1-1-2004

Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections

Richard Owens

Recommended Citation

Turning Worms: Some Thoughts on Liabilities for Spreading Computer Infections

Richard C. Owens†

A Time of Plague

The Internet teems with malevolent computer code created with malice, from boredom or callous greed. Often classed with other invasive software as "malware", it comprises viruses, worms, Trojan horses, spyware, and the like.[1] It is a rare computer that has not suffered in one of the many recent epidemics — Win32, the sobig virus, the Slammer worm, beagle, and so on.[2] An infection gives rise, potentially, to many symptoms. One's computer and address book may be used as a junk electronic mail relay,[3] or as a spam generator in a denial of service attack.[4] Perhaps computer operations will stop so a message will appear on the screen; perhaps all the data and programmes in the computer hard drives will be deleted. Serious damages often ensue. Faced perhaps with the remains of a trashed hard drive, a user might, then, overlook the fact that he or she has also been an unwitting agent of the spread of a worm, which has hijacked his or her computer and address book to fulfil its vermian destiny, visiting havoc on his or her fellows.

In such circumstances, it would be cruel indeed not only to find a hard drive trashed, but to be sued for damages arising from an unknowing role in the spread of a worm, to boot. Could it happen? The extent of liability for an inadvertent role in turning a worm is difficult to gauge. But the consequences of infections are so serious and so widespread that it is only a matter of time before this, and a plethora of other legal questions arising from the proliferation of worms and viruses, come before the courts.[5]

Two aspects of the virus/worm liability problem are of particular note. The first is how tightly the Internet binds together many possible defendants; those who build and run it, those who populate it with increasingly complex electronic commerce Web sites, those who provide terminal software, those who send electronic mails, those who design its security algorithms, those who insure it, and those who hack it, amongst others.

The second aspect is how speculative such a review is. Little case law pertains. Even the language of the law (what does it really mean when we assess liability on the basis of a "trespass" in cyberspace?) sometimes obscures analysis.

This article, then, is a brief speculation on liabilities in Canada for the spread of viruses and worms.[6]

A Steady Diet of Worms

As we are reminded in Shakespeare's Hamlet, "your worm is your only emperor for diet",[7] meaning that the worm feasts equally on the low and the mighty. As we look at the mounting financial carnage from computer worms, their omnivorousness is apparent.

Damages arising from viruses and worms are universally estimated to be enormous. The SQL Slammer worm is said to have caused over US$1 billion in damage worldwide in 2002.[8] In 2001, the costs of the Code Red worm and Code Red II virus were estimated at more than US$2 billion. A recent study suggests that damage from worms and viruses in the United States in 2003 exceeded US$55 billion. In 2001, a PriceWaterhouseCoopers study estimated the annual global costs of malicious computer use at US$1.6 trillion.[9] Such figures are inherently unreliable, but certainly indicative of the order of magnitude of such harm. Recently, the Symantec Internet Security Threat report stated:

> In August 2003, the Win32.Blaster blended threat rapidly spread worldwide, and several other highly severe worms followed. In only eight days the pace and frequency of these threats created havoc for systems administrators as well as for PC home users, with an estimated cost of damages running up to $2 billion … some corporations were prepared and not affected by these threats while others were unprepared.[10]

The scope of the problem, and in particular, the scale of damages in notable cases, can be hard to calculate; worm attacks often go unreported because many corporate victims do not want the existence of security weaknesses known.[11] According to one U.K. security researcher, viruses and worms targeting Microsoft systems cost users $64.5 billion in productivity loss, hard-

ware and software upgrades and data recovery in the third quarter of 2003 alone.[12]

Far more such damage will certainly arise. It once was difficult to create a virus or a worm, and it once required a significant effort to spread it to other computers. Today, software applications that any user can use to create worms can be readily downloaded from the Internet. These applications are easy to find and to use, and since a worm is self-propagating, the resulting creations are easily spread. In fact, in 2001, worms became the most widespread computer infections, surpassing macro and boot viruses.[13]

Even the FBI has, apparently, risked incurring liability for spreading viruses. In its magic lantern scheme, the FBI itself planned to distribute a virus-like computer programme. This programme would have installed itself on the computers of certain Internet subscribers targeted for surveillance. It would have recorded, and reported to the FBI, the click streams[14] of the computer users, circumventing privacy enhancing technologies on the computer. (These might include, for instance, encryption of electronic mail.) Since the complete click stream could be caught, it would have also provided access to a great deal of other data entered into the computer. To distribute this programme required the co-operation of Internet Service Providers ("ISP") and anti-virus software makers, which in both cases was generally withheld, apparently because of their concern for ill effects on the computer systems of their customers, and the attendant liabilities of those effects. The reputational effects of being party to such an invasion of privacy could not have eluded them either.

Taxonomy of Pests

Viruses and worms are computer programmes designed to propagate and to perform certain behaviours that are damaging to, and out of the control of the owner/operator of the computer that animates them. A virus spreads itself by infecting — travelling on the back of — a certain computer file or files, often a .exe file. A standard virus only spreads when an infected file is transferred from one computer to another, and opened. A worm, on the other hand, does not infect a specific file, and it sends itself from one computer to another without needing to ride in a particular file.[15] The biological metaphors "virus" and "worm" are apposite; given in particular a true virus's ambiguous status as an independent life form, it is unable to propagate without a cellular host. Worms are clearly parasitic, but autonomous.

Computer worms fall broadly into two categories, differing in the way that they spread from one computer to another. A co-dependent (or mass-mailer) worm enters a computer by hiding in an e-mail attachment. Once the user opens the infected e-mail attachment, the worm infects the computer, and then e-mails itself to everyone in the computer's e-mail address book. A network-aware (or loner) worm spreads itself from one com-

puter to another by entering security holes.[16] This loner worm bypasses the user and infects his or her computer. From there, the worm scans the Internet for other computers that also have a security hole through which it can enter, and then infects those computers.[17]

An example of a loner worm is the SQL Slammer worm. The Slammer worm took advantage of a flaw in Microsoft's SQL Server software and used it as a means to enter computers, copy itself, and spread to other computers.[18] The SQL Slammer worm infected over 120,000 computers throughout the world in January 2003,[19] interfering with bank machines, ISP operations, telecommunications, and many corporate networks.[20] A patch was issued by Microsoft six months prior to the spread of the SQL Slammer worm to fix the security hole that the worm used to spread itself, yet many companies did not apply the patches to their IT networks.[21]

In most respects, the rules for determining liability relating to damage for a virus will be like those for a worm. But viruses, and some worms, are activated when an attachment to electronic mail is opened. This adds an element of volition to their spread or, at least, a clear chance to avoid harm, which could be significant for a determination of liability. In virtually all cases of infection, a user could be alerted to the activity of the worm or virus, regardless of whether he or she took a deliberate step to bring it to life. Depending on the nature of the infection and the configuration and use of the software, signs of unusual activity in the user's computer might be evident. For instance, if a central processing unit capacity monitor (an integral part of Microsoft Windows) were open and running, unusual activity not accounted for by the user's behaviour would be indicated. Slow response times could be another tip-off. Ignoring such signs might be described as reckless of the risk one's infected computer posed or, indeed, negligent.

The vigilance of network administrators and software vendors means that various notices often attend, or precede, the arrival of a worm or virus. By creating an opportunity to avoid harm, they can be expected to increase the risk of liability for those whose failure to heed them results in damages. There are perhaps, broadly speaking, two sorts of such warnings, and they are not always as clear or as prompt as they might be. In the first, a software maker, alerted by normal maintenance activity or by an alert user, detects a flaw in the software's security structure. A warning is provided and a patch prepared. Such warnings might be sent by electronic mail to systems administrators, and would in any event be posted on a Web site. But such alerts are issued frequently. Which ones merit quick action? How often ought a responsible user visit the Web site to search for such warnings? The second type of warning is that a particular worm or virus is on the move. This warning typically arrives in one's mailbox sometime after the worm itself, presumably attenuating the warning's legal effect.

Even if a warning were received, however, there might be reason not to heed it. For reasons discussed below, a user might reasonably consider whether the risk of installing the software patch proffered as a solution to the identified security risk is itself a greater risk than the uncertain threat of an infection.

Digital Hygiene

Patches

Operating systems, browsers, and other software can provide an unwitting welcome to a virus or worm. Indeed, the intervals grow ever shorter between the distribution of a software version with such a weakness, and its discovery and exploitation by worm breeders.[22] A flaw might be a coding error that left a hole for an infection. Alternately, it could arise from a deliberate "back door" left in a software release when it was distributed. This might have been done to permit maintenance access, to permit use to be cut off in the event of failure to pay licence fees (a tactic of dubious legality), or for other, more sinister reasons. Presumably, leaving an undisclosed back door that promotes an infection could increase the chance of licensor liability — and could undermine the efficacy of contractual exclusions from liability.

