COMPUTERIZED BULLETIN BOARD SYSTEMS: CIVIL LIABILITY FOR ROGUE PROGRAMMING

Dale Tarzia

I. Introduction:

Computerized bulletin boards and networks are among the fastest growing sectors in personal computers and communications. In fact, they represent what many have called the information superhighway of the future. The amount of information which can travel through networks and bulletin board systems ("BBS's") can be staggering in both speed and quantity. This is especially true because modem communications are constantly increasing in speed, and data transfers can occur faster than a computer can process them. Not surprisingly, the ever increasing speed is expected to expand the customer base of people who use BBSs and other future interactive media.

BBSs provide open forums, which allow users to exchange ideas, messages, data and programming. But, the exchange of data and programming exposes users to the risk of obtaining virus-contaminated material. Computer viruses are programs, hidden from the user, which infect both the boot sector of computer disks and the fixed and floppy drives. Generally, they have the ability to replicate themselves on the disks of a computer and usually gain entry into computers by attaching themselves onto other programs. The result of an infection by a computer virus ranges from annoying messages to actual destruction of data on disk drives. Currently, there are over 2,000 viruses in existence, many of them variants of one another.

Computer viruses are referred to as "rogue programming" because they are unwanted programs which cause a multitude of effects on computers. Rogue programming can be divided into several categories: computer viruses, worms, trojan horses, and time bombs. Worms are programs that spread in communications networks from computer to computer and consume valuable computer time. Sometimes purposely used to monitor computer systems, worms are self-contained programs that try to hide themselves. Trojan horses are programs which are disguised as other programs but do not perform according to the program description. While these programs can cause destruction to files, they differ from viruses in that they neither replicate themselves, nor hide themselves within other programs. Time bombs are usually found in features or subroutines contained within application programs. The "bombs" are designed to disable the application program, or upon the occurrence of an event such as a specific date or an amount of computer usage, act like a computer virus. Time bombs are frequently placed inside the programs by the programmer himself, and may be used to enforce licensing agreements which are meant to limit use to a certain amount of time.

The different types of rogue programming can also incorporate features of one another, and thus, blur their distinctions. For example, a virus can act like a time bomb and execute its programming on a certain date, while at the same time replicating itself on other computer systems. Some of the more noted rogue programs have been the IBM Christmas Card, the Michelangelo Virus (a time bomb type virus), the Internet Worm, and the Brain Virus. The damage and cost caused by these rogue programs can be substantial. For example, the Internet Worm infected nearly 60,000 computers and used valuable computer time.

To combat the damaging effects of rogue programming, the computer industry has responded with anti-virus programs which are designed to prevent, detect, and clean systems. Despite these preventive measures, rogue programming continues to create questions concerning the legal duty to prevent the spread of viruses, and the civil liability which should be imposed on BBSs which fail to meet the minimum requirements of prevention.

BBSs are diverse in description, accessibility, and cost. While some BBSs charge hourly or monthly rates for access, and also charge additional hourly rates for access to data and software services, others offer access for free or sell individual programs for a fee. As a result of the different types of BBSs, either the Uniform Commercial Code ("U.C.C.") or tort law is applied to determine the liability of BBS operators. Although some courts have treated the sale of software as a service, and thus, have applied tort liability, others have treated these transactions as the sale of goods and subjected them to the warranties provided in the U.C.C.

II. Applying U.C.C. Article 2 to Liability of Spreading Rogue Programming to BBSs:

The U.C.C. provides buyers of goods with specific rights and remedies based on the warranty of goods under Article 2. In some instances where software is being licensed and not sold, courts have looked beyond the contract to the transaction and found that there may be a sale of goods based on the licensing arrangement alone.
warranties and remedies in U.C.C. Article 2 are important to BBS operators because they provide the limits of liability for those who sell software as a good.

A contract for the sale of goods is required under the U.C.C. Thus, liability under the U.C.C. can be found where BBSs specifically sell programs and data, and possibly where additional “fees” are charged to users who access the file and data areas for downloading. Therefore, a sale may occur when a user pays for access to download programs and data. Specifically, the sale takes place as the bits are transferred to the downloader’s computer. Additionally, contract formation occurs when users sign or acknowledge an agreement of terms which discloses the nature of the relationship between the parties, and the fees or costs being charged.

