ETHICAL ISSUES IN NETWORK SYSTEM DESIGN

Duncan Langford
Computing Laboratory
The University
Canterbury
Kent, CT2 7NF
D.Langford@ukc.ac.uk

ABSTRACT

Today, most desktop computers and PCs are networked — that is, they have the ability to link to other machines, usually to access data and other information held remotely. Such machines may sometimes be connected directly to each other, as part of an office or company computer system. More frequently, however, connected machines are at a considerable distance from each other, typically connected through links to global systems such as the Internet, or WorldWideWeb (WWW). The networked machine itself may be anything from a powerful company computer with direct Internet connections, to a small hobbyist machine, accessing a bulletin board through telephone and modem.

It is important to remember that, whatever the type or the location of networked machines, their access to the network, and the network itself, was planned and constructed following deliberate design considerations.

In this paper I discuss some ways in which the technical design of computer systems might appropriately be influenced by ethical issues, and examine pressures on computer scientists and others to technically control network-related actions perceived as 'unethical'. After examination of the current situation, I draw together the issues, and conclude by suggesting some ethically based recommendations for the future design of networked systems.

INTRODUCTION

Consensus definitions in this field are sometimes difficult. For example, information systems specialists may argue that any computer network is an information system; while hardware engineers, approaching the same point from a different direction, might consider physically linking one or more computers in such a way that they can share data forms a computer network automatically.

Computer networks themselves, of course, might be further classified according to their geographical extent: Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN). Networks may also be grouped according to the specific protocols used, and indeed by a wide variety of other measures. For our purposes, however, such specialist distinctions are an unnecessary complication. We may consider computer networks as principally falling into just two groups, one a sub-set of the other. These groups, discussed below, are closed networks, and open (or Internet linked) networks.

To most users, networking design decisions are essentially invisible. In reality, user consideration of networked computer systems operation is probably limited to visible problems — complaints about connection speeds being among the most common. Such an emphasis is quite understandable, as designers of networked computer systems have always been principally concerned with technical issues. Systems analysis, which provides explicit design criteria, may take on board user pressure for facilities, but traditionally — legal questions aside — designers of networked systems normally only respond to non-technical issues if such consideration is directly requested by a client.

Focusing of this kind is certainly comprehensible. Limited budgets and heavy pressures on development time combine to reduce space for consideration of wider issues, especially problems that are not clearly an essential part of the technical specification.

However, whether or not appreciated by client or development team, there *are* wider questions that have an important role to play in the development of modern networked systems. Increasingly, society is no longer prepared to allow the free development of networked computer systems — especially globally networked systems.

The definition of 'network design' used in this paper is consequently broad. It covers not only the physical arrangement of connections and links, but also the negotiated steps through which individual users must pass to obtain networked communication.

As an example, consider a user employing a service provider in order to obtain access to an Internet hub. To obtain a view of their local-to-user facilities, aspects such as links to service provider, links from service provider to hub — and, of course, the Internet itself — all need to be examined. Distance between computing systems is not considered (as this is a communications media problem); the size of the computing system is similarly irrelevant.

My intention is to look beyond the immediate appearance of a networked system, to what lies behind it.

CLOSED NETWORKS

The simplest form of networking is probably micro-micro linking. This is usually in the form of an uncomplicated connection of one PC to another, so each may exchange information and data. Further machines may be added, in the form micro-micro*N (where N is a potentially large number). The result is the linking of a *group* of computers together, so that each may communicate and share information with any or all of the others. Such a connection, which typically permits local email (electronic mail) together with exchange of data and files, is probably the most common type of office system. FIGURE ONE, below, represents one typical way in which a closed group of computers may be linked.

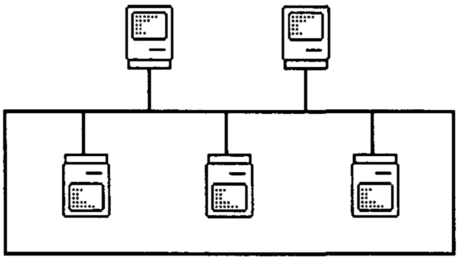

FIGURE ONE: A TYPICAL 'CLOSED' NETWORK

The original small loop may of course be extended, to take in further machines located elsewhere in a building. Additionally, a series of such network loops may themselves be linked together, or even (using telephone or other links) connected with machines and similar networks in different geographical locations. Although this may appear to be moving beyond the definition of a closed network, the essential aspect of a closed system remains: however large a 'closed' system may become, no connection is ever possible to machines outside the organisation.