A security flaw might not result from a true error. It might simply reflect a small and temporary deficit in a responsible programming team's approach to the unending "arm's race" between software companies and hackers. Again, the nature of the flaw can be expected to influence a finding of negligence or breach of warranty. Either negligent work or a deliberate back door justify liability. Security weaknesses commensurate with industry best practices (however deficient such practices might seem, in hindsight) do not.

Flaws in software might or might not matter in terms of security; many bugs have no such implication. As security flaws (and other bugs) are discovered in software with an installed base of customers, repair code is developed and made available on the licensor's Web site. These individual repairs are called "patches". It is up to the user to access and install the patches, or not. Some software includes the ability to automatically access updates and patches; in fact, this is increasingly the case. For a user to avail himself or herself of this automatic update facility, he or she must have registered with the distributor of the software. Additionally, the user must not interfere with the preferences settings that allow the service to run or, if they are not on as a default when installed, activate them. If a dialogue box requests confirmation to run the update routine and, afterward, to restart the computer to allow the updates to take effect, consent must be given.

Whether or not a duty of care existed to avoid infection by the installation of a patch will depend upon proof that a particular patch was available, known, and perhaps whether its installation could have been expected to be reasonably convenient and non-disruptive in relation to the harm it might potentially avoid. And, to make matters still more ambiguous, now some worms themselves arrive disguised as patches.

With respect to complex platforms, especially enterprise networks, patches pose problems magnified by the scale of the enterprise. Security patches might interfere with the operation of complex systems that combine a number of software packages, so administrators may reasonably decide not to install certain patches some of the time. Furthermore, the patches themselves can be buggy.

Keeping up with the patch stream for one's business software is an increasing productivity drain. It means taking down Web sites and other applications that owners want operational all the time. It means redirecting scarce resources to unpredictable maintenance requirements. In many enterprises, solving the problem means the tedious work of installing the patch and rebooting not a few but thousands of individual servers and personal computers, each with its own copies of vulnerable systems.[23] Yet to maintain a computer network open to the Internet and not to patch promptly, and thereby provide a weak node in which to breed worms and provide the central processing unit ("CPU") cycles to propel them on their cyberspace journey, might be regarded as unneighbourly, or even negligent.

Anti-Virus Software

Symantec Corporation ("Symantec") and McAfee (part of Network Associates, Inc.) are software manufacturers who are among the leading distributors of virus protection software. Such software relies on filters that scan network traffic and local memory and storage for the presence of worms. The ability to recognise a worm is dependent on whether the software is able to match invading code to a reference point in an up-to-date library of worms on the same computer; to have an up-to-date library obliges the user to download updates from the applicable Web site regularly. To fail to update the library is to avoid an opportunity to prevent infection. Often, such updates occur automatically and regularly, giving rise to the question of when a "special" update is an obligation because of potential risk. Whether not acquiring any such update is part of a given standard of care will depend on the sophistication of the user and the extent, nature, and duration of publicity and warnings about the damaging bug.

Symantec's Web site tells us just how intense the war against computer bugs is. Describing its efforts, Symantec reports:

> With over 20,000 sensors monitoring network activity in over 180 countries, Symantec has established one of the most comprehensive sources of Internet threat data in the world, giving Symantec's analysts a superior source of attack data from which to spot important trends.[24]

Tainted Meat

Spam, or junk e-mail, is an acknowledged public policy problem.[25] As we will see later in this paper, it is a growing source of the proliferation of worms. The common occurrence of receiving e-mail from strangers also helps worms to intrude. Thus, spam filters might also prove a useful anti-worm weapon.

Unsafe Computing: of Quarantine and Carriers

Potential Defendants

Who might be liable for worm infestations? Potential defendants would vary with the circumstances of the infection,[26] but they would certainly include the worm's author, and anyone who modified it or used it to launch an attack.[27] Hardware manufacturers would generally seem to be relatively remote from liability. Firewalls, which are generally software barriers to intrusion, are sometimes hardware-based. Where such a solution is implemented and proved faulty, liability would seem more likely.

Vulnerabilities to worms are primarily a problem for computer operating systems. Other software, such as databases and e-mail systems, helps to spread viruses and worms. The liability of hardware manufacturers, therefore, would seem most likely to arise from the software they choose to bundle with their products. Such liability, however, might be avoided because they succeeded in making clear to the plaintiff at the time of purchase that the software manufacturer, and not the hardware manufacturer, entered into the supply relationship with the plaintiff.

Hardware supplier responsibility could also be denied based on an issue of causation. If an operating system chosen resulted in harm from a worm because of vulnerabilities, how could a hardware manufacturer have avoided that harm? Perhaps Microsoft Windows is known to be a popular target for viruses, but how can software manufacturers not bundle it? It is not as though, after all, many alternative operating systems that would be immune present themselves as practical alternatives, and are acceptable to the consumer. Liability might be less likely to arise, therefore, on the theory that a poor product was chosen and supplied, than on a failure of a duty to warn, which is discussed further, below.

Whether a customer realizes that a third party supplied bundled software is an issue that will test the techniques used to bring software licences, and their attendant liability restrictions, to the customer's attention when a computer is purchased. Perhaps such a test will come up in the context of a class action suit by purchasers who failed to notice the ribbon around their keyboards, for instance. Amongst the numerous techniques to bring to the attention of computer purchasers

the terms of the licences governing the installed software has been that of a notice wrapped around and fastened to the computer's keyboard, preventing the computer's use without first seeing and removing it. Sometimes the notice of a license is put on the shipping box. In any event, the problem is the same — ensuring both that the consumer is aware that he or she is entering into a relationship with a different business in respect of the software components of his or her purchase, and that his or her use of those components is governed by its own set of terms. These terms, in the normal course, would provide for exclusions of certain types of liabilities; if the drafter of them were sufficiently adept, it might include losses owing to invasions of worms and attendant liabilities to third parties.

In addition to the foregoing, the list of potential defendants for an action arising out of an infection is long. They include:

- anti-virus software manufacturers;
- the proprietor of an electronic commerce Web site, whose customer base becomes prey to a worm, resulting in further spreading of the worm and breaches of privacy;
- a consultant, systems integrator, distributor, retailer, or other vendor who recommended or provided vulnerable technology, particularly in the case of a holding out of a special capacity to deal with security issues;
- consultants hired to assess security or fix vulnerabilities;
- security auditors;
- a provider of managed security services;
- an application service provider;
- an outsourcing vendor with responsibility for an electronic commerce Web site, applications software, or computer desktop management; and
- an Internet service provider.[28]

Contractual Defences

The liability of any party would vary with the nature, and enforceability, of contractual terms. Particularly relevant provisions would include limitations of liability, limitations of damages, waivers of implied warranties, limitations of warranties, and the like. Such defences will benefit the service provider and licensor. Needless to say, infections (like human varieties) do not spread only among relationships of contractual privity or other close relationships. Their independent spread across a network will result in damage arising from one network node in another that is entirely unknown. Often there will be no contractually based defences that would apply between infecter and infectee. Infection by a stranger, however, might implicate other contractual relationships. For instance, a Web site that collected names and electronic

mail addresses from clients might be able to argue that the terms of its Web wrap or other form of agreement with them would apply to limit damages arising from the propagation of worms to the e-mail list.

Liability of Individuals

While many of those particular defendants encompassed by the list above will prove to be corporate entities, the potential for individual liability also arises. In some cases, some of those described above will not have been part of a corporation. Even if they were, individuals will be directly responsible, at some level, for the causes of the damage, even if they are doing so in the name of a corporation. Given the trend to relax the requirements of contractual privity to allow employees to shelter behind contractual limitations of liability favouring their employers,[29] individual coders or posters of patches, network administrators, or any number of other individuals in the world of network and software services and maintenance will probably be safe from damages occasioned by them in the course of their work (assuming that their employers negotiated adequate and enforceable contractual limitations of liability in the first place). Needless to say, while an individual would probably benefit from contractual exclusions of liability, except in circumstances of fraud or undisclosed agency, he or she would not be liable for performance of the contract. He or she would not be subject to liabilities for covenants or warranties contractually imposed in the inter-corporate transaction. This is not the case for his or her individual liability in tort, however, where the foreseeability of harm could result in personal liability.

Individual investors who have involved themselves with a software firm through a partnership structure so as to take direct advantage of tax losses could be in for nasty surprises as direct owners, and therefore licensors, of computer software. Again, they would benefit from the terms of the licence (and, in any event, such structures have been out of vogue for some time, not least for reasons of potential liability).

