Computer "Insecurity" and Viral Attacks:Liability Issues Regarding Unsafe Computer Systems Under Quebec Law[1]

Nicolas VERMEYS

Lex Electronica, vol. 9 n°1, Hiver 2004
http://www.lex-electronica.org/articles/v9-1/vermeys.htm
http://www.lex-electronica.org/articles/v9-1/vermeys.pdf

Introduction

1. Computer viruses which hold the power to bring complete computer systems to a halt are no longer exclusive to the field of science fiction. The SQL Slammer worm, one of the most recent incarnations of this annoying malware, caused private networks across Asia, Europe and the Americas to shut down momentarily, affecting everything from flights to ATMs[2]. What's worse, this incident could have been prevented: "the worm […] attacked via a vulnerability discovered six months ago in SQL Server 2000 software from Microsoft Corp. […] Microsoft has offered a free patch to fix the trouble spot, but not all users of the server software installed the patch"[3].

2. Such negligence, or so it would seem, originating in major corporations, has persuaded many in the legal profession to submit that « [t]here exists a strong need to create liability for companies who do not maintain adequate security on their computer networks »[4], since inadequacy could be prejudicial to third parties[5]. However, before condemning system administrators[6] for not keeping their networks up to security standards, one should stop to think what liability could and should stem from their actions (or lack thereof).

3. Quebec courts have yet to be presented with a case involving computer virus liability, and very few authors have addressed the topic[7]. This being said, although it remains speculative to predict how courts will deal with the issue when it does appear before them, it is possible to draw a general outlook of how the question of viral liability should be addressed in regards to the basic principles of liability under Quebec law by focussing on similar liability issues in this and other jurisdictions when applicable[8].

Part I: Quebec's general liability regime and its relevance in the computer security field

4. Civil liability in Quebec, as in many other jurisdictions, is governed by the general principle that one who causes injury to others by not abiding to the rules of conduct which lie upon him (according to circumstances, usage or law)[9] is at fault and must fully compensate the injured party. This general principle, established by articles 1457 through 1481 of Quebec's Civil Code,[10] applies to all liability issues whether they stem from computer security flaws, faulty merchandise or a fistfight.

5. Article 1457 of Quebec's Civil Code states that:

> *Every person has a duty to abide by the rules of conduct which lie upon him, according to the circumstances, usage or law, so as not to cause injury to another.*
> *Where he is endowed with reason and fails in this duty, he is responsible for any injury he causes to another person by such fault and is liable to reparation for the injury, whether it be bodily, moral or material in nature.*
> *He is also liable, in certain cases, to reparation for injury caused to another by the act or fault of another person or by the act of things in his custody.*

6. In their analysis of this article, courts have established that, in order to prove liability, one must establish three components: fault, damage and a causal link between the two[11].

Fault

7. Fault can be inferred in two different ways. The easiest and most trivial is by establishing that the defendant has committed an act which is contrary to law[12]. The second, which is more complex in its application, is by determining whether the defendant has transgressed the general duty of not causing harm to others[13]. This can be done by examining if a reasonable, prudent and diligent individual would have avoided the reproached act[14]. Since no laws forbid the presence of security flaws, it is in the general duty not to harm others that we can find whether or not having vulnerable security systems can be considered faulty behaviour. This brings forth a first predicament: "[a]t this point, there is no reliable standard of behaviour which can be relied upon in [liability] litigation. Indeed, there is a certain amount of controversy over what the "rational computer programmer" would do under the circumstances"[15].

8. It has been established by the courts that fault can be intentional or stem from negligence, which can be summarized as not taking all normally required precautions not to cause injury to others[16], i.e., not applying due diligence. This being said, "[t]he basic legal principles of negligence law are not altered simply because a computer is the instrumentality being used. Those who use a computer have a duty to do so with care"[17]. Therefore, in order to establish negligence in a digital environment:

> *a potential plaintiff must show that a manager breached his or her duty of reasonable care. A systems manager might be found to have breached a duty of reasonable care for a number of reasons, such as the failure to recognize defects in a system, the failure to correct defects, or the failure to warn of defects. […] Breach of duty might also arise from failure to train and supervise employees, or the failure to use reasonable means to secure the system from unauthorized and unintended use.*[18]

9. It could therefore be argued that a party which has not taken all normally required precautions to protect his system from intrusion is negligent, and consequently at fault. The problem remains: what should be considered "normally required precautions" in the computer security context? Or, as one author puts it:

> *what are the definitive responsibilities of computer center employees or persons having access to software and information to the public they serve […] in creating an 'environment of security' and in practicing solid ethical standards in regard to the valuable data they use when performing their jobs*.[19]

10. A impulsive answer to this question would be to use reasonable means to secure the system from unauthorized and unintended use[20]. Unfortunately, such an answer only brings forth more dilemmas, the very notion of "reasonable means" being an uncertain one. Do reasonable means consist of testing and inspecting a system? If so, how much testing and inspection is enough to guarantee that there can be no finding of negligence[21]. After all, no amount of testing can insure that a system is positively virus-free[22].

