Main content

Chapter 17

Making Decisions about Computers, Information, and Society

Change font sizeMain content

Chapter Contents

Chapter Introduction

r studying this chapter, you will be able to:

Use ethical reasoning to evaluate social issues related to computing
Understand the issues involved in digitally sharing copywritten intellectual property, such as music, videos, photographs, books, and video game software
Discuss trade-offs between the rights of personal privacy and governments' concerns with safety and security

Provide arguments that support and oppose hackers who claim to be performing a social good
Describe cyberbullying and why legal remedies are so difficult to apply
Explain the potential dangers that have arisen from the enormous growth of social media

Discuss how social media makes it easier to globally disseminate rumors and false information that can have a profound effect on governments worldwide

Main content

Chapter Contents

17.1 Introduction

Most of this book has focused on the *technical* issues of computing. For example, you have read about the mathematics of algorithmic efficiency (Chapter 3), the hardware implementation of computer systems (Chapters 4 and 5), computer networks (Chapter 7), and software development (Chapters 9 and 10). However, in this chapter, we focus on the *human* issues lurking behind these technical details. We can't provide a comprehensive list of such issues; such a list would be way too long, and it is growing daily. Instead, we introduce skills that will help you to think and reason carefully when making personal decisions about computing. This chapter also discusses important societal issues related to information technology and personal privacy and points you toward resources to help you explore these issues in greater detail. Making critical decisions about computing technology is unavoidable. Increasingly, our society is being driven by the access to and control of information. As citizens of our communities, our country, and the world, we want our decisions to be well informed and well reasoned.

Whenever humans make decisions about things they value, there are conflicts and trade-offs. The field of **ethics**, the study of moral philosophy, has a long history of looking at how to identify and resolve such conflicts, and we will borrow from several classical theories of ethics. In this chapter, we present a number of case studies built around complex ethical issues related to computing and information. For each case study, we present the issues as well as arguments used to support and oppose certain positions. We then describe methods that allow us to understand and evaluate these arguments in terms of their ethical implications. Finally, we will investigate the enormous impact that social media is having on both our personal privacy and our access to information. When you finish this chapter, you should have an increased appreciation for the complexities of human/computer interactions as well as an enhanced set of skills for thinking and reasoning about these complex interactions.

Main content

Chapter Contents

17.2 Case Studies

17.2.1 Case 1: Is It Sharing or Stealing?

You are probably familiar with the concept of movie and music "piracy." You may have been bombarded with advertisements from the recording and movie industries warning of the negative repercussions of copying or sharing copyrighted material, such as music, videos, photographs, books, and video game software. In this section we introduce the basic concepts of ethical decision-making through a case study, the case of the first successful peer-to-peer file sharing system, Napster.

“Sharing” of music and movies was already commonplace prior to the popularity of the Internet, but it was fairly limited. At the time, music and movies were distributed on tapes, and it was not hard to physically duplicate a tape and give it to a friend. Although this type of sharing was illegal (and the recording and movie industries took some steps to prevent it), it wasn’t a major threat to their businesses because the amount of labor involved in copying was high, and copies were usually only shared with a small number of close friends. True “piracy” involves the mass production of bootleg products for sale, not small-scale sharing between friends.

In the spring of 1999, two Northeastern University students, Shawn Fanning and Sean Parker, created a system intended to simplify the sharing of computer files with strangers. The users of the system were mostly other university students, who had ready access to fast Internet connections and who were interested in obtaining music files that other students were willing to share. Fanning and Parker called their system “Napster,” and it became so popular that several universities noticed their campus networks slowing to a crawl because of student music downloads.

The Napster system is a wonderful example of how technical achievements in computing can have significant social effects. The Napster software set up what’s called **peer-to-peer file sharing**. As diagrammed in Figure 17.1, Napster’s software electronically “introduced” two users who are distant from Napster and from each other. Once Napster helped these users find each other electronically, the file sharing took place between the users, *not* through Napster. This meant that although thousands and thousands of bootleg copies were being made, Napster itself wasn’t making or distributing them. Napster simply helped connect individuals to enable one-to-one swaps. It was not clear if what Napster was doing was even illegal, let alone unethical.

Figure 17.1Peer-to-peer file sharing system created by Napster

In many ways Napster was acting like applications such as Angie’s List or Home Advisor. These applications publish lists of companies who provide useful services such as plumbing or home remodeling. Users can digitally search these lists, select someone to provide the needed service, and contact that individual directly. The listing service itself only connects users to providers; it does not do any of the actual work.

On December 7, 1999, an organization of recording companies filed suit against Napster in U.S. district court on grounds of copyright infringement. During the highly publicized arguments that followed, the recording companies insisted that Napster was a conspiracy to encourage mass infringement of U.S. copyright law. By most accounts, the majority of music that Napster users “shared” was copyrighted, and most of the copyright holders objected to the copying of their music without royalty payments. The recording industry saw Parker, Fanning, and Napster as no different from the bootleggers who were mass-producing fake copies of CDs and movies.

Napster's supporters argued that the system was merely acting as a search engine, providing information on songs and their location, but not participating in the actual exchange of copyrighted information. They argued that Napster could not be held responsible for what peers (Users A and B) did with that information in the peer-to-peer file-sharing system depicted in Figure 17.1.

In addition, Napster contended that there were significant legal uses for the service. It pointed out that copyright law allows a person who has purchased a recording in one format to transfer it to a different format as long as it is for personal use and is not resold. Someone who legally owned a song on CD could use Napster to acquire a copy in MP3 format, something they are legally entitled to have. Furthermore, both peers in each swap were transferring the file without any payment to each other or to Napster, and therefore (according to Napster) the copying should be considered *fair use*, the legal doctrine that allows for brief excerpts of copywritten material to be copied or quoted under certain restricted circumstances.

Eventually, Napster lost the case and subsequent appeals, and it ceased operating as a file-sharing site in 2001. However, other peer-to-peer file-sharing systems sprang up on the web, and illegal music sharing (as well as movie, book, and video game software sharing) via the Internet continues, much to the chagrin of recording companies, publishers, game developers, and the movie industry. BitTorrent (the most popular peer-to-peer file sharing system) represents about 5% of all Internet traffic, while YouTube currently accounts for about 25% of all music streamed worldwide, far more than any other site.

This case leads to many ethical questions, but two are worth special attention:

1. Is it right to swap copyrighted music or book files, download and watch copyrighted videos, or use copyrighted photos without permission?
2. Is it right to provide a search engine whose only purpose is to allow users to search each other's databases of copyrighted music and book files, videos, and photos?

At its core, these are neither technical nor legal questions. The law tells you what you are allowed to do, while technology determines what you are able to do, but neither can tell you whether it is morally right or wrong to do it. In the best case we try to establish what is right, and then write the laws so as to encourage this type of right behavior. So how do we reason about what is right?

Asking Ethical Questions. A legal question, we take to a judge. A technical question, we take to a scientist or an engineer. But who can help us with an ethical question? In this section, we look to ethicists for guidance about getting an answer to an ethical question.

Earlier we defined ethics as the study of moral philosophy—how to decide if something is morally right or wrong. A fundamental question in ethics is what criteria to use when "measuring" the rightness or wrongness of a particular act. Over the centuries, ethicists have championed different criteria and developed schools of thought about how to label an act as good or bad, better or worse. One of the most influential schools is called **consequentialism**. As the name implies, a consequentialist focuses on the consequences, or outcomes, of an act to determine if the act is good or bad. If the consequences are on the whole good, then the act is good. If the consequences are mostly bad, then the act is bad. However, in focusing on the goodness of an act, we have to ask, “Good for whom?” For instance, in our music example the copying is certainly good for people who get free music. But, just as clearly, most music copyright holders are convinced that music copying without the payment of royalties is bad.

The most well-known consequentialists are the utilitarians. Utilitarians answer the question “Good for whom?” with a hearty, “Good for everyone!” Imagine a cosmic calculator that is capable of adding up human happiness. **Utilitarianism** holds that a moment before an act takes place, the cosmic calculator adds up all human happiness and puts a happiness number into the variable HAPPINESS_BEFORE. Then the act occurs. We wait awhile, long enough for the consequences of the act to become visible; then we use our cosmic calculator again and put a second happiness total into the variable HAPPINESS_AFTER. According to a utilitarian, the act in question is “good” if (Just to satisfy the law of trichotomy, if HAPPINESS_AFTER = HAPPINESS_ BEFORE, a careful utilitarian would declare the act to be ethically neutral.)

HAPPINESS_AFTER > HAPPINESS_BEFORE

or “bad” if

HAPPINESS_AFTER < HAPPINESS_BEFORE.

Of course, there is no cosmic calculator, and quantifying happiness is no easy task. Clearly, using the utilitarians’ criterion requires subjective judgments. But making consequences count and ensuring that all people are taken into account when making an ethical judgment both seem like good ideas. So let’s try out two short utilitarian arguments to explore whether mass copying of music files (as well as movies, books, photos, and videos) is morally right.

Utilitarian Argument #1: Copying Is OK. First, there are many more music listeners than there are music publishers. Music listeners are very pleased to get convenient, virtually free access to all this music. Furthermore, music publishers should be pleased to get so much free publicity for their product. When radio stations play music, it’s free to listeners, and many listeners go out and buy the music that they’ve heard on the radio. The same thing happens to listeners who download music files. Many choose to buy legal copies, even though they do not need them, so that artists get paid, or they may choose to purchase additional music by the same artist. There is some market research that shows that downloading music files can even increase music sales. Although opponents of music file sharing point out that overall music sales revenue has fallen dramatically since 1999, this cannot be completely blamed on file sharing. During the CD era, people bought whole albums. Today music retailers like iTunes and Amazon encourage consumers to buy one song at a time, which has also hurt overall album sales.