Needless to say, a corporate veil will not shield a hacker from criminal liability.

Liability of ISPs

By virtue of their position, ISPs are in a position to become aware of the risks of a worm, and the increased traffic and effects on Internet operation, earlier than end users. In the right situation, perhaps they could prevent damage by shutting down their servers, or by filtering out messages that appear wormy or virus-bearing. Yet, the principle of the Internet is end-to-end neutrality. The Internet community does not expect its messages to be legitimately intercepted or snooped; indeed, absent a grant of permission under the customer agreement, section 342.1 of the *Criminal Code* (Canada)[30] would presumably apply.

Steps to mitigate the effect of worms are being taken by ISPs. They are beginning to actively seek out customers whose computers have been turned into "zombies" — that is, spam relayers — where the volumes of messages spike. Customers are contacted or cut off. It should be noted, though, that false results can arise from mail system responses to hacker probes. Also, working groups of ISPs have been organized to share information on spam and worm attacks.[31] To engage in such proactive oversight could enhance the risk of liability, as it has with respect to liability for libellous content on their servers.[32]

Radin has argued[33] that liability will converge on ISPs as technology to detect and quarantine virus-laden traffic becomes available, making them the least cost avoider of harm. However, it is far from clear that adding and maintaining such a layer of costly security, with its potential for disruptions, mistakenly seized e-mails, and the like, would truly be "least cost". Even if it were installed, it is unlikely to be perfect. The remaining potential for failure would result in high levels of redundancy, as users would rationally continue to install their own anti-virus protection. This might defeat societal cost savings. There could also be the risk of a false detection resulting in intercepted, uninfected mail, or delayed deliveries. Failure to update the software firewall could create a basis for a negligence claim. It has also been suggested that ISPs might have a duty to warn of the risks of contamination attendant on the use of their services, particularly high bandwidth.[34] Finally, it is a difficult context in which to try to pin down who the least cost avoider is, for such a determination will always, at least, be contingent on the selection of particular technologies available at any given time. We must be careful not to constrain the inventiveness that will produce that selection by limiting incentives with premature choices of liability rules.

In the case of copyright infringement, ISPs, as telecommunications services providers, are held harmless for merely providing facilities over which infringing content is communicated. Perhaps a case exists for similar protection to be extended to operating general application worm protection facilities.

Theories of Liability

Criminal Liability

The *Criminal Code* (Canada)[35] does not specifically address the propagation of worms and viruses. Criminal liability pertaining to certain abuses of computers is dealt with in sections 342.1 and 342.2, and subsections 430(1.1) and (5.1). Depending on the precise circumstances of the attack and its consequences, one of these provisions could apply.

Section 342.1 deals with the offence of "Unauthorized use of Computer". Subsection 342.1(1) states that:

> (1) Every one who, fraudulently and without colour of right,
>
> > (a) obtains, directly or indirectly, any computer service,
> >
> > (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
> >
> > (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
> >
> > (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

This section is directed at hacking into computer systems without authorization or payment, but its expansive language could apply to the author of a virus or worm attack.

Paragraph 342.1(1)(a) would almost always apply to an infection by a worm. The worm diverts the operation of the computer to the purposes of the worm and its author. In some cases, the result might not be very constructive, even from the author's perspective, leading one to quibble whether the worm-triggered computer response was, indeed, a "service". But since that response is intended by the author, it would hardly lie in his or her mouth to disclaim that he or she valued it to any extent as a service. It would obviously apply, in particular, to the use of a Trojan horse borne by a worm to commandeer CPU cycles. Or, consider the Code Red virus, which gave the attacker "complete administrator access to systems, which means it had the potential to plunder data, delete files and destroy systems".[36] Viruses used to take over a computer to propagate spam would appear to fall clearly within the intent of the section.

Since paragraph 342.1(1)(a) so clearly applies, it is not troubling that paragraph (b) is slightly more problematical. While a worm is almost certainly a device (or, if not, the combination of the worm and the computer that launched it would be), it is less clear that a virus in many circumstances can be said to "intercept" a function. Paragraph (c) would apply, since the author's computer system would have been used at least with the intent of committing an offence under paragraph (a).

Under section 342.2, "Possession of Device to Obtain Computer Service", the manufacture, possession, sale, or offer to sell any instrument, device or component under circumstances that could create a reasonable inference that it was intended to be used to commit an offence under section 342.1 is illegal, and could result in two years' imprisonment, or a finding of guilty of a summary conviction offence.[37] Again, the section is directed at devices, like the famous Captain Crunch whistle[38] or

other, more sophisticated electrical acoustic devices ("blue boxes"), which circumvent security systems to provide access to systems without permission. But it is no stretch to extend the section to apply to the author of a worm, to an individual in possession of the worm, or at least to the worm and a computer capable of launching it.

Subsection 430(1.1) of the *Criminal Code* deals with mischief to data:

> 430(1.1) Every one commits mischief who willfully
>
> > (a) destroys or alters data;
> >
> > (b) renders data meaningless, useless or ineffective;
> >
> > (c) obstructs, interrupts or interferes with the lawful use of data; or
> >
> > (d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
>
> A person convicted of this offence could be sentenced for up to five years in prison, or found guilty upon summary conviction and subjected to a lesser sentence.[39]

Again, this section was not intended to deal with worms and viruses, but to set loose a worm or virus could often result in liability under it. If the worm did not actually destroy or alter data, however, paragraph 430(1.1)(a) would not apply (although the attempt provisions of the *Criminal Code* would, depending on design of the virus). But the slowing of computer operation, or its unresponsiveness, frequent results of worms, could be obstructions or interruptions in the lawful use of data described in paragraphs (c) and (d).

Based on the foregoing, then, it is likely that the *actus reus* of an offence could be made out in the case of a worm attack. Criminal liability depends also on proof of intent. While it would apply to the hacker creator of malicious code, it would not to the unwitting provider of the equipment, networks, or computing power used to disseminate worms.[40]

Other criminal liability might attach, depending on the means of worm delivery. Examples such as the recent virus purporting itself to be a patch from Microsoft might qualify as a forgery under section 366 of the *Criminal Code*. So, too, might the offence of fraud, under section 380, be made out.

The difficulty of tracing the origin of worms, and the great cost of doing so, bring into question the efficacy of criminal deterrence as a solution to the worm problem. As one commentator put it

> Although nearly 63,000 viruses have rolled through the Internet, causing an estimated $65 billion (U.S.) in damage, criminal prosecutions have been few, penalties light and just a handful of people have gone to prison … One person has been sent to prison in the United States and just two in Britain …[41]

The absence of credible criminal enforcement is obviously a problem. To remedy this, Microsoft recently set aside US$5 million to fund rewards for worm authors.[42]

Contractual and Quasi-Contractual Liability

Various warranties, covenants, or representations — by software licensor to licensee, outsourcer to client, ISP to client, etc. — could be breached by a worm attack, or by attendant service or system failures. Such terms would usually be found in a written (or electronic) contract, but might also be collateral.[43]

Common contractual terms that could be breached include:

- warranties relating to the performance of software designed to enhance system security, or to the expertise of those providing security-related services;

- covenants in an outsourcing contract to maintain the currency of software versions, or of hardware and software in use, where a prompt change would have corrected a vulnerability;[44]

- covenants in an outsourcing contract directed more generally to ensuring continual adoption of best available technologies;[45]

- covenants to maintain online disaster recovery servers, where such servers themselves fell prey to the infection and so become unavailable;

- up time covenants by Web hosts or outsourcing service providers;

- overarching standard of performance covenants (i.e., "outsourcer will in all circumstances perform in accordance with the highest industry standards …");

- security standards specified by or to system integrators; and

- privacy policies of Web sites (a form of Web wrap, to the extent that reliance can be said to have been induced).[46]

There will certainly be others. Rest assured that imaginative counsel will visit afresh outstanding information technology and Internet contracts with the same eye to vulnerability that the hacker displayed in attacking the computer system. Both law and code, after all, are systems of risk management, and all systems are vulnerable to some degree. In this context, the clever litigator is not unlike the clever hacker. And the solicitor who designs protection for his or her clients is at the peril of an unknowable future.