An inherent liability problem arises because most major BBSs do not charge a fee for each program, but rather for access time to download the programs. This could be analogized to the purchase of steak by the pound, where the seller is liable for the whole cow. In this context, the user is paying for the program by size according to the length of download time. U.C.C. Article 2 warranties are most likely to apply to those BBSs that act as distributors for software manufacturers. Tort law liability, however, should apply to BBSs that are free or charge flat fees per month.

The warranty provisions of the U.C.C. may arise both during and after the transfer of rogue programming. These warranties and their limitations are set forth under § 2-313, express warranties, § 2-314, implied warranties of merchantability, and § 2-315, implied warranties of fitness. U.C.C. § 2-313 provides for express warranties by affirmation, description, or sample, and can be applied to almost all BBS file transactions which fall under the U.C.C., because almost every file which can be downloaded has a rudimentary description of its contents and a descriptive file name. U.C.C. § 2-313 (1) provides for express warranties where (a) an “affirmation of fact or promise made by the seller to the buyer which relates to the goods and becomes part of the basis of the bargain creates an express warranty that the goods shall conform to the affirmation or promise.” Subsection (1)(b) provides that the description of the goods that is part of the bargain creates an express warranty that the goods will conform to that description. Subsection (2) specifically states that while formal words such as “warranty” or “guarantee” are not necessary to create an express warranty, a statement of the seller’s opinion does not create a warranty.

Section 2-313 is applicable in cases in which the BBS claims to have virus free files. This warranty can also apply when trojan horses are “sold” accidentally. Section 2-313 also makes the BBS operator liable for the statements made about rogue programming and the actual content of the files where contamination by trojan horses occurs. For example, the trojan horse file would not be the file for which the user paid and, therefore, would not comport with the description of the requested file. The BBS operator can avoid making express warranties by checking the program for rogue programming and letting the buyer know of the methods through which it was done. Furthermore, the BBS operator can set forth the limitations of the specific methods used to check for the rogue programming, and can avoid liability by actually running the programs to make sure they are not trojan horses.

As with all warranties, the seller may be liable for incidental damages and for making any statements which become part of the bargain. Therefore, it may be expensive for BBS operators to provide express warranties that cover actual content. These warranties can be waived, however, through express language stating that no express warranties are given in respect to the content of files.

Another avenue of liability under the U.C.C. is that of implied warranties of merchantability. Section 2-314 (1) provides that:

Unless excluded or modified (Section 2-316), a warranty that goods shall be merchantable is implied in a contract for their sale if the seller is a merchant with respect to goods of that kind. Also, § 2-314 provides under subsection (2) “Goods to be merchantable must be at least such as (a) pass without objection in the trade under contract description, and ... (c) are fit for the ordinary purposes for which such goods are used; and ... (f) conform to the promises or affirmations of fact made on the container or label if any.

Implied warranties of merchantability are especially troublesome for BBSs because they set minimum standards with respect to the quality of goods provided. Thus, the standard practices of some BBSs may be implied to all BBSs, subjecting them to a minimum standard for inspecting for rogue programming. For example, BBSs may be required to use the latest version of virus checking software as well as updated virus definition files. BBSs can avoid liability, however, by excluding implied warranties under U.C.C. § 2-314 (1) when following U.C.C. § 2-316 Exclusions or Modification of Warranties. U.C.C. § 2-316(2) provides (subject to subsection (3)) that to exclude the warranty of merchantability the language must mention merchantability. Subsection (3)(a) further allows waiver of implied warranties through language such as "as is" or "other language which in common understanding calls the buyer's attention to the exclusion of warranties.

Therefore, for BBSs to avoid implied warranties under U.C.C. § 2-314, they must make or display waivers of those warranties. This becomes apparent under U.C.C. § 2-314(3) which provides that, "unless excluded or modified (under Section 2-316) other implied warranties may arise..."
from course of dealing or usage of trade." Course of dealing and usage of trade are not defined in the context of BBSs and are subject to rapid change caused by the evolving nature of BBSs. But, BBSs also can avoid this type of liability by offering explicit generalized waivers of warranties or providing files on an "as is" basis.

