10th BILETA Conference Electronic Communications

March 30th & March 31st, 1995 Business School, University of Strathclyde, Glasgow

Sysadmins in the Cyberspace

Leo van der Wees & Pieter Kleve, Erasmus University Rotterdam

Keywords:

Sysadmins - Sysops - Bulletin Board System (BBS) - Cyberspace - Copyright protection - Child pornography

Abstract:

It has been stated that information is almost impossible to control, particularly in a society which has become heavily networked. If this statement is true, it must have consequences for the position of system administrators (sysadmins) and bulletin board system operators (sysops). Will they be liable for activities using their systems that might be illegal? Will they play a significant role in the dissemination of all kinds of information that might have an illegal nature? Or will they become an influential controlling node in the world's networks? This paper examines the possible legal consequences of the problems sysadmins and sysops might encounter in the cyberspace.

Introduction

Due to the fact that the networked environment is growing rapidly, it has been stated that information has become almost impossible to control. This must have consequences for the position of system administrators (sysadmins) and bulletin board system operators (sysops). Are they responsible for the material being transmitted over their system? Can they be held liable for breaches of copyrights? And what of child pornography which might pass through the networks?

A US Supreme Court verdict once said 'the Federal law against child pornography requires the Government to prove that those who distribute or receive sexually explicit films or photographs of minors are aware that the performers are not adults'. So it seems sysadmins and sysops are better off not trying to track down illegal (child pornographic) material on their systems. Can and will this same rule be applicable to other (il)legal activities making use of their systems or do sysadmins and sysops have a certain level of responsibility as well? In other words, will they (continue to) play an important role in the dissemination of all kinds of (il)legal information or will they become an influential controlling node in the worlds networks just to avoid responsibility and liability?

After describing the environment sysadmins and sysops work in, this paper will examine the possible legal consequences of having pirated material or child pornography in a specific part of a network or on bulletin board system.

Bulletin board system (BBS) and Internet

A bulletin board system (BBS) is an electronic notice board which can be used to place all sorts of data. At the moment, the most important services provided by a typical BBS are electronic mail (messages from user to user), discussion platforms (messages from one user to multiple users) and putting software and computer files at the disposal of users. In its simplest form a BBS consists of a Personal Computer (PC) connected to the telephone network via a modem. Communication software makes it possible for users to contact the BBS from their PC via the telephone network and use the services offered on the BBS.

BBSs are established and managed by private persons as well as organization's. At the moment, about 400 BBSs are active in the Netherlands. A small number in comparison with the United States, where approximately 150000 BBSs are active. The private BBSs are often managed for fun or for idealistic purposes. Most of these systems are specialised in a subject the manager of the BBS, the sysop, is interested in. However, in the business sector in the Netherlands it seems that interest in bulletin board systems is increasing. Companies and organizationhave discovered BBSs as being a cheap way to provide client support. For example, Wegtransport, a logistics enterprise, has established a BBS on which the company makes available information on the sending of goods (No , 1994). Microsoft has a substantial number of BBSs all over the world providing support to the users of their products. The Microsoft BBS contains a database in which clients can find solutions to their problems with easy to use search software. For Microsoft, the BBS is an attractive alternative for the usual telephone support service. BBSs are also used as an alternative means for standard interchange

of information using Electronic Data Interchange (EDI; Olsthoorn, 1994).

Many BBSs are connected to an organization (e.g. Fidonet) which offers sysops the opportunity to be a part of a world-wide network of communicating bulletin board systems. Unlike Internet generally, this is not a permanent connection. A BBS periodically makes a connection with another BBS to exchange data. In turn, this other BBS makes a connection with one or more BBSs. This enables users to send data throughout the world.

The Internet hype has drawn the attention of the BBS world as well. As a result, many BBS services are also available on Internet. Thanks to its permanent connections, Internet has some significant advantages. Electronic mail (e-mail) and NetNews (a sort of Internet bulletin board) are faster and more reputable than comparable international BBS services. Moreover, Internet provides cheaper connections to world-wide computers. At present, many BBSs offer their users Internet services. Bulletin board systems like Compuserve can be reached via the telephone network as well as via Internet.

The computers that make up Internet are permanently connected to the network. E-mail and News (the Internet name for discussion platforms) can be sent from one continent to the other more quickly and reliably. The permanent connections of the Internet make it possible for a user to retrieve files and documents from a remote computer at any time in any place. And, for example, the establishment of Microsoft's Internet 'BBS', ftp.microsoft.com, eliminates the need to start a service in every individual country.