Any claims that the manufacturer or developer made about the resistance of its hardware or software to infection that were found to be incorrect could be considered negligent misrepresentations that could make the manufacturer or developer liable to the licensee of the software, whether or not such representations formed a part of the contractual terms relating to the provision of the software.[47]

Virtually every ISP and software licensor will have contractual exclusions of liability in place that, presumably, will apply to worm and virus damage. It is, however, worth noting that such contractual terms are strictly construed, which could limit their application if it is ambiguous in respect to the infection in question. Moreover, generic — and non-negotiated — disclaimers may not be legally enforceable in all jurisdictions.[48]

Indeed, in theory, system users might not only be unable themselves to collect from service or software providers for the damages they have suffered because of contractual exclusions, but standard terms could make them liable to online services they infect. ANZ Bank's standard online banking terms got them in hot water when it was noticed that they made customers contractually liable for passing on viruses.[49] Such terms are not unusual. They are also, arguably, not advisable. No bank is likely to sue a customer for failed operations (except where such failure was the result of a deliberate act); why provoke them with such a clause? The clause might succeed on the principles of contract law. But if it did, it would produce a situation that practically begged for legislation to overrule it.

Unless effectively excluded by contract, provincial sales of goods legislation could affect liability for breaching warranties or conditions of sale, particularly the warranty of fitness for the purpose intended by the purchaser, or the condition of merchantability, for selling products that contained latent defects.[50] Typically, however, any terms of sales of goods legislation that might apply are excluded by the terms of the software licence. In any event, sales of goods legislation may not apply to software alone, since software is an intangible (although packaged software is a "good" for Ontario Retail Sales Tax purposes). Thus, a claim against a software vendor based on sales and goods legislation may fail. On the other hand, a claim against a hardware vendor, perhaps relating to a bundle of hardware and software, might succeed. Section 15 of the Ontario *Sale of Goods Act* ("SGA")[51] states that if the buyer has notified the seller of the expressed or implied purpose for which he plans to use the goods, there is an implied condition that the goods sold by the seller are reasonably fit for that expressed or implied purpose.[52]

The implied conditions and warranties of the SGA can be contracted out of through an express agreement between the parties,[53] except in consumer sales.[54]

It is an inherent characteristic of the spread of worms that large groups of people are affected. The Korean litigation (described in footnote 5) is a good example of the large classes of potential defendants. A gap in contractual protections, perhaps by the application of the SGA, could provide the foundation for a class action.

Tort

Intentional Torts

The FBI's Magic lantern worm, mentioned above, is a reminder that worms are spread for a variety of reasons: simple destruction, for political or ideological reasons,[55] for surveillance, or, in the case of the propagation of spam, for commercial gain.[56] Recently, Trojans have been installed in computers to enable access to online bank accounts to facilitate unauthorized withdrawals.[57] While the existence of intent will be important to prove certain offences and torts, the nature of the intent, in the case of civil liability, should not be. If a computer crashes, or data are destroyed, compensation for the loss should not be diminished if the intention were to intrude with fewer ill effects.

The challenging case for intention is one where the authorship of the worm is not in doubt, but its escape is proved to be accidental. Perhaps, then, liability would flow from analogy to release of noxious substances.

Trespass

In Canada, no case has yet found liability for intentionally infecting a computer with a virus. It is undoubtedly an actionable wrong, but the exact nature of liability awaits elucidation. In the United States, the doctrine of trespass to chattels has been used to find that Web sites that experienced reduced bandwidth capacity through receiving spam or being subjected to unwanted data-gathering programs suffered property damage that could be recoverable in tort, specifically the tort of trespass to chattels.[58] While the idea that causing a worm infection is a form of trespass has the attraction of superficial analogy — it is, after all, to put someone else's creation in a forbidden place — it is a novel interpretation of the law. Opinions vary on whether a court could stretch trespass doctrine in Canada to provide redress for worm infections. Indeed, the trend of academic opinion in the U.S. seems to resist this application of trespass law.[59] An advantage of this legal theory, however, is that it helps avoid the problem of pure economic loss, described below.

Misrepresentation

Another intentional tort that might come into play for distribution of malicious code is misrepresentation. To make a false representation that systems were secure against intrusion could expose one to tort liability for someone who relied on it, whether or not there was a contract. The representation would have to be made to the victim or reasonably foreseeably heard and acted on by the victim. Similarly, since worms and viruses often arise in electronic mails, which disguise their contents, perhaps an action for fraudulent misrepresentation would lie against the author.

Nuisance

It is also possible that nuisance law could be extended to provide a cause of action for the effects of worms. If nuisance provides a remedy for annoying telephone calls,[60] why not for other nuisance communications?

Negligence

Any number of situations of vermian damage could give rise to claims of negligence. To succeed, a plaintiff must prove that the defendant had a duty of care to the plaintiff; that that duty was breached by failing to exercise the appropriate level of care, causing the injury complained of; and that the plaintiff suffered actual loss or damage.[61]

Duty of Care

A duty is owed to all those whom one ought reasonably to foresee would be affected by one's actions.[62] The Supreme Court of Canada has established a test for determining if a duty of care existed between two parties in private law.[63] The first stage of the two-stage test is used to determine if the relationship between the parties was sufficiently proximate that carelessness by one would damage the other. If a proximate relationship exists between them, the test permits the court to limit or negate the scope of the duty, the class of persons to whom it is owed, or the damages that arise from the breach,[64] based upon policy considerations.[65] Thus, in *Hercules Managements Ltd. v. Ernst and Young*,[66] the duty of an auditor was circumscribed, to avoid the risk of indeterminate liability for a negligent statement in a financial report that may have been put to use for purposes other than the original purpose for which it was intended.[67]

An auditor is a paradigmatic example of one who, if negligent, could fall prey to an unpredictably and unmanageably large number of lawsuits. This could make the position of auditor untenable; hence, the need to limit auditors' exposure one way or another. Similar considerations must limit liability for negligently allowing the propagation of a virus or a worm over the Internet, however the policy is expressed.

The first stage of this test is difficult when dealing with damage caused by network proximity, and it therefore compels careful consideration of the test. On the Internet, everyone is your neighbour — millions and millions of entities with separate title to terminal facilities, each of whom is a potential plaintiff (or defendant). And, since the travel of worm packets is unpredictable, someone in Chad or Mongolia is as proximate a neighbour as someone down the street. In the case of the author of the damage, we are surely content to let him or her find his or her legal peril, wherever his or her mis-

deed leads him or her. For an individual user, potentially culpable only for negligence, if at all, such open-ended liability is unjust. Assuming that it were possible to trace the path of a particular infection to its immediate source, a defendant would be exposed to a sort of lottery of mischance. Can your unhygienic computer be shown to have passed the problem only to the neighbour's child's computer, or also to the U.S. and Russian governments? Did it unwittingly pass on a bit of code that causes a brief notice requesting a moment of silence on Remembrance Day to appear, or one that shuts down a national economy? Faced with such a hazard, it is difficult to describe the scope of a duty to other users. Thus, whether for considerations of proximity or policy, we would expect courts would rarely find a duty of care where one is a careless node in the propagation of a worm.

A similar policy calculation would hold for the manufacturer or developer of vulnerable software provoking the creation of a particular worm, and helping it to spread. That manufacturer would have a duty to the parties whom it ought to reasonably foresee would be affected by defects in its products. This would include immediate clients, and those in contact with the clients. The entire installed base could be affected (creating, presumably, a good basis for a class action). Third parties who might have benefited had the software performed to promise, but who had not themselves purchased the software, are unlikely to be able to sustain a claim of duty owed to them by the manufacturer. Indeed, were they able to, they would almost certainly be in a better position than the licensee, since rights would be limited by the licence to which it had agreed.

Also, damages from worms would be principally economic, recovery for which is limited under Canadian law.[68] There are many reasons for this, including the prevention of indeterminate liability, and the duplication of lawsuits that would be launched under contract law.[69] However, *Canadian National Railway v. Norsk Pacific Steamship*[70] has established that in Canadian law, there can be recovery for economic loss if there is a sufficient proximity between the negligent act and the loss (along with the usual requirements of the presence of a breach of duty and foreseeability of the loss).[71] The test established in *Cooper v. Hobart*[72] is used to determine if a sufficiently proximate relationship exists between the parties, and if any policy considerations should limit or negate the scope of the duty or damages awarded. Recovery for economic losses under tort law can occur if the plaintiff can establish that his or her losses arose from the defendant's tortious act, were foreseeable, and sufficient proximity existed between the parties.

Recovery of purely economic losses is confined to limited categories of relationship.[73] While courts can be expected to add to the existing categories in appropriate cases, the prospect of huge and unforeseeable losses

arising from the unknowable path of a worm is not a likely case.