Both closed and open networks may need a 'server', which in this context is a dedicated machine used to handle communication issues. The client-server communication is normally in the form of request and response messages — a client machine sends requests to the server, and reads responses returned by the server. This dialogue permits, for example, the exchange of electronic mail, as well as other communication matters, such as file transfers. Exact details of the request and response formats are less important than that they occur. It is particularly important to note that in these circumstances communications are invisibly handled by a computer that is outside the direct control of the user.

Closed networks, then, are those where a potentially large number of computers are linked together. The size of the network and the physical location of the involved computers are irrelevant, *provided* no link has been made which extends communication beyond the limits of the concerned organisation.

Ethical issues in closed networks

It must be remembered that to ensure effective operation, all computer networks must be administered, or serviced. By definition, the individual carrying out administrative duties has to be allowed complete control of 'their' system. This inevitably means that an individual user is totally dependent upon the ethical views of their administrator. If a relaxed view is taken on examination of data, no file can be private; no mail safe. If an organisation has not established clear rules and guidelines, there is little beyond an individual sense of responsibility to prevent a network administrator misusing their privileges. Such misuse is, of course, quite invisible to individual users, who may be quite unaware of any interference with their data.

Sometimes, a company itself may rely on unethical network systems administration:

> Dave was employed as a computer specialist by a medium-sized company, principally to support their network and electronic mail. It became clear that the Technical Director, who had originally set up the mail system, maintained a log of all email messages, and made copies of all private mail of interest to him. Dave learned he was expected to continue monitoring mail (although, interestingly, was told not to actually read it himself), and to pass on copies of mail from and to selected employees.
>
> (Langford, 1995)

The ethical issues involved in monitoring of networks are clear — users of closed network systems surely need to be aware of any external oversight of their work. It is insufficient and impractical to leave such issues undefined, in the hope that individuals will eventually work something out for themselves. In these circumstances, it is the responsibility of management to clarify company expectations of employee behaviour. If the sort of monitoring experienced by Dave is felt to be necessary, management should at least be open about it. Secret monitoring of network use can be hard to justify ethically.

OPEN NETWORKS

As would be expected, an 'open' network provides all the resources of a closed network system, but with a significant added link. This link, normally made through an Internet Service Provider (ISP), gives an additional channel that allows communication to the Internet — and hence to other computers and networks throughout the world.

FIGURE TWO illustrates a typical arrangement. The original computer (or closed network) located at (A) establishes links with a 'proxy server', (B). This server can act as a local store of external information — to prevent frequent reloading of the same data. It is directly controlled by company (A), who may monitor and set limits on its use. The use of a proxy server has an additional positive role, in providing a 'firewall', helping prevent attack by external 'hackers' on company systems.

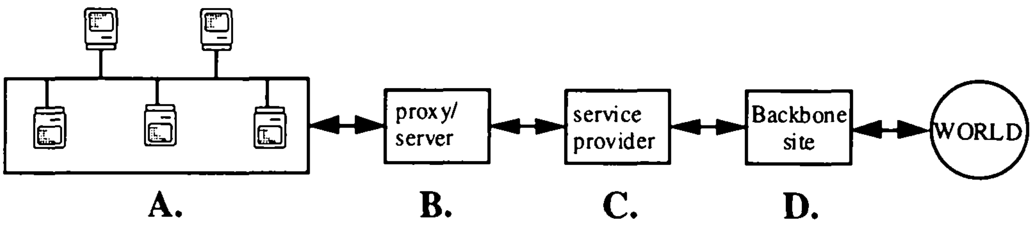

FIGURE TWO: A TYPICAL 'OPEN' NETWORK

This server in turn is connected to an external 'service provider'. There has been an explosive growth in service providers — companies who exist in order to sell Internet connections. They are very roughly analogous to those businesses who sell portable telephones, and who, without themselves owning a network, arrange connection to one of the mobile 'phone networks. Their activities are beyond the immediate control of those purchasing their services, and even further beyond the individual user of a company computer.

All Internet service providers must make a further connection, to a national 'backbone site'; this site (which is, again, under the control of a different set of administrators) is directly connected to the wider Internet.

This series of network links is always followed, except in the case of a single user. Here, rather than using a proxy/server, the proxy stage is often omitted. Personal computer and small company users normally establish a direct link to their service provider, generally by telephoning a special modem number.

Ethical issues in open networks

We may have a situation where an individual company user may wish, for example, to access a WordWideWeb site in another country. FIGURE TWO shows the steps that must be progressed; but what does passing through this succession of links mean in practice?

First, only the original computer is under the direct control of the user. (In the case of a company computer network, of course, even this may not be true.) All other stages in the connection of user to Internet are, inevitably, dependent upon others, and may consequently generally be controlled and influenced by factors that are external to the user. Such control can be, and normally is, invisible.

Secondly, because access to the Internet involves access to, and distribution of, information and data, it is important to appreciate that *specific* access might be limited or controlled.

