Unfinished Chapters on Internet Ethics

Michael A. Covington
Artificial Intelligence Center
The University of Georgia
Athens, GA 30602 U.S.A.
mc@uga.edu

Printed July 5, 2008.

This material was originally written for a collaborative book project that was not published.

Contents

Chapter 1

First principles

This is a book about the neglected *human* side of computer security and ethics, especially on the Internet. We believe firmly that accountability is for humans, not just for machines. We feel that for a long time there has been too much emphasis on making computers "more secure" by technical means, and not enough emphasis on human responsibility and human cooperation. In the following chapters we will explore just what this implies.

This book is written for non-experts; we hope that the experts won't feel that we're talking down to them. If you're an expert, feel free to skip any chapter that is telling you things you already know. If you're new to computers, pay close attention to Chapter ***, which explains how the Internet works, and other chapters that fill supply technical background information.

1.1 Accountability is for humans, not machines

Before we look at computer security, consider a much more mundane piece of security technology – the lock on your front door. It keeps out burglars, right? Well, not exactly. It's perfectly possible to break down a locked door or even to pick a lock; people do it every day.

Yet the lock *does* prevent burglaries. The reason it works is that society

catches burglars and punishes them. The lock doesn't make burglarly impossible; it just makes it more easily detectable. Its main purpose is to distinguish between forced entries and normal ones, and to prevent honest mistakes, such as people wandering into the wrong apartment. The lock doesn't prevent crime by itself; it helps society hold people accountable for what they do.

If you forgot that, you'd have a strange perspective on burglary. No burglar claims a right to go around trying to pick locks and to enter the houses whose locks he can pick. Yet computer "crackers" make analogous claims routinely, and they often get their victims to believe them. "Our computer got cracked (broken into via the Internet) because its security software wasn't up to date." Well, yes, but that's like saying your house got broken into because you didn't have the very latest model of lock. The real reason your computer got cracked is that someone chose to crack it.

That is why it's vitally important for the computer-using community to develop a shared sense of ethics. The biggest reason houses seldom get burglarized is that ordinary people know that burglary is wrong and won't tolerate it. They don't ignore signs of burglary when they see them; still less do they admire a neighbor's tales of successful lockpicking. Computer security needs to work the same way.

Moreover, deliberate tampering is not the whole of computer security, and it hasn't been since the world's computers got networked. The Internet is a community with its own rules, and well-meaning people transgress these rules every day, often coming into bitter yet unexpected conflicts. Newcomers to the Internet community need lots of guidance about how to live together online.

Consider for example the controversy over advertising by e-mail ("spamming"). Plenty of entrepreneurs see nothing wrong with e-mailing their sales pitch to millions of people. After all, the advertisements cost them almost nothing to send out. But many people object very strongly to receiving e-mailed ads. The reason? E-mail imposes costs on the recipient. The reason it costs so little to send out is that the delivery costs are borne at the receiving end. Not only that, but receiving unwanted e-mail takes appreciable time – as much as several minutes for a long message through a slow modem – during which other communication is slow or impossible. And *that* puts spamming in a whole new light. If you didn't

know that e-mail costs money and time at the receiving end, you wouldn't see why spamming is objectionable.

Besides simple economic factors, there are community standards. Even if spam were not expensive to receive, the fact would remain that the Internet community, by and large, objects strongly to it. In the same way, the community objects to off-topic messages in discussion forums (such as used-car ads in *rec.pets.aquaria* or *sci.chem*). There is even a strong unwritten rule against debating whether a previous message is off-topic, since that wastes even more time than the original off-topic message would have done. This and other unwritten rules have stood the test of time, but if you're new to the Internet, you won't know about them. As we'll see, good intentions are not enough; on the Internet you are always other people's guest, and you have to know what the community expects of you.

We are therefore not here to offer a new technical panacea. In this book we will cover some basic technical issues, but we refer you to technical security handbooks – of which there are many – for further details. In so doing we also have a word of caution: don't lose the big picture through preoccupation with details. Remember that computers don't have a life of their own; instances of computer misuse are human acts, not natural phenomena; and that if anyone built a perfectly secure computer, it would probably not be versatile enough to be useful.

We are also not here to stir up panic. We realize (and the Year 2000 Problem has demonstrated) that it's easy to sell books by scaring people about relatively minor hazards. We have resisted this temptation. Precisely because we see computer security as a human problem, we have confidence in human means of dealing with it.

1.2 Security is for the whole community

Because computer security is a human matter, it cannot be left to specialists. All too often, particularly at universities, a computer technician is expected to be judge, jury, and executioner in cases of misconduct. That's an unwise practice; it requires technicians to do things

for which they not trained, and exposes them to possible lawsuits if they blunder.

A busy technician handling an incident generally wants to take limited, quick action (such as cancelling an account) and get it over with as quickly as possible. That often imposes too little punishment on the determined computer abuser, who was planning on losing the account anyway and has others already open under assumed names. For these and other reasons, decisions about guilt and punishment should be made by those qualified and authorized to do so.

More importantly, the whole community, not just the authorities, needs to know what is proper and improper use of the computer. We emphasize throughout this book that good intentions are not enough; people must actually know the rules by which the community lives.

Three things go wrong if computer users aren't adequately educated about ethics and security. First, as Will Rogers put it, they'll "know things that ain't so." Some people will assume they have rights that they don't really have; in particular, they'll confuse what is legal *on the Internet* with what is permissible *on a particular computer,* such as their employer's, which may not have capacity to spare for their personal pursuits. Others will assume, without warrant, that their computer usage is heavily restricted; they can't understand why so much of what looks like pure recreation is permitted on their school's or employer's computer.

Second, lots of time will be wasted by pranks and nonsense. Plenty of hoaxes are circulating by e-mail; some of them go back many years and will apparently never die. If people get e-mail that says, "Urgent virus warning – mail this to all your friends," or "This pyramid scheme is legal," or "Tell everybody to send postcards to Craig Shergold," will they be wise enough to be skeptical, or will they continue to clog up networks with useless messages? We return to e-mail hoaxes on page **??**.

Third, people can be manipulated for malicious purposes. Can a stranger get a user's password by phoning and saying, "This is so-and-so in the computer center and I'm working on your account…"? Quite often, yes. Plenty of people will believe any authoritative-sounding message on the telephone or in e-mail, unless explicitly warned to look out for tricks.

Any computer-based community, and particularly the Internet, is an

unfamiliar place where ordinary people often have to make ethical decisions about unfamiliar acts. They need explicit instruction. Following the crowd or doing what one has always done is not enough.

1.3 Cyberspace is not a place

Some people say the Internet exists in "cyberspace," a new kind of non-physical place where information can be stored, business can be transacted, and people can interact. The implication is often that cyberspace is a radically new environment where society's laws and conventions do not apply.

We consider this a misconception. First, cyberspace is not new. It has existed at least since the ancient Greeks invented paper money, making it possible to trade gold and silver without carrying them around or even knowing precisely where they were kept.

Second, cyberspace is not a place. Every computer, and every computer user, is located in a particular place on Planet Earth and is subject to the local laws. Sometimes a computer-based activity is spread over different countries in a complex way, but – in principle – this is no different from the telephone, telegraph, and radio networks, or even banking systems, that existed in pre-computer days.

Third, even if cyberspace *were* a place, you wouldn't be the only person in it. Computer networks are fundamentally a means of communication between *people*. Fundamentally, the reason you can't escape human society on the Internet is that the Internet is part of human society.

1.4 Three generations of Internet users

Newcomers to the Internet are sometimes unaware that the Internet is not a company and does not have a headquarters. As its name implies, it's a network of networks that have linked together voluntarily. The most fundamental principle of Internet ethics is that each subnetwork – each network controlled by a particular company or institution – is the guest

of all the others. We will explore this further in Chapter ***.

People have joined the Internet in at least three major waves. Each wave brought in a different set of people with different expectations, and the process of harmonizing them has not always gone smoothly.[1]

The first wave comprises academics – professors, students, and employees of research labs – who used the Internet in the 1980s, before it became commercial. They relied on their colleagues to have a very high degree of professionalism, personal responsibility, and eagerness to cooperate and build up the community. Not only that, but the network was totally non-commercial; private individuals never paid for computer access, and commercial use of the network was strictly forbidden.

Some of the old-timers of the Internet view the Net's subsequent development as nothing but a decline. They remember the courtesy, mutual respect, and high ethical standards of what was, at one time, an all-professional community of people profoundly grateful for the expensive, heavily subsidized network they were allowed to use. They are dismayed when principles of ethics that they worked out years ago seem to be entirely lost on the newer generations.

It would be a serious mistake either to disregard the old-timers of the Internet or to enthrone them as unquestioned authorities. They are the people who know how the Internet came to be what it is. Often, they will recall that some modern proposal (for censorship, for instance) was tried and proved infeasible long ago. At the same time, they are not only people for whom the present Internet should cater. Their nostalgia is that of the old aristocracy, not the new middle class, and like landed aristocrats, they are accustomed to a subsidized environment that can't be extended to everyone.

The second wave comprises computer hobbyists or enthusiasts who joined the Internet when private commercial accounts became available in the mid-1990s, often coming in from earlier commercial networks such as America Online or CompuServe. Their appearance on the Net caused immediate conflict because their assumptions were so different from those of the first wave; there were jokes about how "aol.com" implied

[1] In case you're wondering, the authors of this book are a first-waver (Covington, who was on BITNET in 1979) and a third-waver (Larson).

ignorance or ineptitude.

The problem was twofold. The newcomers were paying for access, so they often felt, quite mistakenly, that they were paying the whole cost of whatever they wanted to do, such as sending out mass mailings or posting irrelevant messages in forums. At first, nobody made it clear to them that a commercial Internet account is only an admission ticket; once you get on the Net you are still other people's guest. When you post a message in a newsgroup, for example, you are, at most, only paying for it to be posted on one machine. The other machines on other subnetworks pick it up voluntarily, and they are relying on you not to misuse the Internet.

The newcomers also failed to appreciate that not everyone on the Net was a hobbyist. Michael Covington remembers once, late at night, getting a "talk" request from someone in Australia. Did he need urgent help with something, or at least have a pertinent question? No; he just wanted to chat. It didn't occur to him that Covington was at work. Of course, he's not entirely to blame. You can't always tell from an address whether the person using it is at liberty to surf the Net and correspond with pen-pals.

Since then, a third wave has appeared. The newest Internet users are neither research professionals nor computer enthusiasts; they are people who are on the Internet because they need its services, either for work or for personal interests. (It's like the shift from people in the 1920s who were interested in radio technology to people in the 1940s who merely wanted to hear things on the radio.) These are people for whom the *Internet* may be a hobby but the *computer* isn't.

As regards computer ethics, third-wavers are a diverse lot. Many of them have plenty of common sense from their experience in business and other human activities. Unlike first- and second-wavers, they don't consider themselves a privileged elite. On the other hand, they sometimes misjudge the culture of the Internet, largely because they don't know its history. In the old days, the Internet was a research network and commercial use was flatly forbidden. Nowadays, advertising and commerce are permitted, but only if you pay your own way, and it takes some knowledge to sort out exactly what that entails. Some third-wavers are all too easily recruited into spamming, pyramid schemes, or other money-making schemes that the Internet community considers highly

unwelcome.

1.5 The hot issues change from year to year

The hot issues in computer security have not always been the same. Before 1980, practically the only issue was deliberate tampering with business records, a concern that remains, but has been dealt with by developing standard techniques.

In the early 1980s, computer games became common, and a major concern was recreational use of one's employer's or school's computer. (There was often real doubt whether this cost anybody anything.) Thanks to the falling price of personal computers and the availability of private Internet access, work-versus-play is no longer such a hot issue.

Meanwhile, in the late 1980s, there was an epidemic of account cracking, fueled by (false) legends that successful crackers would be rewarded with high-paying jobs; cracking then went out of fashion but has recently reappeared, together with the legends that fueled it.

The late 1980s and early 1990s saw a wave of quarrels in online discussion forums. When newsgroups first became available to the public, many users failed to realize that every user is everyone else's guest; newsgroups are paid for by the whole community (not just the site to which you are paying an access fee) and each newsgroup is reserved for a specific subject. Advertising a car for sale in *rec.pets.aquaria* is not and never has been welcome. Eventually, most people caught on; "cancelbots" (p. ****) were deployed to deal with really obnoxious misusers; and the problem diminished.

By the mid-1990s, the hottest issue was improper commercialism: unwelcome e-mailed advertisements ("spam"), schemes to make money privately with an employer's or school's computer, and even gambling and pyramid schemes. As you will see throughout this book, this problem has not yet been solved; it is still a major source of friction, especially since the people most eager to make money are usually dishonest, and their messages are not merely annoying but actually fraudulent. More about this in later chapters.

The next hot issue will be copyright. The World Wide Web has made it easy for ordinary people to reach large audiences. Unfortunately, newcomers to web publishing often fail to realize that it is wrong (and illegal) to republish other people's material without their permission. Copyright infringements that were overlooked during early experiments are going to raise serious objections as online publishing ceases to be experimental. Meanwhile, it is often genuinely unclear how laws designed for book publishers should apply to the World Wide Web. Many issues will have to be worked out in a combination of legislation, court decisions, and user education.

Coming up next will be the issue of computer reliability. This is not specific to the Internet, but there's trouble brewing: the Year 2000 Problem demonstrated just how little confidence manufacturers have in their products, and we are now in the comical situation of having software that is guaranteed to calculate the date correctly but not guaranteed to do anything else. We predict that by 2005, the public will be demanding that hardware and software makers stand behind their products. Disclaimers that were appropriate for experimental products in 1976 are not appropriate today.

