Java Methods

A & AB

Object-Oriented Programming
and
Data Structures

Maria Litvin
Phillips Academy, Andover, Massachusetts

Gary Litvin
Skylight Software, Inc.

Skylight Publishing
Andover, Massachusetts

Skylight Publishing
9 Bartlet Street, Suite 70
Andover, MA 01810

web: http://www.skylit.com
e-mail: sales@skylit.com
support@skylit.com

Library of Congress Control Number: 2005910949

ISBN-10: 0-9727055-7-0
ISBN-13: 978-0-9727055-7-8

Appendix F: Computing in Context: Responsible and Ethical Computer Use

F.1 Prologue

When early humans harnessed the power of fire, they found it kept them warm, helped prepare their food, and kept wild beasts at bay, but could also burn down their huts or rage uncontrollably as a forest fire, destroying everything in its path. Humans have been playing with fire ever since. Technological progress has brought new benefits but also new dangers and fears. For instance, advances in nuclear physics promise unlimited sources of cheap energy. But they also threaten to pollute our planet with nuclear waste or destroy it completely in a nuclear war. Advances in chemistry, biology, and medicine are helping eradicate devastating diseases, develop new life-saving drugs and vaccines, and increase food production. But they also brought pollution, large-scale production of mind-altering drugs, and hideous chemical and biological weapons. Computer technology seems pretty harmless by comparison: bits and bytes flipping inside tiny silicon chips. But is it?

At the beginning of the twenty-first century we are still at the very dawn of the computer era. What will it bring us? This technology goes to the very core of humanity: the human mind, the way we acquire and process information and communicate with each other. Will computers help make us safer, better informed, or more free? Or will we become a population of networked slaves, duped by misinformation, serving an invisible master? As science-fiction authors have imagined the worst, professional ethicists and system developers have thought a great deal about how to keep it from happening. Issues of responsible computer use, computer ethics, security, and privacy have been in the foreground since the first computers were built. This field of inquiry, in fact, is much broader and more complicated than computer technology itself. In this brief overview we can only give you a glimpse of the many complex issues involved.

The first difficulty is the newness of the field. The use of more traditional technologies is governed by laws and ethical principles accepted in a community and transmitted from the elders to new generations. Computer technology, however, is developing and changing so fast that laws have been unable to keep up and customs and traditions have had no time to develop. Right now it is the younger generation, the teenagers, who have the most experience and savvy in using computers and the Internet. Your parents most likely can not teach you ethical computer behavior or good Internet manners. You are on your own, and you are holding the future in your hands.

Another problem is that Cyberspace is the first truly global phenomenon. It has no boundaries, no tariffs, no customs inspectors, no immigration visas. The distance

between point *A* and point *B* in Cyberspace is measured only by the common interest, opinion, and intent.

Of course, this allows inter-regional and international collaboration projects of unprecedented speed and scale. For instance, an organization called the Global Schoolhouse [1] maintains the Internet Project Registry, which lists hundreds of collaborative projects for all ages. However, like any society, the global society of Cyberspace has its "bad guys." A malicious computer virus released in a remote country can reach computer systems all over the world in seconds. A user in the United States can log into online gambling or pornography sites located halfway around the world. The Internet unites communities and countries with different legal systems, different customs and cultures, and different languages. How do you go about developing universal legal and ethical codes for all one billion users?

F.2 Responsible Use of Computer Systems

F.2.1 Formulating Ethical Guidelines

As in any other science and technology, the trained computer experts have a great deal of power to decide whether this technology will be used for good or for evil. Many professions, including doctors, lawyers, and civil engineers, have developed codes of conduct to describe the ethical and responsible behavior that defines a professional. They also have developed licensing requirements, which can include some knowledge and adherence to a professional code of ethics. The oldest professional code, the Hippocratic Oath [1, 2], was written around 400 BC, but its principles are held sacred by physicians to this day.

Until recently, the computer software profession was considered too technical or arcane to develop its own code of ethics. This is beginning to change. Professional societies have been developing and publishing codes of conduct for computer professionals.