Thirdly, the technical limitations inherent in a networked system can themselves restrict access. For example, there is a straightforward relationship between the volume of traffic carried by a network, and its functional efficiency. The dramatic growth of Internet traffic has resulted in difficulties in speed and access to many users. Such problems — despite increases in network bandwidth — can only grow worse. The demands of large numbers of new Internet users are compounded by technical advances, such as the bandwidth demands of full motion Internet video. Routing algorithms and hardware decisions taken to offset these problems must inevitably affect individual users.

SPECIFIC ISSUES

So far I have discussed the way in which a simple closed network is controlled, and have examined the stages through which information must pass when a closed network becomes 'open', through connection to the wider Internet. I will now look briefly at each level of network control, identifying specific points that may repay further ethical investigation.

Local network management

A local network administrator has the ability to access, modify and delete all files of all local users. It is therefore important that the responsible managers have clearly defined their expectations of their administrators, and that individual administrators are working within clear and understandable rules and guidelines.

Furthermore, it is essential that users of the networked system are aware of measures that are taken to control the system they use, and are told, for example, if specific monitoring procedures are in place. While it is reasonable for a company to ensure its technical resources are not being used to support the private interests of its staff, secret monitoring and logging of staff access to Web sites may be hard to justify ethically.

A local proxy/server has the ability to keep a detailed log file of its operations — monitoring of use is consequently trivially easy. Should employers monitor this information? James Derk works for the Indiana based *Evansville Courier.* His views are those of a concerned and informed professional:

> The original post (on the subject of newsroom Internet monitoring) said nothing about reading personal E-mail. It talked about looking in the Netscape cache, which I agreed was potentially slimy. However it is certainly less an invasion of privacy--on a company owned computer-- than reading E-mail, which I can't condone under any circumstances. It's also dreadfully easy.
>
> (IRE mailing list, 1996)

Company oversight of employee network use is clearly an ethical issue; but there is an additional way in which a local proxy may be used to control individual users. This is by forbidding them access to certain sites that are felt 'unsuitable'. This restriction is directly comparable with the employment, by an individual user, of an application such as 'Net Nanny'. (One of a number of commercial applications that interfere with the operation of an Internet browser.) Individual network users may wish to prevent, for example, their children accessing pornography. Restriction of this sort, whether by employer or parent, is understandable, and may be perfectly justifiable, with certain provisos. Not the least important proviso is that the censoring process is 'open', and the justification for it made clear.

However, use of Nanny-type applications may not be without further ethical problems. Recent disturbing allegations concerning the nature of these programs have emerged from the USA. Commercial gate keeping applications must, inevitably, contain a list of 'forbidden' Internet sites and news groups, those which they consider should not be accessed. Although this information is coded, following a 'hacker' cracking lists for most of the popular gate keeping applications have been revealed. It appears lists of forbidden sites may not be limited to pornography. Political and other censorship may also be taking place, all the more disturbing because it is hidden.

Whether it is true or not — I have been assured by a US journalist of its truth — this case illustrates the relevance of ethical oversight. Use of guardian applications and control of local proxy hosts surely need informed consideration and evaluation.

Service Provider (ISP) issues

Internet Service Providers (ISPs) simply act as distribution points (and collection points) for Internet data. They are in effect acting as a clearing house for information, and, as a commercial service, have to convince customers that their provision is preferable to that of another company. Because the service itself — Internet connection — is virtually identical, service providers have to maintain a distinction in other ways. The chief ethical problem they face is probably that of the distribution of 'pornography' and other material perceived by some as inappropriate. Here they are in a classic cleft stick, bound to upset some customers whatever their choice. If they operate a restricted service, forbidding access to 'undesirable Web sites and refusing to relay 'inappropriate' Internet news groups (such as the infamous alt.sex. hierarchy) then a large proportion of prospective customers, aware of the free speech ethos of the Internet, will just go elsewhere. On the other hand, if such material is made freely available, then the provider is liable to be the focus of public anger, and perhaps legal action.

For example, in February 1996, the state prosecutors of Bavaria and Baden-Wuerttemburg were concerned over Internet dissemination of neo-Nazi Ernst Zuendel's views. The major international ISP CompuServe, under threat for providing access, responded by preventing their German subscribers from viewing certain Usenet news groups. Unfortunately, as there was no easy way of screening out German users, this effected CompuServe subscribers globally, and resulted in massive protest. However, despite the enormous inconvenience CompuServe's attempted censorship caused, the attempt to completely block access could not have worked without additionally closing down the whole of Deutsche Telekom. German users could otherwise just use ordinary modems and standard voice lines to access any alternative ISP in any country.