11. One way to resolve the issue of quantifying "reasonable means" is to look at what is customary in the industry. If 90% of system administrators use technology A or better, it becomes arguable that the use of technology A is a "reasonable means". Such a measuring stick does, however, have a basic flaw: businesses would not be compelled to develop better security measures; just to stay on par with their competition. Therefore, though industry standards can be helpful in establishing what "reasonable means" consist of, they should not be considered the only available reference:

> *Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission*[23]

12. Following this principle, the Canadian Supreme Court has stated that respecting industry norms cannot guarantee that a particular defendant will not be held liable since these norms are just those created by the industry for the industry[24]. More often than not, the individuals that will be ultimately affected by such norms (consumers for example) do not have a say in their development.

13. It has therefore been recommended by some authors that, when it comes to computer security, the normally required precaution should be to use all reasonably accessible technology that the system administrator knows or should know exists[25]. As for what the expression "reasonably accessible technology" implies, it has been suggested[26] that all technology that is less expensive than the probable damage (estimated damage multiplied by the risk)[27] should be considered to be reasonably accessible.

14. To conclude, a court which is presented with a case concerning computer security liability issues, will most probably address the following questions:

> 1. Is a suitable technology generally available?
>
> 2. If so, is it available at a cost than can reasonably be afforded by the defendant (probably but not necessarily a corporation)?
>
> 3. Does this technology have at least a limited use in the industry for the purpose involved?
>
> 4. Are safety precautions so imperative that this technology must be used to ensure safety?
>
> 5. Was the absence of this technology a direct cause of the injury?[28]

15. A positive answer to these questions would most probably be considered an admission of fault within the meaning of the Civil Code of Quebec. Companies should thus keep these questions in mind when setting up their computer systems.

Damage

16. Damage caused by computer system failure can take many different shapes, most notably the costs associated with "repairing" a system[29], down time[30] and loss of data. This later source of damage may however be somewhat problematic since data, as such, is not a "thing". Data is not tangible, which has caused some American judges to consider that loss of data is not damage since the "thing", i.e. the disk on which the data is stored, is rarely incapacitated by viral attacks[31]. As explained by Clive Gringras:

> *it is initially necessary to establish that altering the orientation of magnetic particles, how programs and data are stored, is damage to property. […] To damage a program or data […] is not to cause any physical damage in the way in which it is normally considered: all that is occurring is that the magnetic particles are being altered*.[32]

17. Since damages are not physical, there is no prejudice. Fortunately, this line of reasoning is no longer being followed by recent American case law[33], and it is doubtful that Quebec courts will take that route, especially since recent legislation, most notably the Act to establish a legal framework for information technology[34], go against this very idea. This being said, Quebec judges will have to address this issue if and when it crosses their docket, and they will be the ones to choose which current they want to follow.

Causal link

18. Fault has to be the direct cause of damage, or damage the immediate effect of fault[35]. Such is the definition of causal link under Quebec law. In many cases, causal link goes without saying: if I shoot you and you are killed by the bullet, it goes without saying that I killed you. But what if two people shoot you almost simultaneously and either hit could have constituted the fatal act[36]? Obviously, one bullet didn't cause any damage since you were already dead when it hit, which would mean that, under civil law, one of the two hitmen did not injure, and, since it is impossible to prove which one, neither should be held liable[37]. The same problem exists in the case of computer system vulnerability. If a system is attacked by two copies of the same virus which were transmitted by two different sources, how can one establish which is liable? In order to solve such dilemmas, the Quebec legislator has come up with the following disposition:

1480. Where several persons have jointly taken part in a wrongful act which has resulted in injury or have committed separate faults each of which may have caused the injury, and where it is impossible to determine, in either case, which of them actually caused it, they are solidarily liable for reparation thereof.

19. This disposition of the Civil Code therefore allows victim to put aside factual causal link and present possible causal link in cases where two parties are at fault, but only one has caused damage.