Not long ago, The Association for Computing Machinery (ACM) has developed a General ACM Code of Ethics and Professional Conduct [1] and a Software Engineering Code of Ethics and Professional Practice [1]. ACM [1] is the oldest and largest organization for computer professionals. Founded in 1947, it has over 80,000 members worldwide. In the introduction to this code, the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices states:

> To ensure, as much as possible, that their efforts will be used for good, software engineers must commit themselves to making software engineering a beneficial and respected profession. In accordance with that commitment, software engineers shall adhere to the following Code of Ethics and Professional Practice…

The ACM's Software Engineering code includes the following principles:*

1. PUBLIC - Software engineers shall act consistently with the public interest.
2. CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
5. MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
6. PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
7. COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
8. SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

Many web sites (see, for example, [1, 2, 3, 4, 5, 6]) have collections of links to other codes of ethics, as well as courses, papers, case studies, and other educational recourses.

* Copyright (c) 1999 by the Association for Computing Machinery, Inc. and the Institute for Electrical and Electronics Engineers, Inc. This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice.

F.2.2 Maintaining Professional Standards

Professional licensing is a formal procedure, usually mandated by the state government. Its purpose is to ensure public safety, health, and welfare and to protect consumers. Certification is usually voluntary; it documents the completion of a course of study and/or passing a certification exam. Professional licensing is common in many professions: civil engineering, accounting, the medical professions, and teaching. Licensing is often called certification, too.

The idea of certifying software professionals has run into many difficulties and faces some objections from the professionals themselves. The main difficulty is posed by the rapid changes in the field and narrow specialization of the software professionals. It is hard to formalize what constitutes professional competence and even if one manages to do that, the formula may change drastically in just a few years. Proponents certification point out that certification can still test core professional knowledge, including computer ethics and responsible computer use.

ACM [1] started a certification program in the early 1980s, but abandoned it later due to the lack of interest and resistance among its members. In 1998, the Texas Board of Professional Engineers adopted software engineering as a distinct discipline under which engineering licenses can be issued. The Texas rules have been widely discussed as a model for licensing software engineers in other states. However, the current status of the Texas program is unclear, and other states did not pick up this initiative. In Canada, at least three provinces (Alberta, British Columbia and Ontario) license software engineers.

At the national level, the most influential professional organizations for certification of software engineers are The Institute for Certification of Computing Professionals (ICCP) [1] and IEEE (the Institute of Electrical and Electronics Engineers, pronounced Eye-triple-E) [1]. ICCP offers a certificate for Certified Computing Professional (CCP™) [1]. Sample certification tests are available at the ICCP web site. IEEE offers Certified Software Development Professional Program [1].

Most successful certification programs, however, are managed by the software companies and are geared towards specific software technologies that these companies offer. Microsoft, for example, has a number of certification programs, including Microsoft Certified Software Developer (MCSD) and Microsoft Certified Application Developer (MCSA) [1]. Sun Microsystems has many narrowly specialized certifications for Java software professionals, such as Sun Certified Developer for the Java 2 Platform, Standard Edition or Sun Certified Web Component Developer for the Java 2 Platform, Enterprise Edition [1].

F.2.3 Regulating Users

Apart from ethical issues for computer professionals, there are ethical rules and acceptable use policies for computer users. Almost every school, college, and company has established a set of rules for using its computers and networks. A typical set includes rules for maintaining system integrity, rules against storing, posting, or e-mailing obscene or offensive material, rules against downloading copyrighted materials, and a ban on exceeding allocated bandwidth by downloading or sending excessive amounts of data via the organization's LAN or WAN. Users are prohibited from intentionally introducing computer viruses, hiding their identities or impersonating other users, spreading chain letters, and so on. Refer to your school's acceptable use policies. The acceptable use policy may also define the user's right to privacy and stipulate the organization's right to monitor communications and system access by its students or employees.

