 89 N.Y.2d 489, 678 N.E.2d 456, 458, 655 N.Y.S.2d 844 (N.Y., 1997).

109 *Ibid.*; *Jackson v. Millar*, [1976] 1 S.C.R. 225 at 235; *Hellenius v. Lees*, [1972] S.C.R. 165 at 172.

110 *Jones v. Commerce Bank*, 06 Civ. 835, 2007 U.S. Dist. 15543 (S.D. N.Y. 2007) [RNF].

111 *Ibid.* at 12.

Although the doctrine of *res ipsa loquitor* is now extinct in Canada by virtue of Supreme Court of Canada's decision in *Fontaine v. British Columbia (Official Administrator)*,[112] it is survived by other legal principles, which shift the burden of proof to the defendants in appropriate circumstances, or which allow the court to infer negligence where necessary. Notwithstanding, it is doubtful from the above analysis of U.S. case law, that the Canadian courts will apply the surviving principles in litigation arising from security breaches of personal information.

Proof of damage and causation have consistently become difficult obstacles to successful data security breach litigation. However, the plaintiffs in *Bell v. Michigan Council 25*[113] were able to overcome this obstacle because of the unusual peculiarity of their case, which presented good evidence of damage and causation. In *Bell*, an employee of the defendant Council was in the habit of taking home documents containing personal information of the Council's members. She did this for the convenience of working from her home. She continued to do so over a long period with the tacit approval of the defendant Council until the employee's daughter unlawfully misappropriated the plaintiffs' personal information. The plaintiffs were able to prove damage by presenting evidence to the effect that the data theft left their collective credit in ruin. There was also evidence of illegal phone services and goods purchased in the plaintiffs' names. The jury accepted this evidence as sufficient proof of damage.

With regard to the element of causation, there was evidence before the Court that, when the defendants' employee's daughter was arrested for her role in the identity fraud case, a notebook was found in her room, which contained the plaintiffs' personal information. This circumstantial evidence seems to have established the element of causation in the case. However, it should be noted that this case did not establish any general rule as to liability in cases of data security breaches. Even the Court was quick to acknowledge that each case is unique and the determination of liability must be made only after considering the relevant factors and the circumstances of the particular case.

What seems to make *Bell* different from the other cases, discussed above, are the circumstances; the other cases did not deal with actual damage resulting from the breach, or where there was actual damage, there was no evidence of causation. *Bell* presents a unique combination of actual damage and causation. This does not imply that once there is a reported incident of data security breach and the personal information of the plaintiff (which constitutes part of the breached data) is used to perpetrate fraud, the plaintiff is automatically entitled to damages. As has been noted above, the element of causation must also be established.

Consequently, we arrive at the conclusion that the position in the common law tort of negligence is that, to be successful in an action for data security breach arising from the negligent act of the defendant, the plaintiff must, *inter alia*, show that the breached data or personal information has been used or misappropriated to the detriment of the plaintiff, thus resulting in immediate harm as opposed to risk of

112 *Fontaine*, *supra* note 100.

113 *Bell*, *supra* note 76.

future harm. Failure to prove such use or misappropriation, resulting in damage, may warrant dismissal of the plaintiff's case.

This standpoint in common law puts victims of data security breaches in a very delicate position. For example, if a victim is unable to prove present damage arising from the use of his personal information in an action for negligence, resulting in the dismissal of his case, can he present his case sometime in the future, when damage can be ascertained from the detrimental use of the stolen data? It seems that he may not, as the principle of *estoppel per res judicata* may become operative. Assuming, for the purpose of argument, that he could, his chances of success would be minimal, as the passage of time would have made it even more difficult to establish causation.

Second, the rule also shows that even damages or losses suffered, as a result of efforts or attempts to forestall future loss likely to result from such a breach, are not recoverable in an action for negligence arising from that breach. The rule, therefore, leaves victims of data security breaches in a delicate legal quandary. In cases of data security breaches, it is not reasonable to expect an immediate fraudulent use of the personal information, resulting in damage. The immediate damage that is reasonably foreseeable will definitely be the financial cost incurred by the victims in taking preventative measures to forestall future harm from the use of such personal information.