The U.C.C. also provides for implied warranties of fitness for a particular purpose. Under § 2-315 the seller must have reason to know any particular purpose for which goods are being bought and the buyer must rely on the seller's judgment in providing the proper goods. This type of warranty could apply where a user downloads files with a specific description and the program turns out to be a trojan horse. The BBS could then be found to have breached the warranty of merchantability. With other implied warranties, however, this can be avoided with express language. If warranties are explicitly waived with clear language, the BBS, as a seller, can avoid most of the liability created under U.C.C. warranties. Used effectively, the BBS can provide files with little worry about the content if the waivers of warranties are properly worded. Nevertheless, BBSs may not be able to avoid all liability relating to the spread of rogue programming if tort law is applied.

III. Civil Liability for Rogue Programming Under Tort Law:

Tort law, particularly negligence and strict product liability, can provide significant liability problems for BBS operators. Unfortunately, tort liability is not as easily avoided as is liability arising under U.C.C. warranties. Negligence consists of four specific parts: 1) a duty to the user; 2) a breach of that duty; 3) the breach was the cause of a loss; and 4) the breach was the proximate cause of that loss. In the context of BBSs and rogue programming, these specific requirements are best defined as: 1) the BBS operator has a legal duty to use certain measures to prevent the transmission of rogue programming; 2) the BBS operator failed to use some or all of those measures; thus breaching his/her duty; 3) the BBS operator's failure to use those measures "caused" transmission of the dangerous code to the claimant's system and "proximately caused" damage to the claimant or the claimant's system; and 4) that damages occurred.

The duty of the BBS operator to prevent rogue programming may vary depending on whether the BBS is free or whether the operator charges a fee for use. This duty arises simply with the knowledge that rogue programming exists and that there are measures to avoid it. Moreover, although the required precautions employed to avoid the transmission of rogue programming are not clearly defined, a certain minimum duty of care still exists.

Breaches of this minimum duty to prevent rogue programming may occur at any time and can result in negligence if the other requirements of the tort are present. Because updates for virus signatures are available for a relatively low price, and the procedures employed by the BBS for preventing rogue programming are mostly automated, there are few excuses for not taking proper precautions.

A BBS operator can meet the minimum standard of care by performing three steps: 1) checking the files for infection through the use of readily available virus checking software; 2) checking the files for trojan horses prior to allowing them to be available for download; and 3) notifying the users that files may contain rogue programming that is undetectable using current methods and, therefore, frequent back-ups of their systems should be performed to minimize loss. These precautions cause minimal intrusion into the operation of a BBS and, with the exception of checking for trojan horses, are currently employed by many BBSs.

Causation may be more difficult for the user to prove than breach of duty because there is always the possibility that the user may have had his system contaminated through means other than downloading contaminated software from a BBS. For instance, contamination may occur by using a floppy disk from another computer which is infected by a virus or worm, or through software purchased at a retail store which contains rogue programming. Proof of causation by BBS users, however, may be made by showing the actual intrusion route of the rogue programming by tracing through the back-up of the computer system and finding the entry point of the virus. If it can be shown the rogue programming entered through the BBS, causation will be proven.

Once causation is proven, the next element required to prove negligence is proximate cause. Proximate cause exists when the breach is the actual cause of the resulting damage to the computer system. For example, when a BBS fails to scan files for viruses, the file is downloaded, and the file ultimately damages the user's computer system, proximate cause is established.

BBSs may also be subject to strict products liability of which there are three different types of liability: warning defects, manufacturing defects, and design defects. Specifically, warning defects apply to BBSs because of the potential dangers of rogue programming present in downloaded files. Strict product liability in tort presents two related problems. First, is the transaction between the BBSs and users a sale or service? Second, how does product liability apply if the courts are inconsistent when characterizing the transaction? The Restatement (Second) of Torts sets forth the requirements of strict product liability:

(1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is
subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property if (a) the seller is engaged in the business of selling such a product, and (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold. (2) The rule stated in (1) applies although (a) the seller has exercised all possible care in the preparation and sale of his product, and (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller. 65

Under Section A, a product is defective if "at the time it leaves the seller's hands [it is] in a condition not contemplated by the ultimate consumer, [and] which will be unreasonably dangerous to him." 66 The danger is that the user's downloaded software may contain a rogue program capable of destroying the users' disk drive files. Strict liability could protect the user where he reasonably believed that the BBS had taken sufficient measures to prevent the spread of rogue programming. Thus, the test is one of reasonableness. Therefore, the BBS must use reasonable methods, not every available method, to eliminate rogue programs.