However, no set of rules and regulations can replace general politeness and common sense. Just like in other areas of life, computer and especially Internet users should develop a kind of etiquette, a set of good manners for dealing with others. *Netiquette*, or good manners in Internet use, are widely discussed on the web. A Google search for "netiquette" returns over 22,000,000 hits! A good place to start is `netmanners.com` [1]. Note a popular quote from *Letters on a Regicide Peace* (1796) by Irish political philosopher Edmund Burke [1] (1729-1797) at the bottom of that page:

> "Manners are of more importance than laws. Manners are what vex or soothe, corrupt or purify, exalt or debase, barbarize or refine us, by a constant, steady, uniform, insensible operation, like that of the air we breathe in."

As in any etiquette, the most important rule is to remember that there are human beings on the receiving end and to care about them.

F.3 System Reliability and Security

To most casual computer users, system security and reliability mean keeping their computer virus-free and backing up their files once in a while. We rarely think about the enormous problem of maintaining the security of computer systems and networks. In a developed country, computers run military and civilian communication systems, utilities (electrical grids, water purification plants, etc.), financial institutions, (banks, brokerages, stock exchanges, etc.), space exploration

systems, medical records and patient monitoring systems, industrial facilities, online commerce, media, document archives, and so on. All these systems are vulnerable to malfunctions, sabotage, or terrorism; yet they need to provide uninterrupted service and maintain the integrity of data.

F.3.1 Avoiding System Failure

Even in the absence of malice, hardware and software reliability pose huge problems for developers. A system's overall complexity and the interdependence of its components sometimes exceed the ability to test and manage them effectively. Anecdotes abound of major failures and losses caused by tiny errors in software code. The Mars Polar Lander crash in 2000, for example, was reportedly due to a single faulty line of code that used the wrong units of measurement [1].

The costs of system failures to businesses can be staggering. According to a fairly recent study [1], amazon.com, for example, would have lost $180,000 per hour of unplanned downtime in the year 2000. This number would be much higher now. A brokerage would have lost, on average, $6,450,000 per hour!

One of the early projects on fault-tolerant computers was sponsored by NASA's Jet Propulsion Laboratory (JPL) in the 1960s. JPL invited Algirdas Avizienis, a researcher from the University of California Los Angeles, to develop a fault-tolerant computer system for use on long space missions. In those days, computer failures occurred much more frequently than now. A computer on board a deep space mission could not afford to fail. Avizienis named his computer design STAR, for Self Testing and Repair. The reliability of the STAR computer was achieved by integrating several duplicate redundant versions of each subsystem [1].

All mission-critical applications employ some level of redundancy: uninterruptible hot-swappable power supplies, multi-path input/output adapters, and so on. But hardware alone cannot assure reliability. To operate without failures, a reliable system must have trained personnel available and sound management and control procedures in place. There are experiments in fault-tolerant software, too. The same critical software module may be implemented in two versions by two independent teams of developers, then run in parallel on two systems that compare the computation results at critical junctions.

F.3.2 Maintaining Data Integrity

Another aspect of system reliability is the problem of maintaining data integrity in large databases and data archives. Electronic data is often the most valuable asset in an enterprise. The integrity of data is achieved through established back-up procedures and data validation.

Digital data archives pose their own problems: besides protecting data repositories from physical damage, the data must be protected from obsolescence and what is known in the industry as "bit rot" or "bit decay" [1, 2]. The optical or magnetic media that store the data have a limited life span; the data must be periodically reproduced on new devices and in new formats that are currently in use.

F.3.3 Protecting Secure Systems

To most of us, system security appears in the form of antivirus software and a few passwords we use to log into web sites for e-mail or shopping. But computer system and network security is a much larger problem. Security is essential in military applications, financial and business systems, e-commerce, law enforcement, and other areas. Security issues include physical protection for computer systems and data storage, secure access to data, and secure communications. The primary techniques for secure access are authentication through password protection, data encryption, and encrypted data transmission with authentication of sender.