Whatever happens, the next ten years of personal computing and the Internet are not going to be dull.

Chapter 2

Computers and the People who Use Them

A key point in computer ethics, and in the management of computer-using communities, is that computer users are not all alike. For some, the computer is inherently fascinating and opens up a new world to explore; for others, it is just a tool with which they do their jobs.

Because of this, different people approach computer ethics with different preconceptions. Some people see the Internet as a radically new society to which existing laws and rules need not apply; others see it as an extension of society's existing institutions. We call these the *old-world* and *new-world* approaches to computer ethics. They arise indirectly from another cultural split, that between *power users* and *utilitarian users* of personal computers.

Power users are instinctive computer enthusiasts. Regardless of their background, when given the opportunity they become self-taught computer experts, and this expertise becomes part of their self-image. From the management perspective they are either very valuable, because they enjoy helping their colleagues, or constantly troublesome, because they consider themselves exempt from ordinary people's policies or because their computer experiments disrupt their own or other people's work.

Utilitarian users are those for whom the computer is a means, not an end.

They're using the computer to get some kind of work done, whether it's word processing, accounting, or even scientific research, and if the work didn't require a computer, they wouldn't use one.

The distinction is not just a matter of degree of expertise. Some utilitarian users have plenty of technical knowledge. What's crucial is that no matter how much they know about computers, they don't consider computing their specialty, and they have little inclination to explore capabilities of the computer that are not relevant to their real work.[1]

As you might guess, utilitarian users are inclined toward the old-world approach to computer ethics, and power users are inclined (though not compelled) to take the new-world view. To leave it at that, however, would be a dangerous oversimplification. There have been many cultural splits between one group of computer users and another, and at this point we must review some history.[2] Not only are there different kinds of users, but the proportion of each type at any given site is also constantly shifting.

2.1 The rise, fall, and rise of the computer priesthood

When mainframe computers appeared in the business world in the late 1950s, people were in awe of the "giant brains" or "thinking machines" as they were often called. These machines were tremendously expensive but also tremendously efficient at menial data-processing tasks. Since these were *computing* machines, it was taken for granted that the people who programmed them were mathematical geniuses. Computer programmers and operators became like priests, mediating between ordinary mortals and the powerful machines. The term "computer priesthood" was used to describe this situation almost from the beginning.

[1] Of the authors, Covington is a power user and Larson is a utilitarian user. The term *power user* has been widely used since the 1980s; *utilitarian user* is our own term, introduced by Covington in "Design and Implementation of a Campus Computer Ethics Policy," *Internet Research* 5.4:31–41 (1995).

[2] I want to thank Bob Stearns for helpful comments on this chapter. —M.C.

The priesthood culture was reinforced by the fact that computers were often very hard to use, and no one seemed interested in making them easier. Software was always created and used by very experienced specialists. A simple act like copying a file – done nowadays by dragging an icon or typing a one-line command – could easily require ten lines of intricate IBM JCL (Job Control Language), delivered to the computer on punched cards. The art of using computers seemed, to outsiders, to consist of closely guarded secrets thought to be beyond the grasp of people of ordinary intelligence.

Back then, there were no personal computers, and outside of schools and research labs, there were no computer *users* in the modern sense. Technical specialists programmed and ran the computers; everyone else just supplied data or received results. Very few individuals used a computer, single-handedly, for their own work. Timesharing systems at educational institutions gave some people a foretaste of what personal computing was going to be like, but most of the public had no contact with it.

The Altair microcomputer in 1974 and the Apple II in 1977 suddenly put computing in the hands of the masses – at least, masses of technically inclined hobbyists. Microcomputing drew enthusiasts away from electronics, photography, and even coin collecting; by 1981 it seemed that every gadgeteer in America and Europe was having fun writing simple programs in BASIC. Very limited computers, some with less than 16K bytes of RAM, were popular; any taste of computer programming was better than none.

The business world was hesitant to accept personal computers, but the first spreadsheet program, VisiCalc, helped popularize the Apple II and created the first class of utilitarian users. It also opened up a market for bigger and better microcomputers.

In 1981 IBM introduced a personal computer aimed at the business market. The IBM PC was more expensive than the Apple II, but also more powerful and more solidly built. Best of all, it looked like a business machine and had IBM's trademark on the front. Microcomputing gained a foothold in the business world. In fact, because IBM did not patent the hastily designed machine, dozens of companies were soon manufacturing "clones" (equivalents).

At first, only power users (basically semi-hobbyists) used PCs; soon utilitarian users began to appear around them. Though far from complex by today's standards, the IBM PC required some technical astuteness, especially if you wanted to write programs or add peripherals. In practice, what happened in most offices was that each power user would assist a group of utilitarian users. All this was informal; management seldom recognized the need for PC technicians, even though there might be a fine technical department running the company's mainframes.

The Apple Macintosh (1984) was the first computer designed explicitly for use by nonspecialists. It corrected the IBM PC's main design flaws, the limits on memory size and lack of a standard graphics system.

More importantly, the Macintosh introduced a mouse-and-windows user interface derived from Xerox workstations and MIT's Lisp machines. The Macintosh set new standards for ease of use; not only the software but also the hardware were designed to be as foolproof as possible. Unfortunately, because of the mouse-and-windows interface, most pre-existing UNIX or PC software could not be ported to the Macintosh. This fact led to a software shortage that the Macintosh has never entirely overcome.

Meanwhile, Microsoft scrambled to make PCs catch up. By 1990 they had a good graphical user interface, Microsoft Windows, and by 1995, they had overcome all the significant limitations of the original PC, meanwhile retaining full compatibility with earlier PC software. What's more, networking was built in. Windows 95 ruled the world.

What had happened to the computer priesthood? It died out, then came back. By 1990 most computer-using companies and institutions recognized the need for technical support personnel, not to run the computers, but to configure and maintain them and diagnose problems. This was often contracted out to PC vendors. A new priesthood was forming.

By 1999 these technicians had become absolutely necessary in order to support networks and complex multimedia hardware. Today, the standalone personal computer is almost a thing of the past, and computer users are again dependent on network service providers and technicians. The IP addresses, nameservers, and router configurations of today are

like the JCL of the past – they are the secret codes and rituals that separate the priests from the ordinary mortals.

2.2 The hacker ethic

Alongside the business computing environments we've just described, a different computing culture was developing at universities and research labs. There, individuals often programmed and and operated computers on their own. Thus, they experienced personal computing before the advent of microcomputers, and at the same time, because many individuals shared a single computer, they were drawn together into close-knit communities.

By 1970, research and educational computing was usually done through timesharing, with many keyboards and screens connected to a single CPU, rather than by submitting programs on punched cards. The Digital Equipment Corporation VAX (1978) was a popular computer for this purpose, and using it was much like using an MS-DOS PC.

In this context, many people discovered the joy of programming for its own sake, a joy later shared by microcomputer hobbyists. They called themselves "hackers," a word that originally had only positive connotations: a hacker was someone who loved programming challenges and hacked away at them day and night.

Hackers were, in general, very intelligent but somewhat shy and bookwormish. Often, their fellow hackers were the first people with whom they had ever shared deep intellectual interests. Much of the early hacker culture is chronicled in the "Jargon File," assembled at MIT and published as *The New Hacker's Dictionary* (M.I.T. Press, 3rd ed. 1996), and in *Hackers*, by Steven Levy (Doubleday, 1984). Microcomputer user groups and wide-area networks (the precursors of the Internet) helped extend this culture to everyone interested.

Hackers felt profound gratitude for being allowed to work in such an interesting place and for the help they routinely received from their fellows. Sharing of ideas and techniques was the order of the day. Back then, you couldn't go to the nearest shopping mall and buy a copy of

Fortran Programming for Dummies. Except for the most basic textbooks, technical literature was almost nonexistent. Large amounts of knowledge needed to be discovered, gathered, and packaged in usable form; hackers routinely did this for each other. Much technical knowledge was passed along by oral tradition; you learned and used it, then taught it, without formal documentation.

The hacker community always judged people by their knowledge and intelligence, not their social status or educational attainments. Professors, technical staff, undergraduates, and even high school students mixed freely, viewing each other as equals. People often wanted credit for their ideas, but they never dreamed of becoming rich or building empires. Bill Gates' fortune was far in the future; most hackers had some inkling that money could be made in "business computing," but they felt it would be boring. The highest attainment was simply to be admired by a large number of fellow hackers.

2.3 The UNIX operating system

One can hardly mention hacker culture without mentioning also the hackers' favorite operating system, UNIX. (The name is a pun on an earlier operating system called *Multics* and is a trademark of Lucent Technologies, formerly AT&T.)

The Internet as we know it grew up on UNIX and its close relatives such as Digital Equipment Corporation's VAX/VMS. That's why most forms of Internet communication use (at least by default) the seven-bit ASCII character set and text files with variable line length. If IBM mainframes had been dominant at early Internet sites, we might be using EBCDIC characters and fixed 80-character lines.

UNIX was developed experimentally at AT&T Bell Labs in the early to mid-1970s. At the time, AT&T had a legal, regulated monopoly on telephone service in most parts of the United States and was forbidden to sell anything else. Accordingly, instead of being licensed commercially, UNIX was distributed for the cost of copying. It became extremely popular at research labs using medium-sized computers such as the VAX

and, later, Sun workstations and Pentiums. Linux, a close derivative of UNIX, has always been distributed free of charge.

UNIX was designed to be as versatile as possible. It made key use of two theoretical concepts that were new at the time, *recursiveness* and *orthogonality*. Recursiveness means that, as far as possible, structures can have structures of the same kind inside them; for example, any directory can contain directories, and any running program can start more programs running. Orthogonality means that features are broken down into the simplest elements and all valid combinations of these elements are supported. For instance, instead of having a subsystem for tapes and a separate subsystem for disks, UNIX treats tapes and disks alike, distinguishing between them only when actually necessary. In fact, it is easy to make a printer, a plotter, or a block of memory act like a disk file because almost all the same operations are available.

What is crucial about UNIX is that *all* its internal workings were freely disclosed to programmers rather than being concealed by the manufacturer. UNIX was distributed in source code, as ready-to-compile C-language programs, so that it could easily be ported to a wide variety of computers. Thus, UNIX provided an unprecedented opportunity for the entire hacker community to learn how an operating system works and modify it to their hearts' content.

Unfortunately, UNIX was not designed for a high level of security. In research labs, great security was not needed. Users had passwords, of course, and the passwords were stored in encrypted form, but tremendous numbers of people had the time and opportunity to devise ways of getting around the security system. Gradually, security has been beefed up in commercial UNIXes, but to this day, most of the computers that get broken into are running some version of UNIX.

2.4 The cracker counterculture

In the 1980s "hackers" gave way to "crackers." That is, the word "hacker" came to denote, not a benevolent computer expert, but an amoral or even malicious tamperer, someone who specialized in cracking

password-protected accounts. These people were quickly renamed "crackers" by those who wanted to preserve the original meaning of "hacker."[3]

Why all this happened would make an interesting historical study; the details are not altogether obvious, but several factors were at work.

For one thing, hackers had always had a somewhat casual attitude toward computer security; they took it for granted that passwords served mainly to prevent accidental blunders, and that any security system could and should be defeated by an intelligent person with a good reason. It was often necessary to circumvent a password in order to fix a technical problem or help a fellow user. Being insulated from "business computing," hackers had little or no really confidential data, and surrounded by cooperative colleagues, they were optimistic about human nature.

It was all too easy for this casual attitude to turn into amorality or even tolerance of malice. Already in the 1950s, some electronic experts, mainly younger ones, engaged in "phone phreaking," unauthorized manipulation of the telephone system to get free long-distance calls. Phone phreaks had a real tendency to disregard questions of ethics when facing a technical challenge. They didn't consider their free phone calls to be theft. This attitude sometimes carried over to the hackers' adeptness at circumventing computer passwords.

Hacker culture was already, in its own way, elitist: hackers had powers that ordinary people didn't. It was all too easy for this benign elitism to turn into a real contempt for uninitiates. Like phone phreaks, some hackers began to feel they had a right to break into computers that were guarded, inadequately of course, by their intellectual inferiors.

Meanwhile, in the early 1980s, hackers suddenly became glamorous. The rise of personal computers created a sudden shortage of computer experts, and hackers were no longer just eccentric scientists – they were hot property. Lots of people wanted to join the hacker culture without really understanding what it was.[4] For many of them, the most obvious

[3]Including us. Some people still use "hacker" to mean "cracker," but we preserve the distinction.

[4]See *wannabee* in *The New Hacker's Dictionary.*

credential of a hacker was that he could "hack" (or crack) password-protected systems.

Finally, by 1984 or so, modems were in the hands of the masses. Although the Internet had not yet gone public, hobbyist bulletin-board systems (BBSes) and dial-in access to university computers were common. Quite a few PC users bought modems and then found themselves unsure what to do with them; if you didn't have an account at a university or subscribe to CompuServe, there was nothing to connect to except a few hobbyist BBSes. Unless...

Unless you could find something more interesting and crack into it. BBSes made it easy to share information anonymously about how to do this. The "phone phreak" mentality was in full flower: ethics meant nothing in the face of a technical challenge, and anyhow, it was easy to rationalize that no real harm was being done. What's more, folklore said that if you cracked an account at a major lab, they'd recognize you as a computer genius and offer you a high-paying job. Phone phreaks, earlier, had had the same folklore.