20. Section 1480 of the Civil Code also covers subsequent faults. For example, if the gun used in the previous example belonged to a third party who left it unattended, he could share liability. Three criteria have been established to address this type of second hand liability issue:

1. The third party action made the prejudice objectively possible;

2. This prejudice was reasonably predictable;

3. The time and place of this third party action was logically situated within the causal chain of events[38].

21. Such a way of addressing third party liability is particularly important in the field of computer security since, more often than not, those who transmit viruses do so unwillingly after they themselves were infected. Therefore:

The manager of a computer system would have a duty to use reasonable care to secure the system when it is reasonably foreseeable that failure to secure it would result in injury to others. While "others" encompasses a potentially unlimited group, there are limits on how far liability would extend. A duty of care runs only to "foreseeable plaintiffs," any person or class of persons who could reasonably be expected to be injured by the systems manager's negligence.[39]

22. But how does one establish who the “foreseeable plaintiffs” are when the computer system in question is connected to the Internet? Is such cases, couldn’t it be alleged that “the controller of an infected system is in a sufficient proximate relationship with the owner of any equipment which becomes infected by the virus emanating from his system”[40]? This would mean that a company’s liability could be practically infinite if it were established that its security flaws were, at some point in time, responsible for transmitting a virus to a third party. Although the third criterion mentioned above – the time and place of this third party action within the causal chain of events – may prevent a potential plaintiff from going back further than necessary in order to find a defendant which he feels contributed to his loss[41], in cases where the company’s fault is easy to establish, this criterion might not be given as much importance by the courts.

23. Therefore, if a company wishes to limit future liability claims, there are certain safety precautions which should be taken. It must be noted that none of these precautions will guarantee success if liability claims are subsequently brought against the company. They will, however, go a long way in helping to prove that the company is reasonable, prudent and diligent in the management of its computer system.

Part II: How businesses can address liability issues associated with computer security

24. As mentioned above, the standard of care adopted by Quebec courts to establish whether or not a defendant is at fault when it comes to liability questions is that of a reasonable, prudent and diligent individual[42]. This implies that, whenever liability has to be addressed, the court must ask itself whether a reasonable, prudent and diligent individual who possesses the same characteristics as the defendant (i.e. has the same career or is in the same general field) put in the same scenario could have avoided the injury. Therefore, the standard of care for information security protection becomes "would a reasonable, prudent and diligent system administrator have repaired these security holes?". If the answer to that question is positive, then liability must be inferred.

25. So how does one qualify as a reasonable, prudent and diligent system administrator? Such a question unfortunately has no clear-cut answer; it will be up to the Courts to respond on a case by case basis. This being said, there are some general provisions which will go a long way in limiting a system administrator's liability:

A. General provisions designed to limit computer security liability

1. Limit your liability contractually

26. The civil code allows parties to contractually limit their liability for any injury other than moral or bodily harm[43]. It is therefore wise for businesses to include clauses limiting their liability in cases of computer security breaches in any and all contractual relationship they enter into. This, however, presents another dilemma related to cyberspace: one may interact with other people's computers in many ways that do not depend on traditional contractual relations. Data, including harmful data such as viruses, passes through various channels from one computer to another. For one example relating to the difficulty of setting up a contractual disclaimer of liability, consider this question: does visiting a website constitute "an agreement of wills by which one or several persons obligate themselves to one or several other persons to perform a prestation"[44]?

27. More and more websites put up disclaimers in order to limit their own liability in case of security breaches or virus infiltration, yet it remains unclear as to what these clauses are worth from a legal perspective[45]. It is indeed established that "[a] person may not by way of a notice exclude or limit his obligation to make reparation in respect of third persons"[46]. It therefore becomes essential to ascertain whether these disclaimers are contracts or mere notices, something the Courts have yet to decide.

28. According to Clive Gringras :

> *It is an obvious and important point that any disclaimer of damage from the site must be shown on the home page and throughout the site. If the disclaimer is buried at the 'back' of web pages there is a risk that the viewer's computer becomes infected before liability is disclaimed*.[47]

29. This is an extremely important point since, even if it were found that visiting a website constitutes an implicit contract[48], the party which brings up the disclaimer must prove that the other party was aware of its presence when the contract was formed[49]. If the disclaimer is

"buried in the back of web pages", it is not part of the initial contract and, therefore, should not bind the web user[50].

30. Whatever the ultimate enforceability of disclaimers, if nothing else they are a good way of warning web users of the dangers associated with visiting a website, which will be taken into account in case of eventual lawsuits[51].

2. Adopt and enforce a well crafted security policy

31. Businesses who do not have adequate computer security policies could be held liable if it were established that a reasonable, prudent and diligent business would have adopted such a policy, and if having a security policy would have prevented the damage, or not having one contributed to the damage. In other words, there is not an absolute duty to have a security policy, regardless of the causative effect.

32. On the other hand, although adopting a security policy and implementing it does not guarantee that a business will not be held liable in case of security breach (the standard of care being that of the reasonable, prudent and diligent business owner or system administrator), a judge will probably be more inclined to rule in favour of a defendant who shows that he takes security issues seriously, and that he has taken precautions. Of course, the extent of the policy and the manner in which it is applied will go a long way in affecting liability one way or the other.