Launching computer viruses and breaking into secure systems is not only unlawful; it is also unethical. Unfortunately, talented computer enthusiasts sometimes consider it a badge of honor to launch a new virus or to "hack" into a secure system or a web site. The same person would never enter your home without permission; but, for no obvious reason, a hacker considers it okay to break in to a computer system, often causing panic and millions of dollars in damage. Other forms of abuse include the "denial of service attack" — programming multiple dummy service and authentication requests from web site servers, which tie up and may potentially shut down the site. There also have been reports of personal computers with a fast Internet connection being invaded by so-called "Trojan horse" software, which surreptitiously used the computer to relay "spam" (junk e-mail) or sexually explicit material [1].

F.4 Legal Issues

The rapid emergence of Cyberspace has posed difficult questions for lawmakers and legal experts. The existing laws for protecting security, privacy, and intellectual property rights are not always applicable to the new environment. They have to be reinterpreted and extended, and new laws must be written. More importantly, laws ultimately reflect the prevailing customs and practices of their community. But with Cyberspace a new community has emerged that has no national borders and no traditional customs. The overwhelming majority of people in this community are children or teenagers. This new generation of computer users is creating new customs and practices that will eventually be codified in law. Therefore it is important that this new Internet generation be better educated in the value of the rule of law, the application of existing laws, and the concepts of ethical behavior and responsible use.

The legal issues in Cyberspace that have generated most debate are privacy, freedom of expression versus censorship, and intellectual property rights. As the recent debate has demonstrated, these are complicated issues on which thoughtful people can sometimes disagree.

F.4.1 Privacy

Over the past several decades, judges and constitutional lawyers in the United States have come to recognize a "right to privacy" as one of the fundamental rights guaranteed by the first ten amendments to the US Constitution. This right, enshrined and expanded in several landmark decisions of the US Supreme Court, means that a government agency must show it has a "compelling state interest" before it can intervene in a citizen's personal affairs. The requirement for employers is similarly strict.

At the same time, as technology in developed countries gets ever more sophisticated, the expectation of actual privacy is becoming more and more unrealistic. In any developed country, there are hundreds of computer records for nearly every citizen. In the United States, the federal and state governments keep social security records, tax records, and driver's license and motor vehicle registration records. Insurance companies keep insurance policies and health records. Credit bureaus keep credit card and mortgage records. Banks and investment firms keep financial records. Clinics and hospitals keep health records. Utility companies keep your account records, including a record of every phone call you make. Your every e-mail may be archived on several computers. Every web site you visit is logged in a server log

somewhere. If you go on a shopping spree to your favorite mall and your credit card processor is alerted to your unusual spending, a fraud agent can track you in real time as you go from store to store charging purchases.

Who has access to all this information? "Authorized personnel" — that is to say, thousands of government and private sector employees. Is this information secure? We can only guess.

Each citizen of the real world has an electronic incarnation in Cyberspace. In the last several years, "identity theft" has become a new and serious threat to privacy [1]. In this crime, a criminal uses your personal data (such as your social security number, address, and credit card accounts) to assume your identity, opening credit cards or bank accounts in your name.

Another important privacy issue is the right of employers to monitor the telephone, e-mail, and other communications of their employees or to monitor employees using video cameras. With inexpensive web cameras, even a home computer user may be tempted to monitor a babysitter or a cleaning person while away from home. Is this legal or ethical? Legislators and ethicists are still struggling with these complicated issues. At the time of this writing, Google, Inc. is fighting in court a federal government's request to release search records [1]. The government is seeking a sample of records in order to justify its efforts to revive a law making it harder for children to see online pornography.

F.4.2 Censorship vs. Free Speech

In many societies, citizens are accustomed to enjoy great freedom of expression and the press. In the United States, these freedoms are defined as "fundamental rights" and protected by the First Amendment to the Constitution. There are limitations, though. Obscene speech, hate speech that incites to violence, and certain other forms of expression may be banned or restricted to adult audiences. These restrictions are much harder to control on the Internet because information is more readily accessible and minors are often the savviest computer users in the family.

Some have argued that technology, as it creates new ethical problems, also sometimes creates the means of solving them. For instance, filtering software can screen material on the Internet for certain types of words or images, automatically denying a user access to sites deemed obscene. However, software programs are not great judges of subjective human categories like obscenity. As an example, activists point out that word-screening pornography filters can also block access to information about breast cancer. As usual, the promise of a technological "quick fix" is illusory.