The movie *Wargames* (MGM, 1983) helped glamorize account cracking. Within a couple of years afterward, the cultural break between old-time hackers and new-style crackers was complete. Crackers were often profoundly ignorant of computer programming; all they knew was a few lock-picking procedures that had been passed to them by fellow enthusiasts. Following the instructions to the letter, they eventually found computers they could break into; then they could pretend that they were computer geniuses and rebels against an evil establishment.

It was not at all clear to early crackers whether they were operating in the real world or in "cyberspace" (wherever that might be) and whether they were subject to the law of the land. Indeed, the unfamiliarity of police departments with account cracking, together with confusion about jurisdiction in incidents carried out remotely, tended (and still tend) to reinforce the impression that computers are, somehow, above the law.

That brings us back to the distinction between new-world and old-world theories of computer ethics. Much of the Internet community favors the new-world view, which is implicit in many of the positions taken by the Electronic Frontier Foundation and other activist groups. This probably

reflects the general preference of hackers to reinvent things from scratch rather than learn existing systems. Utilitarian users tend to prefer, and even assume, the old-world approach. So – after considerable reflection – do we. In fact, this whole book can be viewed as a defense of it.

Chapter 3

How the Internet Works

*** Revise this chapter later; some gaps remain.

The Internet was created in the 1980s by combining the ARPAnet (established in 1967 by the U.S. Defense Advanced Research Projects Agency, DARPA); the Usenet (UUCP) network of UNIX users; and several academic networks including BITNET, JANET, and CSNET. In 1993, the Internet was opened up for commercial use; before that, it had been restricted to educational and research institutions.[1]

The ARPAnet set most of the technical standards. It was designed to survive military attacks, and the Internet preserves its crucial feature: lack of central control. The Internet has no "central site," no headquarters, no single computer that must run in order for the network to function. If any part of the ARPAnet or Internet is destroyed, the undamaged parts will still function. If communication lines are cut, other communication paths, if they exist, will be found automatically within seconds.

This lack of central control has made the Internet into the most democratic culture the world has ever seen. The Internet is run by its users as a community; very little power is in the hands of individuals or

[1]This chapter is not intended to be a complete technical guide. For more details, see Barry M. Leiner et al., "A Brief History of the Internet," *http://www.isoc.org/internet-history/brief.html*; Floyd Wilder, *A Guide to the TCP/IP Protocol Suite* (2nd ed., Boston: Artech, 1998); and Lawrence Hughes, *Internet E-Mail: Protocols, Standards, and Implementation* (Boston: Artech, 1998).

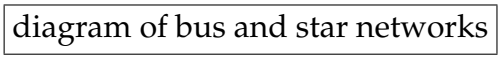

Figure 3.1: Typical computer networks. Every data packet reaches all the computers and is ignored by all but one.

small groups. Unlike commercial networks that preceded it – Prodigy, CompuServe, America OnLine – the Internet is not controlled by a single company. Censorship of unpopular opinions or offensive messages is not merely unwelcome, it is in most cases physically impossible because messages do not pass through a central site.

The nearest thing the Internet has to a central authority is the Internet Society (*http://www.isoc.org*), which sets technical standards but does not attempt to run or control the network. Since the 1960s, most of these technical standards have been published as "Requests for Comments" ("RFCs") rather than officially approved documents. That made it possible for standards to be proposed, modified, and adopted by widespread consensus without waiting for a standards committee to vote.

3.1 The crucial invention: data packets

If computer network connections were like telephone calls, we would not have the Internet. On the telephone, two people have to have a pair of wires all to themselves the whole time they're talking. Computers used to be networked the same way, but such networks are extremely expensive. Fortunately, the Internet doesn't work that way.

On the Internet, computers communicate in *data packets* rather than continuously. A packet is a small block of data (typically a few hundred characters), preceded by codes identifying the sender, the destination, and the "port" or piece of software to which the data is addressed.

Data packets make it possible for several computers to communicate over the same cable at the same time (Fig. 3.1). Each one is sending packets

Figure 3.2: Routers are special-purpose computers that pass packets between subnetworks.

only at brief moments. Each packet reaches all the computers but is accepted only by the one to which it is addressed; the others ignore it.

If two computers try to transmit at the same time – a common event – each of them waits a different, random length of time and tries again. The waiting times are varied randomly so the computers don't act like Archie and Edith Bunker, who collide going through a door, back up, and collide again. Even so, with many computers trying to transmit, there can be several collisions in a row before a packet actually gets sent out. Indeed, counting the number of packet collisions is a good way to determine how busy a network is.

3.2 Connecting one network to another

The networks in Figure 3.1 are suitable for a single office or small building. Larger networks are made by linking subnetworks.

Figure 3.2 shows how this is done. If two large networks were simply connected together, they would clog each other up; any packet transmitted anywhere would be sent to all the computers. *Routers* (formerly called *gateways*) are special computers that prevent this. Routers accept packets and pass each packet along only to the appropriate subnetwork. A packet traveling across the United States on the Internet can easily go through ten or fifteen routers.

There is no fixed limit to the number of computers that can share a network cable, but that doesn't mean the capacity is infinite. As the amount of network traffic increases, eventually a point is reached where transmission is going on almost 100% of the time and almost all

transmissions have to be retried repeatedly due to collisions. At that point, the full *bandwidth* (data-carrying capacity) [2] of the network is in use and network connections begin to "time out" (fail because of excessive delays).

When a chain of routers is involved, the bandwidth of the whole connection is, at best, that of the slowest or most congested link. Many of us in the late 1990s bought high-speed modems only to find that some other, slower, link still stood between us and the Internet.

3.3 Addressing

The data packet format used on the Internet, as well as numerous other networks, is called TCP/IP (Transport Control Protocol/Internet Protocol). TCP/IP relies on a three-layer scheme to assign addresses to computers.

First, every network card has an address built into it that uniquely identifies the hardware and cannot change. This address consists of six two-digit hexadecimal numbers, such as 12:34:56:78:9A:BC. It guarantees that all of the computers on the network will always be distinguishable.

Second, another kind of numeric address, the (*IP addresses*), is assigned to each computer by network administrators. Each of these consists of four numbers ranging from 0 to 255, and authority for them is assigned in blocks. For example, 128.192.12.88 is the address of a computer in Michael Covington's lab. It comes from the 128.192 block, which is assigned to the University of Georgia.

You can use IP addresses for e-mail and web browsing; in fact, some web sites give their addresses in numeric form, as *http://128.192.12.88* or, equivalently, *http://2160069720* (treating the four numbers as components of a base-256 numeral). Although popular with pornographers and other people who want their location concealed, this is not a very convenient way to identify computers.

That's why TCP/IP also had a third kind of address, the *domain address,*

[2] From Nyquist's theorem, which relates data rate to frequency bandwidth.

such as `aisun0.ai.uga.edu`. Here `aisun0` is the machine, `ai` is the internal department, `uga` is the organization (University of Georgia), and `edu` is the type of organization (educational).

Domain names are practical because of *nameservers*, an automatic look-up service. Originally, networked computers had to maintain complete lists of each other's addresses. Nameservers change all that. Nowadays, any computer on the Internet can locate any other computer – including one it has never heard of before, one that didn't even exist an hour before – through the Domain Name Service (DNS). Every computer is assigned one or more primary nameservers which it consults to identify ("resolve") addresses. If the primary nameservers don't know where an address is, they consult other nameservers in an orderly way, and within a minute or so, even the most obscure site anywhere in the world can be positively identified.

3.4 Snooping, sniffing, and spoofing

Recall that every data packet travels to all of the computers on its subnetwork and is ignored by all but one of them. If this strikes you as a security risk, you're right. It is relatively easy to intercept messages on a network by reading packets as they go by on the way to another machine. This is called *packet sniffing* and requires nothing but special software. It is sometimes done legitimately for testing purposes. More often, it is a tactic for intercepting passwords, credit card numbers, or other confidential information.

There are two main defenses against packet sniffing. One is to keep packets confined to the subnetwork in which they are actually needed. This is accomplished by appropriate use of routers and *firewalls* (routers that check packets before passing them along). If confidential packets don't leave the local subnetwork, and everyone there is trustworthy, the problem is solved.

For communicating across the Internet, that's not possible, and the appropriate tactic is to encrypt (encode) the contents of the packets, so that even if they're intercepted, they can't be read. Encrypted packets are

used in secure Web connections (secure HTTP) and secure UNIX login connections (`slogin`).

It is also relatively easy to put a computer on the Internet with a false address. This can be done on several levels. Any e-mail software, for instance, can easily be set up to use any "From:" address that the user wants; this capability has legitimate uses when a person sends mail from one computer but wants to receive replies on another. The discrepancy between the "From:" address and the actual origin is evident from the e-mail header (p. **??**).

More serious is *IP spoofing*, making one machine impersonate another. Suppose `xyz.com` is temporarily unavailable. Some enterprising person can set up another computer and give it `xyz.com`'s IP address, and if routers and firewalls permit, that computer will immediately start receiving and responding to `xyz.com`'s packets. The most common motive for doing this is to publish fake, altered versions of `xyz.com`'s web pages; other deceptive practices are also possible. Careful use of commands such as `traceroute` (p. **??**), and examination of e-mail headers if there are any, will reveal that the fake `xyz.com` is in the wrong place.

*** Any actual cases of IP spoofing?

Finally, there is *port spoofing*, a common mechanism for forging e-mail. Every data packet is addressed not only to a particular machine, but also to a particular *port* (software service). This provides a quick way to distinguish various kinds of traffic and route each packet to the appropriate piece of software on the destination machine. For example, port 25 is for delivering e-mail; port 80 ***confirm is for web connections; and much higher port numbers are sometimes used for testing web pages.

If you connect to port 25 on a computer using Telnet (see below), then type the text that would be transmitted by an e-mail program, the receiving computer will think you are delivering e-mail to it. This can be a legitimate way of testing the e-mail transfer software. However, you can actually type anything you want, thereby creating mail with elaborately falsified headers. Somewhat similar tricks are possible with HTTP, FTP, and other communication protocols.

3.5 Internet services

The Internet provides many different communication services between computers. Here we will describe the most important ones, roughly in the order in which they were invented.

3.5.1 Telnet and `rlogin`

One of the oldest and most fundamental functions of a computer network is to let you use your computer as a *terminal* (keyboard and screen) on other computers. The program that allows you to do this on the Internet is called Telnet and usually emulates a Digital Equipment Corporation VT-100 terminal, with cursor arrow keys but no mouse or graphics. A related program, TN3270, imitates an IBM 3270 terminal for connecting to IBM mainframes. Connecting from one UNIX system to another, you can use a more sophisticated program called `rlogin` (remote login), or an even better one that encrypts its data packets, `slogin` (secure login).

Naturally, to get into a multi-user computer, you must have an account and password, just as if you were sitting down at its console. Often, these passwords are easy to guess or to obtain by trickery. Account cracking (Chapter ***) is invariably done through Telnet.

3.5.2 File transfer (FTP)

Perhaps even more important than Telnet is file transfer. The File Transfer Protocol (FTP) provides a standardized way to transfer files from one computer to another. FTP was more important in the 1980s, before large files could be e-mailed and before files could be placed on the World Wide Web.

There are two ways to use FTP. You can log in with a particular account name and password, just as with Telnet, and access the disk space assigned to you on the remote machine; or you can do *anonymous FTP,* which means that you log in as "anonymous" and download files from a publicly available library. Nowadays, anonymous FTP is supported by

Figure 3.3: An FTP file library as viewed with Internet Explorer.

web browsers; you just give your browser the address of the FTP library, and you see a display like Figure 3.3, from which you can download any file by clicking on it.

In the early 1990s, many FTP libraries also accepted anonymous uploads. This quickly proved to be a very bad idea, as anonymous users would quickly fill any available disk with any files they wanted to exchange, often pirated software or pornography. Nowadays, most FTP libraries do not accept contributions, and if they do, the accepted way to contribute is to e-mail a file to the person who manages the library. To this day, one of the most popular motives for account cracking is to use the victim's disk space to set up a secret FTP library.

FTP is not the same thing as actual sharing of disk drives, a practice that is common on local-area networks but rarely done over long distances. Many different protocols and software exist to allow one computer to use another's disks; among them are Samba and Sun NFS (Network File System). It is important to remember that if you make the disks of your personal computer publicly accessible through the network, and then connect to the Internet, you may be making your data available to total strangers. The odds of total strangers discovering this are, however, quite low.

3.5.3 Electronic mail

Electronic mail (e-mail) is the electronic transmission of short texts from one person to another, combining the speed of the telephone with the convenience of postal mail. In the early 1980s, it would sometimes take e-mail several days to get relayed from one site to another, but nowadays, almost all e-mail is delivered within seconds. In the 1990s, e-mail

protocols were extended to permit transmission of fies of any kind, including executable programs, graphics, and ready-to-view web pages.

We will say more about e-mail in Chapter ***. E-mail has always been relatively easy to manage because people generally know who they're communicating with. Forged e-mail and "spam" (unsolicited advertisements) are relatively recent developments.

3.5.4 Newsgroups

Now consider how people might use a computer network to conduct a group discussion. One way would be to e-mail all the messages to all the participants; that technique is called a *mailing list* (or *listserv,* after a popular program from distributing such mail) and is widely used.

But mailing lists have disadvantages. They are expensive; every message must be replicated for each member. If there are 1000 members and each sends one message, the system must carry not 1000 but 1,000,000 messages.