Since, in almost all cases, the victims are hardly responsible for the breaches, it will be commonsensical to expect that, in an action for negligence arising from a breach, the victim should be able to recover out-of-pocket expenses incurred by taking the necessary preventative measures to forestall future damage.[114] Unfortunately, this has not been the case, as such expenditures have been viewed as pure economic loss. Furthermore, I shall examine the current state of Canadian legal jurisprudence to show that legal principles established in Canadian case law could be applied to enable victims of a data security breach to recover some economic loss and damages resulting from data security breaches.

(c) The Duty of Care and Economic Loss Rule

Duty of care has been described as the analytical starting point for all negligence claims in common law.[115] In the famous "neighbourly principle" formulated by Lord Atkin in *Donoghue v. Stevenson*, his Lordship stated:

> You must take reasonable care to avoid acts or omissions which you can reasonably foresee would be likely to injure your neighbour. Who, then, in law is my neighbour? The answer seems to be — persons who are so closely

---

114 Although, in some cases, the organization or company from wherein the breach emanated may undertake the cost of credit monitoring and alert. This, in most cases is done out of corporate responsibility and image laundering as there is no legal obligation on their part to undertake such responsibility. U.S. S.B. 2290, *An Act Relating to Protection From Security Breaches*, 23rd Legislature, Reg. Sess., Haw., 2006, s. 3(f).

115 Currie, *supra* note 58 at 81.

> and directly affected by my act that I ought reasonably to have them in contemplation as being so affected when I am directing my mind to the acts or omissions which are called in question.[116]

The duty of care in the context of tort of negligence, according to Lord Akin, is owed to neighbours — that is, "persons who are *so closely and directly* affected" by your acts that you ought reasonably to have them in contemplation. Since 1932, when the "neighbourly principle" was formulated in *Donoghue*, lists of judicial decisions across jurisdictions have sought to broaden the tentacles of duty of care. The courts are currently faced with the somewhat difficult issue of how the tentacles of the "neighbourly principle" or duty of care could be extended to cover the digital neighbourhood designed and created by modern technology. The guiding principle, with regard to the extension of duty of care to "novel" situations, was laid down in the tests formulated in *Anns v. Merton London Borough Council*.[117] The principle was later reformulated by the Supreme Court of Canada in *Nielsen v. Kamloops (City)*[118] and most recently in the case of *Cooper v. Hobart*.[119] The two prong tests are:

1) is there a sufficiently close relationship between the parties (the [defendant] and the person who has suffered the damage) so that, in the reasonable contemplation of the [defendant], carelessness on its part might cause damage to that person? If so,
2) are there any considerations which ought to negate or limit (a) the scope of the duty and (b) the class of the persons to whom it is owed or (c) the damage to which a breach of it may give rise to?

(i) Relationship Between the Parties

The first part of the test examines the relationship between the plaintiff and the defendant so as to justify the recognition of a *prima facie* duty of care and, consequently, the imposition of liability on the defendant for the damages caused to the plaintiff. According to the Supreme Court of Canada in *Cooper v. Hobart*,[120]

> Defining the relationship may involve looking at expectations, representations, reliance, and the property or other interests involved. Essentially, these are factors that allow us to evaluate the closeness of the relationship between the plaintiff and the defendant and to determine whether it is just and fair having regard to that relationship to impose a duty of care in law upon the defendant.

This aspect of the test is very important, as it also attempts to address the problem associated with indeterminate liability or situations where legal responsibility is extended to strangers. Although in tort law, the factors that may satisfy the require-

---

116 *Donoghue*, *supra* note 63 at 580.

117 *Anns v. Merton London Borough Council* (1977), [1978] A.C. 728 (U.K. H.L.).

118 *Nielsen v. Kamloops (City)*, [1984] 2 S.C.R. 2 (S.C.C.) [*Kamloops*].

119 *Cooper v. Hobart*, [2001] 3 S.C.R. 537 (S.C.C.).

120 *Ibid.* at para. 34.

ment of proximity are diverse and depend on the circumstances of each case, such proximity need not be confined to mere physical proximity. On the contrary, it "extends to such close and direct relations that the act complained of directly affects a person whom the person alleged to be bound to take care would know would be directly affected by his careless act."[121]

In cases of data security breaches, there is sufficiently close relationship between the plaintiff (the victim) and the defendant (data possessor). This relationship arises when the data possessor comes into possession of the plaintiff's personal information, which must have been requested for and/or obtained in the usual course of a business transaction between the parties.[122] It is this close relationship between the parties that results in the defendant's creation of a database that contains, among others, the plaintiff's personal information.