3. Have your system audited

33. As stated earlier, there is no guarantee that any precautions will provide a "safe harbour" against liability, since it is ultimately up to the judge to decide whether or not the defendant was negligent in the maintenance of his computer system. However, since establishing foreseeability is necessary to prove fault[52], one could argue that any system flaws that were not discovered by a professional auditor were not foreseeable. A judge would most probably accept such an argument and refuse to hold the defendant liable for damages caused to third parties by the audited system. However, since the auditor may have been the company's agent at the time of the audit, and since article 1463 of the Civil Code states that a principal is liable for his agent's fault, the company could still be held to compensate possible victims if it can be established that the auditor was at fault. Of course, article 1463 also holds that the company retains its recourse against the auditor if the fault can be attributed to the latter.

34. As for the auditor's liability, it will obviously be determined by his general competence. If he fails to notice a flaw that would have been pointed out by any reasonable and diligent auditor, then his liability will be hard to avoid. Otherwise, it will be difficult to infer liability if the system is subsequently attacked (unless the auditor contractually − but improbably - agrees to take the blame in any and all liability litigation resulting from flaws in the audited system).

4. Keep your systems up to date

35. It would technically be very difficult for someone to argue that an administrator that failed to use known patches or install software to fix known flaws was still being diligent, prudent and reasonable. Liability would therefore probably ensue under article 1457 of the Code (or possibly 1458 if the relationship is contractual). Furthermore, since patches are normally free, one would assume that there is no way to legally justify not using them, if the principles of the Learned Hand formula are taken into account.

36. However, costs are not only monetary. The effect a given patch will have on a system must also be taken into account[53]. This therefore raises a more complex issue in regards to system administrators who do not automatically apply patches, possibly because they do not fully trust that the modifications will be beneficial for their systems and, therefore, their clients[54] or because the given patch, although it might solve one problem, may cause others which, in the eyes of the system administrator, are more dangerous than the first. Liability will thus depend on the information which was available at the time of the breach, which brings us to our final point.

5. Stay well informed

37. Availability of information is key in defining whether or not a misinformed system administrator is being negligent by not staying up to date. If an administrator does not take notice of available and well known information, he is not being diligent and is therefore at fault. However one cannot expect even the most diligent of administrators to have read every study, every white paper and every book ever written about his field[55]. Negligence, or lack thereof, will depend on how well known the information becomes in a given field. If it can be established that the information was almost common knowledge in that field, then the judge will consider that the administrator was negligent in not staying well informed. However, if the information was obscure and relatively new, negligence will be much harder to infer.

38. In other words, "a party that fails to make use of available and accepted technology may find itself held liable on the theory that such a failure breaches the obligation (duty) to exercise reasonable care"[56]. The key word in this statement is "accepted". Unfortunately, Quebec courts have yet to address the issue of "accepted technologies" in regards to computer security and computer viruses.

39. Whenever the law is silent in cases relating to information technology, Quebec lawyers, like their colleagues elsewhere, usually resort to analogies with other legal spheres[57]. Although courts have, at times, been cautious about such comparisons[58], this technique has proven to be very effective.

40. Computer viruses have often been likened to their biological namesakes by both legal scholars and computer experts[59]. Without going into detail, the similarity between computer and biological viruses are numerous[60], which has made a strong case for comparisons in "treatment", whether it be preventive or curative. In keeping with this notion, as explained in Berard-Guillette v. Maheux[61], a doctor cannot be held liable for not proposing treatment which is still in its experimental stages. Roughly translated, the court's opinion reads as follows: "the conduct of the defendant must not be evaluated in regards to what would have been ideal, but rather in comparison to the standard conduct of good doctors for that period in time"[62].

41. Taken back into the computer context, this would mean that system administrators are not required to automatically install all available patches as soon as they become available, or as soon as the system administrator finds out about them. This would go against common sense. They are, however, required to stay well informed of the evolution of available technology and must keep their systems in step with industry standards[63]

42. Of course, the comparison between medical science and computer technology is imperfect since computer technology often evolves at a much faster pace (i.e. patches are developed more rapidly than medicine can be), which means that system administrators must react to new

technologies more quickly than doctors might. Nevertheless, the medical analogy does give us a general idea of how courts will probably evaluate liability in the computer field.

B. Other legal issues to be considered while addressing computer security liability

1. Manufacturers' liability

43. Article 1465 of the Civil Code states that, when equipment is the reason for the system failure, the person who has custody of that equipment is liable for injury resulting from the autonomous act of the thing. The system administrator will therefore be held liable. However, as stated above, liability is always shared between all those whose fault, i.e. whose negligent action, has contributed to the damages for which compensation is being sought. As a result, system operators, and the companies who retain their services, should not be the only ones to bear the weight of liability in case of security flaws; the manufacturers or distributors of the equipment used could also share part of the blame.