Newsgroups are a solution to the problem. They originated on the Usenet (UUCP) network of UNIX users, and to this day, the newsgroup system is called Usenet, although it is no longer a separate network.

Newsgroup messages look like e-mail, but instead of being delivered directly to the recipients, they are stored in disk files where anyone can read them and contribute ("post") additional messages. Each newsgroup is actually one of these files and has a name indicating its intended subject, such as `sci.astro.amateur` or `rec.pets.aquaria`.

The computer on which the files are stored is called a *news server*; people nearby read and post news by connecting to it.

But most newsgroups are distributed worldwide. This is accomplished by automatically copying the files from one server to the next, meanwhile discarding messages more than a few days old. In this way, every message is distributed all over the world within a few hours or days, without incurring the huge cost of distributing messages by e-mail.

There are currently more than 10,000 newsgroups, and although the

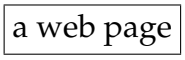

Figure 3.4: A typical web page. Click on any underlined word for more information about it.

collapse of the newsgroup system has been predicted many times, it has not yet happened. Newsgroups are the heart, soul, and (one might even say) Achilles' heel of the Internet; they bring out the best and the worst in it. Newsgroups have been the setting of a huge number of quarrels and unpleasant encounters, but they have also provided a quick way for individuals to learn the culture of the Internet, learn how to function in an intellectual community, and exchange ideas fruitfully on any subject. We will discuss newsgroups in more detail in Chapter ***.

3.5.5 The World Wide Web

Now back to file transfer. Recall that FTP libraries are efficient but not very user-friendly; you can't look at a file until you've downloaded it. In the 1990s, a number of techniques were developed for delivering information directly to your screen from a remote library of files. This technology culminated with the Hypertext Transfer Protocol (HTTP) and the World Wide Web (WWW) of computer files.

Hypertext is text that is enhanced with *links,* connections to other texts, so that if you click on a word, you can jump directly to related material elsewhere. Particularly when enhanced with graphics, hypertext is a very efficient way to present information to people. They can read it in their own way at their own speed, following the links that interest them.

A *web page* is a file, written in HTML (hypertext markup language), residing in an HTTP library and containing links to other files. The reason the whole thing is called a "web" is that, of course, millions of files are tied together in various ways by links.

We will say more about the World Wide Web in Chapter ***. For the standpoint of culture and ethics, it has been a very positive development. Just when newsgroups and e-mail were beginning to be plagued by anonymous sniping and deliberate abuse, the Web introduced a welcome element of personal accountability. Instead of sniping at others, Web users invariably publish something of their own that they can take pride in. False or deceptive content on Web pages is uncommon. Instead, the Web is everyone's opportunity to send messages to the world. What's more, Web pages make it easy to identify and check out people who might otherwise be known to you only through an e-mail address. There is no guarantee that the content of a web page is truthful, but at least the author is saying it to everybody, not just you.

3.5.6 Chat rooms

A *chat room* (or Internet Relay Chat, IRC) is an open forum that operates in real time rather than through relaying of newsgroup messages. That is, participants all communicate with, and through, a single computer, and messages are relayed to all of them almost instantly. It's like joining a conversation at a party, or perhaps like talking on a CB radio.

Culturally, chat rooms are a great deal more hobbyist-oriented and game-like than other Internet services. Since they leave no permanent record, they are seldom used for transmitting important information. People normally identify themselves by pseudonyms and conceal their real identity. Quarrels are common.

3.6 Who pays the bills?

One of the oddest things about the Internet, from the commercial point of view, is that it has no mechanism for keeping track of costs. Routers do not charge each other for the packets they relay; e-mail systems do not collect postage.

There are two reasons for this. First, the Internet originated as a completely subsidized research network. Second, the cost of accounting

would be appreciable; it might well cost more to count the packets, and bill for them, than to just keep forwarding them free of charge.

The same seemed to be true of the American telephone network in the 1970s, and many of us foresaw the day when telephone calls nationwide would be free, like local calls. Unfortunately, that day never came; accounting systems became more efficient, and although long-distance charges fell, they never disappeared. Indeed, small charges have appeared for some calls that used to be local.

If it has to, the Internet can probably develop a cost-accounting system that is reasonably inexpensive to run. Unfortunately, it will lose much of its present freedom when it does so, since each site will have to comply with financial, not just technical, standards, and it will be much harder for experimenters to set up small sites on their own.

Many issues in computer ethics revolve around the Internet's failure to track costs. The biggest is the spam problem: the cost of sending e-mail is not charged to the sender, or even measured, so it appears to be zero. Advertisers who don't mind making a million enemies – or who are slow to learn that their public image matters – can flood the network with unsolicited ads of an obnoxious nature. Also, much of the appeal of account cracking and theft of FTP services is that one can claim that it "didn't really cost anything" since no charges were billed.

3.7 Ostracism of rogue sites

The Internet community has one powerful but rarely-used way to punish uncooperative members: ostracism. Precisely because my site doesn't pay the other sites for net access, they are under no legal obligation to accept my site's packets. If my site makes a pest of itself, other sites can and will cut it off.

*** kill files

*** Usenet death penalty

*** other anti-spam tactics

*** research this; information in ”Stopping Spam” ***

Chapter 4

Names and addresses on the Internet

*** Some work still to be done at end

One thing that everybody knows about the Internet, no matter how far they've stayed away from it, is that lots of addresses begin with `www` and end with `.com` ("dot com"). This chapter will survey the Internet domain naming system, including some abuses of it.

4.1 How names are assigned

The last part of a domain address is called the *top-level domain*. It is either a three-letter code for the kind of site or a two-letter country identifier. There are just seven three-letter codes, all of them originally used in the United States:

`.com` for commercial sites;

`.edu` for colleges and universities;

`.org` for other organizations;

`.net` for network service providers;

`.mil` for U.S. military sites;

`.gov` for U.S. government sites;

`.int` for international organizations (rarely used).

More recently a shortage of available names under `.com` has led to increased use of `.net` and `.org` for commercial addresses.

There are dozens of officially assigned country codes. Here are a few:

`.us` for the United States (used by schools and not much else);

`.ca` for Canada (which also uses `.com` and `.edu` extensively);

`.uk` for the United Kingdom;

`.au` for Australia;

`.de` for Germany (*Deutschland*);

`.ch` for Switzerland (*Confoederatio Helvetica*);

`.su` for the Soviet Union (obsolete);

`.ru` for Russia (largely replacing `.su`).

In many countries, the two-letter code is preceded by an indication of the type of site. For example, `.ac.uk` denotes an academic site in the U.K.

Each top-level domain has an official address registrar that assigns *second-level domains* to particular organizations. For example, `microsoft.com` is Microsoft, and `cam.ac.uk` is Cambridge University. The full address of each machine, such as `phx.cam.ac.uk`, is then assigned locally. You can identify the registrars for all the domains through *http://www.allwhois.net* and *http://www.isoc.org*.

The same machine often has different names for different purposes. For example, the main World Wide Web server at any organization usually has a name starting with `www`, and the main FTP server has a name starting with `ftp`. These can perfectly well be the same machine; they can also be different machines at different times, so that if web service is moved from one computer to another, the address can be moved with it.

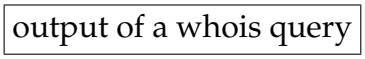

Figure 4.1: The `whois` information for `uga.edu`.

4.2 Using `whois` servers

Whenever a domain name is registered, certain information has to be registered with it, including the name, e-mail address, and telephone number of at least one responsible person who can be contacted in an emergency. For example, Figure 4.1 shows this information for `uga.edu`.

You can retrieve this information by using the UNIX `whois` command or through the World Wide Web. Unfortunately, as this is written (1999) the `whois` system is changing, and we cannot give detailed instructions for accessing it. Consult your system administrator, check *http://www.allwhois.com* (which attempts to keep track of `whois` servers for all the top-level domains in the world), or go to a major search engine such as *http://www.yahoo.com* and look for *whois*.

Remember that organizations have `whois` data but subnetworks within them do not. For example, `uga.edu` is listed in the appropriate `whois` servers but `ai.uga.edu` is not.

4.3 E-mail and URL addresses

The domain address of course identifies only a machine. When sending e-mail or accessing a web page or file library, you normally have to give further information, such as the name of the user or file. There are standard ways to do this. For example, `jones@alpha.beta.net` is the e-mail address of user `jones` on machine `alpha.beta.net` (a made-up example).

An even fuller kind of address, used on the World Wide Web, is the

uniform resource locator (URL). A URL specifies not only the machine, but also exactly what kind of service is requested from it. Here are some examples of URLs:

- `mailto:jones@alpha.beta.net`

  Send e-mail to `jones` at `alpha.beta.net`.

- `telnet://gamma.ac.uk`

  Open a Telnet connection (defined below) to `gamma.ac.uk`.

- `ftp://delta.edu/pub/doc/april1.txt`

  Download the file `april1.txt` from directory `/pub/doc` on `delta.edu`.

- `http://www.epsilon.com/~jones`

  View the main web page (named `index.html`) in the directory of user `jones` on `www.epsilon.com`.

The *tilde* character (~) denotes the directory assigned to a user name. As in UNIX, and unlike DOS, the slashes that separate directory names are always forward (/), not backward (\).

4.4 The domain-name shortage

If domain names were needed only for organizations that actually operate computer networks, there would still be plenty of names to go around. However, most businesses want domain names of their own so that their customers can find them more easily on the web. The address of Joe Bloggs' Used Cars is much easier to remember if it's `www.bloggs.com` rather than `www.server.net/users/~bloggs/cars.html`.

It is therefore normal practice is to register many domain addresses and make them point to different directories on the same machine, so that businesses and organizations can operate under their own names rather than the name of their Internet service provider.

By the end of the 1990s there was a serious shortage of usable second-level domain names in the .com domain. Of course, a gigantic number of names remains available if you count nonsensical strings such as p0f7uyuy87645.com, but such names are not recognizable or memorable.

And the millions of businesses in America, let alone the rest of the world, do not all have distinct names when reduced to a single memorable word. When Michael Covington started to register his consulting firm, Covington Innovations, in 1999, he found covington.com, covington.net, covington.org, coving.com, covi.com, cov.com, innovations.com, and ci.com already taken – by eight different organizations! And *Covington* is a relatively rare name.

4.5 Alternatives to .com

As a stopgap measure, Network Solutions, Inc. (the .com, .net, and .org address registrar until mid-1999) encouraged clients to use .net and .org indiscriminately as substitutes for .com. That is not entirely satisfactory. Suppose John Doe gets doe.net rather than doe.com. Since he's a commercial entity, his customers will still expect him to have a .com address and will tend to remember his address as doe.com.

Another stopgap measure is to register domains in another country. Many countries will gladly issue domain addresses to organizations and servers elsewhere. Tonga (.to), for example, has plenty of second-level domain names available, and most of them are never going to be needed in Tonga. The Tongan registrar would much rather receive fees from Americans than receive no fees at all. Other small countries are in the same situation. In 1998, the network managers at Oxford University discovered that one of the machines on their internal network was registered as a domain in Liechtenstein.

Practices like this strike us as risky. They make it look as though addresses are being faked somehow – and the Internet community is cracking down on deceptive use of addresses. Even if the domain is properly registered, you can expect problems if almost everyone seeing it

thinks it's fake. It is quite likely that in the future, use of domains outside one's own country will be forbidden or will require special justification.

The `.us` country code is available, but the current American standard requires the city and state to precede it; Michael Covington would have to be `covington.athens.ga.us`, which looks unwieldy and is easily mistaken for the nearby town of Covington (`covington.ga.us`).

There is a proposal for an additional series of addresses ending with `.firm`, but they are not yet available. Even so, it will remain impossible to guess whether a particular company is a `.com` or a `.firm`. Some kind of division according to the nature, or at least size, of the company would be more helpful – perhaps `.corp` for shareholder-owned corporations, `.tech` for individuals and small providing technical services, `.vend` for sites that sell products through the Web, and so forth. These issues are being discussed, and changes in the system are expected by the end of 2000; see *http://www.isoc.org* for the latest news.

Another solution is to use third-level domains. If `covington.com` and `covington.net` are not available, how about `covington.xyz.net`, where `xyz` is the (preferably short) name of some Internet service provider? Such an address could be assigned locally by the service provider and would be easy to remember and to dictate over the telephone, since it contains no slashes or tildes.

4.6 Domain naming vs. trademark law

When the Internet went commercial in 1993, there were few restrictions on registering domain names. The managers of the addressing system took it for granted that people would cooperate. That assumption held true when the Internet was a research network, but it did not fit the ruthless world of capitalism.

In particular, there was no attempt to apply trademark law to the Internet – to require people to use only their own names or names they had a right to use. Addresses were not considered trademarks. You didn't have to be named McDonald or Kodak to get `mcdonalds.com` or `kodak.com`

respectively. The appropriate Internet Society document said only this:[1]

> In case of a dispute between domain name registrants as to the rights to a particular name, the registration authority shall have no role or responsibility other than to provide the contact information to both parties.
>
> The registration of a domain name does not have any trademark status. It is up to the requestor to be sure he is not violating anyone else's trademark.

In short: Nobody made any attempt to synchronize domain-name practice with trademark law.

It didn't take entrepreneurs long to realize that they could play tricks with domain names. For example, `internic.net` was for a long time the registrar of `.com` addresses; but `internic.com` is a completely separate domain name broker. Apparently the latter organization chose its address in the hope of attracting people who were looking for the former.