A fairly recent debate can serve to illustrate these tough new questions. The debate is over whether public libraries should be required to ban access to pornographic web sites. In a 2003 ruling, the US Supreme Court upheld a law that requires public libraries to install pornography filters on all computers with web access in order to continue receiving federal subsidies and grants. Interestingly, the American Library Association (ALA) argued against this decision. In its statement [1], ALA says:

> "Libraries are a major information source in our society for access to the larger world of human expression. For some, they are the only available access point. Libraries connect individuals with the ideas, information, and images they seek. Libraries that raise barriers to access damage their credibility with their users.
>
> By providing information across the spectrum of human interests, and making them available and accessible to anyone who wants them, libraries allow individuals to exercise their First Amendment right to seek and receive all types of expression, from all points of view. Materials in any given library cover the spectrum of human experience and thought, even those that some people may consider false, offensive, or dangerous.
>
> In the millions of Web sites available on the Internet, there are some—often loosely called "pornography"—that parents, or adults generally, do not want children to see. A very small fraction of those sexually explicit materials is actual obscenity or child pornography, which are not constitutionally protected. The rest, like the overwhelming majority of materials on the Internet, is protected by the First Amendment."

Yet in many states, minors are forbidden from unsupervised access to explicit sexual material in other settings (movies, magazines, etc.). Neither the Supreme Court's decision nor the ALA's objection is likely to end the debate on this issue.

A more recent controversy surrounds Google's and Yahoo's decisions for their operations in China to comply with the Chinese government censorship laws that prohibit free political speech [1, 2].

F.4.3 Intellectual Property and Copyright Issues

Another heated debate is raging over intellectual property rights, or, to put it plainly, the right of Internet users to copy and swap MP3s, videos, and books. The battle line is drawn between the recording industry and the young generation of Internet users who are used to getting their music free on the web. The most celebrated case was

Napster, which was litigated out of existence a few years ago. Aficionados of free music retaliated by embracing peer-to-peer (p2p) networks, which enable Internet users to locate and swap music and video files without a central repository.

Are such networks ethical? Are they legal? Again, there is no single answer to these tough questions. About the ethics there is serious disagreement. The recording industry argues that recording artists, producers, and engineers should get fair compensation for their hard work. Music fans claim that music sharing on the Internet actually promotes music, helps less known artists, and ultimately increases CD sales. After all, they argue, if you set up a shelf for swapping books, no one will find it illegal or unethical. Many youth hostels and vacation spots have such take-a-book-leave-a-book shelves. More people get involved in reading and eventually buy the books they liked. For many young people, the Internet offers such a swap center for music.

From the legal prospective, it is clear that copyright laws protect intellectual property such as books, music, videos, and computer software [1, 2]. Recently, the recording industry took larger p2p software providers to court and claimed some victories. But enforcement alone cannot stop people from getting around the law. For example, music swapping web sites can be set up overseas in countries that have not joined the international convention on copyright protection. Because the industry must rely on the good will of its customers, conflicts like this will eventually be resolved through some market-demanded compromise. The music companies cannot afford to alienate their best customers, and music lovers cannot afford to keep breaking the law. New technologies and service models have emerged to meet the demand, such as a pay-per-song model.

F.5 Searching the Internet

The vast amount of material on the Internet raises another question with ethical implications: how can a user distinguish good information from bad?

F.5.1 How to Tell Good Information From Bad

In a library, you can be sure that a librarian has screened every item before putting it on the shelf; it may not all be true, but at least someone knows it's there. Similarly, every newspaper or magazine is required to publish a column called a "masthead," which tells you who is on the editorial staff, where it is published, and so on. The Internet, however, provides no such screening mechanisms. There is no editor, no masthead, and no librarian. Anyone can post anything, in any language, impersonating anyone and claiming anything.

Everyone who posts on the Internet should check that what he or she is posting is accurate. But not everyone does so. Therefore it is your responsibility as the user to take all the needed precautions. It's up to you to keep people from stealing your money – or wasting your time.