Death of a Dinosaur

The Virgin Megastores in New York City’s Times Square and Union Square were the two largest music stores in the world, sprawling over 180,000 square feet of retail space and selling an estimated $55 million worth of recordings every year. Not only were they important economic engines for the entertainment industry, they were also popular gathering places for hard-core music lovers and emerging artists. Unfortunately, even megastores with massive sales volumes and huge financial backing are finding it difficult to compete with online music sites like iTunes and the ease of digital copying. “It’s clear that the model of a large entertainment specialist working in a large retail space is not going to work in the future,” said Simon Wright, the CEO of Virgin Entertainment Group, North America.

In February 2009, the Times Square store closed its doors for good, with the Union Square store following suit just four months later. In the words of a former Virgin employee, "The large retail music store is a dinosaur, and we all know what happened to them!"

Utilitarian Argument #2: Copying Is Not OK. Although some early research suggested that music file copying may have initially encouraged CD buying, later research has shown that overall retail music sales have declined rapidly—down over 50% since 2000. That's the real, long-term effect of widespread copying of copyrighted materials. If the people who publish music can't make a fair profit, then less and less music will be published. Eventually, both music listeners and music publishers (including the people who make the music) will lose. In addition, copyright protection is the law. This widespread criminal activity will result in a widespread disrespect for the law in general, and that is a very dangerous consequence.

We have used an ethicist's idea, a utilitarian argument, to try to clarify the music file copying question, but instead of getting a clear answer to our question, it seems we've only managed to make things more confusing. Both sides of this issue seem to have some reasonable points. How are we to decide between them?

Let's admit something up front: Deciding what is morally right and wrong is not always easy. There isn't an all-purpose "ethics algorithm" that is guaranteed to provide a definitive answer to every ethical question. Still, we do have to make decisions about these issues, and we want to make those decisions on reasonable grounds, not just on whims or gut instinct.

Ethicists depend on what is called a **dialectic** to try to make better ethical decisions. In a dialectic, we move back and forth between different viewpoints, criticizing each and trying to learn from each. In a debate, one side is trying to win by undermining the opposition and building up the arguments for its position. However, in a dialectic the ultimate goal is for both sides to "win" by moving closer to the truth from two different perspectives. It's perfectly OK for people engaged in a dialectic to change their minds; in fact, that's the point. By systematically reasoning about the issue, the back and forth of argument can bring all parties to a more well-reasoned and justified decision. There's never a guarantee that the two sides in a dialectic will arrive at identical positions (although that is possible). More often, the participants end the dialectic still disagreeing, but hopefully with a better understanding of the other side's viewpoints.

In the spirit of a dialectic, let's examine the strengths and weaknesses of the two previous utilitarian arguments on the issue of music file copying. Both arguments cite evidence about music sales to bolster their position: People for copying claim that it increases the sales of music; people against copying claim that it decreases overall music sales. This is an example of a difference in fact, not just a difference of opinion. If the effect of music file copying is, in fact, to increase music sales, then the "copying is OK" people have a strong argument; if the effect is instead to decrease sales, then the "copying is not OK" people have a strong argument. When the dialectic uncovers an empirical question at the heart of a disagreement, the smart move is to check the facts.

According to published statistics, by 2016 global revenues from the sale of recorded music were less than half what they were in 2000. Even with the introduction of legal alternatives like iTunes, Spotify, and Amazon Music, album sales have continued to decline. So it seems that, on this point, the file copying opponents have a stronger argument.

What about the happiness of the legions of listeners who get free music? The opponents of copying again make an argument about short-term and long-term effects of copying: In the short run, listeners might get tremendous benefits; but in the long run, there may be far less music available for copying because artists and publishers will have far less incentive to create and disseminate music. This seems to make a certain amount of economic sense.

A third point raised by opponents of music file copying is the issue of illegality. The claim is that widespread disregard of copyright protections will have as a consequence widespread disrespect of the law, leading to more illegal copying of movies, videos, books, game software, or photographs. This claim is harder to demonstrate empirically than the music sales claim, but file copying advocates don't often claim that breaking the law will have beneficial effects, and we don't see many legitimate claims for anarchy.

The dialectic so far seems to favor banning music file copying, but there are a few interesting counterarguments. For example, some musicians (particularly relatively unknown ones) are enthusiasts of free music sharing. These musicians have not yet been able to get recording contracts, so they use Internet file copying as a way to distribute and publicize their music as well as generate ticket sales for upcoming live performances. For them, copying has positive consequences for both listeners and music makers. Advocates of copying also point out that only a small percentage of the money spent on legally purchased music goes to the artists. The rest of the money goes to the people who market the music. Some artists (both famous and not) have decided to give away their music on the Internet and make their money via live concerts. They are content to accept reduced sales of their albums if it means more people listen to their music, and hence come to their concerts.

An ethical dialectic rarely has a clear stopping point. We can almost always make better and better arguments, and there are often good points remaining on both sides of an argument. For example, we haven't discussed the fact that some music copying takes place using university and corporate computers, equipment that isn't supposed to be used for these purposes. Another persuasive argument is that if the United States decides as a country that we are better off without copyrighted music, then the law should be changed. Until then, it seems unethical to encourage breaking the law that currently protects copyrighted music.

In response to these concerns, some distributors have come up with new ways to sell music online. Apple's iTunes music store has shown that consumers will opt for legal copying if the system is convenient and reasonably priced. (See the Special Interest Box titled "The Sound of Music.") Starting in 2011, online music storage services (such as Apple iTunesMatch, Amazon Music, and Google Play Music) started to appear. These services allow users to store their digital music in a "locker" in the cloud, and then listen to that music on any of their digital devices (smartphone, tablet, computer, or game console). Users can upload any music they want to the locker and the locker does not have a way to verify whether the music was legally acquired. Users pay a monthly or yearly fee for this service, and part of this fee is used to pay back music studios. Arguably, this allows the locker services (and through them, the music studios) to make at least some money from illegally acquired music. Another approach is the Creative

Commons (CC) License, which is a copyright approach that allows intellectual property creators to have more control over copyright specifications, while encouraging legal sharing of music, videos, texts, and other intellectual property. Many artists release their works under a CC license, in return for donations through Patreon, Kickstarter, Indiegogo, or other crowdfunding sites.

The Sound of Music

Peer-to-peer music sharing became popular because it offered users virtually unlimited access to free music. Many computer scientists and ethicists thought that once people were accustomed to this, it would be virtually impossible to break them of the habit and charge for music. Steve Jobs and Apple Inc. did not believe this. Instead, they thought that if costs were reasonable and value-added services were provided (such as previewing, Billboard charts, audiobooks, and movie trailers), people would be willing to pay for legal access to copyrighted music. In 2003, Apple went public with the iTunes music store, a paid online music downloading service for its iPod MP3 player. The service started small with access limited to Mac OS X users and a few thousand songs on its playlist. However, it was an immediate success with more than 1 million downloads in the first week, and by 2016 it had reached nearly 30 billion downloads. It rapidly expanded to Windows machines as well as European and Asian users. Currently, the iTunes Music Store has the rights to hundreds of millions of songs and other audio and video materials. Amazon Prime uses a model where Prime users get free, legal access to millions of music tracks plus playlists and stations as part of their Prime membership. Obviously, those who did not think people would pay for online music after having free access were wrong. Perhaps the desire to act ethically is more deeply ingrained than we had thought.

Practice Problems

Review the music files you have listened to and movie files you have watched recently on your smartphone, tablet, or computer. What was the source from which you obtained these files? Do you know whether or not the files are legal to use? Or, if you have watched movies or listened to music on a site that allows user uploads (like YouTube, Twitch.tv, or SoundCloud), how do you know that the uploader didn't violate copyright? If you discover that a file was uploaded illegally, do you have any ethical obligation to stop using it?

Not every decision is an ethical one. For example, we usually don't think of choosing an ice cream flavor as being "good" or "bad." Write down 10 choices you have made in the past week. Then go back over the list and label each as ethical or not ethical. (Note: "Not ethical" is different from "unethical"; "not ethical" means there are no ethical issues involved.) After you've labeled all 10 choices, see if you can convince yourself to change your mind about one of the choices you labeled "not ethical."

To effectively build a utilitarian argument, we need to think of all the people who are affected by a decision. We call these people "stakeholders" in the decision. Choose one of the "ethical" choices you listed in Practice Problem 2. Now write down all the people or groups of people who are potentially affected, directly or indirectly, by your decision. Finally, list what each stakeholder may gain or lose from your decision.

Change font sizeMain content

Chapter Contents

17.2.2 Case 2: Legalized Snooping—Privacy vs. Security

Modern telecommunications networks have created significant problems for law enforcement. Over the past century, state and federal law enforcement officers have come to rely on the ability to set up "wiretaps," which allow them to intercept and record telephone conversations between suspected criminals. As phone technology has changed, however, it has become increasingly complicated to set up these wiretaps.

In the past, an intercept might have literally involved tapping a wire, using a piece of hardware similar to the Y-connector you might use to plug two sets of headphones into a single music player or smartphone. Such hardware could be installed at the local exchange (where the wire from your house connects to the phone company), and a recording device could be set up to record all calls.

Today, however, more than 50% of U.S. households have no landline-based phone, and that percentage is growing rapidly. Instead, people are turning to cellular phone and Internet phone technology (known as Voice over Internet Protocol, or VoIP) for their voice communications. This has created headaches for phone companies because it is no longer possible to tap a particular phone by simply hooking on to a particular wire in the local exchange. Cell phone calls can be made from anywhere, even from places where a person's phone company owns no cell towers. VoIP calls can be made from any place that the user can get an Internet connection, including the thousands of free wireless access points in cafes, libraries, and colleges. Phone companies now need complicated automated systems to follow a user from place to place, intercept his or her conversations, and forward them to law enforcement. Creating these **lawful intercept (LI)** systems can be both complex and expensive.

Furthermore, to make sure that every phone call could be tapped, it is necessary for Internet service providers (ISPs) to get involved. It is not hard for law enforcement to partner with phone companies, because there are only one or two major phone companies in each region of the country. With ISPs, however, there are sometimes dozens or even hundreds operating within a single city, and it is estimated that there are approximately 7,000 ISPs operating in the United States. It is also necessary for makers of VoIP software to get involved. In Chapter 8, you learned about cryptography and the use of encryption to protect communications on the Internet. If VoIP providers choose to implement cryptography on their systems, it would render wiretaps useless. Even though the police could listen in on the call, they would not be able to decrypt it, and it would sound like random pops and static.

