Introduction

Ethics is a branch of philosophy that deals with issues of morality, that is, consideration of which human actions and reactions are morally right and wrong.

Why This Matters

It is important to make intelligent decisions from an ethical perspective about the actions that we take—that is, to consider whether our actions feel right or wrong to us and why. These actions range in scope from personal actions to the actions of our businesses and organizations, the actions of our governments, and ultimately the actions of our species. Digital technologies have provided new opportunities and dangers for our species and many new ethical considerations.

Consider This

In recent years, we have seen the rise of a new type of hacker group. Hacker activists, or hacktivists, hack computer networks for a perceived righteous cause. Hack collectives such as Anonymous, LulzSec, and AntiSec have claimed responsibility for breaking into the networks belonging to hundreds of businesses, law enforcement agencies, and government agencies, including the FBI and U.S. defense contractors, all in the name of “justice.” Typically, hacktivists choose their targets based on some injustice that has occurred or in order to retaliate against agencies that threaten hacktivists. In one case the hacktivist group Anonymous took on the Ku Klux Klan by taking down several KKK websites with denial of service attacks and hijacking major KKK Twitter accounts.

Once a target is hacked by a hacktivist organization, the group may publish embarrassing or revealing stolen information on the web. For example, a group of hackers, calling themselves the Impact Team, hacked the database of cheating site AshleyMadison.com, threatening to publish the personal information of 32 million users unless Avid Life Media, owner of AshleyMadison and its companion site Established Men, took down the two sites. The sites were not taken down and the private data was published.

Today many hack attacks are carried out for some righteous cause rather than for money. In some cases, the result of hacktivist attacks has had the intended effect: embarrassing the targeted company and those associated with it. However, hacking is still illegal. Dozens of hackers have been jailed for their participation in these hacker collectives. Many law-abiding individuals and businesses live in fear of these digital vigilantes. The web has certainly empowered many to advance righteous causes. What do you think? Should hacktivist groups be condemned by the public or supported? Why?

Essential Information

This unit addresses ethical issues surrounding the use of digital technologies. Although computer ethics is typically defined as relating to ethical issues confronted by computing professionals, this section addresses computer ethics in a broader sense. Computing touches everyone—not just computing professionals—at home, at work, and in our roles as citizens. We confront important ethically charged computer-related decisions in all of these areas. This section discusses personal ethics, professional ethics, and governmental ethics, along with related topics.

Lesson 2.1: Computer Ethics

Lesson 2.1 Introduction

Computer ethics refers to the responsible use of computers in all contexts and applications, by individuals, organizations, and governments.

It is easy to forget that computers and their users do not exist in a vacuum; every action involving computers, from the time they are designed and manufactured until they are decommissioned and disposed of, involves choices that impact society and the environment in significant ways.

Even before a computer has been powered on for the first time, many ethical decisions have been made. Computer components are manufactured in facilities around the globe, and building a manufacturing plant has an impact on local ecosystems and economies that should be carefully considered. How much do workers assembling computers get paid, and are they able to afford the same products they spend many hours building? Are the minerals that are refined and processed into chips and components mined responsibly, or does their extraction leave local environments and societies burdened with toxic byproducts? Once assembled, packaged, and shipped to retailers, are computers priced and marketed to all users, or as luxury goods only available to a few? How has your computer changed the world before you've pressed the power button?

Reading: Personal Computer Ethics

Personal Computer Ethics

Personal computer ethics refers to the responsible use of computers by individuals outside of professional environments.

Why This Matters

Computer users face many ethical choices in their casual use of today's technologies. Some software and online services make it possible to engage in unethical and sometimes illegal behavior—they may even encourage it. It is important for computer users to consider their actions carefully and intelligently to determine the course of action that best matches their own code of ethics and sense of responsibility. Too many computer users follow the pack and adopt others' sense of ethics, even when it goes against their own beliefs and conscience. Today's best leaders have a solid sense of what they hold to be ethical and unethical, and they exemplify those beliefs through their actions, while remaining open to new ideas and intellectual growth.

Essential Information

Each person has his or her own sense of what is right and wrong regarding computer use and behavior. Often computer ethics are learned from our parents and teachers. As we mature, those ethics are altered to suit our own belief systems. Personal computer ethics is a highly subjective topic, except in issues of local, state, and federal law, where ethical issues are clearly defined. Using a computer to create and distribute malware, steal credit card numbers, invade privacy with spyware, or steal copyright-protected

work or someone else's intellectual property is illegal. Those who participate in such activities might pay a price in terms of jail time and fines.

