Computers & Security, 8 (1989) 25–27

Legal Options To Computer Viruses

Bernard P. Zajac, Jr.

"Buy your software from a reputable source" has been used by many as one means of reducing the threat of a computer virus infection. In this article the author explores legal opinions about the options open to the user in the United States. – H.J.H., editor.

Computer viruses have become the "hot" topic in the computer security industry. Nearly every computer conference has a session on how to protect your computer from computer viruses and other security threats. There are several computer virus "vaccines" on the market.

Most of the "vaccines", security policies, and devices deal with prevention. But what happens if you become the victim of a virus? You could be out several thousand dollars in both software and time, and a price cannot generally be placed on the aggravation factor.

What recourse do you have, legally, if you have been a victim of a virus? One software manufacturer recently said to me, "you, as a user, have a recourse; you just sue them (the software manufacturer)!" Interesting idea, but can you?

There has not been extensive case law concerning viruses in the United States, so I posed the question, concerning what recourse, if any, a person or corporation may have if they were the victim of a virus, to a number of attorneys.

Kirk W. Tabbey, head of the Washtenaw County Computer Crime Task Force, an assistant prosecuting attorney in Ann Arbor, Michigan, said, "You'll always have a criminal case if you can find the person who did it (created the virus), because a virus is a malicious act;" surreptitiously inserting a virus in a program is, in itself a malicious act, therefore a crime. But, this is against an individual or individuals who created and/or inserted the virus. But what about the person who sold you the software or the software manufacturer? Are they liable? What damages can you recover?

It seems you can recover damages, but it is not a simple matter. James J. Ayres, an attorney with the Chicago firm of Magee, Collins and Lodge, a part-time faculty member of DePaul University's College of Law, points out that recovery can be approached in several different ways: it could be a pure contract law case between two or more parties; a Uniform Commercial Code case between buyer and seller; or a tort liability case. Within tort liability, it could either be a straight tort or a negligent tort, depending on the facts of the case, each providing its own unique advantages and disadvantages. Or it could be a cause of action under the Electronic Communications Privacy Act of 1986 [1].

When software is sold today, the box containing the software generally has a contract on the outside stating that if you break the seal on this box you agree to the terms of the contract. The contract generally states that the sold software is "as is" and the manufacturer is not to be held liable for defects and/or damages to your machine: a "shrink-wrap" contract.

0167-4048/89/$3.50 © 1989, Elsevier Science Publishers Ltd.

Tabbey points out that there are certain liabilities you are always responsible for. "I can create a law that says, if you want to come into my yard, I will not be liable for slips and falls. I will not be liable for anything than happens at all on the premises. That is overly broad – you cannot legislate away liability," explained Tabbey.

Robert I. Brown, of Schlussel, Lifton, Simon, Rands, Galvin and Jackier in Southfield, Michigan, points out that the enforceability of a "shrink-wrap" contract may be challengeable. "A lot depends on whether the contract is actually negotiated or if it was simply a 'boiler plate' agreement. If it was a 'boiler plate' contract, if it was entered into without negotiations, and there is a limited number of dealers in the area, then the court may have the discretion to disregard liability limitations," said Brown.

Ayres says "shrink-wrap" contracts are unenforceable, pointing out that the State of Illinois recently passed a "shrink-wrap" law providing for the enforceability of "shrink-wrap" contracts, but repealed the law in less than 4 months after heavy pressure from software manufacturers' lobbyists and end users. Ayres noted that the United States 5th Circuit Court recently upheld Louisiana's district court's opinion striking down Louisiana's "shrink-wrap" as being pre-empted by the copyright act.

Robert P. Bigelow, counsel to Warner and Stackpole in Boston, former editor of the *Computer Law Service* and correspondent to the British publication: *Computer Law and Security Report,* echoes Brown on "shrink-wrap": a lot depends on the contract and depending on the state the contract was executed in, "You might have separate rights. For example, let us assume, that a particular program was for personal use. There is in Massachusetts, a separate statute [2]. You can argue the shrink-wrap software will fit into the classification of goods for the purposes of the Uniform Commercial Code and one of the things they have in that Code is the application to the 'Merchantability' and fitness of goods."

Ayres noted, "I think you would be hard pressed to argue that any commercially available software that comes in a box is a service." He said, "Customized software is more up the spectrum of service." Ayres said courts have held that information can be a product.

If software is a good or product, then, as Ayres, Bigelow, Brown all noted, the Uniform Commercial Code has provisions for certain warranties [3].

The argument that the manufacturer or publisher of the software has a responsibility that the product is "virus free" is true to a point. Said Ayres, "Did the publisher know or should he have known" the software contained a virus? If so, then they are probably negligent. Explained Tabbey, "If they can come into court and they can prove that they are 'state-of-the-art' for checking for viruses, and they missed this one, it would be pretty tough, not only to hold them strictly liable, but it would be pretty tough to hold them liable at all!"

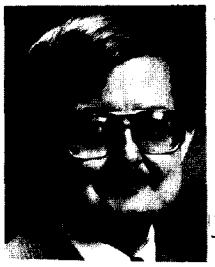
As you can see, if you were the victim of a virus, you could have several options: go after the person who sold you the software, go after the publisher/manufacturer of the software, and if you know who inserted or created the virus, criminally go after that person or persons.

Criminally charging someone for a virus or a computer crime is not new; as many convicted hackers know, it has been done and there is a body of supporting case law. However, civilly charging someone is new. The courts have yet to address this.

It seems that you do have recourse under the Uniform Commercial Code and under the concept of tort liability. But it won't be easy, since there is little or no current case law to use. You would be blazing new legal ground.

As viruses become more virulent and prevalent, and the apprehension of the perpetrator more difficult, victims, both corporations and indivi-

duals, will start looking to software manufacturers and vendors for a higher level of assurance that the software is "virus free" and recovery for damages should they become a victim.



Bernard P. Zajac, Jr. is the database/data security manager of the ABEX Corporation of Chicago where he is responsible for physical and internal security of its databases, investigation of computer abuse and database design. Prior to joining ABEX, he was a police systems analyst for the Illinois Criminal Justice Authority where he worked on the Authority's Police Information Management System. At the authority he also reviewed and tested data encryption/decryption equipment. He has almost 15 years of data processing experience and was in law enforcement for five years. He has spoken and published articles in the United States and Europe on computer crime, computer security and police systems.

References

[1] U.S.C. 18 §2510.
[2] Mass. Gen. Laws Ann. ch 106 §2-316A.
[3] U.C.C. §§2-312-318.