4.7 Domain-name poaching

Even worse is *domain name poaching* or *domain name hijacking*, the practice of deliberately registering a domain name that you don't intend to use, simply so that you can later sell it to its "rightful" owner. The tactic is to register domain names that resemble the names of major companies that are not yet on the Net. When they want to get on the Net, they'll (supposedly) pay you handsomely to release the names to them. At the very least, you'll have a sense of power from being able to stand in the way of a major corporation.

In our opinion, there are trademark-law issues here that have not yet been tested in court. Common sense tells us that any kind of identifying name *is* potentially a trademark, even if it is also a network address. As this is written, the question is wide open. Concerns have even been raised

[1] J. Postel, "Domain Name System Structure and Delegation," RFC 1591, 1994, available from *http://www.isoc.org*.

that efforts to solve the problem could work the other way – aggressive application of trademark law could make it too easy for large corporations to bully small businesses that have similar, but completely legitimate, names.

*** need specific cases, etc.

Chapter 5

Illusions and misconceptions

The trouble with the world, said Will Rogers, is not ignorance; it's "the things people know that ain't so." The Internet is so large, so complex, and so new that people easily get mistaken impressions of it. These comprise *illusions,* which come from the misleading appearance of one's environment, and *misconceptions,* which are spread from person to person. Anyone managing an Internet site will often have to correct these illusions and misconceptions. Here are the most important ones we have encountered.

5.1 Illusions about costs

5.1.1 "It doesn't really cost anything"

As we noted in Chapter 3***, the Internet does not have a mechanism to keep track of costs. Some Internet service providers charge a flat rate, and some charge by the hour; what you do during each hour is entirely up to you. Costly activities tend to go slowly, but users are not charged extra for them.

The Internet was originally created for education and research, and concealment of costs is a sacred academic tradition. Scholarly research cannot be done with a view to monetary profits. Basic scientific

discoveries often pay off not immediately, but ten, twenty, or a hundred years later. Thus, universities and research labs routinely hide the cost of nearly everything they do, not just running computer networks. Scientists aren't charged for using the library or walking around in the college gardens.

In the early days, Internet users realized that although the costs were hidden, the network was expensive and should be used only for worthy, or at least interesting and creative, purposes. They also realized that their colleagues' time was valuable. Nowadays, the value of people's time is likely to be as much an issue as the cost of network usage. Someone who sees fit to send out 500 copies of a trivial e-mail message isn't just consuming bandwidth, he or she is consuming other people's time and attention (and would never have dreamt of making 500 phone calls to those same people).

5.1.2 "I'm entitled to make money, right?"

At the other end of the spectrum from the old-time academics are newcomers to the Internet who sometimes know little about it except that fortunes can supposedly be made there. From their viewpoint, the purpose of the Internet is to help them make money, mainly through advertising, and any cultural expectations that stand in the way are going to be disregarded or flouted. ("I'm paying thirty dollars a month for this account and I have a right to use it!")

Part of the problem, of course, is that even when you're paying an access fee to *one* site (your service provider), you're still the guest of all the *other* sites, particularly in the newsgroup and e-mail systems. We'll get back to this in Chapter *** ("The Spam Problem").

A second point of contention has to do with standards of honesty. Internet culture was formed by professional scientists, who, regardless of their personal character, have very high standards of honesty. You just can't do science any other way; scientific deceptions are inevitably found out and bring disgrace to the perpetrator. Even if not found out, they produce useless results that can't be built upon.

Thus, among old-timers, there is a strong expectation that, on the

Internet, the truth will not be stretched even slightly, at least not by those with something to gain from doing so.

Some people who advertise deceptively don't even realize they're doing it. They rationalize that it's all right to get people's attention by creating a false belief *temporarily*, and that petty deception is expected. ("All's fair in love, war, and business" – to compete, you have to be as dishonest as the next man.) This is part of a more general phenomenon we've observed: Dishonest people think everyone is dishonest and that it's necessary to be dishonest to survive. Meanwhile, their honest colleagues and competitors are often leaving them in the dust.

Some entrepreneurs feel that intrusive advertising is legitimate; TV commercials interrupt TV shows, and surely interrupting a newsgroup is no worse. The difference, of course, is that the TV advertiser is paying for the show as well as the commercial; the person who spams a newsgroup is not even paying to distribute his own material, much less the context into which he inserts it.

Many advertisers, especially web page designers, imitate TV commercials in another unwelcome way – they waste time by displaying twirling trademarks rather than delivering information. They fail to realize they don't have a captive audience; in ten seconds the viewer will tire of the twirling trademark, click another button, and go far away.

Sometimes, all you can say to such people is, "We don't do things that way here."

5.2 Misconceptions about safety and security

5.2.1 "The machine will prevent all wrongdoing"

We computer professionals assure beginning computer users that they will not damage the machine by typing on it, even if what they type is incorrect. We also set up passwords to keep people out of others' accounts. In short, we build computers, particularly large multi-user computers, so that they cannot easily be damaged by the effects of ignorance or malice.

Unfortunately, some users conclude that these safeguards completely supplant any need for ethics on their part. If something is wrong, the computer should prevent it, and conversely, *if the computer doesn't prevent something, it's not wrong*.

That conclusion tends to be used more as an excuse than as a real ethical principle. It is common for would-be account crackers to search and search for loopholes in the security of a computer, and then, when caught, say triumphantly, "The computer let me do it." In educating computer users, we have had to emphasize that permission is granted by people, not machines, and that physical ability to use a computer resource does not constitute permission to do so.

5.2.2 "Security is a purely technical challenge"

Computer technicians often fall victim to a more sophisticated version of the same misconception: Computers should prohibit all wrongdoing, and if wrongdoing still takes place, it's because the computer was technically inadquate. "If my computer gets broken into, it's my fault for not having the latest security patches installed." Naturally, account crackers applaud this conclusion and glory in it.

The trouble is, of course, that no computer is ever perfectly secure, and there may be legitimate technical reasons to leave a computer less secure than it could be. There is a trade-off between security and versatility. Attempts to make a computer super-secure can interfere with legitimate work as well as consuming excessive time and effort.

5.2.3 "My account doesn't need protecting"

Utilitarian users, especially those who seldom use the computer, often feel that their accounts don't need protecting because they contain no confidential data and, indeed, little data of any kind. They feel that it's all right to be casual with passwords because so little is at stake.

Unfortunately, that's not true. Rarely-used accounts belonging to beginners are exactly what account crackers want. Such an account can

be used illicitly for a long time without the owner noticing anything wrong, and can serve as a springboard for further mischief. It is common for account cracking to take place through a whole chain of Telnet connections from one computer to another, so that half a dozen or more innocent people will have to be investigated before the real perpetrator is identified.

In educating new users, we emphasize that the computer is no more secure than the least secure account on it.

5.3 Illusions of the Internet culture

5.3.1 "Everybody here is just like me"

The Internet is so good at bringing together like-minded people, and concealing their differences, that it's easy to overestimate how much you have in common with the people with whom you are communicating.

In this respect, the Internet just amplifies a general characteristic of human society. I don't know what other people are like, and I have no choice but to assume they are like me except for the differences I can detect. When these differences are concealed, and particularly if I'm naive, I'll assume that everyone is just like myself. Recall the *New Yorker* cartoon: "On the Internet nobody knows you're a dog."

The tendency to see oneself in everyone else sometimes produces comical results or petty annoyance. Hobbyists think everyone is a hobbyist; students think everyone is a student; idle people with time on their hands think everyone is idle.

5.3.2 "Everybody here is trustworthy"

The Internet also places a high value on trustworthiness, and newcomers quickly see people helping each other and relying on each other to a high degree. From this, it is all to easy to extrapolate and conclude not just that trustworthiness is *common,* but that it is *universal* – everybody is bonded

together by the brotherhood of cyberspace.

5.3.3 "Only a small circle of friends can see this"

Going even further, it's easy to get the impression that the people with whom you communicate are not only like you, and reliable – they're also isolated from the rest of the world, and you can confide in them.

Results of doing so can, of course, be disastrous. Every Internet site administrator can recount incidents where someone posted private information in a very public forum – perhaps a newsgroup or web page, viewable by everyone in the world – and then was startled when the information got to someone outside their small circle. "Don't tell my boss about my cocaine habit" is a genre of newsgroup message that actually does occur.

5.3.4 "It's all just a game, hobby, or fantasy"

Different, but equally common, is what we call the *video game illusion,* the impression that the Internet is not part of the real world – it's all just a fantasy game with multiple players.

Consider how this impression can arise. Fantasy games with multiple players do exist and are popular on the Internet. It's all to easy for someone deeply involved in such games to venture out into newsgroups, e-mail, web pages, and the like without quite realizing that he has left Fantasyland.

Combine this with the fact that many video games revolve around violent attacks on imagined enemies or competitors, and you can see what might happen. Rivalries within games turn into quarrels in newsgroups; tactical moves within a game are supplemented by account cracking or denial-of-service attacks on the adversary's computer; and the fact that real people are involved, many of them quite uninterested in video games, is forgotten.

One warning sign of the video game illusion is the use of fantastic pseudonyms in e-mail and on newsgroups. Most users choose account

names that reflect their real names in some way. Some users, though, choose names that reflect an active fantasy life. Our experience has been that such users are likely to get into quarrels and flout security rules; they seem to forget that their fellow Net users are humans in the real world.

They also forget how easy it is to make a silly impression. Michael Covington's students turn in homework by e-mail; nearly every semester he has to remind someone that real names are required, and there is no "Zork Dragonslayer" or "Frodo Baggins" registered for Computer Science 6540.

5.4 Misconceptions about law and ethics

5.4.1 "Good intentions are enough"

One of the most pernicious misconceptions about computer ethics, all the more dangerous because it sounds so noble, is the idea that one need not actually learn about society's rules – good intentions are all that matter.

For example, someone blitzes their employer's e-mail server with 500 chain letters asking for contributions to help a nonexistent dying boy. When challenged, they respond, "How *dare* you criticize me for wanting to help a dying boy? It was all for a very good purpose!"

Maybe so, but the e-mail bandwidth wasn't yours to take, no matter how noble the intention, and if the dying boy doesn't exist or the charity turns out to be a fraud, it's not really a good cause.

Similarly, "I didn't mean any harm" is the universal excuse offered by account crackers and other tamperers. In the late 1990s, a teen-ager using the computer in his father's University of Georgia lab wanted to contact a friend who was deeply immersed in an interactive game on the Internet. Since the friend could not receive e-mail or telephone calls at the time, he chose to send a signal by deliberately slowing down the friend's net connection. This was done by flooding the cable with packets, and it closed down a commercial network for several hours. His defense? "I shouldn't be punished because I didn't *intend* any harm."

It is vitally important to know what you're doing, know how the Internet works, and know what's expected of you – not just convince yourself that your motives are pure.

A milder form of this same misconception afflicts people who have trouble accepting facts about the law of the land. Certain things – pornography, for instance – are illegal whether or not you feel they ought to be. Disagreeing with the law does not exempt you from it.

5.4.2 "All they can do is take away my account"

Unfortunately this misconception is all too often the truth. Many Internet sites punish abuse of the Net purely by revoking the offending account. This move is quick and usually inappropriate. When imposed on naive users, it is too heavy-handed – one should *prevent* misuse by educating the users, rather than execute them after the fact.

More importantly, truly malicious people expect to have their accounts taken away; they're often using a stolen account in the first place, and they have plenty more accounts ready.

Taking away an account that was provided as a free trial is no punishment at all. Free trial accounts provided to unidentified people are a serious hazard to the security of the Internet.

5.4.3 "Laws don't apply here"

For numerous reasons, people often think that on the Internet, they're beyond the reach of the law. One misconception is that laws don't apply "in cyberspace" (wherever that might be). Another is that the only laws that apply to computers are those that specifically mention them. That's like thinking it must be legal to steal elephants in any state whose criminal code does not specifically mention elephant theft. We will return to this point in Chapter ***.

We have often seen young people assume that the law doesn't apply to them, or at least they can't be punished, because of their age: a first offender under 18 has a right to be left off with a warning, or so they

think. In educating users we emphasize that this is not so. Serious computer crimes have been committed by young people whose malice was just as genuine as that of a bank robber.

Finally, there is a great deal of confusion about whether laws apply across boundaries of jurisdiction. Traditionally, petty crimes are local, and only serious crimes span long distances. Thus, the FBI and Interpol do not have to chase shoplifters. A few federal regulations and international treaties have gradually been put into place to deal with long-distance but small-scale crimes such as mail fraud.

The Internet has opened up new ways to commit minor offenses over great distances, often in such a way that the trail has to be followed through several jurisdictions. (An example would be a case of account cracking with little documented damage.) Police agencies are gradually developing ways to deal with such things. What is important in the meantime is to assure users that they *can* be held accountable for illegal acts committed by remote control. Even if not extraditable, they could end up being wanted in, and therefore unable to visit, some other country or state.

5.4.4 "If I crack an account I'll be hailed as a genius"

One of the most enduring legends of the Internet is that someone, somewhere, cracked some accounts, was caught, and ended up getting a high-paying job because of his obvious computer expertise.

This is an old story whose origin we have not been able to trace. Michael Covington heard it in 1972, about phone phreaking, and it was old then. Unfortunately, if it really happened, we can't confirm it.

In any case, even if it *did* happen to someone, once, that doesn't mean it's going to happen to every account cracker that comes along. Account crackers often have delusions of grandeur; such people call themselves "elite hackers" and claim to be exempt from society's rules because of their great genius.