However, when a significant portion of a population in a democratic society opposes a law, there arises substantial pressure on the government to change the law or change conditions in society. For example, the digitization of music, movies, photos, and other creative work has created a situation where many otherwise law-abiding individuals may be actively violating copyright law by copying and enjoying media files (music, movies, photos, books) without securing a license by purchasing the item. In many such cases, courts have affirmed that owners of the intellectual property, the record companies, movie companies, or independent artists, deserve compensation. Through a process of court battles, technological solutions, and adjustments in the market, a slow but purposeful change has been occurring in views on intellectual property and the manner in which it is distributed and protected. An ideal solution accommodates both the public's need for robust, easy, and inexpensive access to intellectual property—such as art, music, and videos—and the creator's need to make a living.

This is how governance and law evolve. These institutions should not be rigid and unchanging, but flexible and responsive to society as it evolves. Good laws evaluate a situation from all perspectives and implement a solution that provides the greatest public good. If individuals can examine situations intelligently and unselfishly, then personal ethics will also serve the greatest public good.

Personal ethics regarding computer use typically combine legal considerations, what is best for the public good, and what is best for the person in terms of mental, physical, and spiritual well-being. Fear of the law may keep an individual from hacking a computer network. A feeling of social responsibility may guide a computer user to treat others online with respect. A person's own sense of morality may keep that person from becoming involved with web content that has a negative impact. What that content is may differ for each individual. Personal computer ethics requires an examination of one's own conscience and the weighing of benefits against costs in terms of personal, social, and legal considerations.

Reading: Professional Computer Ethics

Professional Computer Ethics

Authored by: Courtesy of Google Inc. License: Fair Use

Professional computer ethics involves the ethical issues faced by professionals in their use of computer systems as part of their jobs.

Why This Matters

The ethical issues faced by professionals who use computer systems as part of their jobs include a responsibility to customers, coworkers, employers, and others with whom they interact and who are impacted in some way by their computer use on the job. Because computer systems are integral tools in today's businesses, professional computer ethics often equates to business ethics. In today's connected professional environments, businesses need to be concerned with more than the bottom line. They should also be concerned with the ethical treatment of their customers and employees, protecting private information, and protecting the interests of investors. Businesses that create technologies need to consider the impact their products have on humanity and the natural world. Business computer systems and computer products provide powerful tools for both unethical and ethical behavior.

Essential Information

Professional computer ethics involves those who produce computers, software, and information systems as well as those who use them at work. Besides governing personal behavior, laws are also designed to govern professional behavior and the behavior of businesses. For example, the Identity Theft Protection Act of 2005 requires businesses to secure sensitive data physically and technologically and to notify consumers nationwide when such data is compromised. The Children's Online Privacy Protection Act of 2000 prohibits businesses from collecting personal data online from children under the age of 13. This is the primary reason Facebook and other online services either do not allow children under 13 to become members or require parental consent. This type of ethics is imposed upon a business by the government.

Many organizations and associations go beyond what is required by law and establish their own codes of ethics. Codes of ethical conduct can foster ethical behavior in an organization and give confidence to people who interact with the organization, including clients and customers. Some organizations and associations that have developed a code of ethical conduct include:

- Computer Professionals for Social Responsibility (CPSR)
- Association of Information Technology Professionals (AITP)
- The Association for Computing Machinery (ACM)
- The Institute of Electrical and Electronics Engineers (IEEE)
- The British Computer Society (BCS)

Such codes of ethics typically include consideration for general imperatives, such as avoiding harm to others and being open and honest, as well as more professional responsibilities, such as achieving high quality in your work, respecting intellectual property, and respecting client privacy.

Lesson 2.2: Government Rules and Regulations

Lesson 2.2 Introduction

Government rules and regulations are intended to balance the needs of citizens and business for freedom, opportunity, and security.

The rapid pace of change in the digital economy poses an acute challenge to lawmakers responsible for protecting citizens and businesses from threats on the Internet. Additionally, the complexity and interconnectedness of digital technology means that there are seldom simple answers to difficult questions, and any legislation designed to address those questions will necessarily be a compromise between conflicting interests.

Computers and the Internet have highlighted the tension between governmental guarantees of security and freedom. In order to provide protection against potential threats, governments need to be aware that they exist. When billions of people are online and able to communicate instantly with anyone else, this means that a few threats may be hidden within incomprehensible volumes of private conversations. Monitoring all of this data traffic is an enormous undertaking, and one that threatens privacy in order to provide an incomplete promise of security.