Enterprises could also be vicariously liable for the actions of their employees, such as the deliberate forwarding of an infected joke, e-mail, or movie clip. Such activity might or might not qualify. It would often breach explicit employer guidelines, but it would be a use of an employer system during business hours. The negligent conduct of a systems administrator could make his or her employer liable through vicarious liability. Employers are vicariously liable in two situations:

> (1) for employee acts that are authorized by the employer, or (2) unauthorized acts so connected with authorized acts that they may be regarded as modes (albeit improper modes) of doing an authorized act.[74]

Standards of Care

At any given time, the actions required to meet a standard of care for protection from spreading worms will depend on the particular risks of the day and the technologies available to meet them. The expected standard of care to avoid spreading a worm or virus will also vary with the identity of the defendant. It will be higher for a professional IT consultant than for a personal computer user, higher where legislation sets specific standards, such as where the requirements for security of data in the *Protection of Personal Information and Electronic Documents Act*[75] apply, or where levels of IT security and robustness are the subject of regulatory oversight, as in the case of financial institutions.[76] Where damage from a worm arose because of a breach of a statutory standard of care, civil liability might be based on the statutory breach.

There are several IT security organizations, such as CERT[77] and SANS,[78] who have suggested measures that IT professionals should take to better safeguard the Internet.[79] The European Union is also setting up the European Network and Information Security Agency, expected to be operational early in 2004.[80] CERT also has guidelines for the disclosure of known vulnerabilities.[81] Also significant is the International Organization for Standardization standard ISO/IEC 1799:2000 Information technology — Code of practice for information security management.[82] But there is no agreed standard, nor any body governing the profession to set one. The publications of CERT or SANS or ISO will have some persuasive power, but no more, unless the defendant has made an explicit commitment to a particular standard. Such a commitment can be useful for marketing purposes (such as boasting of ISO 9001 quality control certification), and is often made. Another body with a mandate including protection of computer infrastructure is the Office for Critical Infrastructure Preparedness ("OCIPEP"), which has a programme of evaluating and providing warnings about information technology security failings. OCIPEP also helps to certify security worthiness of technologies.[83] OCIPEP's mandate, how-

ever, is far broader than information technology (its Web site, for instance, contains a grimly fascinating database of Canadian natural disasters).

In computer services outsourcing contracts and other services contracts, service providers will sometimes agree to overall standard of service covenants. Such a covenant might, for instance, promise standards of service in accordance with the best professional standards of the industry. Such a covenant would help to resolve any ambiguity in determining appropriate behaviours.

The standard of care for the maker of anti-virus software is complex. There is no guarantee that effective anti-virus software is always possible — that the coding power of the good guys is always stronger than that of the bad guys. Even when a solution is possible, the timeliness of its delivery must be subject to reasonable limits.

Discussion in security circles is full of talk of liability for spreading viruses. Such discussion began when diskettes were used, long before it was assumed such viruses would travel over the Internet. This is bound to be useful to a plaintiff's counsel proving standard of care. Thanks to the Internet, such discussion is now well documented and easily accessible. In any event, given the scale of the problem and its topicality, it would be a rare case indeed in which ignorance could be successfully argued.

Causation

Worms fast become ubiquitous on the Internet. For every attack, one might receive several copies of an infection. At the height of the transmission of an infection by electronic mail, it has been estimated that a significant portion of all e-mail, exceeding 10%, is infected. Even if there were a duty in a particular case, such as a duty to warn, it is not clear that a particular infection is the result of its breach. Any solution — a warning, a patch, the addition to the database of anti-virus software, might not be timely, or might not be effective. It has, in fact, been argued that due to delays in installing patches, announcing a security failing might be of greater service to those who would exploit it than to those who should fill the breach.

The determination of causation is also frustrated by the difficulty of tracing the origin of a virus. Many viruses are polymorphic, which means that they contain mutation engines that change their encryption routines each time they are passed on to a new computer.[84] Therefore, the virus that infected the upstream computer may have been in a form that was not recognizable by its anti-viral protection measures. Thus, even if reasonable measures were taken, it could have mutated into a different form that was recognizable by standard anti-viral precautions by the time it moved downstream. This would create significant evidentiary problems in a negligence lawsuit. The virus would have been detectable at the downstream computer but not at the upstream one — making it hard to impose liability on the upstream computer, or to gauge what standard of care should have applied.[85]

Contributory Negligence

Contributory negligence may result in the apportionment of liability amongst several of the potential defendants listed above. Foreseeability of harm to oneself through one's actions is the key component for contributory negligence.[86] If the downstream party did not take reasonable measures to prevent viral infections, then it may be at least partly liable under contributory negligence for the damages that it incurred.

Other Statutory Liabilities in Tort

Viruses and worm infections could lead to breaches of statutory duties.

With enough warning of a security risk, a software manufacturer might be in the possession of a material fact as defined under applicable securities legislation, requiring timely disclosure to the regulators and the markets. Failure to do so might result in expensive shareholder litigation. But whether or not it is a material fact depends to an extent on one's assumptions about potential liability. It can also depend on one's business; a bug can be good for business, too, if your business is repair and data recovery.

Canada's federal privacy law, like its financial services legislation, contains obligations of data security, and obligations of confidentiality.[87] However, the legislation contains its own remedial mechanisms. Whether the Act's rules give private parties any rights to bring their own action has not yet been determined, although in the case of *Englander v. Telus*,[88] an application was heard to grant relief following the Privacy Commissioner's failure to do so (the application was rejected). Other duties, regulatory, statutory, or at common law, can also apply to certain types of information, such as financial and health-care-related data. The *Bank Act* (Canada) also contains certain data security and IT operation requirements; in some cases, it imposes the obligation directly on the bank's board of directors.[89] In an instance in which directors approved confidentiality guidelines inadequate for their purpose, perhaps an action against them could result. It would appear to be difficult for a director to argue that viruses and worms ought not to be contemplated as risks to confidentiality of data. Again, such potential liability would only be invoked in a limited subset of hacker attack, one in which confidential data were disclosed.

Product Liability

Liability for failure to warn has been imposed on manufacturers and suppliers of dangerous products. They are required to warn all those who may reasonably be affected by potentially dangerous products[90] (including parties who are not party to the contract of sale).[91] It is unlikely, however, that this obligation could extend to products causing risks of service disruption or risks to data, since that is not truly "dangerous" as con-

templated by that duty. This would not be the case, however, if the machine at risk had a life-saving function, like a radiation therapy device or an ambulance dispatch service, or controlled a dangerous process such as in a nuclear reactor or chemical plant. However, one would hope that such devices would be thoroughly isolated from contact with the Internet and any other foreseeable sources of worms.

For the duty to warn to apply, the potential user must be reasonably foreseeable to the manufacturer or supplier; "[however,] manufacturers and suppliers do not have the duty to warn the entire world about every danger that can result from improper use of their product."[92] Networked computer products would not become "defective" — that is to say, use-impaired by reason of infection — without the intervention of the worm. Indeed, in some sense, the device ceases to be the manufacturer's "product", since the sole characteristic making it dangerous is created by a third party. But this might not prove to be an impermeable defence. A computer infection is not like a rider-mower souped up for racing. In the mower case, the owner of an isolated product has used it as the basis for a different, more dangerous thing; it is his or her responsibility and initiative. Viruses and worms, however, mirror their product, and their make up is determined by the deficiencies in the product's security — security intended to provide precisely against the avoided harm. Moreover, those deficiencies present a risk of extraordinarily widespread harm. In many cases, the manufacturer has the ability to easily contact the software users by mailing to a database of electronic mail addresses. The manufacturer is in the business of monitoring the weaknesses of the product, providing patches and new versions. Clearly, the risk of physical harm is such that it is unlikely product liability law should apply, but who can say that liability for negligence might not follow? Or that, in this new age, courts will not find reasons to expand the reach of product liability law into the ethereal, but altogether costly, realm of cyberspace?

Intellectual Property

It would be interesting to be able to invoke intellectual property laws against worm authors. Admittedly, given the plethora of other remedies to which they could be made subject, this aspect of the rights of the injured might be of only academic interest, but it is an intriguing question for the legal scholar. It would appear, on balance, that if a worm were sufficiently original, there would be no reason in principle why it could not avail itself of the limited protection of copyright laws afforded to computer software. Such protection, however, is curtailed where software is expressed in its particular form as it is, because of certain types of interface requirements it must meet.[93] Since a worm is designed to exploit a particular security flaw, this rule of copyright law would significantly limit the scope of permitted protection for the resulting code. To the extent that authoring tools come to determine the structure of the code as well, the author's rights to prevent copying would be expected to be limited.

Ironically, since viruses are often written for non-commercial reasons, they might have a better claim than the average software for moral rights. Worms are usually designed to convey political messages of one kind or another, and shutting down the SCO or Microsoft Web sites, while unquestionably criminal, might be just such an instance that merits moral rights protection, in theory. It is, however, unlikely to expect much judicial deference to such rights.

