CS101
Social and Legal Issues

Chapter 14 of your textbook gives a fairly comprehensive overview of the many social and legal issues that pervade computer technology today. In this handout we will cover a few highlights presented in the book. Since there are many open questions regarding social and legal issues, you will have an assignment to discuss some of these issues with your classmates on the electronic discussion forum. However, you should read the entire chapter in the book.

If you continue in computer science and earn a degree, you will be empowered to create new technologies that can have a profound impact on society. As such, it is a good idea to stop and think a bit about some of the important issues impacting us today.

The Dark Side of Technology

For most of this class we have been quite positive and enamored with technology. We talk about how technology can transform society and allow us to do things we could not do in the past. Thanks to computer networks, we can share information instantly across the globe. We can access vast databases of knowledge, perform financial transactions, and do business in new and exciting ways.

However, there is always a dark side to such rosy pictures. Technology can supplant existing industries, putting companies out of business and workers out of jobs. For example, the US Postal Service has indicated that the rise of email has had an effect on the volume of letters that it normally carries. As email becomes more popular, the problem will likely increase (together with postal rates). Digital technology in watches hurt the business of Swiss watchmakers. The introduction of the calculator put slide rules out of business.

Technology can introduce additional problems as well. For example, pollution and disposal of old computers and hazardous equipment have become serious issues. Many believe that in the near future, when a computer is purchased you will also have to pay for a disposal fee for when the computer is eventually destroyed or recycled.

Moreover, there is the way that technology is used. Like any other tool, computers and technology can be used for good or malicious purposes. Computers have opened the door for entirely new types of crime. Naturally, there are some gray areas in between the good and bad. One of these is the issue of privacy.

Privacy Issues & Encryption

The Privacy Act of 1974 regulates how the government can conduct wiretappings, harassment, questionable use of personal records, search, and seizure of personal information. It was intended to prevent abuses by the government. For example, consider the many databases of information that the government has likely collected about you:

- Personal information (age, marital status, gender)
- Location information (address you live at now, old addresses)
- Motor vehicle and driving records (what you drive, accidents, violations)
- Legal hearings and judgments
- Income from tax payments
- Credit History

You may not want this information to be made public. The privacy act of 1974 requires procedures to protect the security of this information and prohibits disclosure without consent.

One controversial use of this information is computer profiling. This is typically used to identify people to watch as suspected criminals, and is a hot topic, especially after the 9/11 tragedy. For example, perhaps a group of terrorists fit a particular profile of personal information (e.g., middle eastern descent), tend to drive a particular vehicle (e.g., mini vans), and tend to have a particular income and immigration status. This information could be used to identify other potential terrorists. While this can be quite useful, there is a good chance that an innocent person happens to fit the terrorist profile. The innocent person might then be subjected to search and detention as a mistaken terrorist.

The issue then remains, should profiling be used, or is it unlawful?

The government is not the only organization with such databases, although theirs is perhaps the most vast. Consider the other data that is likely stored about you somewhere, although likely distributed among various organizations:

- Credit history via credit bureaus
- Student loads
- Bank accounts
- School records
- Medical records
- Telephone calls
- Insurance information
- Utility records
- Grocery purchases
- Online purchases
- Likes and preferences (filled out a survey on these recently? This data is commonly used for marketing)

Some people have proposed that all of these databases be linked to one massive database to enable better profiling. On the flipside, it could also enable easier access to personal information and make crimes such as identify theft easier. (In some sense these are already linked through your Social Security Number, since this number is often used to identify you, even though state and federal institutions are not supposed to use it. Private organizations do not have such restrictions).

A related issue to privacy is that of encryption. Encryption can allow privacy. However, it is possible for criminals to use encryption to their advantage. For example, there have been reports of terrorists using publicly available encryption software to communicate with one another to prevent government agents from learning of their plans. Until recently, the US government enforced strong rules against the export of encryption software and algorithms. There is still debate as to what level of encryption should be made public. Some believe that the regulation of encryption algorithms is akin to the government attempting to hide mathematical concepts and truths, a task that is somewhat Orwellian and likely impossible.

Computer Failure and Legal Responsibility

As computers become more integrated into our lives, we become more dependent on them. Usually we expect them to work correctly, but this is not always the case. Here are some notable computer failures:

- During the Gulf War, a software error prevented the Patriot missile system from intercepting a SCUD missile
- In 1990, AT&T's long distance network collapsed for many hours due to an error in a C program. An "if-then-else" statement was improperly constructed.
- In 1999, the $125 million Mars Orbiter spacecraft crashed due to an error converting between metric and English units

These failures fall upon the programmers and engineers that did not responsibly verify their code or design. There are several cases where human lives were lost as a result. It is still an open issue of what might be done to prevent these failures, aside from more rigorous testing. Can some legislation be passed? Should a programmer be held legally liable and responsible if his software fails and results in the loss of business productivity or even worse, the loss of life? Or should perhaps non-computerized alternatives be used for certain situations instead? How well can we trust computer models and computer simulations to make policy decisions?

Computer Crime

Computer crime covers a wide range of activities. Many of these include "traditional" crimes such as theft, fraud, embezzlement, etc. However some new crime includes stealing data, cracking, viruses, and piracy.

Data stealing refers to unauthorized access to private data stored in a variety of databases. In some cases, the Internet has made this easier by allowing an alternate point of entry rather than physical infiltration. One spectacular case involved the online retailer CD Universe. In January of 2000, a hacker claimed to have stolen 300,000 credit card numbers from CD Universe and distributed up to 25,000 of them on a Web site after the retailer refused to pay a $100,000 ransom. A similar incident also occurred with America Online.