World Wide Web, the service that has brought Internet to the masses, can be seen as one huge hypertext document that is stored on a large number of computers. Clicking on a hypertext link in a document stored on a Dutch computer enables the user to retrieve a document stored on a computer in Hong Kong. This distributed way of storing information is made possible by the direct connections of the Internet.

Although a comparison between a BBS and Internet is hard to make, one might say that Internet is a gigantic BBS. BBSs offer a limited amount of services and data, but once on the Internet a huge number of data and services becomes available to the users. As BBSs have specializations, Internet has its specialities as well. Supervisors of these (special) parts in a network environment are referred to as system administrator (sysadmin), while the manager of a BBS is called a system operator (sysop). Although environment as well as tasks are slightly different, these terms are interchangeable in the framework of this paper. After all, it seems the differences between the two are becoming less distinct. Bulletin board sysops tend to have more interest in the computer network environment at present and often provide an Internet connection as well. The users of BBSs are more often participants in cyberspace, while users of Internet can consult BBSs. This paper, therefore, refers to sysadmins and sysops and their possible legal problems. And, if a reference is made to a BBS it could very well be replaced by an Internet site.

BBS, Internet and copyright

'The Internet is the world's biggest copying machine', said Marybeth Peters in U.S. News & World Report (Sussman, 1995). Supposing this statement is correct, then one would tend to think that, as a result, the Internet would lie unused. The opposite is true; according to the Internet magazine ".Net" of December 1994, 30 million people use Internet world-wide and the figure is growing at a rate of one million new users a month (Winder, 1994). This does not mean that the statement that Internet is the greatest copying machine is exaggerated. After all, according to the Software Publishers Association pirated software costs the industry 9 billion dollars a year, which means illegal copying activities must take place on a large scale (Sussman, 1995). A thread on the Internet discussion list on copyright showed copyright incidents do occur. And it would not be surprising if they will occur more often as the number of Internet users increases. In addition, the more users Internet has, the more infringements might occur, but also the more infringements might stay unnoticed.

A message on the Internet discussion list on copyright of 1 December 1994 had as its subject: 'Elvis now gone from cyberspace too'.(Internet, 1994a) This message did not mean that Elvis was alive and well in cyberspace until 1 December 1994 but had then unfortunately died and left that space too. It was a message from the Elvis Internet site which existed for almost a year. This site was created by a student at the University of North Carolina, USA, and contained snippets of Elvis recordings, photos and a 'Cyber Graceland Tour' with images of his Memphis home. However interesting, the site was disbanded at the request of the Presley estate's (Elvis Presley Enterprises Inc.) lawyers because it included copyrighted material.

In the Sega v. Maphia case, 30 USPQ.2d 1921 (N.D. Cal. 1994), a BBS was used to distribute pirated versions of Sega games. The sysop was held liable for copyright infringement, trademark infringement, and unfair competition (Internet, 1994b).

Another interesting incident is the US v. LaMacchia case. The US government wanted a wire fraud conviction against a sysop, a student, who helped himself to space on the Massachusetts Institute of Technology (MIT) computers and used

this space to trade pirated software on a non-profit basis. In fact, the MIT student ran a bulletin board system allowing users to extract copies from more than 1 million dollars worth of software at no charge. The government used the wire fraud statute to circumvent a Congressional decision which said that such actions (non-profit infringements) were not copyright violations. LaMacchia's lawyers argued that the federal government may not use the wire fraud claim to circumvent this Congressional decision (E.g., Pamela Coyle, Techno Trials, ABA Journal, 10/94 at 66). The latest news in this interesting case is that the MIT BBS software pirate, was dismissed. While calling the student's actions 'heedlessly irresponsible', the judge said the government's charges would make even legitimate copying, such as for backup purposes, illegal (Internet, 1994b; Internet, 1994c; Internet, 1994d; Sussman, 1995 (1)).