Insurance

Insurance companies play a role in establishing standards of care, since the ability to get insurance for infections is conditional on having adequate anti-viral measures in place.[94] A limited number of insurers offer coverage for e-business and its attendant liabilities, although such coverage appears currently to be limited and expensive.[95] Insurers, including AIG[96] and Zurich[97] offer coverage for a wide range of electronic business-related interruptions, including liabilities relating to forwarding a virus or worm. Presumably, risk managers will ensure that processes to maintain anti-virus protections and to patch regularly will be in place, so as not to void coverage. As coverage becomes more common in the market, therefore, standards of practice are likely to be clarified, and to become more exacting.

Currently, according to one source, only 11% of "organizations" have insurance against cybercrime, which might include virus infestations.[98] The potential scope of damage for computer failures and hacking is great enough that such insurance is typically not cost effective — its high price reflects the difficulty of quantifying the risk. Increases in security and clarifications of liability risks will permit it to be priced more accurately, and potentially increase its uptake.

Next Steps

The costs of computer infections, the number and size of potential defendants, the industry's unorthodox approach to contracting, the increasing role of insurance — all these increase the probability that computer infections will provoke increasing litigation. Criminal prosecution is straightforward; legislation is in place to penalize worm authors, and it is entirely appropriate to do so.[99] But questions of civil liability, and the bases for them, are more amorphous.

A cautious approach to sorting out civil obligations is needed. We cannot wish perfect technology into being; patience must attend the diligent efforts even of a technologically adept behemoth like Microsoft. Liability for failures of widely installed systems may well discourage innovators to participate in the market. Con-

versely, of course, inadequate risk of liability might not encourage sufficient diligence. The societal gains of widespread computer access and use emerge in part from affordability, which, in part, arises from the ability of sellers of computer equipment and services to control and understand their liability risks. It might be the case that a clearer liability regime would cause resources to be redirected to installing or creating new security measures, assuming better measures could be made available. The net effect of those security measures — their cost less avoided harm — might or might not be economically efficient. One thing is sure: perfect security will always be technologically infeasible. Duty must be built on a basis of reasonable efforts.

It is not easy now to identify least cost avoiders of the harm of worms. If it is ISPs, then legislation extending some protection to them in the course of taking reasonable anti-virus measures would probably be needed.

Moreover, it is up to each individual and business to weigh the risks and rewards of the Internet, and bear some of those risks, paying for what best seems to them an appropriate level of security. It has been suggested that to expose a business to the Internet might itself be negligent:

> "Right now, you have an infrastructure that allows anyone to connect without standards," he said. "That creates a major threat. [Businesses] are exposing services on the Internet that have no business being exposed."[100]

The scale of the installed base of Windows (and, perhaps, increasingly of Unix) and its related e-mail clients both enhances the opportunity for the spread of worms and viruses, and greatly magnifies the potential for harm. It has recently been suggested that the unavoidable risks borne by users of mass-market software militate for an enhanced and clarified liability regime for software distributors.[101] Indeed, Microsoft is being sued on the basis that the ubiquity of its software presents a global security risk. The suit is based on an identity theft but cites also the Blaster worm. Counsel for the plaintiff also suggests that Microsoft's warnings about security issues help hackers more than consumers, who are often too slow to install patches — slower than the hackers who attack their systems. The case is seeking class action status.[102]

Our dependence on networked computers is enormous, and growing. The regular increases in the power of networked personal computers means that more and more functions migrate to them. Thus, tasks once performed manually and discretely are automated, and, so,

sensitive to disruption; tasks once safe on a mid-size or mainframe computer, secure in part because of its different operating system, also migrate to the desktop. This means that vulnerable infrastructure — the infrastructure of corporations and governments and electronic commerce — is no different than that in a hackers' bedroom, greatly facilitating worm attacks.

To make matters worse, irresistible network effects cause users to converge on the same systems, ensuring that not just user groups but whole societies are susceptible to the same weaknesses. This is a process antithetical to an analogous genetic diversity that safeguards populations by ensuring not all weaknesses are shared by individual specimens. Obviously, for now, the market has decided to trade off the protection afforded by diversity, in exchange for focused development efforts and network effects. The more risk averse can take refuge in Apple computers, safer largely because the installed base is small enough that vandals ignore it.

The fact is that the enormous number of home and small business personal computers — the very market software makers and service providers are trying to reach — will always be an Achilles heel to the Internet. The provisions of service agreements and licences aside, it must make sense to encourage a solution to be effected by bigger players, because only that will work (if anything will). Perhaps operating system manufacturers should be required to bundle anti-virus software, with an automatic update system that could not be overridden.

Otherwise, small users (though not only they) are a great systemic problem — many points of weakness linked to an essential public infrastructure. We can think of it as not unlike a water utility, the difference being that every user, a huge population reflecting all the vagaries of human infirmity and weaknesses of character, has an equal power not only to take water out, but to put it in. Historically, this sort of commons has been far better protected by common law than public oversight. The analysis in this short paper points to no clear policy for major legislative intervention, save for the limited suggestions set out above. Nor does an optimal rule for apportioning liability in cases of alleged negligence jump out. The gathering and weighing of evidence in the emerging cases will guide us on the path the law should follow. The end point of that path, however, is not in doubt. Worms are a major scourge in an essential public infrastructure, and law must contribute what it can to seeing that they sleep with the fishes.

Notes:

[1] Robert Lemos, "Year of the Worm: Fast-spreading code is weapon of choice for Net vandals" *CNET News.com* (15 March 2001) online: CNET News.com http://news.com.com/2009-1001-254061.html?legacy=cnet [*Lemos*].

[2] Rare for Windows computers, that is. Ironically, it is the Apples that are not wormy; their small market share, and their different and more resil-

ient operating system, have created a sort of immunity in the highly infectious environment of the Internet.

[3] The use of viruses to convert computers to junk mail relays is a rapidly growing problem, a problem which is expected to grow significantly in 2004. See Antone Gonsalves, "Spam-virus: leading Internet threat next year", *TechWeb News* (5 December 2003) online: TechWeb http://

www.techweb.com/wire/story/TWB20031205S0009 [*Gonsalves*]: "Relaying spam through other computers enables spammers to remain anonymous and avoid law-enforcement agencies. By hiding the original source of the mass mailings, spammers also can avoid blacklists used by filtering software to separate spam from legitimate messages."

[4] In a denial of service attack, many distributed computers are used, with or without the intention of their owners, to generate great volumes of Web site enquiries with the aim of taking the subject Web site out of service.

[5] Woo, Yun, Kang, Jeong & Han, "Online Users to Sue for Internet Disruption" (18 September 2003) online: International Law Office http://www.internationallawoffice.com/Ld.cfm?i=38527&Newsletters__Ref=7363. This story relates to a lawsuit initiated in Korea by various plaintiffs, including an Internet café service provider, many Internet cafés, users, and others, against several ISPs, the Korean government, and Microsoft Corporation for damages arising from the SQL Slammer worm. The basis for the allegation of liability appears from the press to be negligence. See also the other cases and emerging cases cited in this article.

[6] Computer worms, at least. Writing on the topic has led me to speculate, repelled, on other harmful worms, and to ensure that my dog's heartworm medications are up to date, lest I carelessly infect others' pets. A survey of cases in the U.K., Canada and the U.S. about tapeworms, ringworms *et al.* reveals, frankly, nothing really useful in this context, although there are a few cases considering liability for failure to disclose the existence of worms in livestock, or for negligent treatment, or failure to diagnose the presence of worms of various sorts in people. Meiring de Villiers, in his article on the role of the Res Ipsa Loquitur doctrine in negligence actions for virus or worm infections (*infra* note 84), cites the following: "An English court held that a defendant who stored biological viruses had a duty to cattle owners who would be affected by the spread of the virus. *Weller and Co. v. Foot and Mouth Disease Research Institute*, [1965] 3 All E.R. 560 at 570: '[T]he defendant's duty to take care to avoid the escape of the virus was due to the foreseeable fact that the virus might infect cattle in the neighborhood and cause them to die. The duty is accordingly owed to the owners of cattle in the neighborhood …'".

[7] Act IV, scene iii.

[8] Robert Lemos, "Counting the cost of Slammer", *CNET News.com* (31 January 2003) online: CNET News.com http://news.com.com/2100-1001-982955.html.

[9] Deborah Ghose, "Computer viruses, Worms and Insurance: Risk or Certainty?" online: About.com http://insurance.about.com/cs/lines/a/virusesandworms.htm.