By the mid-1990s, law enforcement officials saw these problems coming. They assumed (correctly) that smaller ISPs, VoIP software makers, and even some phone companies would not build LI systems unless required to. After all, building and operating an LI system costs a lot of money. As a result, many countries, the United States included, passed laws requiring everyone involved with telecommunications to cooperate with law enforcement and build LI capabilities into all of their systems.

Critics of LI worried that it would be a tempting target for computer hackers. Modern LI systems allow an authorized user to create a wiretap by filling in a few blanks in a computer program. It is no longer necessary to attach new hardware to create a wiretap. Because all phone calls now travel through computers as streams of data, that data can simply be copied and stored as it flows by. It is even possible to forward phone calls to another number, so every time a phone call is placed from a monitored number the police officer's phone rings, and he or she can pick up and listen in on the call in real time. For spies this functionality would be tremendously attractive. What if you could listen in on every call the president makes, or to all the phone calls of finance ministers or heads of major corporations?

This is exactly what happened to government and industry figures in Greece in 2004–2005. Persons unknown broke into the LI system for the major cellular phone vendor in Greece and installed illegal wiretaps on over 100 important Greek business leaders, civil servants, and politicians, including the prime minister. For nearly a year, hackers used the LI system to forward calls from tapped numbers to a series of "shadow phones," which allowed the hackers to listen in on conversations. This tapping was massive in scope and went undetected for almost a year. A more recent controversy over communications interception involved not hackers but the U.S. federal government itself, detailed in the Special Interest Box, "Hero or Traitor?"

Hero or Traitor?

In the summer of 2013, the exploits of American computer professional and former U.S. National Security Agency (NSA) contractor Edward Snowden came to light when he leaked classified information from the NSA to the international news media. Snowden disclosed thousands of classified documents that revealed the extent of the NSA's global surveillance programs, including monitoring of U.S. phone and email traffic and the phone conversations of over 35 world leaders. To some, Snowden was a hero, a "whistleblower" who showed how concerns for national security could be used to trample basic constitutional rights and invade personal privacy. To others, he was a traitor deserving imprisonment or worse. The U.S. Department of Justice charged him with violating the Espionage Act (punishable by up to 30 years in prison), and the State Department revoked his passport. Currently, Snowden lives in an undisclosed location in Russia and has received a Russian residency permit good until 2020. He has also applied for asylum to 21 countries, mostly in the European Union and South America.

Snowden's leaks have sparked numerous debates over mass surveillance, the proper balance between national security and personal privacy, and the constitutionality of the NSA's bulk data collection practices. The issues his case has raised will continue to be among the most controversial facing computer professionals and ordinary citizens alike in the years to come.

© Rena Schild/Shutterstock

In this case study, we will focus on the ethical implications of the decision to require all Internet and telecom companies to participate in the lawful intercept of voice communications. How does this decision impact personal privacy? How does it impact national security? We used utilitarian arguments to explore ethical questions about music file copying; but in this case study we will use a different kind of argument, argument by **analogy**, to explore questions about lawful intercept.

Analogies are commonplace, and that's one of the reasons they can be a useful way to think about ethical concerns. Most people are familiar and comfortable with the idea of explaining something unfamiliar by comparing it with something better known: "Rabbit tastes like chicken." However, when we apply analogies to ethics, we need to be more careful about the analogies we choose.

In any analogy between two "things," there will be both similarities and differences. For example, someone might say "swimming is like riding a bike—once you learn it, you never forget." Clearly, swimming is not *exactly* like riding a bike. (Just try swimming on a driveway or riding a bike in a lake.) The point of this analogy is clear: The person making the analogy thinks that the similarity (you don't forget it once it has been learned) is most important to the current conversation.

Analogies serve several purposes in ethical reasoning. When an analogy fits well, it helps us take advantage of decisions we have made in the past because if two situations are sufficiently similar we can apply the solution for the original problem to the new one. If the analogy does not fit well, this also provides useful information. If we can precisely identify the mismatch in the analogy, this often highlights some ethically significant aspect of the case.

In our analysis of lawful intercept, we consider two analogies that bear directly on privacy concerns raised by LI.

Analogy #1: Lawful Intercept Is Like Requiring Everyone to Record Their Face-to-Face Conversations. The first analogy focuses on Internet VoIP phone systems such as Skype, but most of our arguments apply equally well to cellular phone systems because they use similar technologies. Here's an expression of the analogy:

> If you and I decide to go for a walk in the woods and just talk, no one in his right mind believes that we should be forced by the government to carry microphones along to record our conversation so that they can listen to it. Before all this technology came in, every conversation was private. —Phil Zimmermann * in *Life on the Internet: Cyber Secrets* (PBS, 1996).

Using Analogy #1 to Analyze the Case. In this case, we can see some clear similarities between face-to-face verbal communication and Internet phone calls. They are similar in that people want to communicate directly with each other, and both types of communication are meant to include only the two individuals involved in the private discussion. In both types of communication, however, the actual audience may be larger than intended: In a voice conversation, people may be eavesdropping either by being physically close but unnoticed by the speakers, via a hidden microphone, or by a distant parabolic listening device. With VoIP, the conversation may be intercepted at any number of places along the electronic path between the sender and receiver.

In U.S. society, private conversations are, by default, free from government intrusion. This is not an absolute right—court orders can be obtained by law enforcement to use technology that invades private physical conversations. But these are the exceptions that prove the rule. Unless law enforcement officials can demonstrate probable cause, they are not permitted to take extraordinary measures to listen in on private physical conversations.

In both cases (VoIP and face-to-face conversations), there is a trade-off between privacy and security. In the case of face-to-face conversation, our society has decided not to record all conversations all the time, but to allow law enforcement officials to record certain conversations under the condition that they can demonstrate that they need to do so.

The analogy implies that requiring lawful intercept for all Internet-phone equipment would be the same as requiring everyone to record all of their private conversations, and to provide such recordings to the government as needed.

Problems with Analogy #1. The conclusion we reached just now may conflict with your intuition about the case. Notice that the argument we made applies to normal phone tapping as well as tapping VoIP. We know that most people accept the need for the occasional use of regular phone taps, so this seems to indicate a problem with the analogy. Our analogy must have left out some ethically significant factor.

This demonstrates another powerful use of analogy, which is to discover which parts of the case are most ethically relevant. Sometimes, when you make an analogy, the answer does not match your intuition. This could be because your intuition is wrong, but it could also be because the analogy simply does not fit. In this example, where is the mismatch?

There are many reasonable criticisms of analogy #1, but one big problem is that it has only three significant parties: The two parties in the private conversation plus the government. In the case of lawful intercept, there is a very significant fourth party, the telecommunications company. In the previous analogy, Zimmermann points out the absurdity of requiring individuals to record their own conversations and provide them to the government. But what if there was another party that was already well positioned to record any conversation? Could the government require that party to do so, and to hand over the recordings? This is exactly the case with Internet phone services. The Internet service provider is always in a position to record calls and provide them to the government. So the current analogy seems to fall down in that it is asking private citizens to perform the same task as a government-regulated telecommunications company. Perhaps we should look for an analogy that has this “middleman” feature built in.

Analogy #2: Lawful Intercept Is Like Suspicious Activity Reporting in Banking. There are two critical resources needed by criminals and terrorists that each require the help of a large corporation: means of communication and means of transferring and transporting money. With regard to the second need, U.S. banks are required to keep detailed records on all transactions and to notify the U.S. Department of the Treasury (through a Suspicious Activity Report, or SAR) whenever they detect unusual or suspicious transactions—for example, any deposit greater than $10,000. This careful recordkeeping and monitoring is expensive, but it allows law enforcement to find links between suspects and to discover and defeat criminal networks. In the same way, phone calls are an excellent source of information about the relationships between people—for example, intercepting phone calls between suspected terrorists is necessary to discover and prevent attacks.

Using Analogy #2 to Analyze the Case. This analogy seems to support the idea that telecommunication companies can be required to monitor phone usage and report certain data about suspicious activity. This would be consistent with the monitoring and reporting requirements placed on financial institutions. So, again, reasoning by analogy allows us to apply our solution to an old question (should banks be forced to report suspicious activity?) to a new one (should telecom companies be forced to report suspicious activity?).

What can we learn about lawful intercept from suspicious activity reporting? If you do a bit of research, you will discover that suspicious activity reporting differs in two very important ways from current lawful intercept systems. First, the suspicious activity report is initiated by the bank. The government does not get to continuously monitor what is going on in a bank. Instead, the bank is responsible for deciding what constitutes suspicious behavior and reporting it using the SAR form.

The SAR form is very simple, and this is the second major difference. It requires identifying information for those involved in the suspicious activity and a written description of the financial transaction. That is it. There is nothing in this comparable to completely recording a telephone call. The list of parties involved in the suspicious activity would be similar to listing the phone numbers or names of the people on the call. Listing the amount of the activity and the dates on which it took place would correspond to the times and dates on which phone calls took place, the lengths of the calls, and so on. But a financial transaction does not include the wealth of data that a phone call does, because a financial transaction is not a conversation.

So analogy #2 lends some support to the idea that we might require telecom companies to keep careful track of call records to monitor this information for suspicious patterns and to report suspicious activities to the government or law enforcement using a reporting form similar to the SAR. Like the previous analogy, it seems to contradict the idea that the government or law enforcement should be allowed direct or unsupervised access to the data. It does not seem to tell us, directly, whether or not the telecom companies should be recording and storing the actual contents of calls.

Making a Decision. In most cases, just having a convincing analogy is not enough to be sure we are making the right decision. Even if an analogy appears to fit, there is always a good chance that we are overlooking some morally significant factor in the case that would invalidate the analogy. Analogies are tremendously useful, however, in brainstorming. The analogies help us identify the most morally significant factors of a case, and they help us identify potential solutions based on previous solutions to similar problems. Nonetheless, it is always wise to double-check a solution using other methods.