Some people, figuring they'll trust the market, use a "relevance ranking" to choose which sites to believe. However, no search engine is perfect in ranking documents. In addition, some unscrupulous web sites use artificial tricks to improve their rankings in search engines. Google, which has become so trusted that "to google" is now used as a verb, is slightly more helpful. Google lists sites in order from starting with the site most often linked to by others, serving as a built-in popularity index; a top spot on a Google search means many people found this site worth linking to. However, certain tricks could boost a site's ranking there as well. Your ultimate judgment may be subjective: does this appear to be an honest, competent, and objective attempt to share knowledge with you?

The following rubric may help separate the wheat from the chaff:

- Reliability:
  Who posted this site? A Student? A teacher? A college professor? An organization?
  Do I know this person or organization? Should I learn more about it first?
  How did I get here? From a search engine? From a reputable list of annotated links?
  Is there evidence of the mastery of the subject matter?
  Is there a hidden ideological agenda or bias?
  Is there a commercial interest?
- Relevance:
  Is this information relevant to my subject of interest? Does it answer my questions?
  Is it concise enough?
  Is this the primary source or just rehashing stuff from another website?
  Does it have links to more relevant sites?
- Timeliness:
  Is this information current?
  When was this site last updated?
  Does it reflect recent developments or events?
  Is the bibliography, if any, fairly recent?

- Completeness:
  How complete is this information?
  Are there links to other web sites?
  Are there bibliographical references to books or magazine articles?
  Do I know of any facts or topics that are not covered here?
- Presentation:
  Is it readable?
  Does it look like a professional or an amateur effort?
  Do the spelling and diction suggest that the author is well educated and has put some care into developing the site?
  Is this the best way to present this information? Would other ways be more effective?
  Is the site fairly logical and easy to navigate?

Don't waste your time with questionable sources: other web sites are just a click away.

F.5.2 Effective Searches

Now you are ready to search. Where do your begin? A good search engine will help you navigate through an ocean of documents, but ultimately it is your searching skill that determines where you land. Some colleges offer a semester-long course on the best search strategies to help students master this tricky tool. We can offer only a few quick pointers designed to help you get started.

First, try "googling" *effective internet search strategies*.

```
Search: effective internet search strategies
```

This search will give you about 101,000,000 hits. Now try putting the same query in quotation marks:

```
Search: "effective internet search strategies"
```

Notice that you get fewer than 500 hits. The quotes indicate that you are searching only for the complete phrase with all the words grouped together in that order. This gives you more relevant hits. When you follow some of these links, you will receive invaluable free advice from experienced librarians and researchers on how to search. Apply the above criteria to choose a good site.

Now, suppose you need to write a general report on eagles and their habitat. You google *eagles*.

```
Search: eagles
```

What do you get? 75,200,000 hits. Sure enough, the top one is the official site of Philadelphia Eagles, a football team. The next one is the site of the Eagles band. You have to be more creative and specific. For example, you can use the "Advanced Search" option to exclude football. You can construct more complex "Boolean" queries including certain words and excluding others. For example (*eagles* and (*habitat* or *"birds of prey")* but not *football* (Figure F-1). It also helps to replace the plural *eagles* with the singular *eagle*, which is more likely to be found in scientific texts.