BBSs can avoid imposition of strict liability by warning the users of the potential presence of rogue programming. Comment j of §A provides that a dangerous product may become safe to use if adequate warnings are provided. 67 Specifically, a BBS can provide this warning in the system identification tag that is usually placed in a downloaded file. 68 Also, products liability insurance may be available to BBS operators, but sufficient coverage could be costly because the files can transfer to many users quickly.

The BBSs themselves may be able to limit tort liability by placing some of the risk of damage onto the users. This could be done by express disclaimers about the dangers of downloading files. 69 Also, BBSs could argue that users assumed the risk because, BBSs commonly cause the spread of rogue programs, and the measures to limit the damage from rogue programs is as readily available to users as it is to BBSs. 70

IV. Policy Issues Involved in the Liability of Rogue Programming:

Even though BBSs can take measures to limit their U.C.C. or tort liability, should liability nevertheless be imposed upon them? The criminal aspects regarding the purposeful spread of rogue programming have been addressed in many states, as well as by the federal government. 71 Consequently, many legislatures have found that purposeful transmission of rogue programming is harmful to society and should be criminalized. 72 The rationale supporting criminality is that society wants to be protected from the spread of rogue programming, and accordingly, BBSs must take responsibility for its prevention.

Arguably, placing responsibility on BBSs for transmission of rogue programming imposes a burden on them. 73 The precautions against rogue programming, however, are inexpensive, generally not time consuming, 74 and can be automated by the BBS operating programs themselves. Thus, the burden is not significant enough to allow BBSs to avoid their responsibility. Moreover, most major BBSs have adopted policies through which the spread of rogue programming is limited. These BBSs usually use the latest version of virus definition files, and thoroughly run the programs to ensure that they do not contain trojan horses. 75 This could set a minimum standard of care in the industry because a significant portion of BBS users access the large BBS services. Nevertheless, many of the BBSs operate at little or no profit. Thus, placing extreme burdens on them may have the effect of eliminating them from the marketplace. Small BBSs that operate for free may only have to scan the files with a recent version of virus definition files. Those BBSs which are larger and profit-oriented may have the responsibility to scan and thoroughly evaluate all software that is uploaded to it. Therefore, the minimum standard of care must be measured in accordance with the size and profit of the BBSs.

Under the tort assumption of risk theory, users may also have the responsibility to scan the files themselves and minimize the damage which can occur. 76 Software to scan for viruses is easily available to users for a relatively low price. Furthermore, users can also take responsibility for limiting the damage from rogue programming by creating regular back ups to their systems. The caveat is that users often do not keep their virus checking software up to date. Also, new viruses may not have been discovered at the time virus definition files are released.

Some authors have suggested the imposition of strict liability upon BBSs. 77 This could include placing adequate technological barriers to invasions of computer networks and/or to carry sufficient insurance to cover whatever losses may occur. 78 This type of legislation, however, may be problematic. For example, what amount of insurance would be sufficient? How expensive will these technological barriers be? Who will bear these increased costs? Most likely, the user will end up paying the increased costs, possibly resulting in decreased access. Thus, legislative initiatives to impose liability would be unwise in this area because Congressional or state action could impede the free flow of access to information on BBSs and increase operating costs substantially. Moreover, the BBS industry has taken measures to preserve its own good will by attempting to limit the spread of rogue programming. 79 Generally, the computer industry has been characterized as an electronic
playground for computer novices, the openness of which has helped expand the computer and related industries through legitimate experimentation. Legislation, if not carefully and narrowly drawn, could stifle the BBS industry.