(ii) Considerations to Negate or Limit

The second aspect of the test deals with considerations which might negate or limit the scope of the duty, the class of persons to whom it is owed, or the damage to which the breach may give rise to. Such considerations may include, among others, the availability of contract terms or insurance to cover the claim. One of the policy reasons for denial of recovery for pure economic loss is the need to preserve the boundary line between contract and tort, which will be discussed later. Implicitly, the courts may insist that out-of-pocket expenditures, incurred as a result of a data security breach, are only recoverable under a contract and not in tort. Such reasoning will require individuals to negotiate the level of data security and liability

---

121 *Donoghue*, *supra* note 63 at 580-81. See also La Forest J in *Hercules Managements Ltd. v. Ernst&Young*, [1997] 2 S.C.R. 165 (S.C.C.), at para. 24; Wherein he said "[t]he label 'proximity', as it was used by Lord Wilberforce in *Anns*, was clearly intended to connote that the circumstances of the relationship inhering between the plaintiff and the defendant are of such a nature that the defendant may be said to be under an obligation to be mindful of the plaintiff's legitimate interests in conducting his or her affairs."

122 This argument may be somewhat different where the defendant is a data broker who trades on the personal information even without any business transaction or relationship with the data breach victim. Although the relationship, in this case, might not be as close as the one analyzed above, there still exists sufficient proximity to justify the imposition of a *prima facie* duty of care on the defendant. Proximity in this case will arise (even in the absence of direct relationship between the parties) where the defendant in the course of his transaction reasonably foresees that negligence on his part might result in damage to the plaintiff. See *Canadian National Railway Co. v. Norsk Pacific Steamship Co.*, [1992] 1 S.C.R. 1021 at 1114-1115 (S.C.C.); reconsideration refused (July 23, 1992), Doc. 21838 (S.C.C.) [*Norsk*]. See also *Deane J. in Sutherland Shire Council v. Heyman* (1985), 60 A.L.R. 1 at 55-56 (Australia, H.C.). Hence, in this exceptional situation where the defendant profits at the risks of exposing the plaintiff's personal information to unscrupulous third parties, it will not be in the interest of public policy to exonerate the defendant data broker from liability for his data spill. In fact, public interest is best served by holding him accountable.

for the breach of personal information when entering into contracts, with companies or organizations, which warrant the transfer of their personal information. On the other hand, it will also imply that the companies could include, in such contracts, terms that absolve them of any liability for security breaches.

Considering the unequal bargaining power between the two parties, we will witness a proliferation of contractual terms phrased more in favour of absolving companies of their liability for security breaches than those in favour of individual customers.[123] This will be contrary to public policy. In view of this, some legal jurisdictions have passed data security breaches laws, which contain, among others, provisions outlining that a waiver of the rights granted to the data possessor is contrary to public policy.[124] From the analysis so far, it is safe to conclude that the availability of contract terms, through which the parties may be able to allocate liabilities in the event of data breaches, does not justify the negation or limitation of the liability of a data possessor for his negligence, which results in a data spill. But, what about insurance policies?

Typically non-existent or unknown a few years ago, identity theft insurance has become a common product in the insurance market. The policy is designed to cover out-of-pocket expenses associated with reclaiming identity in the event of identity theft.[125] Should the availability and affordability of the policy serve as a factor to negate or limit liability under the *Anns* test? The answer to this question will require important policy considerations. First, it should be noted that identity theft insurance is offered by the same organizations (or their subsidiaries) that have become notorious for negligently mishandling their customers' personal information.[126] Conspiracy theorists will be quick to conceive the policy as nothing more than a ploy, by these organizations, to shift the burden of their prospective negligence to their customers.

Although identity theft insurance policies have the tendency of providing individuals with "peace of mind," their proliferation will result in a diminished sense of responsibility and security on the part of both individuals as well as data posses-

123 Most companies, in this regard, will often employ standard form contracts, which they unilaterally draft. The data subject usually has no opportunity to make any input or negotiate any term.

124 See U.S. S.B. 6191, *An Act Relating to Identity Theft Protection*, 2005 General Assembly, Reg. Sess., R.I., 2005, 2. 11-49.29.