44. Article 1469 of the Civil Code explains that "A thing has a safety defect where, having regard to all the circumstances, it does not afford the safety which a person is normally entitled to expect, particularly by reason of a defect in the design or manufacture of the thing, poor preservation or presentation of the thing, or the lack of sufficient indications as to the risks and dangers it involves or as to safety precautions" (emphasis added).

45. This being said, if the security flaw can be attributed to a defect in the design or manufacture of the thing, logic would have it that the manufacturer or the retailer[64] who sold "the thing" should be accountable, which is what article 1473 of the Civil Code foresees:

> *The manufacturer, distributor or supplier of a movable property is not liable to reparation for injury caused by a safety defect in the property if he proves that the victim knew or could have known of the defect, or could have foreseen the injury. Nor is he liable to reparation if he proves that, according to the state of knowledge at the time that he manufactured, distributed or supplied the property, the existence of the defect could not have been known, and that he was not neglectful of his duty to provide information when he became aware of the defect.*

46. A contrario, this implies that if a manufacturer or developer of computer software is aware of defects in his software or patches and does not warn his clients of such defects, he could be held liable "in proportion to the seriousness of his fault"[65] for any breach of security which can be linked to his faulty software. The phrase "in proportion to the seriousness of his fault" is an important one because it reverts to the idea that liability can be shared when an injury has been caused by several persons[66], which will undoubtedly be the case when considering viral attacks.

2. Customer security

47. Up to this point, we have only addressed liability issues concerning third party victims, but companies « also have a duty of care to create reasonable safeguards against unauthorized access to the computing system or to some parts of the computer system because the penchant of hackers to seek unauthorized entry is well known in the computing community »[67]. Such unauthorized entries could compromise the security and integrity of the information found on company servers, which, as a result could affect their customers. To this end Quebec's recent Act to establish a legal framework for information technology[68] has put forth several guidelines:

Section 19 of the Act states that the system operator must ensure that any document's integrity is maintained while housed on his servers;

Section 25 of the Act adds that the person "responsible for access to a technology-based document containing confidential information must take appropriate security measures to protect its confidentiality, such as controlling access to the document by means of a restricted view technique, or any technique that prevents unauthorized persons from accessing such information or from otherwise accessing the document or the components providing access to the document".

48. According to these sections and others[69], a system operator and, therefore, his employer, has the duty to insure a reasonable level of security for his system[70] in order to protect the documents that it houses, all the more when said documents contain personal data. As explained by Cheryl S. Massingale and A. Faye Borthick:

> *if valuable property is left unguarded and exposed to the public view, it may be anticipated that it will be stolen; if the key is left in the lock of a jewelry store over a holiday, it is not at all unlikely that there will be a burglary." […] Similarly, if a computer system is left unprotected, it is likely that information in that system will be stolen, altered, or lost. With the risk of misconduct clearly foreseeable, the manager must use reasonable means to restrict access to the system.[*71]

49. System operators liability concerns are therefore twofold: they have to prevent others from using their systems in order to attack third parties, but they also have to protect the personal information contained within these same systems from hackers, which are all the more reasons to insure that their systems are as secure as they could reasonably be. Hence:

> *The provider's liability will depend upon the scope of the original foreseeable risk that the manager created through lax security practices. "If the intervening cause is one which in ordinary human experience is reasonably to be anticipated, or one which the defendant has reason to anticipate under the particular circumstances, the defendant may be negligent, among other reasons, because of failing to guard against it*[72].

Conclusion

50. Quebec's courts established long ago that individuals and companies alike must take all normally required precautions so that their activities do not cause injury to others[73]. Although cyberspace makes it easier to circumvent this legal principle at times, it does not affect its applicability. As in the "real world", businesses have a duty to ensure that their systems are secure, and that they stay that way, which means keeping informed of technological advances and applying relevant patches to software when necessary.

51. Of course, as in the "real world", businesses should not be held liable for injuries caused by the plaintiff's own negligence. As section 1478, paragraph 2, of the Civil Code states: "the victim is included in the apportionment when the injury is partly the effect of his own fault". Furthermore, article 1479 of the Code adds that "a person who is liable to reparation for an injury is not liable in respect of any aggravation of the injury that the victim could have avoided". Hence, if a plaintiff whose computer becomes infected attempts to continue working with it nonetheless, he would most probably aggravate his injury[74], and could not sue for damages subsequent to the discovery of the virus.