Reading: Governmental Computer Ethics

Governmental Computer Ethics

Governmental computer ethics refers to a government's responsibility to create laws to protect citizens from unethical computer use and provide citizens with equal access to computers and information technologies as well as their benefits.

Why This Matters

Governments face many of the same ethical considerations as businesses with respect to their use of computers and information systems. However, governments have the added responsibility of guiding the influence of technology on their population. They create laws that govern the use of technology so that citizens are protected from those who abuse others through the use of technology. Besides keeping information and people safe, the government also has a responsibility to give everyone equal access to technology in order to enjoy the associated benefits.

Essential Information

Governments shoulder the computer-related ethical responsibilities of entire countries and cultures. These responsibilities generally fall into two categories: protection and empowerment. A government should protect its citizens from those who wield computing powers in unethical ways. A government should also empower its citizens so that all socio-economic groups can benefit from the power of computing.

Many computer-related social issues are impacted by governmental regulation. Our political representatives are responsible for creating laws that protect us by regulating business use of technologies that are invasive to our privacy. For example, the FCC has passed net neutrality policies preventing Internet service providers from controlling what content users can view and charging more for some online services than others. Governments determine what types of information may be dangerous to the population and should be censored. Governments also wrestle with ethical issues when determining what situation constitutes the use of technology for surveillance and how to balance that with a citizen's right to privacy.

The government is responsible for defending a country's critical infrastructure from foreign governments, cyber criminals, and terrorist groups. This can be a challenge when much of that infrastructure is owned by private corporations. Some in government believe that companies operating power plants, communication systems, chemical facilities, hospitals, train lines, airlines, and other suppliers of critical

national resources should be required to meet performance standards to prove they can withstand attacks or recover quickly from them. However, others in government are against placing unfunded mandates on private corporations, even if it does mean a less secure nation. These are ethical dilemmas that a government faces. In either case, it is clear that the government must partner with businesses to protect the country.

Many governments are also trying to ensure that all citizens have the same basic privileges and opportunities. In the United States and some other countries, these efforts now extend beyond food, housing, and education to include access to computing and information technologies. Many governments are making efforts to extend the reach of the Internet to every citizen, even those living in remote locations. During his time in office, President Obama supported a broadband expansion plan focused on expanding high-speed Internet to rural areas of the country. The plan provides high-speed Internet to 98% of U.S. citizens so that everyone has the opportunity to benefit from what the Internet provides.

At times, some governments have felt compelled to shut down the Internet to stop or slow communication for their citizens. This generally arises in situations where anarchy exists in the population and law and order is needed. Shutting down the Internet is often the last act of a desperate, oppressive regime as it is about to be overthrown by its people.

Some governments withhold access to the Internet from citizens. In North Korea, only 4% of the population has access to the Internet; Burma and Cuba also severely restrict Internet access. The governments of Saudi Arabia, Iran, China, Syria, and Tunisia block sites considered anti-government in nature.

Reading: Accessible Computing

Accessible Computing

Accessible computing refers to the provision of equal access to computers and information technology for individuals with disabilities.

Why This Matters

Computer and information technologies must be designed in a manner that is easily accessible to all users. Unfortunately, in some cases, designers fail to consider the needs of disabled users, and their valuable products become unusable by individuals who have hearing, sight, or motor disabilities.

Essential Information

There is a growing body of law and policy in many countries that addresses accessibility of information and communications technology (ICT), including the Internet and web. Laws differ from country to country. Some treat access to ICT as a human or civil right; others mandate only that government-controlled ICT is accessible to all, including the disabled; others specify that ICT sold in a given market must be accessible.

Section 255 of the U.S. Telecommunications Act of 1996 requires telecommunications manufacturers and service providers to make their products and services accessible to people with disabilities, if readily achievable. The World Wide Web Consortium (W3C) has developed Web Content Accessibility Guidelines for businesses and organizations to use in making their web content accessible to users with disabilities, such as those who are unable to see, hear, or move (see video).

The U.S. Department of Education has developed Requirements for Accessible Software Design to ensure that all software used in schools is accessible to all students, faculty, and staff. The Americans with Disabilities Act of 1990 requires businesses to provide equal access to individuals with disabilities, including access to web content and services. Many countries and regions, including Australia, Canada, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Italy, Japan, New Zealand, Portugal, Spain, the United Kingdom, and the European Union, have instituted similar laws and considerations for the disabled.