125 The cost of this policy could range from $20 to $100 a year. See Herb Weisbaum, "Why ID Theft Insurance Might Not Be Worth It" *msnbc*, online: msnbc <http://www.msnbc.msn.com/id/12692565/>.

126 Such organizations include banks and credit card companies. See About.com, "Should You Buy Identity Theft Insurance or Credit Monitoring Services? Necessary Coverage or False Sense of Security?" online: About.com Financial Planning <http://financialplan.about.com/od/insurance/a/IDTheftInsure.htm>.

sors.[127] This will have the tendency to provide a virile atmosphere for data theft to thrive in. Rather than an aftermath compensation that has the tendency to nourish the crime of data theft, a proactive measure that will compel data possessors to take adequate measures to forestall data breaches is vital. If data possessors are held liable for out-of-pocket expenses incurred by data breach victims, the number of which may run into tens or hundreds of thousands, data possessors will be more responsible in their handling of clients' personal information. On the other hand, if they know that their negligent acts will be covered by some insurance policy, the cost of which has already been borne by the victims, or prospective victims, the opposite will be the case.

The current boom in identity theft insurance policies, prompted out of a desire to buy peace of mind, ought not to serve as a consideration to negate or limit the scope of the duty of data possessors or their liability for out-of-pocket expenditures incurred by the victim as a result of the breach. If the availability of such insurance policies is to serve as a mitigating factor, then the cost for the provision of the policies should be imposed on, or borne by the data possessors.

The economic loss rule is a common law rule that effectively states that a plaintiff in an action for negligence may recover damages for pure economic loss only when there is an accompanying damage to his person or property. Hence, in cases where the negligent act of the defendant results only in pure economic loss without more, the court has often denied recovery.[128] Pure economic loss differs from consequential economic loss; whereas consequential economic loss is a financial loss connected to physical damage to the plaintiff's person or property, pure economic loss is a financial loss suffered by the plaintiff without any physical injury to his person or property.[129]

The economic loss rule seems to have been founded on public policy considerations. Johnson has identified three policy reasons behind the rule.[130] The first is the avoidance of too broad a scope of liability or unlimited liability. Some negligent conduct could have broad economic implications. For example, the negligent act of a drunk driver, who causes an auto accident on a busy highway, could have a broad economic impact on a large number of people, including the careful driver whose car was directly impacted, other drivers who may have to take another (longer) route due to traffic diversion, and the fish monger in the nearby city who

---

127 See Laura Bruce, "Is Identity Theft Protection Worth the Money?" *Bankrate.com*, online: Bankrate.com <http://www.bankrate.com/brm/news/advice/scams/20040804a2.asp>.

128 Ann O'Brien, "Limited Recovery Rule as a Dam: Preventing a Flood of Litigation for Negligent Infliction of Pure Economic Loss" (1989) 31 Ariz. L. Rev. 959.

129 See Linden, *supra* note 107 at 441.

130 Vincent R. Johnson, "Cybersecurity, Identity Theft, and the Limits of Tort Liability" (19 August 2005) bepress Legal Series, Working Paper 713 at 45, online: bepress Legal Repository <http://law.bepress.com/cgi/viewcontent.cgi?article=3530&context=expresso>.

relies on the free-flow of traffic on this road for the timely delivery of his merchandise. It will not be sensible to hold the negligent driver liable for all the economic loss incurred by persons held-up in traffic as a result of the auto accident, neither will it be sensible to hold him liable for loss of profit incurred by some unknown fish monger whose delivery was delayed as a result of the auto crash. The economic loss rule serves to protect prospective defendants from indeterminate liability, or too wide a scope of liability, by curbing the proliferation of litigation arising from negligently inflicted pure economic loss.

The second reason identified behind the economic loss rule is the fact that lost opportunities are not often readily susceptible to precise calculation. Recovery of damages in law (where a cause of action has been established) generally requires proof of damages with a reasonable degree of certainty. The economic loss rule, therefore, endeavours to ensure that compensation is not awarded for amounts that are purely speculative or uncertain. Third and most important, is the rule that marks the boundary between contract law and tort law. This demarcation is important because, without it, contract law stands the risk of "drown[ing] in a sea of tort".[131] The need for this demarcation was upheld by the Supreme Court of Canada in *Martel Building Ltd. v. R.*,[132] where the Court refused to allow recovery of damages for pure economic loss arising from a breach of duty of care in the course of contractual negotiation.