Notes

[1] The following paper stems from a June 2003 study conducted by the author, under the tutelage of Professor Karim Benykhlef and the Centre de recherché en droit public, for the Japanese Ministry of Economy, Trade and Industry (METI). The author would like to thank Professor Karim Benyekhlef and Mr. John Gregory for their help and counsel in the writing of this article.

[2] REUTERS, "Computer worm grounds flights, blocks ATMs", (2003) online at: <http://edition.cnn.com/2003/TECH/internet/01/25/internet.attack/>.

[3]Id. A more recent example would be that of the Blaster Worm attack of August 2003. The worm, also known as W32 Blaster, MSBlaster or LoveSan, "quickly spread around the world, taking advantage of a security hole discovered last month in Microsoft Corp.'s Windows 2000, Windows XP, Windows NT and Windows Server 2003 operating systems". REUTERS, "Internet worm confounds home users", (2003) online at: <http://edition.cnn.com/2003/TECH/internet/08/14/blaster.worm.reut/index.html>. The patch which could have prevented the attack has been available on the Microsoft website since mid July.

[4] Sarah FAULKNER, "Invasion of the Information Snatchers: Creating Liability for Corporations with Vulnerable Computer Networks", (2000) 18 J Marshall J. Computer and Info. L., 1019, 1028.

[5] Id., 1028.

[6] It must be noted that this paper makes no distinction between system administrator liability and the liability of the company that employs the system administrator since, under section 1463 of the Civil Code, "The principal is liable to reparation for injury caused by the fault of his agents and servants in the performance of their duties".

[7] The only complete analysis of computer virus liability under Quebec Law can be found in the following study: Nicolas W. VERMEYS, La responsabilité civile des intermédiaires ayant participé à la transmission de virus informatiques sur Internet, Master's thesis, Université de Montréal, 2003, 171 pp. The present article does not discuss the liability of the original creator of the virus or worm or the persons who intentionally distributed it. The author assumes that such persons would in most cases be liable for the harm caused but probably neither discoverable nor solvent.

[8] It must be mentioned that, since Quebec case law regarding information technology is slow in developing - Quebec's smaller population giving rise to fewer cases than in the U.S. or France - Quebec courts and lawyers regularly look to sources within and outside the civil law to evaluate what conduct might be considered faulty within the meaning of the Code. In keeping with this notion, all references made to the Common Law within the following pages regard principles which are either shared by both legal traditions or produce similar results under civil and common law.

[9] Article 1457 of the Civil Code (S.Q. 1991, c. 64.).

[10] S.Q. 1991, c. 64.

[11] Jean-Louis BAUDOUIN and Patrice DESLAURIERS, La responsabilité civile, 5e éd., Cowansville, Éditions Yvon Blais, 1998, at pp. 56 and 57.

[12]Ibid., at p. 105.

[13]Ibid., at p. 97.

[14]Ibid., at p. 112.

[15] Anne W. BRANSCOMB, "Rogue Computer Programs And Computer Rogues: Tailoring the Punishment to Fit the Crime" (1990) 16 Rutgers Computer & Tech. L.J. 1 at 81.

[16] See Hubert REID, Dictionnaire de droit québécois et canadien, Montréal, Wilson & Lafleur, 1994, at p. 386.

[17] Michael D. SCOTT, Computer Law, New York, Wiley, 1985, p. 7-14.

[18]Cheryl S. MASSINGALE and A. FAYE BORTHICK, « Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services », (1990) 12 W. New Eng. L. Rev. 167, 178.

[19] Karen A. FORCHT, « Ethical Use of Computers », in L.J. HOFFMAN (ed.), Rogue Programs: Viruses, Worms, and Trojan Horses, New York, Van Nostrand Reinhold, 1990, p. 117, at p. 117.

[20]Cheryl S. MASSINGALE and A. FAYE BORTHICK , supra note 18 at 178.

[21] Vicky H. ROBBINS, "Vendor Liability for Computer Viruses and Undisclosed Disabling Devices in Software", (1993) 10 Computer Lawyer 20, 26.

[22]Ibid.

[23]T.J. Hopper c. Northern Barge, 60 F. 2d 737 (2nd Cir. C.A., 1932).

[24] See Roberge v. Bolduc, [1991] 1 S.C.R. 374, at page 437, where Justice L'Heureux-Dubé states that: "It may very well be that the professional practice reflects prudent and diligent conduct. One would hope that if a certain practice has developed amongst professionals in regard to a particular professional act, such practice is in accordance with a prudent course of action. The fact that a professional has followed the practice of his or her peers may be strong evidence of reasonable and diligent conduct, but it is not determinative. If the practice is not in accordance with the general standards of liability, i.e., that one must act in a reasonable manner, then the professional who adheres to such a practice can be found liable, depending on the facts of each case" (emphasis was present in the original text).