In this case, we will use a utilitarian approach to check potential solutions identified by our analogies. So far, we have three possible solutions on the table:

- Option 1: Require all VoIP systems to implement lawful intercept (as in the current law).
- Option 2: Do not require VoIP systems to implement lawful intercept or do any other reporting. Law enforcement officials will have to use physical eavesdropping, after getting a warrant from a judge (as suggested by analogy #1).
- Option 3: Require VoIP providers to monitor and report suspicious activities, but do not build the ability to record conversations into the system (as suggested by analogy #2). First, let's identify the interested parties, and how this decision might affect their happiness and well-being.

- *Those who make or operate VoIP systems*—Increased monitoring costs them money for building in the monitoring and for defending against privacy lawsuits.
- *Law enforcement officials and employees*—Increased monitoring saves them money because they do not have to do as much physical surveillance. This also allows them to catch more lawbreakers and do their jobs better.
- *Hackers—Built*-in lawful intercept provides them with greater opportunities for stealing (and selling) secrets, but increases their likelihood of being caught.
- *Nonhacker criminals*—Increased monitoring increases the likelihood that they will be caught or that their plots will be disrupted.
- *The public*—Increased monitoring means increased efficiency for law enforcement, saving tax money, and possibly increasing safety. It also, however, decreases privacy because it makes everyone's phone calls easier to tap, and possibly decreases safety by exposing the public to hacker attacks or to abuse by law enforcement officials.

For law enforcement officials, Option 1 (lawful intercept) is clearly the best. It gives them the most options and the most direct control over monitoring, at low cost compared with Option 2 (no monitoring). For VoIP providers, Option 2 (no monitoring) is clearly the best. Options 1 and 3 are probably about equally bad for them. Although Option 1 (lawful intercept) requires them to modify their systems significantly and opens them up to hackers, it requires much less manpower to operate than Option 3 (suspicious event reporting), because Option 3 would require humans to review cases, fill out forms, and interact with the police.

The stickiest part of this case, and the reason we will not be able to immediately come to a clear solution, is evaluating the effect on the public. Every option has pros and cons for the public. If we assume that the number of tax dollars going to law enforcement is held constant, then Option 2 (no monitoring) would result in a serious decrease in the effectiveness of the police. Option 1 (lawful intercept) might result in major abuses by hackers and rogue law enforcement officials. Option 3 (suspicious event reporting) might also seriously decrease police effectiveness because they might need the contents of the calls, not just a knowledge of the calls' existence, in order to prevent criminal schemes.

To reach a final decision on this case, we would need to make a prediction about how much harm hackers and rogue law enforcement officials might do if we choose Option 1, and weigh this against the loss of law enforcement capacity caused by Options 2 and 3. This is exactly what members of Congress went through when first drafting CALEA (the Communications Assistance for Law Enforcement Act, which created the lawful intercept requirement).

It may be a bit disappointing to spend so much time on a case without "solving" it, but the fact is that ethical decision making, done well, is very difficult. It takes a lot of time and careful work, just as any important problem does. In this section, however, we have learned about reasoning by analogy. This style of reasoning, by finding similar cases in the past and using them to reason about a new case, is fundamental to ethics and to law.

Practice Problems

An important skill in using analogies is noticing both similarities and differences. This skill can be practiced. Think of a book and a website that contain essentially the same information. How are they alike? How are they different? Make a list of similarities and differences, at least 10 of each. Don't ignore the obvious, but don't limit yourself to the obvious either.

Imagine that your public library decides to go completely digital. The library now has a policy to phase out physical books and replace them with ebooks, digital audiobooks, websites, and public access computers in the library. Using the list you made in Practice Problem 1, make a list of the people who would gain from this decision and a list of the people who would lose. Build a utilitarian argument either for or against the decision.

Some people think that the content of Internet sites should be regulated just as the content of radio and TV is, for example, with rules regarding obscenity and the amount of advertising. Other people think that the content of Internet sites, like private phone conversations, should not be regulated. Is the analogy between Internet sites and radio and TV broadcasts more appropriate, or is the analogy between Internet sites and telephone conversations more appropriate? Justify your position.

ChangMain content

Chapter Contents

17.2.3 Case 3: Hackers—Public Enemies or Gadflies?

During the Middle Ages, a “hacker” was someone who made hoes. In the 17th century, a hacker was a “lusty laborer” who enthusiastically made chopping cuts using a hoe. But *hacker* has quite a different meaning today, far removed from its agricultural roots (see the Special Interest Box “The Metamorphosis of Hacking” in Chapter 8). Today, the term *hacker* describes someone who breaks into computer systems and launches Internet worms and viruses, or perpetrates other computer-related vandalism.

Not everyone sees hackers in this negative light, however. Some people view hackers as social gadflies, people who raise important, but irritating, questions about government or society. The Greek philosopher Plato used the word *gadfly* (Ancient Greek: μύωψ) to describe Socrates’ fractious relationship with the political establishment of his day. While most people agree that purposeless vandalism or outright theft through hacking is wrong, some of the activities categorized as “hacking” may constitute a public service, and several computer hackers have written books and articles about the ethics of computer hacking. Some hackers are even hired by the owners of computer systems to test whether there are any weaknesses in their security software that could make it vulnerable to intrusion by unauthorized individuals.

In this section, we explore whether there is an ethical case to be made in support of computer hackers. To focus our discussion, we concentrate on a single type of hacking: gaining unauthorized access to someone else’s computer system to obtain and publish secret information. This could be as simple as copying files from your company’s private network and posting them on the web, or as elaborate as breaking into a government or military installation and circulating classified documents using an anonymization service to protect the hacker’s identity.

These issues, which in the past were considered largely theoretical, have taken on particular urgency in recent years due to the founding of several organizations that specifically focus on information leaking as a form of **hacktivism** (hacking that is intended as a form of political activism). The two main groups discussed here are WikiLeaks and Anonymous.

WikiLeaks, which was launched in December 2006, is a site that specializes in protecting the identity of government and corporate whistle-blowers. Imagine that you discovered a document that proved your company’s leadership was engaged in significant unethical behavior. Furthermore, imagine that you decide you need to blow the whistle on this behavior. How would you go about it? In the past, one common route was to share the incriminating documents with an investigative journalist. The journalist acts as a firewall between you and the authorities; most journalists hold to a code of ethics that says that they will not identify their sources, even if it is clear that the source has committed a crime. Journalists sometimes go to prison rather than reveal their sources. The problem with this approach today is that it is very hard to share an electronic document with a journalist without leaving traces that law enforcement (or corporate security) officers can follow. Most journalists don’t have the necessary computer security skills to actually safeguard the anonymity of their sources. WikiLeaks’ goal is to provide exactly this kind of technical expertise. It provides a secure electronic drop box, and tips on how to submit documents that will prevent the leaker from being traced. WikiLeaks then provides the submitted documents to journalists. In the past, it has partnered with *The New York Times, The Guardian* (in the United Kingdom), and *Der*

Spiegel (in Germany), among others. WikiLeaks has been involved in several major leaks:

- In 2010, WikiLeaks began to provide leaked U.S. diplomatic cables to various newspapers. The *Daily Mail* (a U.K. newspaper) and others have attributed the 2011 revolution in Tunisia, at least in part, to allegations of Tunisian government corruption contained in the diplomatic cables.
- In 2012, WikiLeaks began to provide over 100 classified or restricted files from the U.S. Department of Defense on the rules and procedures with respect to military detainees.
- In 2016 WikiLeaks released over 8,000 confidential CIA documents related to the tools it uses to break into phones, communication apps, and other electronic devices.

Though not hackers themselves, WikiLeaks employs people with the technical skills required to provide defenses against government and corporate investigators. For example, in 2013, WikiLeaks provided documents for and traveled with Edward Snowden on his flight (both literal and political) from Hong Kong to Russia (see the Special Interest Box "Hero or Traitor?" earlier in this chapter).

The hacker group Anonymous is much harder to describe. Anonymous is a group of hacktivists that seem primarily interested in freedom of speech. Even this characterization, however, is in dispute. WikiLeaks is easy to describe because it has a known public spokesman (Julian Assange), a website, and an advisory board. Anonymous has no such official organizing body, or leader. In fact, its semiofficial logo is a suit with a question mark instead of a head, and members wear masks (all of them identical) when appearing in public. As a result, any hacker or activist can claim to be part of Anonymous, and there is no official spokesman to refute these claims. Among the best-known actions of Anonymous are:

- A 2010 attack in retribution for financial sanctions against WikiLeaks. Several companies, including PayPal and MasterCard, had blacklisted WikiLeaks, preventing donors from using those systems to donate to WikiLeaks.
- Attacks throughout the summer of 2011 that disrupted the government websites of Tunisia, Egypt, and Libya. These attacks were in retaliation for government censorship of the Internet and were meant to help support pro-democracy revolutions in those countries.
- A major sustained operation against ISIS following the 2015 Paris terrorist attacks.

Anonymous has also been accused of threatening the Westboro Baptist Church, a group known for protesting at the funerals of U.S. soldiers. Members of Anonymous have said that these charges are false, that they support all forms of free speech, even by people they disagree with. Due to the leaderless nature of Anonymous, however, facts on what Anonymous has, and has not, done are hard to obtain and confirm.

We will examine the ethics of this kind of hacktivism, first using the two techniques we have already introduced, analogy and utilitarian analysis. Then we will introduce a third analysis technique, deontological ethics. In our analogy, we will focus on the first step of the process, breaking into a computer system to steal information.

Analogy: Breaking into a Computer Is Like Breaking into Someone's House. Imagine that a burglar picks the lock on your back door, wanders around picking up valuables, and then escapes into the night undetected. When you find out you've been robbed, you feel outrage and fear. If computer hacking is ethically linked to burglary, then we will have an instinctive revulsion toward both.