In the Netherlands, a court in Almelo seemed to have no problem with a case like US v. LaMacchia. One important distinction was that the court did not have to take into account a Congressional decision stating that giving pirated copies for free is not considered to be a copyright infringement. A young Dutch 'computer freak' had established a bulletin board system through which he had made several copies of well-known computer programs available. More than 6000 copies were found. The court did not see the actions of the Dutch sysop as being carried out as a profession or a company. It was seen as a hobby which had got out of hand. No profits had been made. Nevertheless, the Dutch court qualified the actions of the sysop as being performances and/or copying which were not authorised and convicted the man for criminal copyright violation (Rb. Almelo 1993).

Putting software at the disposal of the users of a BBS was seen as being an act of performance which would require the permission of the copyright owner. A BBS could be compared with an exhibition; it is not necessarily so that someone will come along to have a look, but it is definitely possible. The BBS is open to the public, although the public has to be well equipped to be able to 'enter' the BBS. In addition, the storage of software on a BBS can be seen as copying according to a new paragraph in the Dutch copyright act. Of course, copying is allowed to use a program for the aim it has been developed for, but storing pirated software is definitely illegal. This rule on the copying of computer programs is a result of the EC directive on the legal protection of computer software.

Although in the USA one might have slight problems in relation to protecting copyrighted material, especially if everyone starts to spread copyrighted material for free, in general one could state that the current protection of copyright, is suitable for use in cyberspace. After all, computer programs, but also digitally stored images, texts and sounds can be subject to copyright and, as a result, action can be taken against illegal copyright activities (see also Kleve 1995). As Wasch, the executive director of the Software Publishers Association, said in US World & News Report, 'copyright is elastic enough to protect material regardless of media' (Sussman, 1995). In addition, it is clear that the net is watched, which might cause a change in sysop behaviour. Less pirated software might be found on the BBSs as a result of the numerous Internet incidents.

On the other hand, contracts and licences might appear to be insufficient instrument to protect and control copyrighted material in digital networked environments. This is particularly true as the use of networks increases. As John Perry Barlow wrote 'If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without its leaving our possession, how can we protect it?' (Barlow, 1993). Therefore, attention should be paid to the possibilities of using technical solutions to protect creative works in a digital format.

In the United States, for example, a system called Electronic Copyright Management System (ECMS) has been developed (Computable, 1994). This means that in this system a key for decryption is required in order to be able to receive digitally formatted information. After having received the key, and after the information has been decoded, it can, of course, be seen, read or heard, but, in addition, data are added to the file containing information about the buyer and the supplier. Suppose the buyer of the product disseminates it digitally, his or her identity is easy to track down. This tracking down and resulting actions could, for example, be done with the help of 'cybercops' of a collective licensing body (Wees, 1995).

A slightly different but also technical approach to the copyright problems in digital networked environments is that of Barlow. Barlow wrote in "Wired", somewhat exaggerated in our opinion, that if a solution could not be found for the intellectual property problems in the digital age we would sail into the future on a sinking ship. He even states that what we know now on intellectual property law will be completely wrong within 50 years. Protection will be founded on technique (and ethics) rather than law. He writes that the technical basis for protecting most forms of intellectual property will be encryption.(Barlow, 1993) Discussions on the Internet on this now famous article indicate that Barlow has some supporters for his statement that encryption will play an important role for the protection of intellectual property in the future. In fact, the ECMS system discussed above tends to indicate that direction as well.

Another way of protecting copyrighted material will be to provide access to data only to a certain group of people or to those who pay. An example of the latter is the online legal database Westlaw. Although one cannot be sure what will happen with the data thereof.

In the cases discussed above, the sysop seemed to be the person who was held liable for infringements. It is, however,

very possible that it is not the sysop but a user of the BBS who is the infringer. A person equipped to make contact with a bulletin board could easily bring illegal material into the system. Will the sysop be liable for having pirated material on his BBS? Eugene Volokh of the UCLA Law School wrote on Internet before he had to speak on a National Information Infrastructure (NII) meeting on BBSs and Internet host liability: 'My basic thrust will be that, in the interests of fairness and progress, the law should make clear that BBS sysops and Internet host owners are not liable for their users' infringements, unless they actively help piracy in some way beyond just providing the same services that other sysops and host owners provide. (I think looking to industry custom as a benchmark is probably the best approach.)' (Internet, 1994h).