The trouble is, account crackers, even clever ones, are not geniuses. Most account crackers are not even clever. All they do is exploit well-known

cracking techniques against vulnerable victims. Like picking locks, account cracking requires some out-of-the-way knowledge, but it does not require a first-rate intellect. Indeed, a really first-rate intellect would probably find something more rewarding to do with his time.

Chapter 20

Developing an Acceptable-Use Policy

One thing the Internet community has had to learn the hard way is that maximum freedom comes from the right amount of regulation, not from the absence of regulation. If there are no rules, bullies will prevail, or at the very least, some people will fail to exercise their rights because they don't know they have them. The same Internet users who claimed total freedom of speech in 1990 were often, by 1995, begging for some kind of authority to stop the flood of spam (bulk e-mail).

Every computer site (that is, every network or place where people are given access to computers) needs an acceptable-use policy (AUP), especially if the site provides access to the Internet. An acceptable-use policy is a set of rules that serves several purposes. It should:

- Specify what the computers are and are not to be used for. The biggest question is generally to what extent people are allowed to pursue personal interests as well as doing the work for which the computers were purchased.
- Tell people about applicable local, state or provincial, and national laws, so they won't engage in illegal practices either deliberately or accidentally.
- Advise computer users about what is acceptable on the Internet,

helping them steer clear of conflicts, quarrels, and embarrassment as well as actual misuse. (This pays off for the administrator, too, by preventing complaints.)

- Shield the site itself from liability for harm done by users. (We're talking about not only lawsuits, but also ostracism or blacklisting by the rest of the Internet community.) Adequate protection is only possible if there are well-thought-out rules and users are aware of them.

Appendix A contains the University of Georgia's acceptable-use policy, which we offer as an example partly because we had a hand in making it, and partly because it is unusually thorough; a university's activities are very diverse, so practically all possible uses of the computers are covered, and the rules are explained in detail. It can be adapted to make an acceptable-use policy for any kind of site, whether corporate or educational.

The acceptable-use policy for any site should be constructed, or at least approved at an early stage, by the people it will affect, or at least by their representatives.

How this will be done depends on the kind of site. A commercial Internet service provider may be a one-person operation; its one and only administrator can simply make up the policy and provide it to clients when they sign up. At the other extreme, a university or large corporation will already contain sub-communities of computer users with their own expectations and unwritten rules that must be taken into account.

The University of Georgia's acceptable-use policy was formulated over a one-year period by a team comprising computer administrators and users, a lawyer, a campus police officer, and representatives of the management units that handle cases of misconduct (Personnel, Student Affas, and Internal Auditing). Crucially, not everyone on the committee was a computer expert; some of them hardly used computers at all.

Criticism of the proposed rules was sought as early as possible from all sources, especially online discussion groups within the University. In this way it was possible to explain to the community, at an early stage, why the rules had to be what they are.

We sincerely hope that others faced with the same task will not have to do quite as much work. It probably won't take a year to adapt the policies in Appendix A to suit another site in another state or country. The University of Georgia encourages others to use their rules as a model and do exactly that.

20.1 Is there a law against stealing elephants?

Part of the content of the acceptable-use policy comes from the law of the land (national, state or provincial, and local law). Most localities have laws that pertain specifically to computers and prohibit such things as account cracking and theft of computer services.

More importantly, computer users must still obey the laws that do not specifically mention computers. If selling marijuana is illegal in Georgia, then selling marijuana is equally illegal "in cyberspace" when the people involved are in Georgia. The same goes for laws against slander, copyright infringement, distributing obscene material, or making terroristic threats.

An analogy that we like to use to explain this is that in Georgia, there is no specific law against stealing elephants, but that doesn't mean stealing elephants is legal. The laws against theft just don't happen to mention elephants specifically — horses, maybe, but not elephants.

At Georgia, we had to hammer this point home because some of the computer users expected to be shielded, somehow, from the law of the land. We found two sources for this expectation. First, there are still those who think the Internet is a secret society beyond the reach of the law, or at least beyond the eyes of the police. Second, there are many who feel that the Internet is so radically new that it must make up its own laws from scratch, or operate on pure philosophical principles rather than messy American laws. It was hard to get such people to accept facts about the law; to accept, for instance, that certain kinds of pornography are illegal whether or not one feels they ought to be.

The law holds people responsible not only for crimes but also for torts (civil wrongs, the negligent or malicious actions that provoke lawsuits).

Deliberate or reckless harm done to others can be penalized even if the acts do not break a specific law. This, too, is a point of which users need to be reminded. One of the most subtle points, all too seldom appreciated, is that threatening a groundless lawsuit is itself a civil wrong.

The task of advising computer users about the law must be handled carefully. Tell them too little, and you set them up for possible trouble. Tell them too much, and you risk making technical blunders; computer site administrators are not, and need not be, lawyers. The approach taken at The University of Georgia was to mention computer laws in some detail, and other laws briefly, without trying to explain how they apply to all situations.

The Georgia acceptable-use policy also warns people explicitly that bad legal advice is common on the Internet. For example, in mid-1998, spammers (bulk e-mail advertisers) started telling each other that the Murkowski bill had passed (which it had not) and that it overturned their previously made contractual promises not to spam (which it did not). Acceptable-use policies should caution users not to believe everything they hear.

20.2 Social-contract ethics

A social contract is an unwritten agreement between members of a community. It obtains its force from the fact that society has established such-and-such an institution, and the institution can't work if people don't follow the rules.

The Internet is built upon a huge, complex, and sophisticated social contract. The acceptable-use policy of any Internet site will have to say a lot about social-contract ethics. For example, newsgroups are based upon an agreement that the people using them will stick to the assigned topics. Posting off-topic messages is physically easy and always will be; the computer can't tell what you're writing about. But if you violate the social contract, you will incur the wrath of your fellow Net citizens.

The appeal of social-contract ethics is that you can use it regardless of the deep philosophical beliefs of your audience. People can't argue with the

fact that the community, or the institution, works in a particular way. Thus, ethical reasoning based on the social contract can be used even when addressing a very diverse set of people.

But social-contract ethics has its limits. The first limit is that it provides no basis for criticizing society itself. As far as social-contract ethics is concerned, people can do anything they agree to do, whether it's good or bad.

The second limit is that social contracts exist only between citizens – and who, exactly, are the citizens? Over the years, human societies have decided, for various reasons, that slaves, indigenous races, or fetuses are not citizens and have no rights under the prevailing social contract. Computer crackers often feel that their inferiors (non-experts) are not citizens; they feel strong ethical obligations to their equals and superiors, but not toward non-experts – and the more pretentious the cracker, the more likely it is that he considers you an unworthy non-expert.

The third limit is that it's not clear whether social contracts govern what you do in secret. Plenty of people fail to see the moral force of copyright law because they feel that acts done in secret, such as software piracy, are no one else's business. According to this line of reasoning, it's even all right to deliberately harm people if they don't know they're being harmed.

For all these reasons, any acceptable-use policy will need to appeal, at least implicity, to some standard of right and wrong other than just the agreed-upon practices of the community. Nonetheless, there will be some individuals whose philosophy is basically amoral, and whose concept of ethics includes nothing beyond the practical necessity of following society's rules.

20.3 What kind of computer facility?

Obviously, the appropriate acceptable-use policy will be different depending on whether you are running:

- A corporate site whose only function is to further the company's

business; or

- An academic site whose purpose is to provide broad education, but not to support commercial activity; or
- An Internet service provider (ISP) that sells Internet access and allows subscribers to use the Internet for any lawful purpose.

Even within these categories, there are gradations. The larger and more diverse the organization, the less restrictive the acceptable-use policy should be; additional limits can be put on specific computers and subnetworks by the appropriate managers. If you forbid too much at too high a level, you run the risk of banning a legitimate activity that you didn't know about. In a smaller organization, you can have more confidence that people with unusual needs will make their voices heard.

Academic sites, of course, are not all alike. Consider colleges and universities first. A large state university provides education on all subjects and, as an arm of the government, is required to be fair to an extremely diverse population; for example, it can't endorse or suppress a religious belief. Further a government institution's resources can't be used to make money privately, except under heavy restrictions.

A private university is much less fettered; in some ways it's more like a commercial ISP, and its resources can be used for any purpose its trustees approve of (unless commercial use of the computers endangers the institution's tax-exempt non-profit status).

Church-affiliated universities are likely to be committed to specific positions on controversial moral issues, which can be reflected in the acceptable-use policy. We caution, however, against being too strict; people may need to be *informed* about things the institution would never *endorse,* and in limiting access to newsgroups, for example, it is all too easy to throw the baby out with the bath water.

Schools below the university level are in a different position because their students are not adults (see Chapter ***, "Children on the Net"). In particular, schools are expected to guide students toward reliable sources of information and impose some limits so that, for instance, thirteen-year-olds do not get their sex education from pornographers or

advice about drugs from drug dealers. As we note elsewhere, the Internet is a city street, not a school library; nobody controls it as a whole, and you can find anything there. It is therefore appropriate for a grade-school acceptable-use policy to impose considerably stricter limits than would be appropriate at a university.

Corporate sites might be tempted to make the acceptable-use policy very strict – nothing but work for us, thanks! – but that can be a blunder. The needs of any large organization are more diverse than anyone can anticipate; lots of what looks like recreation can have legitimate educational value.

Internet service providers (ISPs) need the least restrictive policies because, of course, they are selling access to the whole Internet. At the same time it is extremely important to make users aware that they haven't bought unlimited rights; they must still abide by the community's rules. Detailed guidance (as in the Georgia rule set, Appendix A) may well be in order. At the very least, a commercial ISP should shield itself from liability by explicitly prohibiting illegal activities, and should prohibit acts such as spamming that would result in serious complaints or ostracism. If an ISP gets a reputation for harboring abusive practices, other sites will block communications from it, cutting off its livelihood.

20.4 Just for work, or is exploration encouraged?

Should employees be allowed to pursue personal interests on the Internet using their employers' computers?

The biggest problem the Georgia rule committee faced was a state law that said, apparently, "Absolutely not." By law, the University's resources can be used only for the University's work. Many corporations have similar policies, but at the University of Georgia, it's not just a policy, it's a state law which the computer policy team couldn't modify or ignore.

The trouble is that much of the Internet caters to personal interests and always has done so. It makes no sense to give people access to e-mail, newsgroups, and the World Wide Web, and then prohibit them from using these resources in the normal way. It would be like inviting

someone to a dance and forbidding them to dance when they get there. If Georgia had said "nothing but assigned work," we would have been out of step with the whole Internet community, including the other state universities. There would have been little point in connecting to the Internet at all.

The law seems to say that even when an employee makes a personal phone call from work, it's technically illegal, though tolerated. At first, that's exactly what our lawyers told us, but I (Covington) couldn't accept that; I found it hard to believe that the legislature actually meant to forbid such things.

Eventually, we took a different line of reasoning. We pointed out that if the University decides to allow personal local phone calls, or personal web surfing, as a way of improving the working conditions for an employee, that's legal because it's something the University is doing for its own benefit.

We also pointed out that the Internet has great educational value. Allowing employees to pursue personal interests is good for the University, which wants a broadly educated work force. Even computer games can have some educational value for people who are new to the computer and somewhat afraid of it.

At the same time, we took care not to create an entitlement. Some computer users wanted us to guarantee them the right to surf the Web from the office. We refused to do that. Think of personal phone calls again: the University isn't required to provide telephones for all workers, nor does it have to let employees make personal calls when they need to be doing something else. In the same way, employees are welcome to pursue personal interests on the computer only when the time and computer facilities are available and they have the appropriate manager's approval.

20.5 What about offensive material?

One of the most often-asked questions at Georgia is whether computer users are allowed to view pornography on the World Wide Web. The

answer: There is no University-wide rule against it, but individual labs need not allow it, and if it offends others in the same lab or office, it may run afoul of the University's sexual harassment policy.

Pornography is not the only potentially offensive material. Gruesome pictures of violence, advocacy of obnoxious causes (from fascism to drug use), or even noisy web sites or games can annoy one's fellow computer users.

At the same time, a ban on "offensiveness," so called, would give too much power to people who claim to be "offended." What if I claim to be offended by something arbitrary – by web sites written in foreign languages, by recipes for meat (if I'm a vegetarian), or by text with a purple background? Clearly my eccentricity does not entitle me to take away others' freedom.

Fortunately, this is not an issue peculiar to computers, and the University of Georgia left it to existing policies (especially sexual harassment) and the expectation that management will deal with problems as they come up. The underlying moral principle is that some feelings of offendedness are reasonable and some are not.

20.6 "Thou shalt not be too popular"

The Internet has no good way of controlling the demand for connections to sites, and sometimes too many people want to get on the same site at once. Microsoft found this out, to their chagrin, after establishing online updates for Windows 98; by the end of 1998 so many people wanted the updates that hardly anybody could connect and actually get them!

The same thing can happen with web sites. In 1997?? a student at Northern Arizona University posted, on her web page, some nude photographs of herself. We haven't seen the pictures; we'll assume they were legitimate works of art. But the point is that Northern Arizona University was soon deluged with people wanting that particular web page transmitted to them. Naturally, the university's server couldn't fulfill all the requests. Unfortunately, though, even the *failed* requests consumed time and bandwidth on the network. The Internet lets any

machine try to connect to any other machine at any other time; it's not like the telephone network, where you can get a busy signal. (And even telephone networks have problems when thousands of people dial the same number at once.)

We know of no good solution to this problem. "Thou shalt not be too popular" is not an enforceable rule. Everybody wants their web sites to be as popular as possible, short of actually overloading the facilities. The best recommendation we can make is that every acceptable-use policy should give the management the right to restrict computer usage that is otherwise legitimate but, for unforeseen reasons, consumes unreasonable amounts of resources.