V. Conclusion:

U.C.C. and tort liability can be effectively eliminated or reduced through BBS waiver notices, thus unfairly shifting much of the responsibility for damage done by rogue programs to users. Consequently, liability should be left to the industry practices, because there is some standard of care which should be applied to the largest BBSs, as well as the smaller ones. Nevertheless, BBSs themselves need to define that standard of care. This duty represents a small burden on BBS operators and provides a substantial amount of protection to the users of those systems. Thus, the duty of BBS operators should in no way impede the growth of this industry, but rather help it to expand as the public gains confidence that adequate measures have been taken to prevent the spread of rogue programming.

---


2. Charles A. Radin, U.S. Data Highway Gatherers Speed: Rules of Road Eyed for Computer Network, BOSTON CHRONICLE, Dec. 22, 1992 sec. 3 at 1. The Internet now has an estimated 20 million users and links approximately 10,000 smaller computer networks to BBSs.


5. See generally, Anne W. Branscomb, Rogue Computer Programs and Computer Rogues: Tailing the Fugitive to Fit the Crime, COMPUTER AND COMPETITION IN TELECOMMUNICATIONS (1993).


7. Id.

8. See generally, Branscomb, supra note 5.

9. Id. at 1; Lance Rosen and Jonathan Wallace, SYLTRAN (2d ed.) at 157.


11. Id.

12. Id.

13. Id.


15. Id. the Brain Virus has the ability to replicate itself and execute its destructive programming after a certain amount of time passes from infection.

16. Branscomb, supra note 5, at 10. For example, a software vendor can license a program for one year and after the year has passed, the program self-destructs, thereby relieving the vendor from the expense and trouble of enforcing the license agreement.


20. Id. v. Moten, 928 F.2d 504 (2d Cir. 1991).


22. See generally, Branscomb, supra note 5.

23. Id.

24. Id.

25. These BBSs can be considered "free" but often require an upload/download ratio to allow users access to the files. This can result in some BBS users having to obtain programs for uploading at a cost in order to have uploaded material to maintain a proper ratio so that downloading will be permitted.

26. See generally, Branscomb, supra note 5.

27. See generally, Data Processing Services Inc. v. L.H. Smith Oil Corp., 492 N.E. 314, 315 (Ind. Ct. App. 1986) (where the court found that the sale of custom-made software was a service); WESTERN DRY CLEANING STATION v. COMPUCARE INC., 745 F.2d 59 (6th Cir. 1984) (where the sale of hardware and software was characterized as a sale of goods when the purchaser treated it as such for tax purposes).
28. U.C.C. § 2-105 (1) (1994) defines goods as "all things which are movable at the time of identification to the contract for the sale other than money in which the price is to be paid."

29. REX Industries, Inc. v. Liberty Constr. Inc., 772 F.2d 543, 546 (9th Cir. 1985) (where the court found that the sale of software alone is a sale of goods even though there is a licensing agreement).

30. Id.


32. U.C.C. § 2-106 (1) (1994) provides that "A sale consists of the passing of title from the seller to the buyer for a price (Section 2-401)." U.C.C. § 1-201 (1) (1994) defines a contract as "the total legal obligation which results from the parties' agreement as affected by this Act and any other applicable rules of law."

33. See generally, Branscomb, supra note 5.

34. The major BBSs are CompuServe, Prodigy, Genie and America Online, because they, as individual BBSs, have the largest number of users. These BBSs often charge additional fees over their regular access fees for users to download programs.

35. For example, McAfee Associates distributes its antivirus software through their own BBS. Apogee Software uses a similar distribution technique, but has also allowed other BBSs to become "official" distribution sites.

36. One BBS currently known to this author (The Game Peddler) "sells" software based on the individual program, not by amount of time used or for an access fee.


38. For example, a game might be described as to type (i.e. strategy or adventure) and system requirements. The file names themselves often describe the type program (although under MS-DOS the file name is limited to eight characters). For example, a game file name might be CHECKERS.ZIP suggesting that it is a checkers game.


40. This can be accomplished with specific provision in the membership agreement or under the terms of the sale. An example of language used to limit express warranties: "No express or implied warranties are given in respect to downloaded files, the files may contain rogue programming and the BBS provides available files on an as is basis and assumes no responsibility for incidental or consequential damages resulting therefrom."