Suppose sysadmins could be held liable for the copyright infringements of their BBS users, then they could scan incoming messages to determine whether or not they contain pirated material. In the opinion of Rosenberg, only extremely diligent sysops would be prepared to check their BBS data, and he added, 'is that what we want our sysops or their employees to do?' (Rosenberg, 1994.) The world of copyright will become even more complex because of the development of multimedia applications. More copyright regimes may be applicable to just one product if it contains texts, images, sounds and software (Kleve, 1995; Loundy 1994). This will make it difficult, if not impossible, for a sysop to find out if (partly) pirated material has been uploaded to a BBS.

And, if a copyright notice indicates material is subject to copyright, the sysop still does not know whether the user had the permission of the copyright owner to use the material. However, if the sysop 'ignores' the notice and does not investigate the copyright situation will he or she be a contributor to copyright infringement by allowing the material to be disseminated on the BBS? (Loundy 1994).

Apart from the fact that it might be difficult for sysops to track down pirated material because of the increasing complexity of copyrights in the digital world, if users of BBSs start to use encryption or encryption-like methods as described above it will be as good as impossible to discover piracy. A sysop, however, could forbid users to use encryption, but then again users might use encryption methods which can hardly be distinguished from non-encrypted material (De Mulder, 1993). In short, it seems quite impractical for sysops to operate BBSs if they could be held liable for copyright infringements by the users of the system. The solution Volokh proposes, therefore, may be an appropriate one.

BBS, Internet and child pornography

One area that appears to have nearly universal agreement is the condemnation of child pornography (Rosenberg, 1994). However, because the invention of new techniques (film, video, copiers, telephone) has advantages for the information or creative industries, so they do present opportunities for child pornography exchanges as well. Child pornography producers often appear to be pioneers as far as the application of new techniques is concerned. The new trend, therefore, seems to be the exchange of child pornography via bulletin board systems and computer networks (Haaft, 1994). The invention of multimedia - combinations of image, text and sound - could be yet another 'impulse' for the child pornography 'industry' using BBSs or Internet. In combination with improving compression techniques, multimedia applications can be transmitted easily from one computer to another. Even using the 'old-fashioned' copper cables.

The Lawrence Livermore national laboratory in California fired an employee quite recently who had made himself an archive of almost 90000 'sexually explicit photos' which he had found on Internet. The man will also be sued for misusing government property. To avoid such events in the future, the laboratory is considering developing a system which can 'de-porn' their computer systems (Trouw, 1994). This event clearly indicates that pornography can and will be made easily available and disseminated via computer networks. The same will be true for child pornography.

Sysops as well as sysadmins seem to be concerned regarding the question of liability for the transmission of suspect material is being transmitted over their systems, particularly because a number of sysops have been arrested in the US and Canada and charged with disseminating child pornography (Rosenberg, 1994). A Jefferson County (Kentucky, USA) police lieutenant even broke a major child pornography ring in England without leaving Kentucky. A tip via electronic mail from a source in Switzerland led the lieutenant to an Internet site in Birmingham, England. After about 3 months of investigation that involved downloading of, amongst others, 400 images, the police officer called Interpol, New Scotland Yard and the police in Birmingham, who arrested the distributor (Sussman, 1995).

On eliminating child pornography there is an almost universal agreement exists. In cases concerning obscenities other than child pornography, the situation for sysadmins and sysops is not entirely clear. An example of such a situation concerns a Californian couple convicted by a jury in Memphis, Tennessee, for violating obscenity laws. Using a computer in Memphis, a postal inspector downloaded pictures from the couple's BBS which was based in California. The Memphis jury found that the pictures violated local community standards. An interesting aspect of this case is the fact that the pictures were downloaded from California where they were not regarded as being obscene. So it appears that people can create their own communities in cyberspace based on interests rather than geography, which might cause problems if these communities can be entered via computer networks by people who consider these interests to be

offensive (Sussman, 1995).

Another interesting story is that of the Pennsacola (Florida, USA) BBS raids. According to Internet messages, the FBI was (probably) looking for nudes being send over the net via Pennsacola BBSs. In order to find the nudes, they had done research in a pretty violent way but eventually did not even find what they were looking for (Internet, 1994i). The latter case in particular gives rise to the feeling that police officers not only feel that it is a part of their duty to enforce the law in cyberspace, but that there is also a battle going on between law enforcers and cyber civilians. The enforcers think cyberspace is a hostile, anarchistic environment and the cyber inhabitants think that the authorities want to destroy their self-regulating world. According to US News & World Report 'the Internet buzzes with stories of cops who 'arrest the equipment' by barging into BBS operations to haul off all the electronic gear, as if the machines possessed criminal minds.' (Sussman, 1995).