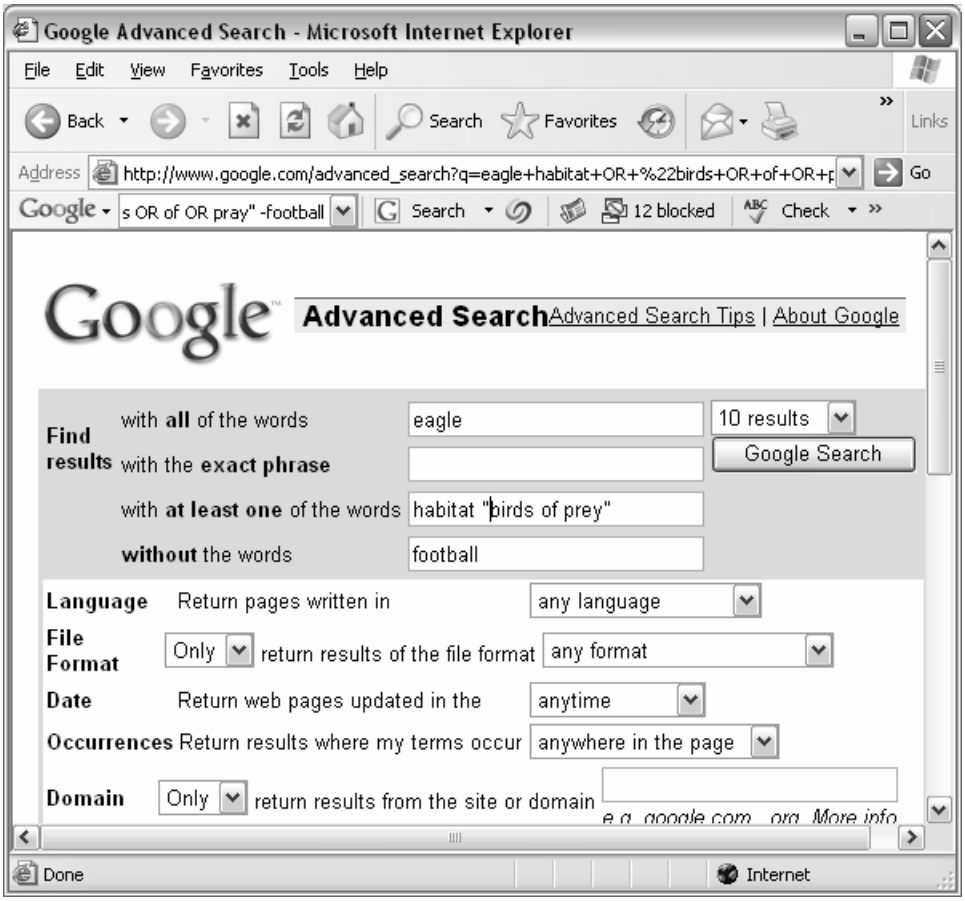

Figure F-1. Advanced "Boolean" search in Google

This more targeted search gives a number of relevant links. Among them is a link to :Cornell University's Lab of Ornithology site which has a link to a detailed page about bald eagle [1]. This page meets our criteria for a reputable source. Another link, to a `zoo.org` page [1], also provides relevant information. Unfortunately, you might find exactly the same information, with the same picture, posted without appropriate attribution on some other web sites, such as [1]. Powerful search engines enable an interested person to find such lapses in judgment easily.

You will also find such links as `eagles.org` and `baldeagles.org` [1, 2]. These sites, run by the same organization, while potentially useful, have an activist agenda for protecting eagles and their habitats. They probably come up near the top of the Google search because they are widely publicized and many other activist sites refer to them. It might be better to leave them for references specific to the conservation efforts. Unfortunately, the description from `baldeagles.org` is copied verbatim without an appropriate attribution on a commercial fishing tour site [1]. Not a big crime, of course, but a brief notice "reproduced with permission..." or "courtesy of ...") would not hurt.

This is the reality of the Internet today. As you can see, the Internet can strain your critical thinking skills to the limit, and, if you are an author of online material, it will also pose some ethical dilemmas. It is in your power to move the Internet in the direction of ethical and responsible behavior.

F.6 Conclusion

This appendix has presented a brief overview of four important ethical issues arising from computer and Internet use. For all of these issues – responsible use, system security, legal rights protection, and accuracy of Internet contents – technology creates some complications, some solutions, and some more complications. As long as humans continue to be curious and ingenious animals, this dynamic will continue.

The best approach to all these issues may be the most general. The survival skills that bring success in school and in life — skills like critical thinking, problem solving, and moral reasoning — are also the best bet for handling the ethical quandaries that computers create. Certain character traits — empathy, adaptability, attention to detail — will help as well. And of course, a mastery of the technical details is almost essential. Used correctly, computers and the Internet can help you in acquiring this knowledge, character, and set of skills.