42. Virus definition files are the signatures that virus checking programs rely on to check for the presence of viruses in programs, disks and in memory. They are updated when new "viruses" are discovered which cannot be identified with the current definition file. The definition files are released sporadically depending on the specific software manufacturer.


44. U.C.C. § 2-416 (2) (1994).


46. U.C.C. § 2-315 (1994); See also, Hollingsworth v. The Software House Inc., 513 N.E.2d 1372 (Ohio Ct. App. 1986) (where warranty of fitness for a particular purpose under U.C.C. was applied to the sale of computer software).


48. Meeting Makers, Inc. v. American Airlines, Inc., 513 So.2d 700 (Fla. App. 3d Dist. 1987) (where the court found that conspicuous disclaimers of all warranties were valid in the sale of a computer system).

49. Lawrence B. Levy & Suzanne Y. Bell, Software Product Liability: Understanding and Mitigating the Risks, 5 How. Tech. L.J. 112 (1990). An example of a limitation of liability clause: In no event will the vendor be liable for any damage, including lost profits, cost of cover or other special, incidental, consequential or indirect damages arising in any way out of this agreement, however caused any on any theory of liability. The customer acknowledges that the fee reflects this allocation of risk.

50. Id. at 16.


53. See generally, Branscomb, supra note 5.

54. Rose & Wallace, supra note 9, at 163. Currently, virus checking software comes in the latest version of the Microsoft Disk Operating System (MS-DOS Version 6.0) and retail for $49.95. MS-DOS is compatible with IBM machines, and is thus available to most computer users, as well as to BBSs.

55. Most software under which BBSs operate have features which allow automatic scanning of uploaded software, and also display messages to the user warning of the perils of using downloaded software and the type of preventive measures that should have been taken by the manufacturer, the BBSs and the user.
Whether the software in question has updated virus signatures may be uncertain because the release of new signature files varies with each manufacturer. Perhaps the checking software should be updated at least within two releases of the previous virus signature update.

This could, at a minimum, entail that the program be decompressed and actually executed to see the results. Software should not necessarily have all aspects of it studied to determine whether a well hidden portion of it contains a Trojan horse.

Most of the major BBS do follow this procedure, probably because of the vast numbers of users and their desire to maintain good will.

Rose and Wallace, supra note 9, have questioned what the duty of the BBSs should entail and whether requiring these procedures violates the First Amendment. Neither concern seems valid because criminal laws regarding rogue programming have been effectively used. Moreover, this content based intrusion is very narrow in that it is intended only to deal with the harmful effects of rogue programming.

For example, after restoring the data from the backup, the user could use current virus checking software to determine which file infected the system. The origins of the contamination can then be easily traced.

See generally, Bramson, supra note 5.

Manufacturing and design defects could be applied to instances in which the BBS is acting as a distributor for a software company.

See generally, Bramson, supra note 5.


Miyuki, at 6 (citing RESTATEMENT (SECOND) OF TORTS § A comment g).

RESTATEMENT (SECOND) OF TORTS § A comment j.

System identification tags are usually placed into the file to identify which BBS the file came from. The tags are placed into the file as part of an automated feature of the software under which BHs run.

Rose & Wallace, supra note 9, at 167. An express disclaimer can consist of the following: "We do not warrant or represent that any of the files available from our system are absolutely free of viruses, Trojan horses, worms, time bombs, or any other type of dangerous computer program. You should perform your own testing to assure that the program files you download are truly free of viruses or other dangerous programs."

See generally, Bramson, supra note 5.


For example, 18 U.S.C. § 1030 (a) (5) criminalizes destruction or damage to federal interest computers and under (a)(6)(c)(2)(a) provides for imprisonment for up to five years.

See Rose & Wallace, supra note 9, at 163.

See generally, Bramson, supra note 5.

The programs are also thoroughly tested in order to ensure that copyrights are not being violated and that they are not contributory copyright infringers.


Bramson, supra note 5, at 25.

Id.

See generally, Bramson, supra note 5.

Bramson, supra note 5, at 21.