Although the common law usually refuses recovery for economic loss unaccompanied by any consequential loss, the Supreme Court of Canada, based on the works of Bruce Feldthusen,[133] now recognizes five categories of compensational pure economic loss.[134] However, this does not imply that the categories of recoverable economic loss are now closed.[135] Nevertheless, before a new category can be created or recognized, the court will most likely embark on an extensive analysis of the policy considerations to satisfy itself of the necessity for such extension.[136] Taking account of these policy considerations, it is necessary to examine whether a new category should be added to the existing five recognized categories so as to allow for recovery of economic loss damages arising from data security breaches.

---

131 See Hood J. in *Sable Offshore Energy Inc. v. Ameron International Corp.*, 2006 NSSC 332 (N.S. S.C.); affirmed (2007), 2007 CarswellNS 257 (N.S. C.A.); leave to appeal refused (2008), 2008 CarswellNS 13 (S.C.C.) citing Blackmun J. in *East River S.S. Corp. v. Transamerica Delavel Inc.*, 476 U.S. 858 (U.S. Sup., Ct.), at 866 (1986).

132 *Martel Building Ltd. v. R.* (2000), [2002] 2 S.C.R. 860 (S.C.C.) [*Martel Building*].

133 Bruce Feldthusen, *Economic Negligence: the Recovery of Pure Economic Loss*, 2nd ed. (Toronto: Carswell, 1989).

134 See *Norsk*, *supra* note 122.

135 Attempts were made (though without success) to create a new category in *Martel Building*, *supra* note 132 and *Status Electrical Corp. v. University of British Columbia* (2006), 6 C.L.R. (3d) 85 (B.C. S.C.) [RNF].

136 See Harry Street, *The Law of Torts*, 6th ed. (London: Butterworths, 1976) at 108. Citing a Canadian case, *Nova Mink Ltd. v. Trans-Canada Airlines*, [1951] 2 D.L.R. 241 (N.S. C.A.) at 254.

The first step in this direction would require identification and analysis of the type of economic loss that usually results from data security breaches.

(iii) Economic Loss Arising from Data Security Breaches

Unauthorized use of personal information usually results in harm or loss to the victim. Where the harm is in the nature of bad credit reputation, the victim will normally incur out-of-pocket expenses to restore his good credit standing.[137] In some cases, where the data thief has perpetrated a crime in the name of the victim that results in the victim being arrested and wrongly prosecuted for the crime, there may be an additional legal cost incurred by the victim in defending the mistaken prosecution. The second loss likely to arise from unauthorized use of personal information is the personal time spent in trying to restore lost good credit standing. The third is the lost opportunities resulting from bad credit.[138] Admittedly, recovery for such loss is not possible under the existing five categories earlier highlighted. Nevertheless, it has been noted that the category is not closed; this calls for examination of the possibility for the creation of a new category of recoverable economic loss in light of the policy consideration that restricts recoverability for pure economic loss.

The first reason for the restriction of recovery for pure economic loss, as earlier stated, is formulated on the need to avoid too broad a scope of liability or indeterminate liability. Since the number of people likely to be affected by the defendant's act may be too broad, in the absence of this rule, the potential liability would be excessive and uncontrollable. Granted, the nature of data security breaches are such that they may result in a very broad liability and a single breach incident could affect the personal information of tens of thousands or millions of people, thus resulting in myriads of litigation across jurisdictions. However, this is one area where the policy consideration relating to scope of liability should be carefully revisited. It should be the responsibility of the defendant to restrict the scope of his liability by restricting the amount of personal information he accumulates in his database.[139] Where a data possessor profits by keeping a large database, it will not

---

137 This out-of-pocket expense could include the cost of credit monitoring services, closing and re-opening banks and credit accounts, costs of re-issuing credit and debit cards, telephone and postage costs etc.

138 Johnson, *supra* note 130.

139 The Office of the Privacy Commissioner of Canada has acknowledged in its report that "Collecting and retaining excessive personal information creates an unnecessary security burden. Thus, organizations should collect only the minimum amount of information necessary for the stated purposes and retain it only for as long as necessary, while keeping it secure." See Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies Inc./Winners Merchant International L.P." (25 September 2007), online: Privacy Commissioner of Canada <http://www.privcom.gc.ca/cf-dc/2007/TJX_rep_070925_e.asp>.

be in the interest of public policy to shield him from the greater responsibility that comes with such a venture by denying a large number of victims recovery for economic loss inflicted on them by a negligent defendant data possessor. The law relating to the restriction of liability should be confined to cases where the defendant has no reasonable opportunity of limiting the number of prospective plaintiffs, and not to cases that deal with data security breaches where the defendant has such opportunity and, not only fails to utilise it, but even profits financially from not doing so.