Clearly there are similarities between burglars and hackers; in both cases, the intruders are there without our permission and (at least in most cases) without us being aware of their presence. In most homes and with most computers, the owners take some precautions to discourage unwanted visitors, precautions that must be overcome by the intruder. There are laws against both forms of intrusion, although the laws against physical breakins are clearer and easier to enforce.

There are also differences between the intrusions. A burglar is likely to take something from your house, and that removal will deprive you of something. A hacker may look at things, and even copy things from your computer, but the hacker is less likely to remove or destroy things from your system. A hacker takes your intellectual property and privacy, and that is different from taking physical objects.

When someone breaks into a house, there is a palpable threat of violence. If a burglar is detected during the act, things may turn nasty. This physical threat is not present in a computer break-in, although the information stolen may be personal and could lead to future physical threats. The pysical degree of separation of a virtual break-in seems to be an ethically relevant distinction.

Utilitarian Argument: Costs and Benefits of Hacking. What is gained and lost when a computer is hacked? First, whoever owns the hacked computer loses some control over the information in that computer, and the hacker gains access to that information. Second, as a consequence of the break-in, there may be intentional or unintentional deletions or corruptions of data on the computer. These changes may be largely benign or may subsequently cause significant harm. Neither the hacker nor the person hacked can know with certainty the eventual consequences of these changes.

When computer system owners or system administrators discover that a system has been hacked, they often increase system security to reduce the probability of another successful intrusion. Some hackers claim that they provide a public service by alerting people to security holes in their systems. As long as the hacker doesn't hurt anything while "inside" the system, and especially if the hacker makes the intrusion obvious, then such hackers would argue that the consequence of the hacking is improved security against malicious hackers. An alternative consequential argument says that increased security wouldn't be necessary if hackers weren't such a threat.

This discussion illustrates two challenges when using a utilitarian argument in a dialectic about hacking:

1. It is sometimes hard to predict consequences with any accuracy.
2. There seems to be a distinction between "good hackers" (who are trying to act in the public interest) and "bad hackers" (who want to do damage or steal things for self-interested or pathological reasons).

These kinds of challenges arise in other discussions, and some people think they are difficult to overcome using a utilitarian argument. Let's try a totally different kind of ethical argument, a *deontological argument*, to try to meet these challenges in a different way.

Deontological Argument: Hacking with a Golden Heart. Utilitarian and other consequentialist arguments focus on the consequences of an act to determine if the act is ethical. Deontological arguments focus instead on the duties of the person acting and the way the act impinges on the rights of others.

The word **deontology** is from the Greek and means "the study of duty and obligation." Perhaps the most famous deontologist was the German philosopher Immanuel Kant (1724–1804). Kant wrestled eloquently about what duties we humans have to each other. He came up with "categorical imperatives" that characterized these duties. His second categorical imperative goes something like this:

Never treat a fellow human merely as a means to an end.

To boil that down to a bumper sticker slogan, we might say, "Every human being deserves respect." Notice that the categorical imperative is really about your mental attitude toward the other person: Do you see him or her as a person, or just as the means to an end? Kant's deontological approach encourages us to consider the intent behind the action, not just the results of the action.

Let's try out a deontological perspective on our question about hacking. Is the act of hacking into another person's computer system inherently unethical? If we take some hackers, such as WikiLeaks, at their word, their intent is not to harm the public. They characterize themselves as a foil against corporate and government abuse, and they characterize hacking as a form of investigative reporting. They also claim to want to help people discover security holes to protect against malevolent hackers.

Let's stipulate that hackers who break into other people's computers for personal gain are doing something unethical by any of the three arguments we've seen so far in this section (analogy, utilitarian, deontological). For the rest of this section, we concentrate on hackers who claim a benign if not benevolent intent to their computer break-ins.

First, we assume that "good hackers" are telling the truth when they claim to mean no harm to the public. In his influential history of hacking, *Hackers: Heroes of the Computer Revolution*, Steven Levy* describes six components of what he calls the "hacker ethic." Here we focus on two:

1. "All Information Should Be Free"—Information sharing is a powerful positive good because it is not possible to make good decisions if important information is hidden from the public. It is the ethical duty of hackers to facilitate access to information whenever possible.
2. "Mistrust Authority—Promote Decentralization"—The strict rules and hierarchical management structures that characterize government and corporate bureaucracies mostly serve to prevent people from getting things done, rather than solving problems. Each hacker should do what he or she thinks is in the public's best interest, and ignore the rules.

In claim 1, the idea of sharing information looks, at first glance, pretty good. But it seems a bit less noble when we remember that much of the information that hackers share isn't *their* information, it's someone else's! It's one thing to share open source computer code (like Linux or Apache OpenOffice) or the works of Shakespeare on the web. It's quite another thing to share material whose copyright is legally still in force (like Lady Gaga's latest hit) or to share classified information that might impact national security. Unless hackers consciously make these kinds of distinctions, and many hackers do not, then the duty to respect other people isn't being met. In the case of WikiLeaks' releases of government documents, WikiLeaks collaborated with major newspapers to help determine which cables were safe to release, and which needed redactions to protect innocent people from harm. Some groups that release leaked documents simply release all documents without doing any such filtering.

The second claim has a similar weakness. Hackers might argue that rules protecting electronic privacy are incorrect and thus can be violated. They might also argue that these rules exist because we expect electronic privacy, but it is that very expectation of privacy that is the problem, not their violation of that expectation. What's missing from the hackers' argument is why their ideas about information ("all information should be free and accessible") should take priority over the individual's view ("some of my personal information should be private"). Ethically, there's no problem with thinking and arguing that all information should be free, or to be suspicious of rules; there is a big problem, however, with acting on that belief in a way that treats people as a means to an end.

The preceding arguments won't convince most hackers, and you too might have some remaining questions about this issue. The sharing of information and resistance to authority are usually moral goods, and these values are part of the American identity. But the fact that these are ideals is not a slam-dunk ethical argument when applied to a specific act. Acts have both good and bad consequences, and utilitarians remind us that we have to weigh these consequences and think of them globally. Deontologists encourage us to remember that acts can be inherently good or bad outside the consequences, if they involve a right or duty, and to examine the intention behind an action. At the very least, the preceding brief analysis raises serious questions about the claims and behaviors of the hacker ethic.

Practice Problems

There are times when you want someone to break into your house. For example, if your house is on fire, you probably won't object if firefighters use an ax on the front door. Can you think of other such situations? Try to make an argument based on an analogy between firefighters and hackers that supports the hacker ethic. Do you find this analogy convincing? Why or why not?

Sometimes we are invited to look into windows and to enter privately owned property. For example, stores spend money to make attractive windows to draw us in. What are some ethically significant differences between a store inviting us in and a computer being hacked? Focus on the issue of intent as you consider this question.

As mentioned earlier, some corporations and even government agencies have employed former hackers to improve security measures; the hackers test the security of the systems at the employing corporation or agency and report weaknesses, an invited form of hacking called penetration testing. Consider the analogy of an auto manufacturer hiring a former auto thief to test how easy it might be to break into a new car model. Is this a reasonable analogy? Does it support the hacker ethic?

Some Internet chat rooms allow and even encourage people to remain anonymous. As people type to each other in real time, the people chatting are identified by fictitious "handles." Is this a good idea? Think of two reasons why such Internet anonymity may be a good thing and two reasons why it may be a bad thing.

Main content

Chapter Contents

17.2.4 Case 4: Genetic Information and Medical Research

So far in this chapter, we've looked at three different cases using three different techniques: utilitarian analysis, deontological analysis, and reasoning by analogy. In this final case study, we propose a "paramedic method" for computer ethics that integrates these three techniques.

"Paramedic Ethics" for Technology. When you get sick, you often need medical help in a hurry. Paramedics aren't necessarily medical doctors, but they know quite a bit about how to help people, and they know who to ask when they aren't certain about a particularly puzzling case. We don't expect you to become a research ethicist by reading this chapter, but we hope you have started to gain some new skills: recognizing ethical questions regarding computing and reasoning carefully about answers to those questions. *When you are faced with an ethical problem, there are several important questions you should ask yourself:*

1. *Who are the stakeholders in this situation?*
2. *What does each stakeholder have to gain or lose? (This is the utilitarian step.)*
3. *What duties and responsibilities in this situation are important to the stakeholders? (This is the deontological step.)*
4. *Can you think of an analogous situation that doesn't involve computing? If so, does that analogous situation clarify the situation that does involve computing? (This is reasoning by analogy.)*
5. *Either make a decision or revisit the above steps.*

Before we illustrate how to apply these questions to a particular case, we need to announce a disclaimer. Unlike the formal algorithms studied earlier in this book, this "paramedic method" is not a step-by-step solution method, guaranteed to produce a result and then halt. Instead, it is an outline that can help guide you in your analysis and help you move toward a better understanding of the problem and toward a better ethical conclusion.

The Case Study. Many people believe that the Industrial Age is over and we are now living in the Information Age. In the last few years, human genetic information has taken center stage in scientific exploration. Computers are an integral part of this research and of the growing commerce connected to the human genome. Because this "new" information is contained in the cells of our bodies, the computerization of this information is simultaneously personal and mysterious. In our final case study, we explore a fictional case involving genetic information. We will use the paramedic method to examine this case from several different perspectives.

Imagine that you are at your family doctor for a routine checkup. The doctor asks you to participate in a research study of genetic diversity and disease by donating some skin cells for the study. The doctor informs you that your skin cells will be identified only by a randomly assigned number and your zip code. Should you donate your cells?*

Step 1: Identify the Stakeholders. According to our paramedic method, the first question to ask is, "Who are the stakeholders?" Clearly the doctor and you are two stakeholders, but are these the only ones you should consider? Probably not. Unless the doctor is doing this study on his or her own (unlikely), there is someone else involved in this research. When you inquire, the doctor tells you that a pharmaceutical company is sponsoring the research and that it hopes to use the information gathered from around the country to identify genetic links to several diseases, some of them fatal. Now you've identified three more stakeholders: the pharmaceutical company (let's call it PHARM CO), skin cell donors all over the country, and people who have or will have these genetic diseases.