[25] See Brian R. BAWDEN, "The Ten Commandments of Computerization," CA Magazine, August 1993, pp. 32-38.

[26] See United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947). Canadian courts and authors have used the Learned Hand formula on multiple occasions. See Allen M. LINDEN and Lewis N. KLAR, Canadian Tort Law: Cases, Notes & Materials, 11e ed., Toronto, Butterworths, 1999, p. 166. Also see Ejan MACKAAY, L'analyse économique du droit, tome 2, not yet published, p. 10.

[27] This, of course, refers to the famed Learned Hand doctrine set forth by the Second Circuit Court Judge for whom it was named. See United States v. Carroll Towing Co., supra, note 26. For example, if damages of $100 occur nine out of ten times, than it would be negligent to not adopt security measures that cost less than $90. Courts could not, however, expect someone to invest $500 in these cases because a reasonable person would never do such a thing.

[28] John Jay FOSSETT, "The Development of Negligence in Computer Law", (1987) 14 N. Ky. L. Rev. 289, at p. 302.

[29] Sascha SEGAN, "Killer Apps" (2002) 13 Smart Computing 54, 55.

[30] Clive GRINGRAS, The Laws of the Internet, London, Butterworths, 1997, at p. 66.

[31] See Robbin A. BROOKS, "Deterring the Spread of Viruses Online : Can Tort Law Tighten the 'Net'?", (1998) 17 Rev. Litig. 343, at. p. 357. It must be mentioned that the Canadian Supreme Court has also ruled that information is not a "thing" (see R. v. Stewart, [1988] 1 S.C.R. 963). However, this case, which only dealt with criminal law, goes on to establish that one cannot infer that the word "thing" has the same meaning in civil or criminal cases.

[32] Clive GRINGRAS, supra, note 30, at pp. 66 and 67.

[33] See, among others, CompuServe Inc. v. Cyber Promotions, Inc., 1997 WL 109303 (S.D. Ohio Feb. 3, 1997), Thrifty Tel, Inc. v. Bezeneck, 46 Cal. App. 4th 1559 (1996) and American Guarantee & Liability

Insurance Co. v. Ingram Micro Inc., No. Civ. 99-185 TUC ACM, 2000 U.S. Dist. Lexis 7299 (D. Ariz. April 19, 2000) (this decision is being appealed).

[34] R.S.Q. 2001, c. C-1.1. The Act goes as far as to state that computerized documents hold the same legal value as their paper counterparts.

[35]Jean-Louis BAUDOUIN and Patrice DESLAURIERS, supra, note 11, at p. 57.

[36] See Labelle v. Charette, [1960] Q.B. 770.

[37]Jean-Louis BAUDOUIN and Patrice DESLAURIERS, supra, note 11, at p. 348.

[38]Ibid, at pp. 354 and 358. Also see Deguire Avenue Ltd. v. Adler, [1963] B.R. 101.

[39]Cheryl S. MASSINGALE et A. FAYE BORTHICK, supra, note 18, 177. However, as mentioned by Christopher J. McGuire, « that question becomes irrelevant in cyberspace because the cost of taking adequate precautions may be roughly the same no matter how the orbit of danger is defined. If a company's computer is reasonably secure against being used as a slave in an attack on one other computer, the marginal cost of protecting it from attacking another 100 million computers is essentially zero. This is because once the machine is reasonably secure, it is secure as to all other machines, not just an isolated one or two ». Christopher J. McGUIRE, « Old Torts Never Die − They Just Adapt to the Internet », (2000) 23 Nat'l L.J. B15.

[40] Clive GRINGRAS, supra, note 30, at pp. 60 and 61.

[41] This will mostly happen if the subsequent parties in the chain of events are insolvent.

[42] See, for example, Ouellet v. Cloutier, [1947] S.C.R. 521.

[43] Section 1474 C.c.Q.

[44] This is the definition of a contract under article 1378 of the Civil Code. A "prestation" is, roughly, the furnishing of goods or services to someone.

[45] Rob GALLAGHER, "Victim or Villain? Viral Liability: Guard against viruses or face legal action", (2001) online at: <http://www.fabit.com/antivirus/businesliab.asp>. Some U.S. cases have upheld terms of use posted on websites, but generally only to block impermissible transfers of data, and not yet to prevent liability for viruses. See a survey of such cases in E.Ziff et al, "[formal title TBA]", forthcoming, 58 Business Lawyer, November 2003. A recent Quebec case in the same vein is Canadian Real Estate Assoc. v. Sutton (Québec) Real Estate Services Inc., (2003) CS 500-05-074815-026

[46]< Section 1476 C.c.Q. Also see Jacques PERREAULT, Des stipulations de non-responsabilité, Montréal, Imprimerie modèle limitée, 1939, p. 149 ; Benoît MOORE, « À la recherche d'une règle générale régissant les clauses abusives en droit québécois », (1994) 28 R.J.T. 177, 211 ; and Garage Touchette Limitée c. Metropole Parking inc., [1963] C.S. 231.