[10] "Symantec Internet Security Threat Report Volume IV" online: Symantec http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?SSL=YES&EID=0&PDFID=551&promocode=ITR 2 [*Symantec Report*].

[11] Margaret Jane Radin, "Distributed Denial of Service Attacks: Who Pays?" (Whitepaper commissioned by Mazu Networks, http://www.mazunetworks.com) [*Radin*].

[12] Scarlet Pruitt, "Microsoft could face security failure liability" *Network World Fusion* (10 March 2003) online: Network World Fusion http://www.nwfusion.com/news/2003/1003microcould.html.

[13] *Lemos*, *supra* note 1.

[14] I.e., the sequences of keystrokes typed by the users of the computer.

[15] *Lemos*, *supra* note 1.

[16] *Ibid.*

[17] *Ibid.*

[18] Robert Lemos, "Worm exposes apathy, Microsoft flaws", *CNET News.com* (26 January 2003) online: CNET News.com, http://news.com.com/2100-1001-982135.html?tag=nl.

[19] *Ibid.*

[20] *Ibid.* See also Jordan Legon, "As Net attack eases, blame game surges", *CNN.com* (28 January 2003) online: CNN.com http://www.cnn.com/2003/TECH/internet/01/27/worm.why/index.html.

[21] *Lemos*, *supra* note 1.

[22] *Symantec Report*, *supra* note 10 at 2.

[23] Jaikumar Vijayan, "Patching Becoming a Major Resource Drain for Companies", *Computerworld* (18 August 2003), online: Computerworld, http://www.computerworld.com/securitytopics/security/holes/story/0,10801,84083,00.html.

[24] *Symantec Report*, *supra* note 10 at 1.

[25] See for instance Industry Canada, *SPAM Discussion Paper — July 1997 Internet and Bulk Unsolicited Electronic Mail*, online: Industry Canada http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00188e.html. Industry Canada, *SPAM Discussion Paper — January 2003, E-mail Marketing: Consumer Choices and business opportunities*, online: Industry Canada, http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/vwGeneratedInterE/gv00189e.html.

[26] In the Korean case, *supra* note 5, defendants include Microsoft, ISPs, and the government of Korea.

[27] In the case of the recent Blaster worm, there have been recent indictments of individuals, sometimes minors, for launching variants of the original infection. See Gene Johnson, "Second Arrest Made in Computer Worm Attack" (27 September 2003) online: Computer Cops http://computercops.biz/article3362.html.

[28] A posting on the Gigalaw Web site points to an actual virus case, in yet another, more complex fact situation: "Hello all, I was wondering if you could give me any clues on where to read up on the subject of virus related damages and find cases similar to this one: two companies have a business relationship, producing a product together, a virus enters in the side of one of them (precautions were taken to assert virus stoping, but …), causing damages to both of them — company is insured for such a case, but not for the loss of profit … The subject is not covered by the contract. Is it all down to "due care", does anyone have any experience or know of a similar case? Thank you for the help, Katja" [All typos as they originally appeared.] Katjuza Oz, "subject: virus/liability/damages" *Gigalaw.com Discussion List* online: Gigalaw.com, http://www.gigalaw.com/archives/0108/gigalaw-discuss-0108-00039.html.

[29] *London Drugs Ltd. v. Kuehne & Nagel International Ltd.*, [1992] 3 S.C.R. 299.

[30] R.S.C. 1985, c. C-46, as amended [*Criminal Code*].

[31] Stefanie Olsen, "Telecoms, ISPs partner in spam fight", *CNET News.com* (13 January 2004) online: CNET News.com, http://news.com.com/2100-1024_3-5140556.html.

[32] See for instance, *Stratton Oakmont, Inc. v. Prodigy Services Co.*, [1995] WL 323710 (N.Y. Sup. Ct. 1995), in which Prodigy's practice of overseeing bulletin board postings on its services was determined to have avoided liability of exercising editorial control, and therefore liable for views expressed in the bulletin board. Contrast *Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991), in which, in a similar situation, CompuServe's "hands off" approach placed it in the position.

[33] *Supra* note 11.

[34] Alex Salkever, "As the Worm Turns: Lessons from Blaster", *Business Week Online* (19 August 2003) online: Business Week Online http://www.businessweek.com/technology/content/aug2003/tc20030819_2562_tc047.htm.

[35] *Supra*, note 30.

[36] Robyn Weisman, "Got a Virus? You're Sued!", *News Factor Network* (8 August 2001) online: News Factor Network http://www.newsfactor.com/perl/story/12529.html.

[37] *Criminal Code*, *supra* note 30, section 342.2.

[38] Computer hacker and noted felon John Draper famously discovered that the tone of a whistle contained in boxes of Captain Crunch cereal emitted a tone that unlocked free long distance service for him, when sounded into a phone receiver. See http://www.webcrunchers.com/crunch/.

[39] *Criminal Code*, *supra* note 30, s. 430(5.1).

[40] But if manufacturers or developers intended to sell software or hardware with features that were intended to be used to commit an offence under section 342.1 of the *Criminal Code*, then those manufacturers or developers could be convicted under section 342.2 of the *Criminal Code*. Unlikely, but not impossible. Such features could include Trojan horses and features causing a cessation of the ability to use without warning, when the term of a licence expired without renewal. Such facts could also result in a charge of mischief under subsection 430(1.1) of the *Criminal Code* for causing mischief in relation to data, since data would be rendered inaccessible. Again, all speculation, and unlikely to actually arise.

[41] M. Mendoza, "Virus perpetrators proving hard to convict", *Toronto Star* (1 September 2003).

[42] Robert Lemos, "Microsoft to offer bounty on hackers", *CNET News.com* (4 November 2003) online: CNET News.com, http://news.com.com/2100-7355_3-5102110.html.

[43] In *Heilbut, Symons & Co. v. Buckleton*, [1913] A.C. 30, a collateral contract (or warranty) was defined as a contract secondary to the main contract that induces the other party to enter the main contract.

[44] Data processing outsourcing contracts often contain covenants that the client's applications software will always be in the most current version, subject to reasonable maintenance and installation lags.

[45] Such covenants are rare, but not unknown. A determination of liability for failure to abide by such a clause would need to consider compliance by both parties with the requirements to consult with respect to such changes, and to cooperatively implement change control processes, etc.

[46] In the unreported case of *Allan Mather v. Columbia House* (6 August 1992), (Ont. Ct. Gen. Div.), a remedy was given for breach of a proclaimed privacy policy, although not part of any "contract".

[47] See *Hedley Byrne & Co. Ltd. v. Heller & Partners Ltd.*, [1964] A.C. 465; *Esso Petroleum Co. Ltd. v. Mardon*, [1976] Q.B. 801; and *Murray v. Sperry Rand Corporation et al.* (1979), 96 D.L.R. (3d) 113 for the liability of parties who make negligent misrepresentations.

[48] *Ibid.* Disclaimers of liability have been avoided for unconscionable breadth. See notably *Robert v. Versus Brokerage Services Inc.*, [2001] O.J. 1341 (Ont. Sup. Ct.) and *Zhu v. Merrill Lynch, HSBC*, 2002 B.C.P.C. 535 (B.C. Prov. Ct.). Enforceability can also be limited for other reasons: See also *America Online, Inc. v. Mendoza*, 2001 WL 695166, in which a court applied local consumer protection statute to deny enforcement of a choice of jurisdiction clause and *Rudder v. Microsoft Corp.*, [1999] O.J. No. 3778 (Ont. Sup. Ct.) in which the court enforced a click-through agreement between consumers and Microsoft.

[49] Darren Greenwood, "ANZ stung by reaction to virus liability clause", *Computerworld New Zealand* (22 May 2002) online: IDGNet New Zealand, http://www.idg.net.nz/webhome.nsf/0/47C9A39A0C9A4C85CC256BBE0079B1A8?opendocument.

[50] The reason for providing a remedy only for "latent" defects is that a buyer who inspects the goods before purchase is expected to discover "patent" (= obvious) defects before completing the sale.

[51] *Sale of Goods Act*, R.S.O. 1990, c. S.1.

[52] *Ibid.*, s. 15(1).

[53] *Ibid.*, s. 53.

[54] See the *Consumer Protection Act*, R.S.O. 1990, c. C.31, s. 34(1) for the definition of a consumer sale in Ontario, and for the provision that prevents the negation of the implied warranties or conditions in consumer sales that arise from the *Sale of Goods Act*.