It is stories like those above which give sysadmins and sysops sleepless nights. Mike Godwin of the Electronic Frontier Foundation describes the nightmare scenario in Internet World: '.. you hear a knock at the door, you answer to discover grim-faced law enforcement agents holding a search warrant and you are forced to stand by helplessly while they seize your system to search it for obscene or child pornographic images' (Godwin, 1994). No surprise that a question often asked by sysadmins and sysops is: 'are we responsible for having child pornographic or pirated material on our BBSs?'.

Statutes have been made to prevent children from being sexually abused. Obviously, these statutes do have consequences for sysadmins and sysops in trying to avoid criminal liability and search and seizure actions as described above. However, the US Supreme Court has 'agreed ... to decide whether the Federal law against child pornography requires the Government to prove that those who distribute or receive sexually explicit films or photographs of minors are aware that the performers are not adults'. Furthermore, 'Under Supreme Court precedents the First Amendment bars obscenity convictions without proof that the defendant is aware of the character of the obscene material.' (Greenhouse, 1994). This means that it might be better for sysadmins and sysops not to check the material on their networks or systems. However, this could cause sysadmins and sysops to deny on a permanent basis that they know what material is on their systems. This would put the government always in the difficult position of having to prove the sysadmin or sysop awareness of having illegal material on their systems.

And, as discussed in the section on copyright, the use of encryption techniques might make it even harder for sysadmins to discover child pornographic material on their system. Even, if a sysadmin does not allow users to use encryption - which seems an impossible request in an ever growing open network environment - people might find ways to hide their pornographic material in non-pornographic material. How 'creative' people can be is indicated by a case in the Netherlands, where dealers were arrested for having hidden child pornographic material on a Walt Disney-like video tape (Haaft, 1994). On the other hand, the main function of a bulletin board or network site is the exchange of all sorts of data with all kinds of people; friends, colleagues but also strangers. Therefore, it might be quite impractical to exchange encrypted data.

At issue is whether or not the sysadmins and sysops will have a certain level of responsibility for the material on their systems. Do they just have to ignore the contents of the data to avoid possible liability claims? Do we consider these people to function as a kind of post office service, which offers the possibility to exchange data by mail without checking the contents? Or do we prefer them to check the bits and bytes and to remove them in case of copyright infringements or child pornographic material? In the latter case, they will act as a kind of censor and this option will definitely cause a reaction from freedom of speech and privacy organization's. Godwin of the Electronic Frontier Foundation stated that 'it would amount to "chilling effect" on freedom of expression if a sysadmin decided to eliminate all newsgroups with sexual content'. He also states that such a tactic will not eliminate the risk because pornographic material could easily be sent to a group of another subject. (Godwin, 1994)

Rosenberg and Godwin clearly adhere to the freedom of speech principle, and, while seemingly admitting that the sysadmins and the sysops are responsible as well. They both advise a number of measures for sysadmins and sysops to take in order to eliminate the risks of being arrested (Rosenberg, 1994; Godwin, 1994). Rosenberg adds that he prefers to create an atmosphere of net awareness through education and demonstrations of the benefits of the network environment, instead of through injunction. And, if incidents occur they must and can be solved with the legal instruments we have.

Conclusion

This paper has discussed two aspects which could cause problems for system administrators and system operators: copyright and child pornography. If the sysadmins or sysops have themselves infringed copyrights or distribute child pornography it is usually clear that their behaviour was illegal. However, if the users of the services of the sysops and the sysadmins have caused incidents, then what will be the position of the administrators and operators? In this situation, it is important to bear in mind the role sysadmins and sysops play. In relation to this any possible friction between the various rights must be examined.

Do we consider the sysadmins and sysops to be a kind of post office service? Do they only offer a platform for the exchange of all sorts of data where freedom of speech and privacy should be respected? This would dismiss sysadmins and sysops from being liable for most of their users' actions in their systems. Only if they are aware of the fact that pirated software or child pornography is in their systems can they be held responsible.

Or, should sysadmins and sysops be more active in preventing illegal material entering their systems? If so, how far should these actions go? Do they have to check every bit and byte passing through? This might cause friction as far as privacy and freedom of speech are concerned. Users will not be pleased if they know their messages are being checked thoroughly for illegal material. In case of doubt the messages might even be removed by the active sysadmin or sysop. Sysadmins and sysops will then have become a kind of network censor.