Step 2: What Is at Stake? Next, we should ask what each stakeholder might gain or lose from our decision. If we say yes and donate our skin cells, then we will undergo some sort of procedure and lose a few cells; our doctor will participate more fully in the study; PHARM CO will get a larger genetic database and may be able to develop new drugs; if the drugs are successful, then people with diseases may have new therapies. If, on the other hand, we say no, then our doctor, PHARM CO, and patients will have a slightly smaller chance of success with the research.

Enumerating these costs and benefits might lead to a few more questions. First, is the procedure for donating the cells dangerous? Your doctor assures you that the procedure is harmless and requires just a moment to scrape a tongue depressor lightly against your arm. You may also have questions about how your genetic information is going to be stored and processed. A logical way to store this information would be to assign a randomly generated number to each donor in the study, perhaps linked to information your doctor already has. We might envision something like the following table, which includes the use of your Social Security number (SSN):

Random Number	***SSN***	***Name***	***Zip Code***	***Gender***	***Doctor***
10568322	532 12 3456	Joe Smith	45321	M	Goodgene
952990981	532 11 9503	Sue Jones	55416	F	Goodgene

.

.

.

The doctor has assured you that only the random number (from the first column) and the zip code (from the fourth column) will be associated with your genetic sample and the information derived from it. If we believe the doctor will in good faith send only that information to PHARM CO, can you be confident that your privacy is ensured? The answer is probably not. If a table such as the one just shown exists, then PHARM CO could potentially link the information it receives from your doctor back to you by gaining access to that table. At the very least, PHARM CO could find out the names and addresses of all the people who donated cells from a particular zip code, and if there were only one or two it would be easy for them to identify you. Furthermore, computerized files like the previous table have a habit of hanging around, in one form or another, for a long time unless they are explicitly and carefully deleted, including all backups and copies stored in the cloud. Unless your doctor has been scrupulous about data deletion, PHARM CO may indeed be able to track down your personal information if it becomes important for the company to do so.

In Chapter 7 you studied technical details about networks and communication over those networks. You know that information on the Internet can be intercepted at various points. Will your genetic information and/or the table described above be sent electronically to PHARM CO or anyone else? If so, will it be protected using one of the sophisticated encryption algorithms described in Chapter 8?

A final question involves finances and ownership of the final results. Presumably, PHARM CO plans to make a profit from the sale of any new drugs. Is anyone being paid for this research? If the government is not supporting this project, and if PHARM CO is paying for all the collection kits and the analysis, then the information collected and any new drugs developed will belong to PHARM CO.

Step 3: Identify Duties and Responsibilities. Your doctor has a primary responsibility to do his or her best to treat you and protect your privacy. You have a duty to pay your bills promptly and to follow instructions that the doctor prescribes. PHARM CO is responsible for developing safe and useful drugs, and in return its customers pay for those drugs. In this research effort, PHARM CO is hoping that doctors will enlist volunteer patient donors, and in return PHARM CO is promising doctors a small fee for each patient who volunteers. Both your doctor and PHARM CO have promised to protect donors' privacy and are obligated to make a good-faith effort to fulfill that promise.

Most of the responsibilities we've discussed so far are fairly straightforward and uncontroversial. There are other possible responsibilities that are less obvious and more controversial. We've already discussed the value of information in the earlier music file copying case. Analogous to the music in that case study, this example also involves valuable information. What if your genetic information includes an important clue to the treatment of cancer or some other fatal disease? If PHARM CO develops an effective drug based on your genetic information, it stands to make billions of dollars. Should you get a royalty on the information in your genes? (This was the argument put forth by lawyers in the case of the cells of Henrietta Lacks that led to the development of many important drugs.) Does PHARM CO have a duty to share your genetic information and the information from others, or does its initial funding of this research give it proprietary control of that information?

Your doctor told you that only a random number and a zip code would identify your donated skin cells. This coding procedure seems to afford you some confidentiality, and that's a good thing. But you might also want to know why the zip code is required at all. Is geographic location part of the research, or is the zip code important for subsequent marketing of drugs? Is this study being done all over the world, only in the United States, or only in select zip codes in the United States? If it turns out your genetic information is particularly valuable, can the doctor give you assurances that your privacy will not be invaded? As we've seen previously, maintaining strict confidentiality would require a sophisticated security protocol to make sure information could not be linked back to you and to protect information stored on computers and communicated over a network. Because both PHARM CO and your doctor want you to volunteer for this process, they have a duty to disclose these kinds of details before asking for your genetic information.

Another question is whether you have a duty to try to help cure disease in this case. If there is a chance for you to advance medicine by a simple donation process, is there an obligation for you to donate? In a situation like this, is altruism required?

Step 4: Think of Analogies. As we move through the paramedic method, the seemingly simple request for a few skin cells has taken on added depth and complexity. Ethical analysis often reveals a broader perspective than our first thoughts about a situation.

An important aspect of this case is the promise of confidentiality to donors. Another aspect of the case that emerged during the first steps is that two of the stakeholders are potentially gaining money, PHARM CO and the doctors. The other two stakeholders, you and patients who potentially will want the drugs developed, are not getting money now and may be paying later. To explore both the confidentiality and the financial aspects of donors and users of donations, we'll use an analogy to blood donations.

The Red Cross solicits blood donations. The Red Cross is concerned about the quality of the blood that it distributes. Therefore, when you make a donation, the blood is tested for certain diseases. If your donated blood turns out to be unusable, then your name is entered into a "deferred donor database" and you are prevented from giving blood. Clearly, the Red Cross cannot offer you complete confidentiality about your blood and any diseases it discovers in your donation. However, the Red Cross is sensitive to the issue of confidentiality. On the website www.redcrossblood.org/donating-blood/donationfaqs, the following appears on an FAQ (frequently asked questions) list:

> The Red Cross regards blood test results as private and confidential information. The Red Cross may contact you by letter or call to arrange a counseling appointment, but the Red Cross does not disclose information regarding positive blood test results to anyone but the donor, except as required by law. The Red Cross maintains a confidential list of people who may be at risk for spreading transfusion-transmitted diseases. When required by law, we report donor information, including test results, to health departments, military medical commands, and regulatory agencies. Donation information may also be used confidentially for medical studies.

The Red Cross is a nonprofit organization, but it incurs processing costs associated with collecting, testing, and distributing blood. To recover these processing costs, the Red Cross charges a reimbursement fee to hospitals that use the donated blood. The hospitals also incur operating costs, which appear on your hospital bill. One of the reasons that the Red Cross prefers volunteer donors is that it has been found that people who donate blood for altruistic reasons are the safest blood donors. Blood donation and skin cell donation (as proposed by your doctor) are similar in that the donors are volunteers, but the collectors and eventual users of the donated materials are paid. In both cases, it is something from donors' bodies that is being collected. And in both cases, the donors are asked to volunteer for altruistic reasons.

There are differences between the two situations. In the case of blood donation, the blood itself is the item of value, and both donor and collector are clear about what will happen with the blood. In the case of the skin cells, it is the genetic information in the cells that is of value, not the cells themselves. Also, PHARM CO is looking for something it might or might not find in your cells. If it finds valuable information, PHARM CO stands to make a profit; if it doesn't find valuable information, it might take a loss on the project. The Red Cross and hospitals presumably won't make large profits on your blood, although they do charge for its use.

Let's examine another analogy: companies that solicit money for a charity. In this case, a for-profit company solicits donations from volunteers. Again, confidentiality is an issue. On the one hand, we expect that a charity will keep records that we can use to confirm our donation if the government audits our tax returns; on the other hand, there are many reasons why we might not want our history of donations to become public information.

On the issue of finances, a for-profit solicitation company takes a certain percentage of donations to pay for its costs in soliciting and processing the donations and then passes on the rest of the money to the charity. This process becomes ethically objectionable when the percentage of money that goes to the solicitor becomes comparatively large. If the soliciting company pockets 80% of the donations it collects and passes along only 20% to the charity, donors feel cheated. If the soliciting organization keeps only 2% of the donations and passes along 98% to the charity, most people would not object.

The charity solicitation scenario is similar to the skin cell donation in that volunteers are asked to donate by someone who has a financial interest in that donation. In both situations, the donors are asked to make the donation for altruistic reasons. In both cases, the amount of money given to the person in the middle (the solicitor or the doctor) seems ethically relevant, as does the control and dissemination of personal information about donors. In all of the cases we've examined, this donor information is almost certainly in the form of computer files and therefore easy to store and distribute.

The scenarios are different in that the donation requested for charity is monetary, not physical. In the charity solicitation, only the solicitor is for-profit. In the skin cell donation, both the doctor and PHARM CO are for-profit entities, although the doctor is making just a little money and PHARM CO is both spending and hoping to make much larger sums.

Step 5: Make a Decision or Loop through the Method Again. We've moved through the first four steps of the paramedic method and now have developed a better understanding of the complexities of this situation. If you have to make a decision right away (the doctor is waiting!), you can do so with a more reasoned response than before. But perhaps you have the luxury of thinking it over some more ("Doc, let me get back to you about the skin cell donation, OK?"). You might want time to ask a few more questions of the doctor or PHARM CO. You also might want to think about such issues as privacy and security a bit more carefully. In cases where the decision is potentially more critical to you or someone important to you, you might want to seek professional help, perhaps a lawyer or accountant, in making your decision. If you have the time, you could revisit earlier steps in the paramedic method, but, at a minimum you have identified and thought about the key ethical issues involved in this important medical decision.

Professional Codes of Conduct

Many professional organizations in the fields of computing and engineering have established codes of ethical behavior to provide guidelines for their members. These codes outline standards of behavior and conduct that typically include general imperatives such as avoiding harm to others and being honest, as well as more specific professional responsibilities and duties such as respecting intellectual property and protecting client privacy. Here is a partial list:

The Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct

www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

The Institute of Electrical and Electronics Engineers (IEEE) IEEE Code of Conduct

m.ieee.org/about/corporate/governance

Computer Professionals for Social Responsibility (CPSR) Technology and Ethics cpsr.org/issues/ethics

Every computing professional should read over the appropriate code periodically, and keep it in mind as a regular part of his or her working life.