[55] Note, for instance, the MyDoom worm, which has proved very successful at using infected computers to generate sufficient traffic to shut down the SCO Group Web site. SCO was targeted because it claims copyright in Linux open source software, a claim odious to a class of technological idealists with apparent vigilante tendencies. See Bernhard Warner, "MyDoom Net Worm Scores Hit, Knocks Out SCO Web Site" *CNN Sunday* (1 February 2004) online: Netscape Network CNN News http://cnn.netscape.cnn.com/news/story.jsp?floc=FF-RTO-rontz&idq=/ff/story/0002%2F20040201%2F0731809773.htm&sc=rontz.

[56] The use of viruses to commandeer computers for relaying spam is expected to become a leading Internet threat in 2004, *Gonsalves, supra* note 3.

[57] Jennifer Sexton, "New net banking scam" *Australian IT* (9 January 2004) online: Australian IT http://australianit.news.com.au/articles/0,7204,8352771^15330^^nbv^15306-15319,00.html.

[58] See *Radin, supra* note 11; see also *eBay v. Bidder's Edge* 100 F.2d. Supp. 1058; *Register.com, Inc. v. Verio, Inc.*, 2000 U.S. Dist. Lexis 18846; *CompuServe Inc. v. CyberPromotions Inc.*, 962 F. Supp. 1015; *America Online v. LCGM, Inc.*, 46 F. Supp. 2d. 444; *America Online v. IMS*, 24 F. Supp. 2d. 548.

[59] See, *inter alia, eBay v. Bidder's Edge* (*ibid.*), Amicus Brief filed by 28 cyberlaw professors: Brief of *Amici Curiae* in Support of Bidder's Edge, Inc., Appellant Supporting Reversal, 22 June 2000, online: Chicago-Kent College of Law http://www.kentlaw.edu/legalaspects1/TrespasstoChattels/readings/eBayAmicusBrief.pdf; and see also *Intel v. Hamidi Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (Cal. 2003), for a less favourable view of the trespass to chattels approach.

[60] See, for instance, *Motherwell et al. v. Motherwell et al.* (1976), 73 D.L.R. (3d) 62 (Alta. Sup. Ct.).

[61] David L. Gripman, "Comments: The Doors are Locked but the Thieves and Vandals are Still Getting In: A Proposal in Tort to Alleviate Corporate America's Cyber-Crime Problem" (1997) 16 J. Marshall J. Computer & Info. L. 167.

[62] *Donoghue (M'Alister) v. Stevenson*, [1932] A.C. 562.

[63] *Cooper v. Hobart*, [2001] S.C.R. 437; *City of Kamloops v. Nielsen et al.* (1984), 10 D.L.R. (4th) 641.

[64] *Ibid.*

[65] *Ibid.* See also *Hercules Managements Ltd. v. Ernst and Young*, [1997] 2 S.C.R. 165 [*Hercules*].

[66] *Ibid. Hercules.*

[67] *See Ibid. Hercules* and *Caparo Industries v. Dickman* [1990] 1 All E.R. 568. In both of these cases, it was found that although the defendants negligently prepared statements which other parties relied upon and suffered economic losses, the defendants were not liable for those losses because their statements were used for different purposes than those intended.

[68] See *D'Amato v. Badger*, [1996] 2 S.C.R. 1071; *Ultramares Corp. v. Touche*, 174 NE 441 cited in *Canadian National Railway v. Norsk Pacific Steamship*, [1992] 1 S.C.R. 1021 at para. 219 [*CNR*]; *supra* note 47.

[69] *Supra*, note 47 at para. 43.

[70] *CNR, supra* note 68.

[71] *Ibid.* at para. 258; see also *supra*, note 47 where it was found that economic losses are recoverable under tort law if they stem from an independent tort unconnected to any contractual obligation.

[72] *Supra* note 63.

[73] Bruce Feldthusen "The *Anns/Cooper* Approach to Duty of Care for Pure Economic Loss: the Emperor Has No Clothes" 18 C.L.R. (3d) 67.

[74] This test, used to determine if vicarious liability exists is commonly known as the Salmond test. Found in R.F.V. Heuston, and R.A. Buckley, *Salmond and Heuston on the Law of Torts*, 19th ed. (London, England: Sweet & Maxwell, 1987) cited in *Bazeley v. Curry*, [1999] 2 S.C.R. 534 at para. 10.

[75] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

[76] See Office of the Superintendent of Financial Institutions, *Guideline: Outsourcing of Business Activities, Functions and Processes* (May 2001, Revised December 2003) online: OSFI http://www.osfi-bsif.gc.ca/eng/documents/guidance/docs/b10_e.pdf; also the requirements for the boards of directors of federal financial institutions to approve guidelines for the confidentiality of information.

[77] CERT is the Computer Emergency Response Service based at Carnegie-Mellon University. Online: CERT Coordination Center http://www.cert.org/nav/index_main.html.

[78] SANS is a computer security institute of interest to computer professionals. Online: SANS Institute http://www.sans.org.

[79] See CERT/CC "Protect Your Web Server Against Common Attacks" online: CERT Coordination Center http://www.cert.org/security-improvement/practices/p082.html; CERT/CC, The SANS Institute, & The Center for Education & Research in Information Assurance & Security (CERIAS), "Defeating Distributed Denial of Service Attacks," online: SANS Institute http://www.sans.org/dosstep/roadmap.php; SANS/FBI, "The Twenty Most Critical Internet Security Vulnerabilities" online: SANS Institute http://www.sans.org/top20/.

[80] "EU Sets Up Internet Security Agency" *SiliconValley.com* (20 November 2003) online: SiliconValley.com http://www.siliconvalley.com/mld/siliconvalley/news/editorial/7309661.htm.

[81] "The Cert/CC Vulnerability Disclosure Policy" online: CERT Coordination Center http://www.cert.org/kb/vul_disclosure.html.

[82] For a brief description of the standard, and for additional information, see the ISO Web site at http://www.iso.ch/iso/en/prods-services/popstds/informationsecurity.html.

[83] Public Safety and Emergency Preparedness Canada homepage, online: http://www.ocipep.gc.ca/home/index_e.asp.

[84] Meiring de Villiers, "*Virus Ex Machina: Res Ipsa Loquitur*" (2003) Stan. Tech. L. Rev. 1.

[85] *Ibid.*

[86] See also *Jones v. Livox Quarries* [1952] 2 Q.B. 608.

[87] *Supra* note 75.

[88] [2003] F.C.J. No. 975.

[89] *Bank Act*, S.C. 1991, c. 46.

[90] *Bow Valley Husky (Bermuda) Ltd. v. Saint John Shipbuilding Ltd.*, [1997] 3 S.C.R. 1210 [*Bow Valley*]. See also *Lambert v. Lastoplex Chemicals Co.*, [1972] S.C.R. 569; and *Hollis v. Dow Corning Corp.*, [1995] 4 S.C.R. 634.

[91] *Rivtow Marine Ltd. v. Washington Iron Works et al.*, [1974] S.C.R. 1189.

[92] *Bow Valley*, *supra* note 90 at para. 19.

[93] *Delrina Corp. v. Triolet Systems Inc.* (1993), 47 C.P.R. (3d) 1 (O.C.G.D.); *Delrina Corp. v. Triolet Systems Inc.* (2002), 58 O.R. (3d) 339 (Ont. C.A.).

[94] *Supra* note 5.

[95] *Ibid.* see also Jon Swartz, "Firms' hacking-related insurance costs soar" *USA Today* online: USATODAY.com http://www.usatoday.com/money/industries/technology/2003-02-09-hacker_x.htm.

[96] AIG Insurance, "Full Coverage for Your Computer System" online: AIG netAdvantage Suite http://www.aignetadvantage.com/.

[97] Zurich North America, "E-RiskEdge offers a unique solution" online: Welcome to E-RiskEdge http://www.zurichna.com/SaFE/erisk.nsf.

[98] Graham Cluley, "Directors face 'cyber liability'", *ComputerWeekly.com* (30 January 2003) online: ComputerWeekly.com http://www.computerweekly.com/Article118957.htm.

[99] That is to say, legislation is in place in Canada and elsewhere. The author of the Melissa virus, arrested in the Philippines, was released when it was realised that no law existed under which to charge him.

[100] *Supra* note 20, quoting Lawrence Baldwin, head of Internet security firm mynetwatchman.com.

[101] See Todd Bishop "Should Microsoft Be liable for Bugs?" *SeattlePost-Intelligencer* (12 September 2003) online: *seattlepi.com*http://seattlepi.nwsource.com/business/139286_msftliability12.html.

[102] Joris Evers, "Security suit against Microsoft could turn huge" *Network World Fusion* (10 March 2003) online: Network World Fusion http://www.nwfusion.com/news/2003/1003secursuit.html.