The second reason for the policy is the fact that lost opportunities are not often readily susceptible to precise calculation; hence, litigation relating to pure economic loss is usually speculative in nature. It is conceded that some economic loss damages arising from data security breaches are speculative. Speculative damage will, no doubt, include personal time spent in trying to restore good credit ratings and lost opportunities arising from bad credit.[140] If the court were to allow victims of data spills to recover for the time spent in trying to restore their good credit and lost opportunities, this would be the height of compensation for speculative damage. Among the problems that will arise, according to Johnson,[141] will be the problem of how to quantify the economic value of lost time and opportunities:

> If plaintiff's time were compensated at his or her usual hourly rate of earnings in employment or a profession, the awards made to professionals, minimum-wage workers, and unemployed homemakers would vary widely-and perhaps without good reason. Similarly, if every victim were to receive the same amount for the value of lost time, how would that amount be set? Ensuring uniformity with respect to this element of damages is a task better committed to legislatures than to the multitude of fact finders who will preside over numerous tort claims.

The problem with regard to lost opportunity is related to the legal principle that requires that damages must be proved before recovery. How does the plaintiff prove that opportunities were actually lost? Even where the lost opportunity is proved, how do we quantify it in terms of monetary value? For example, if the plaintiff is able to prove that, because of his ruined credit he was unable to obtain a mortgage, what yardstick do we adopt in trying to quantify this lost opportunity? Most assertions in this regard would, at best, be speculative. Hence, it can be rightly asserted that economic loss arising from lost time and opportunity as a result of data security breaches cannot pass the public policy test for recovery. However, this argument may not hold with regard to out-of-pocket expenses incurred to restore a good credit rating. In the case of out-of-pocket expenses, the claims are not speculative. They could be proved with a reasonable degree of certainty; the receipts for the expenses incurred are usually available for inspection. More so, the

---

140 According to a legislative analysis, victims of data security breaches spend an average of 600 hours and over two to four years and about $1,400 to clear their names. See Texas Bill Analysis, 2005 Reg. Sess. Sen. Bill 122, online: Texas Legislature <http://www.legis.state.tx.us/tlodocs/79R/analysis/pdf/SB00122F.pdf>.

141 Johnson, *supra* note 130 at 50.

expenses under this head are strictly in monetary terms, hence, there is no problem (as in the earlier situation) as to how to quantify the loss.

The analysis above has sought to establish that the relationship between the victim of a data breach and the negligent data possessor is such that warrants the extension of the duty of care. Since the breach of this duty naturally results in economic loss, it does not offend any public policy to allow victims of data security breaches to recover economic loss damages in the form of out-of-pocket expenses incurred as a result of data security breaches arising from the defendant's negligence.

III. THE NEED FOR LEGISLATIVE INTERVENTION

Legal remedies for data security breaches present a novel legal problem in information technology law. The main barrier to seeking remedy in the tort of negligence arises from the problems associated with proof of damages, and causation and recovery for economic loss, among others. Notwithstanding its historical efficacy in compensating the injured, the ability of the common law tort of negligence to deal with tech torts gives more room for doubt than certainty. Chandler has observed that,

> Tort law has been used in the past to cause careless actors to bear the cost of their own carelessness in order to encourage a reasonable level of care to be taken. Unfortunately, the court have so far found negligence law to be poorly-equipped to deal with the problem.[142]

The growth in information technology will necessitate that individuals must continue to entrust their personal information to companies, organizations and institutions with the inevitable incidents of data security breaches. Although PIPEDA imposed an obligation on organizations to provide security safeguards for personal information in their custody, the same law falls short of providing adequate legal redress for victims of data security breaches arising from the negligent act of such companies, organizations and institutions. The current position of the Act, to say the least, is not of much assistance to victims of a data security breaches in an action for negligence.[143]