20.7 Entitlements and local restrictions

There are two things an acceptable-use policy should not do. It should not create entitlements, and it should not disregard or override the purposes for which computers are set up in the first place.

Take the second point first. The computer in my office was put there for me to use for specific kinds of work, and the acceptable-use policy does not give other people the right to come in and use it. It doesn't even give *me* the right to tie it up with something unimportant that would interfere with the work for which it was intended. More generally, "X is legal" does not always imply "I have the right to do X on *this* computer."

Putting this another way, every computer can and does have strings attached to it beyond the acceptable-use policy. It's perfectly legitimate for managers to reserve a particular computer for a particular kind of work; it would be a disaster if they couldn't.

Now the first point. An entitlement is a policy guaranteeing some resource to some class of people. For example, the University of Georgia presently provides a computer account to every student who wants one; that's an entitlement.

Crucially, however, there are no entitlements in the acceptable-use policy. If they were put there, they'd be too hard to change, and as governments

the world over have learned the hard way, an entitlement program can quickly become horribly expensive. The acceptable-use policy requires managers to be fair, but it does not guarantee any computer facilities to anyone.

20.8 Educating the users

The most wisely formulated acceptable-use policy does no good unless the computer users know about it and take it seriously. User education is therefore vital. It can comprise such things as:

- Material that users must read before obtaining a computer account;
- Seminars, lectures, question-and-answer sessions, and videotapes of them;
- Online discussion; easy access to the computer security team by e-mail and in newsgroups so that questions can be answered and discussed;
- Articles in internal newsletters or magazines.

User education must go on continuously, not just when the acceptable-use policy is first promulgated, for several reasons.

First, there is turnover; people are using the computer now who weren't using it a year ago. Particularly at educational institutions, there is an endless supply of complete beginners.

Second, new computer users often won't understand all of the acceptable-use policy when the first read it. They'll need to be reminded of its main points six months or a year later, when they've experienced more of the situations that it deals with.

Third, genuinely new issues come up. Advertising on web pages, for instance, wasn't a problem when the Georgia team first drafted the acceptable-use policy in 1993, because there was (almost) no such thing as a web page then. Three years later it was a hot issue.

At Georgia we have found that question-and-answer sessions are an important and popular form of user education. Plenty of people want to know exactly how the rules apply to them; a surprising number of them think the restrictions are heavier than they are. An administrator conducting a question-and-answer session can address specific situations that can't be encoded into the rules. Georgia also has a somewhat humorous online quiz (at *http://www.uga.edu/compsec*) that tests people's understanding of computer security and ethics.

Different parts of the population catch on to the acceptable-use policy at different rates. Highly trained professionals and computer hobbyists generally pick it up quickly, except that senior professionals in non-computer fields sometimes see it as red tape that they can and should disregard. The populations most at risk – that is, the people who are most often uninformed or misinformed – are newcomers (of course) and, somewhat surprisingly, secretarial staff. The latter are outside the flow of management information and are trained to follow orders literally – which makes them very vulnerable to hoaxes and forged material that looks official.

20.9 Pitfalls to avoid

By far the most common defect in acceptable-use policies, whether corporate or academic, is that they just don't say enough. Many of them say little more than "Be nice to each other" expanded to half a page or so. The trouble is, of course, that good intentions are not enough; people need guidance to avoid blunders and unintended harm.

The second most common defect is that the users don't know the rules. Having a brilliantly written policy written down on paper, or on a web page, does no good if there is no way of getting users to read it and checking that they have done so. At Georgia, it is extremely commmon for users to sign a statement that they have read the rules when they have done nothing of the sort. Regrettably, most people are all too willing to sign routine-looking documents without reading them. At least we aren't selling used cars.

The third most common defect is that the rules are not enforced. If the community begins to believe that the rules are "just for show" or "just for the lawyers," disaster can ensue – in effect, there *are* no rules. Even with a well-publicized rule set, a surprising number of people won't take the rules seriously. "Oh, I had no idea I actually had to follow that!" is an excuse we have heard often at Georgia, even from people who have been explicitly told the contrary over and over.

(If you think an acceptable-use policy will shield you from liability even if you don't enforce it, think again. Courts will always consider your actual practice, not just what you write down and publish.)

Rules contrary to actual practice are, of course, not enforceable. That's why the acceptable-use policy should not be framed by people who don't know how the computer network is actually used. A strict by-the-book manager who doesn't understand the Internet can easily craft a set of rules that forbid common, even necessary, activities. The result can be worse than having no rules at all.

Appendix A

University of Georgia Policies on Use of Computers

The following is a copy of the University of Georgia's acceptable-use policy.[1]

The University of Georgia encourages other institutions to copy this document and adapt it to their own needs, giving credit to the original. Although designed for a university, this policy can easily be adapted to the needs of a corporate site or Internet service provider.

Purpose

This document has two purposes: to prohibit certain unacceptable uses of the University of Georgia's computers and network facilities, and to educate users about their responsibilities.

Most of these regulations simply restate obligations that follow from other existing policies or laws (see *Relevant Laws* below). They fulfill a Board of Regents directive requiring the University to adopt explicit computer security and ethics policies along the lines of those recommended in Internet RFC 1244.

[1]*** The latest revision of the document will be used here, along with a footnote acknowledging all its creators.

This document is divided into rules and commentary, with the expectation that the commentary can be revised frequently to reflect technical changes and to answer questions that have come up, without materially changing the rules.

Penalties

Violations of these policies incur the same types of disciplinary measures as violations of other University policies or state or federal laws, including criminal prosecution in serious cases.

Definitions

University computers and network facilities comprise all computers owned or administered by any part of The University of Georgia or connected to the University's communication facilities, including departmental computers, and also the University's computer network facilities accessed by anyone from anywhere.

Authorization is permission granted by the appropriate part of the University's governance and/or management structure, depending on the particular computers and/or network facilities involved and the way they are administered.

Rules

(1) No one shall use any University computer or network facility without proper authorization. No one shall assist in, encourage, or conceal from authorities any unauthorized use, or attempt at unauthorized use, of any of the University's computers or network facilities.

Comment: Computers and networks are just like any other University facilities – they are to be used only by people who have permission. Using a computer without permission is theft of services and is illegal under state and federal laws. In addition, the following specific computer crimes are defined by state law (Ga. Code 16-9-90 et seq.):

- *Computer theft* (including theft of computer services, intellectual property such as copyrighted material, and any other property);
- *Computer trespass* (unauthorized use of computers to delete or alter data or interfere with others' usage);
- *Computer invasion of privacy* (unauthorized access to financial or personal data or the like);
- *Computer forgery* (forgery as defined by other laws, but committed on a computer rather than on paper);
- *Computer password disclosure* (unauthorized disclosure of a password resulting in damages exceeding $500 – in practice, this includes any disclosure that requires a system security audit afterward).
- *Misleading transmittal of names or trademarks* (falsely identifying yourself or falsely claiming to speak for a person or organization by using their name, trademark, logo, or seal, Ga. Code 16-9-93.1).

Maximum penalties for the first four crimes in the list are a $50,000 fine and 15 years of imprisonment, plus civil liability. The maximum penalties for computer password disclosure are a $5,000 fine and 1 year of imprisonment, plus civil liability.

(2) No one shall knowingly endanger the security of any University computer or network facility, nor willfully interfere with others' authorized computer usage.

Comment: Many of the other regulations given here deal with specific acts of this kind. You should not assume that other malicious acts or deliberate security violations are permissible merely because there is no specific rule against them.

(3) No one shall use the University's communication facilities to attempt unauthorized use, nor to interfere with others' legitimate use, of any computer or network facility anywhere.

Comments: State and federal laws forbid malicious disruption of computers. The University of Georgia does not tolerate individuals who invade others' privacy, steal computer services, or commit misrepresentation or fraud; nor pranksters who attempt to disrupt computers or network facilities for any other purpose.

Also, you should be aware that *ability* to use a remote computer does not constitute *permission*. Some computer services *are* open to the public, and

clearly identify themselves as such; examples are anonymous FTP sites and Gopher servers. But the mere lack of security measures does not mean that a computer is open to anyone who wishes to use it. The same goes for unauthorized use of communication paths, such as remote dialout modems and the like.

(4) No one shall connect any computer to any of the University's networks unless it meets technical and security standards set by the University administration.

Comments: The applicable requirements depend on what kind of connection is being made. For example, dialing up with an ordinary asynchronous modem does not require any special authorization, but connecting to the campus-wide Ethernet cable does, because one improperly configured machine on a network can cause widespread disruption.

The Board of Regents' contract with MCI Telecommunications restricts the dial-in facilities that University units can offer; for specific information, contact UCNS.

(5) All users shall share computing resources in accordance with policies set for the computers involved, giving priority to more important work and cooperating fully with the other users of the same equipment.

Comments: If you need an unusual amount of disk space, CPU time, or other resources, check with the administrators in charge of the computer rather than risk disrupting others' work. When resources are tight, work that is necessary to the University's mission (instruction, research, and service) must take priority over computing that is done to pursue personal interests or self-training on side topics. Also, no matter how important your work may be, you are only entitled to one person's fair share of the machine unless additional resources are available and appropriate permission has been granted.

Priorities for any particular machine are set by the administrators in charge of it in consultation with the user community.

Obtaining extra computer resources through any form of deception (e.g., secretly opening multiple accounts, misrepresenting the nature of your work, or the like) is strictly prohibited.

(6) No one without specific authorization shall use any University computer or network facility for non-University business.

Comments: By law, the University can only provide computer services for its own work, not for private use. In this respect the University's computers are different

from those owned by private colleges or corporations. If you need unlimited access to computer networks for private purposes, you can subscribe to a private service such as America Online or CompuServe.

The University's mission can be understood broadly as including education, self-training, and discussion on a wide range of subjects, not just those immediately necessary for a person's job or courses.

The University grants the use of its facilities to numerous organizations whose activities contribute to its mission, such as student organizations, professional societies, and the Campaign for Charities. But it is improper to use the University's computers for political campaigns, fund-raising, commercial enterprises, mass mailings, or other outside activities that have not been granted the use of the University's facilities.

Various policies permit members of the University community to earn outside income by writing books and articles related to their academic work, and to use University resources for this purpose, including computers. Most faculty are also permitted to use University facilities for outside consulting jobs provided the University is reimbursed for costs incurred. Check with your supervisor to find out how these policies apply to you.

(7) No one shall give any password for any University computer or network facility to any unauthorized person, nor obtain any other person's password by any unauthorized means whatsoever. No one except the system administrator in charge of a computer is authorized to issue passwords for that computer.

Comments: Giving your password to an unauthorized person can be a crime under Georgia law. The criterion is not whether *you* trust them, but whether the *University* has authorized them.

Passwords protect the University's network, not just the individual machines to which they apply. The University insists that each account be used only by the person to whom it belongs, so that if problems are detected or abuse is alleged, the responsible person can be identified. If a department cannot keep passwords secure, it cannot connect its machines to the campus-wide network.

In general, you should never share your password with anyone else. Likewise, you must never use or disclose a password that was given to you improperly.

A password is like the key to a building – you are responsible for what happens to it while it's in your care. If you give it away, you are endangering the entire machine, not just your own files. In fact, there are computer criminals who would

like to have your password so they can make it look as though you, not they, are committing their crimes.

Do not store the password for one computer in another computer unless your system administrator has assured you that no security hazard will result. It is easy for a stranger to walk up to your personal computer and retrieve passwords that are stored in it.

You are responsible for choosing a secure password. *Don't use names, nicknames, phone numbers, or recognizable words in any language,* because some people guess passwords by automatically trying every word in a large dictionary.

A good way to make up a secure password is to use the initials of a phrase, and include some numbers as well as letters. For example, `57ityMwb` is a good password, and it's easy to remember because it stands for "57 is the year Michael was born."

Your password is secret. System administrators will not normally ask you for it. The computer will never ask you to type it unless you are logging in or changing your password. Beware of computer programs that ask you to "log in again" or type your password at any other time; they are likely to be tricks. (There are rare exceptions on some computers; check with your system manager. If anything that you don't understand ever happens after you type your password, then change your password immediately.)

In some situations the University authorizes more than one person to share a single account, but this is seldom the best way to conduct collaborative work. Instead, use file sharing, groups, and related features of the system you are using. Email can be redirected automatically to a secretary, who can then forward it to you using a separate mailbox.

(8) No one shall misrepresent his or her identity or relationship to the University when obtaining or using University computer or network privileges.

Comments: Naturally, you must not claim to be someone else, nor claim to have a different relationship to the University than you actually do, when obtaining a computer account or access to a lab.

- You must not falsify your name, address, email address, or affiliation when sending email or other messages from a University computer. Doing so can be illegal (Ga. Code 16-9-93.1 and other laws against

misrepresentation) as well as being an unacceptable use of the University's facilities.

- On some systems, there are ways to post messages without revealing your name and address. *Anonymous* communication is permissible when there is a legitimate need for additional privacy. It is not a cover for fraudulent or obnoxious behavior, and in cases of abuse, anonymous messages may be traced to their source. *Deceptive* communication, in which you claim to be some other specific person, is never permitted.
- You can create confusion, and possibly violate trademark law, by using someone else's trademark as your name on the Net. No matter how loyal a Kodak customer you may be, don't call yourself "Kodak." That's their name, not yours.