Of course, viewing censorship as a solution to network information problems is not limited to sensitive German authorities. As *Guardian* journalist Jack Schofield put it:

> The problem with censoring the Internet is that somebody somewhere objects to almost everything. If local German authorities can remove all the right wing content, and all the pornography, then why shouldn't the Chinese remove all traces of capitalism? Why shouldn't American fundamentalist states ban any sites concerned with evolution? Why shouldn't the Vatican demand the removal of all references to birth control? Indeed, a few countries with radical views could quickly remove all religious, scientific and economic debate from the Internet, then all we'd need is a militant vegetarian state to finish things off....
>
> (*Guardian*, 1996)

If outright banning is not possible, what about monitoring and checking data, to ensure no illicit material is being conveyed? Sadly, this too is impossible. Searching the enormous quantity of data that flows through an average ISP is not currently remotely practical — even expensive routers can hardly keep up with forwarding the data. There is certainly no spare capacity to comb traffic for suspect material, even if the inevitable delays this would cause were acceptable. It is barely possible that this situation may change as technology develops further, although, of course, so far use of the Internet is increasing at a far faster rate than technology.

A further ethical problem is related to the 'permission' which ISPs automatically give to their customers to use the Internet, more specifically the ability this provides to easily send limitless quantities of electronic mail. Some of this mail is merely uninformed, and annoying to other users. However, some is intended purely for commercial purposes, and sent very widely — 'spamming', in net speak. Traditionally, the Internet has had a non-commercial philosophy, but even the most tolerant of users can very rapidly grow tired of endless junk email. Can such proliferation of mail be controlled? Perhaps not easily, although one contributor to a discussion on the UK Government's ethics mailing list felt it might, by hitting the ISPs where it hurt:

> ...I do see a role for contractual sanctions after the event however. I would suggest that writing an enforceable contract with financial penalties for say, unsolicited commercial email, or commercial spam would be quite straightforward. If enough ISP's took the position that such activities were a no-no, those that continued to allow them could simply be declared rogue. If any one who connected through them couldn't access any major services, they wouldn't last long.
>
> (UK ethics news group, 1996)

Acting as the focus for users to obtain access to the Internet, ISPs perhaps inevitably provide a focus for ethical debate, too. Their responsibilities, to the communities they serve, the wider population, and the Internet itself, have not yet been the subject of informed debate. Such debate is perhaps overdue.

'backbone site' issues

All practical aspects of operating a national backbone site are related to keeping it operational. Several times, speaking to those involved, I was told that the issue is not how to analyse or monitor transmitted data, but how to keep the system running at all. Backbone sites are very much at the hard edge of technological network development. Backbone sites are even less open to monitoring and control than ISPs. As discussed above, the only viable option open to a government intent on control of the Internet would be to close down their entire communications system — an impossible choice, given the dependence of modern society on international networking thorough Internet links. Even then, of course, the action would be comparable to sawing off a small branch in an attempt to fell a large tree.

SUMMARY

In this paper I have examined the stages through which an individual user may obtain access to the Internet. Looking first at the mechanics of setting up a 'closed' network, I urged that the role of a network administrator is considered carefully, and that their supervision of 'their' network is carried out under clearly defined rules and expectations.

I then looked at the expanding of 'closed' networks into 'open' ones — networks with an onward connection to the wider Internet. The part played by a proxy/server, which provides an essential link between networks, was significant here. A specific issue was use made of data passing through a company owned server — particularly data monitoring by employers.

Finally, I looked at the part played in network communication by ISPs — Internet Service Providers. They have a difficult task, in both facilitating their customer's access to Internet material, and, potentially, limiting access, too. The way in which this is done is clearly important. It is ethically dubious to secretly restrict users from obtaining desired links, particularly if the censorship is carried out under a political agenda.

CONCLUSIONS

Although there may be immediate points to be made, there seems a clear case for debate. Should the design of a networked system, at whatever scale, have as part of its technical design cycle, deliberate consideration of ethical issues? Ought a company which purchases and installs a closed network consider first how that network should be used? When a provider of an Internet link has the ability to restrict access in any way, would it be reasonable to insist that such a restriction is made explicit? Can we depend upon politicians and government to appreciate the technical impossibility of co-ordinated global Internet censorship — the only censorship that could possibly work?

The ease with which it is possible to generate such questions shows a debate is long overdue. I suggest that at their heart is the need for acceptance of a single issue — serious consideration of non-technical issues in the design and development of networked computer systems.

REFERENCES

Ethics group (1996). ethics@ccta.gov.uk, 26 April.
Guardian (1996). Guardian OnLine, 26 January.
IRE mailing list (1996). Investigative Reporters & Editors mailing list (www.reporter.org), 14 February.
Langford, D. (1995) **Practical Computer Ethics**, McGraw-Hill, London.