Hence, the lacuna in common law necessitates comprehensive and dynamic legislation to deal with the current difficulties experienced by victims of data security breaches in maintaining actions for negligence. Such legislation should require that, in cases of data security breaches, companies and organizations responsible for the custody of the breached data should bear the responsibility and the cost for

---

142 Chandler, *supra* note 85 at 25.

143 The victim may only file a complaint with the Privacy Commissioner in accordance with s. 11 of the Act and within 45 days after receiving the Commissioner's report, the victim may apply to the court for a hearing in respect of the subject matter of the complaint. See *PIPEDA*, *supra* note 2 at s. 14.

taking preventive measures to protect the victims of the breach from present and future risk of damage resulting from the breach. This includes notifying the victims of the breach and consumer monitoring agencies,[144] providing credit-monitoring services and, if necessary, credit-repair services on behalf of all victims of such a breach.[145] Where it becomes imperative for the victim to take the necessary preventive measure, he should be able to recover costs or expenses from the responsible organization.

This measure, no doubt, will go a long way in addressing the difficulties currently experienced by victims of data security breaches, for which existing law does not provide a remedy. It will also compel data brokers and organizations, dealing with customers' personal information, to take adequate steps to protect confidential data in their custody. Consumers should not have to bargain with companies over their right to have their personal information kept safe. This ought to be considered a necessary part of doing business when a company seeks confidential customer data as part of its business model.[146]

CONCLUSION

In this article, I have examined the need for judicial reform as well as legislative intervention in two areas of data security breaches. The first is the need for the statutory imposition of a duty to notify affected individuals in the event of a data spill. Admittedly, a blanket requirement to that effect may result in over-notification. However, it is suggested that the problem of over-notification could be addressed by requiring security breaches to be communicated to the Office of the Privacy Commissioner, who should immediately assess the incident to determine whether notification ought to be made, and in what form.

Secondly, I have highlighted the inadequacies or difficulties in the applicability of existing common law rules in data security breaches litigation. This problem constitutes to be a major setback to victims of data security breaches who are seeking legal redress. There is, therefore, a need for judicial reform and/or statutory intervention in this area to deal with the uncertainties in the application of common law rules to data security breaches litigation.

Finally, there is an emerging legal issue relating to breach of data security not covered in this research article, which warrants further research. The issue became evident in the litigations that trailed the breach incidents involving TJX Stores.[147]

---

144 This is a legal obligation under the *Hawaiian Security Breach Notification Act* at s. 3(f), online: Hawaiian State Legislature <http://www.capitol.hawaii.gov/session2006/Bills/SB2290_.htm>.

145 Anita Ramasastry "Data Insecurity: What Remedy Should Consumers Have When Companies Do Not Keep Their Data Safe?" *FindLaw* (6 March 2006), online: FindLaw <http://writ.news.findlaw.com/ramasastry/20060306.html>.

146 *Ibid.*

147 In January 2007, TJX Companies, a large retailer that operates over 2,000 retail stores, mainly in the Unites States, Canada and Puerto Rico, reported that it suffered a massive computer breach on a portion of its network that handles credit card, debit card, cheque, and merchandise transactions. The incident resulted in class action lawsuits,

A breach incident may take the form of hacking of a merchant's database, usually resulting in the compromise of credit or debit card information. In addition to the financial loss that may be experienced by financial institutions as a result of fraudulent transactions associated with the breach, they may also incur financial costs in their effort to protect their customers or cardholders. Such efforts could include the cancellation and re-issuing of new cards to affected customers. Could the banks and credit card companies successfully maintain a legal action against the negligent merchant for the purpose of recovering the costs incurred in the cancellation and re-issuing of such cards? Alternatively, will the court accept a defence argument to the effect that the costs were "solely the result of a perceived risk of future harm" as opposed to "present injury or reasonably certain future injury"?[148] This issue was likely to arise for determination in the litigations filed by various banks in the United States against TJX. However, it is becoming evident that the litigations may all end in an out-of-court settlement, thus leaving the issue unresolved.[149]

---

not just by affected customers, but also by banks and credit card companies who incurred costs in cancelling and re-issuing millions of cards to affected customers.

148 *Wells Fargo*, *supra* note 71.

149 See M.H. Bosworth, "TJX Settles With Banks Over Data Breaches" *Consumer Affairs* (20 December 2007), online: Consumer Affairs <http://www.consumeraffairs.com/news04/2007/12/tjx_banks.html>.