Cracking refers to breaking into computer systems without authorization. Often this is called hacking, although the original term “hacker” was not malicious, but used to identify an individual deeply engrossed with some technology. One of the most infamous hackers today is Kevin Mitnick, who was convicted in 1999 on various counts of wire fraud and sentenced to four years in prison. Mitnick admitted that he broke into a number of computer systems and stole proprietary software belonging to Motorola, Novell, Fujitsu, Sun Microsystems and other companies. Mitnick admitted using a number of tools to commit his crimes, including "social engineering," where he duped unsuspecting employees into giving him access by pretending to be an authorized user. Lessons like these teach us that a computer system is only as secure as its weakest link; in some cases this is the human operator, not the technology itself.

In July of 2002, the House of Representatives passed the Cyber Security Act, which stiffens crimes for hackers. The proposed maximum penalty is life in prison for certain acts that could lead to bodily harm or death (e.g., hacking into a traffic system and turning all stoplights to green when one should be red).

Also lumped into the category of “hacking” are attacks on network servers that do not actually destroy or steal data, but instead disrupt network services. For a week in February of 2000, a Canadian teenager known as “mafiaboy” conducted denial of service attacks on popular sites such as eBay, Amazon, Yahoo, and other Internet sites. These attacks prevented normal users from accessing theses sites. Estimates of the damage in terms of downtime and security investigations ranged from 7 million to 2 billion dollars. Since he was a teen, mafiaboy was sentenced by the Canadian court to 8 months in a youth detention center and 1 year of probation.

Computer viruses are a relatively recent phenomenon that has plagued almost everyone that uses a computer. A computer virus is a malicious program that spreads from one computer to the next, with the potential of destroying data on an infected system. With the advent of the Internet, it has become much easier for viruses to spread quickly across entire networks. A virus usually infects a computer by tagging along through an infected program that an unsuspecting user executes, or through email and other data files with programming languages associated with them. In 2000, David Smith wrote the Melissa virus, one of the first viruses to spread through email that infected Microsoft’s Outlook program. His program spread quickly and cost businesses an estimated $80 million in downtime. Despite attempts to cover his tracks, Smith was apprehended and sentenced to approximately 2 years in prison.

Lastly, computer piracy has been an issue for many decades, but the advent of the Internet has made it even easier to copy and distribute programs. Software piracy refers to the illegal distribution of copyright works. Typically this involves a business that makes multiple copies of a software product themselves and then sells each copy rather than purchasing all original copies from the manufacturer. However, software piracy also covers cases of an individual buying a software packing and then giving free copies to his friends. Piracy is a serious problem internationally since some countries have few or no laws regarding software piracy. In 1998 a German court sentenced an American man to 4 years in prison for copying Microsoft programs In 1999 a University of Oregon student faced 3 years and a $250K fine for Internet software/music piracy.

Copyrights and Infringement

Copyright laws protect a piece of work (e.g. a book, movie, computer program, etc.) from being taken, used or exploited by a party other than the author of that work. Copyrights grant exclusive rights to reproduce, modify and distribute copies by sale or transfer of ownership, or perform and display the work publicly.

Some people erroneously believe that getting a copyright for a piece of work is a complicated process involving lots of paperwork. This is not true. United States copyrights arise automatically once an original effort has been started and some aspect of it has been fixed in a tangible medium. In fact, you do not even have to put a copyright statement on the work (although it is a good idea to do so) since there is an implied copyright for works created after 1978. Actual registration is required only if legal action is warranted. Copyrights eventually expire after the lifetime of the author + 70 years, then the work becomes public domain and may be used by anyone freely.

Before the Internet, copyrights extended primarily to books, music, films, videos, and works of art.

However, with the advent of the Internet, all of the following are copyright:

- Messages, email or posted to a bulletin board
- Computer software
- Data files of all kinds
- Text, hypertext
- Multimedia
- Databases
- Visual images
- Sound
- Animation

This means that with the implied copyright, something as innocuous as an original message posted on a bulletin board is copyright! If someone else copies it, the person that copied the message could be infringing on a copyright! There are exceptions though – "Fair use" allows copying for purposes such as "criticism, comment, news, reporting, teaching, scholarship, or research" and is not an infringement of copyright.

There are several interesting copyright issues that have arisen with regard to the Internet:

- Zeidenberg Case, 1995. Zeidenberg purchased ProCD's CD-ROM of phone listings, and posted the contents to his Internet site. The District Court held that the plaintiff did not violate copyright laws; directory listings were merely "a collection of facts arranged in a commonplace, non-original fashion," and that the listings themselves were not copyrightable. However, the Seventh Circuit Court reversed the District Court decision based on the shrinkwrap licensing agreement.

- Playboy v. Frena. Frena was a bulletin board operator that had one if his users upload copyright pictures from Playboy magazine to his site. Frena argues that since the pictures were uploaded without his knowledge, he was not liable. Despite the defendant's lack of knowledge and direct involvement, the district court concluded that the defendant had infringed Playboy's rights: "[t]here is irrefutable evidence of direct copyright infringement in this case. It does not matter that defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement."

- Religious Technology Center v. Netcom. Netcom was an internet provider while the Religious Technology Center represented the Church of Scientology. They argued that a user of a Netcom account was posting writings of L.Ron Hubbard and violating copyright laws. The District court found Netcom not liable for "incidental copies automatically made on their computers using their software."

One of the most hotly contested recent copyright infringement cases involves sharing online music and media files. Napster software allowed users to share music files with one another over the Internet. Record labels and publishers sued the company for copyright infringement. In the summer of 2000, the court ruled in favor of the record labels. Since then, the company has struggled to survive and appease the media companies. This issue remains a hot one as online sharing of movies and other forms of media becomes more popular.

As you can see, legal issues regarding the Internet are just now beginning to be worked out. Undoubtedly new legal challenges will arise and the judgments made by the court will become landmark cases for the future.