[47] Clive GRINGRAS, supra, note 30, at p. 63.

[48] Pierre TRUDEL et al., Droit du Cyberespace, Montréal, Thémis, 1997, p. 5-63.

[49] Jean-Louis BAUDOUIN, Les Obligations, 4th ed., Cowansville, Yvon Blais, 1993, p. 460

[50] Ibid, p. 459.

[51] Section 1476 in fine C.c.Q. states that "a notice may […] constitute a warning of danger". According to Jean-Louis BAUDOUIN and Patrice DESLAURIERS (supra, note 11, at p. 783), this type of warning has a "partial judicial effect": If it can be established that a third party has taken notice of the disclaimer, his decision to visit the site nonetheless could be interpreted as his accepting the risks associated with the visit. Although this does not imply that the victim forsakes his right to sue for damages (see section 1477

of the Code), it does suggest that he wasn't prudent, which contributed to his own injury (see section 1478 in fine of the Code). The victim will therefore share liability with the website owner.

[52] See Jean-Louis BAUDOUIN and Patrice DESLAURIERS, supra, note 11, at pp. 112 and 113.

[53] For example, the facts that the patch may slow the system down or interfere with other software are also considered costs from an economic perspective.

[54] See Richard FORNO, "Overcoming "Security By Good Intentions", (2003) online at: <http://www.theregister.com/content/55/31094.html>.

[55] See Jean-Louis BAUDOUIN and Patrice DESLAURIERS, supra, note 11, at p. 112.

[56] Monique C. M. LEAHY, "Liability for Mishandled Computer Information", (2001) 49 Am. Jur. Trials 281, § 6.

[57] "[G]iven a new situation, the typical legal response is always to find an analogy to a situation the law has already treated", Sunny HANDA et al., Cyber Law, Toronto, Stoddart, 1997, at p. 204.

[58] See Apple Computer, Inc. v. Mackintosh Computers Ltd., (1987) 18 C.P.R. (3d) 129.

[59] See, among others, Philip FITES et al., The Computer Virus Crisis, 2e éd., New York, Van Nostrand Reinhold, 1992, at p. 28; Susan C. LYMAN, "Civil Remedies for the Victims of Computer Viruses", (1992) 11 Computer/Law Journal, at p. 626; ANONYMOUS, Maximum Security, 3e éd., Indianapolis, Sams, 2001, at p. 326 and W.H. MURRAY, "The Application of Epidemiology to Computer Viruses", in HIGHLAND, H.J. (ed.), Computer Virus Handbook, Oxford, Elsevier Advanced Technology, 1990, at p. 17.

[60]< See Ralf BURGER, Virus : La maladie des ordinateurs, Paris, Micro Application, 1989, at p. 18.

[61] [1989] R.J.Q. 1758 (C.A.).

[62] See page 1761 of the judgment. For more information on this issue, see Pauline LESAGE-JARJOURA and Suzanne PHILIPS-NOOTENS, Éléments de responsabilité civile médicale, Montréal, Éditions Yvon Blais, 2001, at pp. 250 and ss.

[63] However, as stated above, following industry standards does not necessarily mean that liability will not be inferred if it can be established that the industry as a whole has been lagging in the adoption new security measures. See T.J. Hopper v. Northern Barge, supra, note 23. For a Canadian example, see Roberge v. Bolduc, supra, note 24.

[64] Under Quebec law, retailers have the same obligations as manufacturers when it come to the defective products they sell. See sections 1468 and 1473 of the Civil Code.

[65] Section 1478 of the C.c.Q.

[66]Ibid.

[67] Pamela SAMUELSON, "Can Hackers Be Sued for Damages Caused by Computer Viruses?", in DENNING, P.J. (ed.), Computers Under Attack: Intruders, Worms, and Viruses, New York, ACM Press, 1990, p. 472, at p.475.

[68]Supra, note 34.

[69]Sections 22, 26, 36 and 37 of the Act are those most currently referred to when dealing with liability online. Although they were designed to address service provider liability, their definitions are broad enough to be able to include many other intermediaries.

[70]Cheryl S. MASSINGALE et A. FAYE BORTHICK, supra, note 18, 173.

[71]Ibid, 181.

[72]Ibid, 181.

[73] Hubert REID, supra, note 16, p. 386. See also L'oeuvre de terrains de jeux de Québec v. Cannon, (1940) 69 B.R. 112 (at pp. 114 and 118).

[74] Clive GRINGRAS, supra, note 30, p. 69.