Main content

Chapter Contents

17.3 Personal Privacy and Social Media

In the previous section, we examined four issues that demonstrate the relationship between computing and ethics: illegal file sharing, surveillance, hacktivism, and medical privacy. We chose these topics not because they were necessarily the most important (although they certainly are important), but because they were useful in illustrating our four methods of reasoning about ethical cases: utilitarian analysis, reasoning by analogy, deontological analysis, and the paramedic method.

In this section, we look at ethical issues you might face in your everyday life. The concerns raised in the previous section were "big issues," big in the sense of having the potential to cause enormous economic and political damage to a vast number of people—the cracking of military or government databases, stealing intellectual property, and the theft of critical financial or medical information. However, there are ethical and legal issues regarding computing of a somewhat "smaller" nature—smaller in the sense of affecting as few as one or two individuals, but the "smallness" of the apparent harm is misleading. To a person whose privacy has been invaded or who has been subjected to public ridicule and shame, these are certainly not small problems, and the consequences can be devastating.

Bullying is a problem that has been around for a long time—being verbally tormented or physically abused is something that Greek and Roman citizens probably had to deal with thousands of years ago. However, the growth of the Internet and social media has allowed bullying and the violation of one's personal privacy to become much easier and far more virulent: Online taunting allows bullies to remain anonymous, gang up on victims in enormous numbers, harass victims in places they would normally be safe, such as the confines of their home, and have their hateful screeds live on in cyberspace long after they have moved on.

According to the Pew Foundation, about 93% of U.S. children and young adults regularly use the Internet and the web, with the great majority accessing it on a daily, even hourly, basis. Some of the most popular destinations are social media sites such as Facebook, YouTube, Snapchat, Twitter, Instagram, chat rooms, forums, and blogs. These applications are a fun and convenient way to exchange messages, share stories and photos, and keep in touch with friends and family; unfortunately, they are also a quick and easy way to spread personal information, malicious rumors, hate speech, outright lies, and disturbing images to a massive audience.

Cyberbullying is humiliating, taunting, threatening, or invading someone's privacy using the Internet, web, or other type of electronic technology. Cyberbullying can take many forms, from posting hurtful and insulting messages, to leaking sensitive and embarrassing personal data, to online threats of violence and physical assault. One popular form of cyberbullying is *impersonation*. A bully, masquerading as the intended victim, posts provocative images, racist, homophobic, or sexist comments, or knowingly false messages on a social network, chat room, or blog. The intent is to destroy the victim's reputation and invite retaliation from offended individuals and groups. The post will often include a home address and a cell phone number to make it easy for others to find and harass the targeted victim.

As in most high-tech fields, the enactment of state and federal statutes to deal with cyberbullying lags far behind the popularity and use of social media. Although 34 states have enacted laws against cyberbullying, these laws often apply only to minors and only to behaviors committed at school or on public property. Laws focusing on wider audiences, such as private communications between adults, have frequently been challenged and struck down in court for violating First Amendment rights of free speech, even speech that might be considered hurtful or embarrassing. In response, many cases have been prosecuted under other statutes, such as state or federal laws against fraud, bias, or making terroristic threats.

For example, in 2006, 13-year-old Megan Meier of St. Charles County, Missouri, who was being treated for depression, committed suicide after repeated harassment and persecution on the social networking site MySpace. The perpetrator was the 47-year-old mother of an ex-girlfriend posing online as a 16-year-old boy. The mother was not charged with cyberbullying but with fraud under the 1986 U.S. Computer Fraud and Abuse Act, a law written with a totally different concern in mind—the hacking of financial and governmental computer systems. The jury returned a not-guilty verdict, which led the state of Missouri to enact "Megan's Law," making it a felony to use the Internet or other electronic media to harass or frighten a child under the age of 17. In 2009, the first case testing the constitutionality of this new law was filed against a defendant for posting photos and personal information about a young girl in the Casual Encounters section of Craigslist, leading to numerous unwanted phone calls and emails of a sexual nature. In February 2011, a jury again returned a verdict of not guilty, saying the law as written was too vague in its definition of exactly what constitutes online harassment and the invasion of privacy.

In 2010, Tyler Clementi, an 18-year-old Rutgers University freshman, jumped to his death from the George Washington Bridge after a roommate used a hidden webcam to record his private sexual encounter with another man. The roommate then posted the video on the Internet, without Clementi's consent, even inviting Twitter followers to watch it online. In April 2011, a grand jury indicted the roommate on 15 counts, including the transmission of sexual images of another person without his knowledge and bias intimidation, a hate crime, but not cyberbullying because at the time there was no state law addressing this issue. In March 2012, the roommate was convicted on all 15 counts and was sentenced to 30 days in jail, 3 years' probation, 300 hours of community service, and a $10,000 fine. However, in September 2016 those convictions were overturned by an appeals court in New Jersey.

It will likely be many years and many court cases before there is widespread agreement on exactly how to craft a law to deal effectively with the many types of cyberbullying, from the relatively harmless online taunts of young children ("You are stupid," "You have big ears") to the truly frightening threats of disturbed adults and violent sexual predators. These laws need to carefully balance the public's right to a free and unfettered exchange of ideas and opinions, even controversial ones, with the individual's right to control the publication and dissemination of personal information. The difficulty of writing such legislation was highlighted by the judge in the Craigslist case who said that laws addressing cyberbullying and the online invasion of privacy are so new there was virtually no precedent to guide him with proper jury instructions.

Another problem exacerbated by the rapid growth of social networks and online communications is **sexting**, the transmission of sexually explicit messages or images, usually via smartphones or tablet computers, between consenting individuals. A recent poll from the Pew Research Center shows that more than 20% of young adults had recently sent either sexually explicit text messages or nude/seminude images of themselves to friends via a mobile phone.

Like bullying, the consensual circulation of sexually explicit material is not a new phenomenon, and sharing “pin-up” pictures has been around since the 1890s. However, the popularity of digital cameras and smartphones, as well as their ubiquitous use by teens, has greatly inflamed the problem. Unlike images from digital cameras and smartphones, older, film-based photographs generally had to be processed by a third party. If the photos contained questionable sexual content, the involvement of print shop personnel could lead to an embarrassing situation or, in extreme cases, arrest and prosecution. This tended to put a natural damper on the practice of circulating such photos, a damper that no longer exists. To make matters even worse, smartphones can record and transmit not just still images but videos, which can be far more explicit.

Compounding the problem is the ease with which images and videos can be distributed to a huge audience via popular websites, often without the knowledge or approval of the person being recorded, as was the situation with the streaming video in the Tyler Clementi case. Relationships that an individual thought would last forever can quickly turn ugly and spiteful, resulting in the public distribution of messages and photographs that were originally shared in strict privacy. Social networking sites like Facebook and Twitter are enormous in scale and highly persistent, so once documents or images have been posted, there is virtually no way to get them all back and no way to ever know how many people have viewed them. Years or decades later, long after that indiscretion has been forgotten, these photographs can resurface and damage a person’s reputation and career. (An important maxim to remember whenever posting on social media is that “the Internet is forever.”)

In June 2011, U.S. Representative Anthony Weiner (New York) was forced to resign in disgrace when a link to sexually explicit photographs he had placed on the web was accidently posted on his public Twitter account. Only a few months later, U.S. Representative Louis Magazzu (New Jersey), a Democrat, had to resign when nude photos he sent in private to a female “friend” ended up on a Republican activist’s website. It turns out that the friend was really an employee of a political rival.

It is not simply one’s reputation and employment that are at risk—there can be serious legal ramifications when one or both of the individuals involved in the image transmission are under 18. As with cyberbullying, state and federal laws have yet to determine how best to deal with the problem of sexting when the photographs are of minors, even if the transmission is consensual and private. In some states, this issue is dealt with under existing laws against the production and distribution of child pornography, an extremely serious felony that can lead to a long jail sentence and inclusion on the National Sex Offender Registry. For many, this seems like an overly harsh way to deal with the problem of individuals under age 18 who send sexually explicit images of themselves to a boyfriend or girlfriend without any intent to sell or distribute the photos. In 2009, the American Civil Liberties Union (ACLU) filed suit against a Pennsylvania district attorney who was threatening to file child pornography charges against a group of high school girls for posting risqué photos of themselves on a social networking site.

In response to this case, a number of states, including Connecticut, Ohio, Vermont, and New York, have reduced legal penalties for the *consensual* and *private* transmission of sexual images by individuals from age 13 to 17 from a felony to a misdemeanor. Many of these new laws also include mandatory educational and family counseling regarding the real and serious dangers associated with sexting, including encounters with sexual predators, and the humiliation and embarrassment caused by the unexpected distribution of these private photos, a situation that has resulted in numerous teen suicides.

Probably no court decision better exemplifies the complex legal trade-offs between the public nature of social networks and the individual's right to privacy than the 2009 California case *Moreno vs. Hanford Sentinel Inc.* A student at UC-Berkeley, returning during school break to her hometown of Coalinga, California, posted a story on MySpace ("Ode to Coalinga") containing extremely vitriolic and highly unflattering comments about her hometown and its residents. After six days, she deleted the article from her home page; but once an image or message has been posted in cyberspace, it is virtually impossible to control who is able to see it, how many people can copy it, and what can be done with it.

In this case, the offensive posting was viewed by the principal of Coalinga High School who forwarded it to the editor of the *Coalinga Record*, the local newspaper, which published it in full as a letter to the editor, including the author's full name. This led to death threats (a gunshot was fired into the family home), the closing of the father's business, and the family being forced to sell their home and move out of town in disgrace. The family sued the principal, the editor, and the newspaper's owners for invasion of privacy and emotional distress.

The California Court of Appeals ruled that the principal did not invade the young girl's privacy when he sent the article to the newspaper, and the newspaper did not violate her rights by publishing either the article or her full name, both of which had been available on MySpace. The court held that "[She] publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular Internet site. Her affirmative act made that article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have an expectation of privacy regarding the published material." What this decision is effectively saying is that any material posted to a popular social media website should, by definition, be considered public property, without legal protection against the invasion of privacy.