The situation seems to be as described by Godwin in US News & World Report: '... we're still in the turmoil that comes when a new medium is presented to the public and to the government. There's a tendency to first embrace it and then to fear it. And the question is, how will we respond to the fear?' (Sussman, 1995; Branscomb, 1991).

Notes

1 For more information on copyright incidents see: Internet 1994e, 1994f and 1994h.

References

Barlow, John Perry, (1994) The economy of ideas, *Wired*, March.
Branscomb, Anne W. (1991) Common Law for the Electronic Frontier, *Scientific American* , pp.112-115.
Communications, Computers and Networks, Special Issue, September.
Computable (1994)c Beveiliging voor digitaal auteursrecht, *Computable*, 11 November 1994.
Godwin, Mike (1994) The Law of the Net, Sex and the Single Sysadmin: The Risks of Carrying ... GRAPHIC SEXUAL MATERIALS, *Internet World*, March/April.
Haaft, Gonny ten, (1994) Kinderporno in tekenfilms, *Trouw*, 25 July.
Internet 1994a: Keller, Charles, summarizes an article in the Clarion Ledger, Associated Press, Chapel Hill, North Carolina, 26 November 1994, in the thread on copyright incidents on the cni-copyright discussion list on Internet, 2 December.
Internet 1994b: Schlachter, Eric, in the thread on copyright incidents on the cni-copyright discussion list on Internet, 9 December.
Internet 1994c: Noble, John F., Editor, Computer Law Reporter, in the thread on copyright incidents on the cni-copyright discussion list on Internet, 10 December. John F. Noble also mentioned the David LaMacchia Defense Fund World Wide Web site for more information on this interesting case: http://www-swiss.ai.mit.edu/dldf/home.html.
Internet 1994d: Newsflash in the thread on copyright incidents on the cni-copyright discussion list on Internet, 30 December 1994.
Internet 1994e: Brandt Jensen, Mary, Professor of Law, University of South Dakota, in the thread on copyright incidents on the cni-copyright discussion list on Internet, 9 and 10 December 1994.
Internet 1994f: Arnold-Moore, Tim, University of Melbourne Law School, in the thread on copyright incidents on the cni-copyright discussion list on Internet, 14 December 1994.
Internet 1994g: A forwarded message in the thread on copyright incidents on the cni-copyright discussion list on Internet, 14 December 1994.
Internet 1994h: Volokh, Eugene, Acting Professor, UCLA Law School, USA.
Internet 1994I: A message forwarded to the copyright discussion list on 14 December 1994, gives a short outline on the Pennsacola BBS raids.
Kleve, P., and J.G.L. van der Wees (1995) Multimedia and copyright, to be published in the proceedings of IVR '95, Bologna, Italy, June.
Loundy, David. J. (1994) Computer information systems and system operator liability, E-Law 2.0., david@home.interaccess.com.
Mulder, R.V. De (1994) Wetgeving maakt technologie tot veelkoppige draak. In: Nederlands Juristenblad jaargang 68, nummer 39, 4 November.
Noe, Frank (1994) BBS: de elektronische binnenweg, Automatisering Gids, 28 January.
Olsthoorn, Peter (1994) BBS neemt moeiteloos rol Edifact over, Automatisering Gids, 26 August.
Rb. Almelo 1993: Softwarepiraterij - bezit ongekeurde draadloze telefoon, Arondissementsrechtbank Almelo, 12 November 1991, met noot Elisabeth P.M. Thole, Computerrecht, 1993/5.
Rosenberg, Richard S. (1994) Free speech, pornography, sexual harassment, and electronic networks: an update and extension, in: *The Electronic Superhighway, the shape of technology and law to come* (proceedings), Faculte de droit, Centre de recherche en droit public, Montreal, Canada.
Sussman, Vic (1995) Policing cyberspace, U.S.News & World Report, January 23.
Trouw 1994: Tien miljoen dollar om computerschijf te ontgeilen, Trouw, 29 September.
Wees 19: Netwerk + Auteursrecht = Encryptie?, BGGN net-nieuws, jaargang 4, nummer 1.
Winder, Davey (1994) Easy Internet,. *Net*, Future Publishing, Avon, UK, December.