(9) No one without specific authorization shall read, alter, or delete any other person's computer files or electronic mail. This rule applies regardless of whether the operating system of the computer permits these acts.

Comments: Don't even *try* to guess or steal other people's passwords, or read their files, even if the computer permits this. Doing so would be like rummaging through someone else's desk. Even if you can pick the lock, and even if there is no lock at all, you have no right to intrude.

(10) No one shall copy, install, or use any software or data files in violation of applicable copyrights or license agreements.

Comments: This rule forbids making unauthorized copies, for use elsewhere, of software residing on the University's computers. It also forbids installing or using pirated software on University computers.

The price of a piece of software isn't just the cost of the disk – it's also one user's share of the cost of developing and supporting it. It's wrong to use software without paying your fair share.

Not only that, but the University benefits from the generosity and good will of many software vendors; any sign of software piracy would bring this generosity to a halt and result in higher prices for everybody.

As if that weren't enough, unauthorized copying is usually a violation of federal copyright law.

Some educational software licenses forbid the use of the software for

commercial purposes. Some software is “site licensed” and can be used on any University computer. (The terms of various site licenses differ.) Some software is genuinely free; the author allows everyone to use it free of charge. Before copying software, *be sure* what you are doing is legal, and consult people who have full information; don’t just give yourself the benefit of the doubt.

License checks: If strangers show up at your computer site saying they are there to check software licenses, you should immediately contact Legal Affairs and your administrative superiors. After hours, contact Campus Police. Software licenses do not normally authorize these surprise inspections, and there is a substantial risk that the “inspectors” are not legitimate.

(11) No one shall create, install, or knowingly distribute a computer virus, “Trojan horse,” or other surreptitiously destructive program on any University computer or network facility, regardless of whether any demonstrable harm results.

Comments: A virus is a hidden computer program that secretly copies itself onto users’ disks, often damaging data. A Trojan horse is a program with a hidden, destructive function, or a program designed to trick users into revealing confidential information such as passwords. Even when the harm done by programs of these types is not readily evident, they confuse beginning computer users, degrade CPU performance, and waste the time of system managers who must remove them.

(12) No one without proper authorization shall modify or reconfigure the software or hardware of any University computer or network facility.

Comments: Do not modify the hardware, operating system, or application software of a University computer unless you have been given permission to do so by the department or other administrative unit that is in charge of the machine. The other users with whom you share the machine, and the technicians on whom you rely for support, are expecting to find it set up exactly the way they left it.

(13) Users shall not place confidential information in computers without protecting it appropriately. The University cannot guarantee the privacy of computer files, electronic mail, or other information stored or transmitted by computer unless special arrangements are made.

Comments: Ordinary electronic mail is not private. Do not use it to transmit computer passwords, credit card numbers, or information that would be damaging if made public. Bear in mind that students’ educational records are

required by law, and by U.Ga. policy, to be kept confidential. It is also necessary to protect confidential information about employees, such as performance evaluations. This applies not only to networked computers, but also to computers, tapes, or disks that could be stolen; an increasing number of computer thieves are after data rather than equipment.

The University will normally respect your privacy but cannot guarantee it absolutely. There are many ways a normally private file can end up being read by others. If a disk is damaged, a system administrator may have to read all the damaged files and try to reconstruct them. If email is mis-addressed, it may go to one or more “postmasters” who will read it and try to correct the address. For your own protection, system administrators will often look at unusual activity to make sure your account hasn’t fallen victim to a “cracker.”

The Georgia Open Records Act applies to information stored in computers. This act gives citizens the right to obtain copies of public records, including any record prepared, received, or maintained by the University in the course of its operations. Some kinds of records are exempt; among these are student records (including tests and homework), medical records, confidential hiring evaluations, trade secrets (which probably includes unpublished research), and material whose disclosure would violate copyright. Moreover, the Open Records Act is not a license to snoop; requests for information must be made through proper administrative channels.

(14) Users shall take full responsibility for messages that they transmit through the University’s computers and network facilities. No one shall use the University’s computers to transmit fraudulent, defamatory, harassing, obscene, or threatening messages, or any communications prohibited by law.

Comments: You have exactly the same responsibilities on the computer network as when using other forms of communication. You must obey laws against fraud, defamation, harassment, obscenity, solicitation of illegal acts, threatening or inciting violence, and the like. Bear in mind that uninvited amorous or sexual messages are likely to be construed as harassment. If you are bothered by uninvited email, ask the sender to stop, and then, if necessary, consult a system administrator.

Use of the computers to circulate chain letters and pyramid schemes is not permitted. If someone says, “Forward a copy of this to everyone you know on the Internet,” *don’t*. Such messages often contain misunderstood or outdated information, or even outright hoaxes. Even when the information is legitimate,

chain forwarding is a needlessly expensive way to distribute it.

Never participate in schemes to deliberately flood a computer with excessive amounts of email. “Mail bombing” can incapacitate a whole computer or even a whole subnetwork, not just the intended victim.

It is considered good practice to use your real name, rather than a nickname or pseudonym, in the headers of all outgoing communications. Use of nicknames is often interpreted as a sign of immaturity or an indication that you are not taking full responsibility for what you are sending out.

Fake electronic mail: All users should be aware that there is no guarantee that electronic mail actually came from the person or site indicated in it. Deceptive electronic mail is easy to fake, including the technical information in the header. Doing so is of course prohibited and is in many cases against the law.

Hoaxes, scams, and false warnings: Hoaxes, pranks, and con games are common on the Internet. Be on the lookout for misguided “warnings” (about computer viruses, impending legislation, etc.) and false appeals for charity (usually involving dying children). If you get a message that spurs you to take immediate action, it is very likely to be a hoax, even if the person who passed it along to you was perfectly sincere. Also, genuine appeals that are several years old are still circulating as if they were current. Rather than spreading the appeal or “warning,” post a question in *uga.computer-security* so that knowledgeable people can reply.

University letterhead: Use prudent caution when sending out any message that appears to be an official communication from the University. If the header identifies your message as coming from an administrative office or from the office of someone other than yourself (e.g., “Dean’s Office”), recipients will presume that you are speaking for that office or person.

(15) Those who publish World Wide Web pages or similar information resources on University computers shall take full responsibility for what they publish; shall respect the acceptable-use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar facilities.

Comments: Web pages on the University's network are subject to the same rules as other uses of the same facilities. Different University computers are set up for different purposes; some do not permit individual Web pages at all. On other University computers, individuals are allowed to set up Web pages to pursue personal interests, but even then, the available disk space and communication bandwidth are limited. System administrators can advise about what is permitted at any particular site.

When you publish something on the World Wide Web, you are putting it before a potential audience of millions. You have the same responsibilities as if you were publishing a newspaper. If the content is libelous or deceptive, people can sue you and you can be held personally liable.

Since there are laws against distributing obscene material (not just creating it), a link to an obscene web site can be a violation of the law. This is true regardless of the status of the Communications Decency Act or other new laws that specifically mention computers.

There is no University rule that prohibits you from viewing any web page anywhere. However, the University's sexual harassment policy prohibits you from displaying sexually explicit material which interferes with anyone's work or academic performance or creates an intimidating, hostile, or offensive working or academic environment. That is why many campus computer labs do not permit the display of erotic images on screens visible to others.

If you want to reproduce copyrighted pictures, cartoons, or comic strips on your web page, you must have the copyright owner's permission. It is not sufficient to reproduce the owner's copyright notice; you must actually obtain permission for yourself, just as if you were publishing the same material in a newspaper. Brief textual quotations do not always require permission as long as the source is acknowledged and you are not reproducing a complete work (poem, essay, etc.).

You are welcome to include links to businesses and commercial sites for their information value, as long as your links do not constitute advertisements. If you are personally connected with an outside business, you may mention the connection *briefly* on your University web page so that people who are looking for you can find you. (For example, authors of books can include links to their publishers; consultants can include links to their consulting firms; and University units can advertise publications, software, and similar materials produced in connection with their work.) However, you must not solicit outside business or publish commercial advertisements or advertising graphics on a University computer.

You must not accept payments, discounts, or anything of value in return for placing anything on your web page. The University's disk space and communication capacity are not yours to sell. This applies to all computers directly connected to the University's network cables, even if they are privately owned.

A few University sites, such as *Georgia Magazine*, may be authorized to publish paid advertising for outside clients as part of their official function. Because it imposes costs on the whole University network, this activity must be cleared with University-level authorities, not just system administrators or department heads.

(16) Users shall comply with the regulations and policies of newsgroups, mailing lists, and other public forums through which they disseminate messages.

Comments: When participating in Usenet newsgroups and similar forums, you must respect their policies and practices, for two reasons:

- To join these networks, the University has to agree to abide by their policies. Misuse would endanger the University's eligibility to participate.
- Most of the cost of transmitting any message in a discussion is borne by the sites that receive it, not the site that sends it out. Thus, you are the guest of the whole network community, and it is important to abide by the policies and practices of the entire network.

The most ironclad rule is *to respect the announced subject of each forum and not to post anything off-topic.*

Other things that are generally unwelcome include:

- Advertisements (except that many forums permit announcements that are directly relevant to their subject areas);
- Multiple postings of the same material (a general-interest message should go in one general-interest forum, not several specialized ones);
- Survey questionnaires and other mass solicitations;
- Questions that are easily answered by looking in dictionaries, encyclopedias, or readily available software manuals;
- Requests for help with homework;

- Uninformative criticisms of other people's postings (unwelcome material posted by others should be ignored, not discussed);
- Postings that are misspelled, obscurely worded, or TYPED IN ALL CAPITALS LIKE THIS;
- Postings that say "Test message, please ignore" (try out your software when you actually have something to say, or use a test newsgroup).

Before posting anything, make sure that you know how to cancel it in case you subsequently discover that it is redundant or misinformed. Also, before posting in any Usenet newsgroup, read the appropriate guidelines for new Usenet users, and read some of the messages that are already there so you can be sure you have not misjudged the newsgroup's subject or purpose.

Always assume that everyone in the entire world can read what you are posting, that permanent copies will be kept at several sites, and that you will be expected to take full responsibility for everything you say. Do not post anything that you would not want to see quoted in a major newspaper.

Remember that newsgroups are not confined to the United States and are certainly not confined to students. You will sometimes see postings from other countries in their native languages, and you will often see postings from senior professionals in their fields.

(17) System administrators shall perform their duties fairly, in cooperation with the user community, the appropriate higher-level adminstrators, University policies, and funding sources. System administrators shall respect the privacy of users as far as possible and shall refer all disciplinary matters to appropriate authorities.

Comments: The first responsibility of any computer or network administrator is to serve the user community. But regardless of what the users want, system administrators are not free to violate copyrights, software licenses, other legal restrictions, or obligations undertaken by the University in order to obtain funding.

Although computer users' privacy is never perfect, system administrators are expected to respect this privacy as far as possible and refrain from unnecessary snooping. Administrators who must read users' files for administrative reasons must be prepared to justify their actions to higher administrators and to the user community.

System administrators should not normally interfere with users' electronic communication, especially in any way that could be interpreted as favoring one

side of a controversy or suppressing an unpopular opinion or topic. As far as possible, decisions affecting access to online information services should be made in full consultation with the user community, taking into account the cost of the computer resources involved.

The system administrator is not the judge, jury, and executioner in cases of computer misuse. Rather than penalizing users directly for their misdeeds, the system administrator is expected to refer all cases to appropriate authorities who can protect the rights of the accused. If you are accused of any violation that justifies disciplinary action, you have a right to a fair hearing just as if your alleged misdeeds had not involved computers.

It is important to distinguish actions taken to *punish a person* from actions taken to *protect a system*. If your account appears to have been misused or broken into, your system administrator will inactivate it and contact you or wait to hear from you. This is done to stop the misuse and does not presume that you are the guilty person; you can expect to have your privileges reinstated right away, with new passwords, as soon as you identify yourself and indicate willingness to follow the rules. Thus, you can resume using the computer while investigation of the incident continues.

Relevant laws

New state and federal laws concerning computer abuse continue to be passed, and important court decisions occur frequently. For up-to-date guidance about specific questions, consult the Computer Security and Ethics Incident Handling Team. Remember that legal advice circulated on the Internet is unreliable.

Computer crimes defined by Georgia law were mentioned in the comments on rule 1. In addition, there is a specific law against electronic distribution of obscene material to minors (Ga. Code 16-12-100.1).

Federal law (18 USC 1030) provides for fines and imprisonment up to 20 years for unauthorized or fraudulent use of computers that are used by or for the federal government (which includes many of the computers on the net), and for unauthorized disclosure of passwords and similar information when this affects interstate commerce. (Recall that net messages, as well as long-distance phone calls, are interstate commerce and thus fall under this law.)

The Electronic Communications Privacy Act (18 USC 2701-2709) and other

wiretap laws prohibit unauthorized interception of electronic communications, including electronic mail.

Pyramid schemes and chain letters that ask for money or anything else of value are illegal under various state and federal laws and postal regulations. The people running these schemes generally claim to have found loopholes in the law, but their claims should not be believed. Even if a pyramid scheme were legal in itself, it would be illegal to use a University computer to participate in it for personal gain.

Computer users must also obey laws against private use of state property, divulging confidential educational records, copyright infringement, fraud, slander, libel, harassment, and obscenity. Laws against obscene or harassing telephone calls apply to computers that are accessed by telephone. The Georgia Open Records Act applies to records stored in computers as well as on paper.

The University must obey the policies of the University System (Board of Regents) and the regulations of the nationwide and worldwide networks to which its computers are connected.