Many people argue that the best way to ensure personal privacy with regard to online information is simply to assume that any articles, facts, ideas, opinions, rants, photos, or videos you post on a social network might not remain private and, instead, **go viral** (become widely read and widely distributed via social media). Therefore, it is argued, if you don't want a large number of people to read something, *don't post it*.

However, this argument can sometimes lead to the phenomenon of *victim blaming*. Victim blaming is when the victim, rather than the perpetrator, of a crime or harassment is held responsible. It is not unusual for victims of rape to be extensively questioned about what they were wearing, whether or not they had been drinking, and their history of sexual relationships. While one might question a victim's life choices, this shouldn't excuse a crime against the victim. Finding a balance between these two perspectives is an ongoing debate.

In the Internet age, personal privacy is no longer as simple as putting a lock on your diary and hiding the key. When you say something or show something on a social media site, you are effectively sharing it with the world. At the same time, public sharing is not a justification for harassment and bullying.

Practice Problems

Should cyberbullying be made illegal, or should it be something handled (more informally) by parents, teachers, and the social networking companies? Use a utilitarian analysis, deontological analysis, or argument by analogy to justify your position.

Think ahead to 15 years from now. You are Facebook friends (or whatever the equivalent will be in the future) with many of your coworkers. During a messy divorce proceeding, your coworker's ex-spouse posts old sexting messages, sent by the coworker, on Facebook, tagging them so that you and everyone else at work see the pictures. How should you react? What specific actions should you take, or not take, in response? What if you were the manager or owner of the business?

Main content

Chapter Contents

17.4Fake News, Politics, and Social Media

The final topic we will address with regard to social media and the Internet is, in many regards, the polar opposite of the concerns discussed in Section 17.3—online privacy, sexting, and the unapproved distribution of personal information. In those areas, private communications were made public against the wishes of the author and accessed by individuals who should not be viewing these materials.

However, in the case of **fake news**, this is exactly what the author is trying to do—distribute (under the guise of objective news) misleading information, slanted opinions, or outright lies to as many people as possible in as short a time frame as possible. Fake news is not a new phenomenon and, in fact, has been around for hundreds of years, often under the perjorative term *yellow journalism*. However, in the past the ability to produce and distribute yellow journalism was generally limited to wealthy individuals who owned newspapers (such as Joseph Pulitzer and William Randolph Hearst) or had the personal wealth to pay the cost of printing and distributing leaflets, buy air time on radio or TV, or hire people to make thousands of telephone calls. However, the Internet and the web, along with the ubiquitous smartphones and tablets, have changed that situation dramatically. Now, with a single keystroke, an individual blogger can reach thousands of social network followers who may then choose to share that post with tens of thousands more. Suddenly, one person's voice has reached out to millions of readers. Because the Internet, many popular blogs, and social apps are **unmoderated**, that is, not monitored for inappropriate content or fact-checked for accuracy, they become a quick and easy way to distribute any idea we want, true or false, to a massive audience at virtually no cost. In a sense, everyone with a computer and a blog is now a "newspaper owner."

For a long time this ability to inexpensively reach mass audiences was used almost exclusively by mass-market advertisers who sprayed their irritating ads and pop-ups all over our email. The spammers soon followed, but most people quickly learned to ignore those desperate pleas from Nigerian princes who wanted to send us money if we would just provide our bank account number and password. However, as the political landscape has become more polarized and more combative, the idea of using social media to either gain a political advantage over one's opponents, or to generate advertising revenue from the millions of "clicks" of political supporters, is now a far more important usage for fake news and a far more dangerous threat to our democratic system.

While there are many types of fake news (including political humor and satire), some of the most malicious types are:

- *Imposter sites*. This is fake news that uses URLs designed to mimic the addresses of legitimate news sources (e.g., TheNewYorkTimesNewspaperSite.com) coupled with a screen layout that mimics the logos and fonts of the real site. The goal is to get readers to believe they are reading information from a well-known, well-respected news source. The content will most likely be totally false and unrelated to anything that would appear on the actual news site being copied.
- *Manipulated content*. This is when actual news stories or photographs are doctored to make them look like they are legitimate coverage of an actual event. Using apps like Photoshop, photographs can be manipulated for political gain, and real news stories can be edited to add or omit information that provides important facts and context for understanding the significance of what has happened.
- *Fabricated content*. This is what we generally think of when we hear the term fake news. This is information that is 100% fabricated and has no basis in reality. It emerges from the imagination of its creator who is only concerned with increasing advertising revenue or moving political opinions in a particular direction.

  An amazing example of the power of fake news to foment a national political firestorm is the "Pizzagate" scandal of October 2016, during the height of the U.S. presidential election campaign. A white supremacist Twitter site claimed the New York City Police Department had discovered the existence of a child pornography ring run out of the Comet Ping Pong pizzeria near Washington, DC, that involved a number of high-level members of the Democratic party, including Hillary Clinton. The story, which was totally fabricated, was quickly reposted by a number of right-wing message boards, blogs, and fake news sites and then migrated to more mainstream websites such as Reddit and 4chan. In the following days and weeks the story went viral and was seen online by millions of viewers. It became so controversial that, on December 4, 2016, a man entered the Comet pizzeria with an AK-47, threatening to shoot anyone he encountered who was involved in pedophilia. (He was arrested, and no one was injured.) Eventually, the story was shown to be completely fictitious, fabricated to harm the campaign of Ms. Clinton, but by then the political and personal damage had been done.

It is difficult to prosecute the dispensers of fake news because of the free speech and free press guarantees contained in the First Amendment to the U.S. Constitution. Often, those who have been targeted file civil suits for defamation and slander, but even these civil suits can be difficult to win. The person must prove the printed statements were indeed false, actually harmed one's reputation rather than being merely offensive or insulting, and were made with fault—the person publishing the story knew the statements were false but willfully and recklessly disregarded that fact and published them anyway. This is a high legal bar to reach, often too high to justify the potentially huge cost of litigation. In addition, it can take a long time, often years, to bring a civil suit to trial, and in politics the damage done to a reputation usually happens within days or weeks, not years, as was the case with Pizzagate.

So, if the courts and Congress are not the solution, what can we as Internet and social media users do about this explosion of fake news? The best answer comes from one of our founding fathers, Thomas Jefferson:

> An enlightened citizenry is indispensible for the proper functioning of a republic. Self-government is not possible unless the citizens are educated sufficiently to exercise oversight.

This idea can be applied to the functioning of our global communication systems, namely, that each person must educate herself or himself about how to be an intelligent consumer of online content and how to be a well-informed citizen and voter. We must learn to recognize and reject fake news that is presented as valid, objective information.

There are a number of legitimate websites that can help you to identify fake news websites, such as Snopes.com, PolitiFact.com, and FactCheck.org. Some of the techniques to help you spot fake news include:

- *Check the author*. Fake news stories often pump up the credibility and importance of the author of the story by making numerous false claims—for example, Pulitzer prizes won, prestigious university positions held. However, when these claims are fact-checked they turn out, like the story itself, to be fabricated.
- *Check the supporting links*. Fake news stories often include links to official-sounding websites to back up their assertions, for example, WhiteHouseDocumentCenter.com. However, when these links are followed it often turns out the supporting sites are just as phony as the site where the original story first appeared.
- *Look at who else is reporting the story*. In today's 24/7 news environment it would be virtually impossible for an important event to be covered by only one or a small number of blogs. Breaking news stories will (after the delay required to fact-check their authenticity) appear in all the major, responsible news outlets, including television, radio, newspapers, and large online news websites. If the story cannot be found there, it is almost certainly bogus.
- *Consider the apparent intent of the story*. Does the story appear to be heavily biased in favor of a particular point of view; does it contain overly emotional appeals for the "correctness" of that point of view?

So, although the Internet, the web, smartphones, and social media have made it faster and easier to disseminate information, it has become far more complex for people to become discerning and intelligent consumers of that information. It is now our personal responsibility to learn how to determine what is real and what is false, how not to be deceived by the biases and outright lies becoming all too common on the Internet, and not to pass fake news on to others. If we are not willing to accept that important responsibility, these amazing new technical achievements could become the seeds that sow both discord and chaos into our democratic process.

Main content

Chapter Contents

17.5Conclusion

We don’t want to end this chapter without warning you that we’ve only scratched the surface of some of the ethical and legal issues involving technology, privacy, and society. In the chapter exercises, we’ll invite you to look at some of the many controversies in these developing areas of applied ethics. And although we’ve discussed how to apply utilitarian ideas, deontological ideas, and analogies to computer ethics, we haven’t even mentioned Rawlsian negotiation, virtue ethics, or any other number of ethical techniques. We also haven’t explicitly mentioned “science and technology studies,” though many of the themes we’ve described are included in that emerging scholarly field.

You may think that the paramedic method is too involved for your decisions, and perhaps just trying to remember how to spell deontological gives you a headache. But we hope you’ll at least remember that technical decisions involve human values, whether we recognize it or not. And when you have to decide if something having to do with technology is right or wrong, we hope you remember to think carefully about consequences and duties. Computers give us tremendous power. Let’s hope we learn to use the power well. Happy computing!

Main content

Chapter Contents

17.6Summary of Level 6

In this last and highest level of abstraction in our study of computer science, we looked at several case studies involving computer technology and saw how even seemingly straightforward situations, when examined closely, reveal multiple facets of ethical implications. But more than the particular cases involved, this level provided some tools for coping with ethical decision making.

Because of the increasing capabilities of computers and their increasingly pervasive presence in our private and public lives, the path ahead will be filled with instances in which the use of computers, information, and technology will have ethical consequences. As private citizens and as members of society, we cannot avoid making decisions on such issues, because even doing nothing is a decision that has ethical consequences. Finally, ethical decision making seems to be a purely human responsibility, not one that our computers can help us with directly, at least not yet.