Numerous software and hardware tools are available to assist the disabled in using PCs. Individuals may use screen enlargement software to make computer screens easier to read and use. Screen reader software like JAWS enables blind users to interact with the computer by using text-to-speech technology to read words displayed on the screen. The user manipulates the software, using predefined hotkeys, or shortcut keys. Some phone companies offer a service that uses a webcam attached to a hearing-impaired person's computer. When the person makes a call and uses sign language to communicate, an operator translates the hand signals to a hearing person at the other end of the line.

Lesson 2.3: Social and Environmental Impacts

Lesson 2.3 Introduction

Social and environmental impacts refer to the consequences of computer use beyond the immediate context in which they are used, specifically the indirect effects on society and the world in which we live.

Billions of digital devices are manufactured and used annually, which means that small changes to their design can have significant effects on the environment and society. Manufacturers who make a commitment to reducing their use of toxic materials and incorporating recycled components can eliminate tons of pollutants. Designers who incorporate accessibility features empower computer users who would otherwise be excluded from the benefits of digital technology.

Advances in digital technology have created highly visible benefits for users in recent years, but the negative consequences have often been more subtle and less obvious. At the same time that some users have been able to leverage access to these technologies to build tremendous wealth and find new opportunities for creative and social endeavors, many others have been left behind, receiving little or none of these benefits. While computer users in developed nations reap the benefits of computer-aided design and entertainment, those living in developing nations struggle to catch up while dealing with the

hidden byproducts and consequences of the digital age. This situation can be resolved, but it will take a commitment to green computing and inclusion from everyone.

Reading: Green Computing

Green Computing

"Green Computing" by Chad Kainz is licensed under CC BY 2.0

Green computing refers to the efforts of individuals, businesses, and governments to utilize environmentally conscious practices in the manufacturing and use of digital technologies.

Why This Matters

At the same time that many people are spending increasing amounts of their lives online in virtual space, the serious reality of climate change has given many of us a heightened awareness of our natural environment and the dangers it faces. Individuals, organizations, and governments are making efforts to reduce their carbon footprint—the amount of greenhouse gases they produce—and to manufacture and use computing resources in an environmentally conscientious manner.

Essential Information

The Intergovernmental Panel on Climate Change has determined that the buildup of greenhouse gases resulting from human activity, such as burning fossil fuels and deforestation, is primarily responsible for recent trends in global warming. Digital technologies contribute to global warming through the large amounts of energy they require, causing coal-burning power plants to generate increasing amounts of electricity and carbon emissions.

In an effort to improve the world, and perhaps their reputations in the process, many companies are going to great lengths to implement green computing initiatives. Green computing initiatives generally fall into one of two categories: energy efficiency or ecology.

There are many ways that the energy used in the manufacturing and use of computers can be reduced. Companies that manufacture computers are turning to reusable energy sources for a portion of their energy requirements. They are also streamlining manufacturing processes to be more efficient and less energy demanding.

New computing technologies are being invented that use less energy. For example, solid-state drives (SSD) are replacing hard disk drives, providing faster data access and dramatic energy savings. Processor manufacturers such as Intel are working hard to create new, more powerful processors that require less energy to run. New battery technologies are providing environmentally friendly materials that store energy more economically.

In addition to creating more energy-efficient hardware, software can be written in a manner that requires fewer processor cycles, decreasing a computer's power consumption, especially for the operating system. Also, operating systems can incorporate energy-saving features used to power down a computer when not in use.

The Energy Star program was created in 1992 by the U.S. Environmental Protection Agency (EPA) to inspire energy conservation in electronics products. Computers that are Energy Star certified save 20% to 30% on energy consumption on average. The ENERGY STAR 5 requirements for computers went into effect in 2009 and have the strictest energy requirements to date.

The power consumption of an individual PC is a drop in the bucket compared to that of corporate data centers. Some data centers have power requirements equal to that of medium-sized cities. Data centers require massive amounts of power for processing and especially for cooling. Most companies are working to reduce the energy requirements of their data centers. Many companies are replacing older, power-hungry servers with more efficient models and are using virtual servers that allow a single physical server to behave like several servers. Virtual servers maximize the amount of work that can be managed by a single hardware server.

Computer technologies have not traditionally been very ecologically friendly. Dangerous compounds and chemicals are used in the manufacturing of some computing equipment, and recycling programs for digital electronics components have been far from robust.

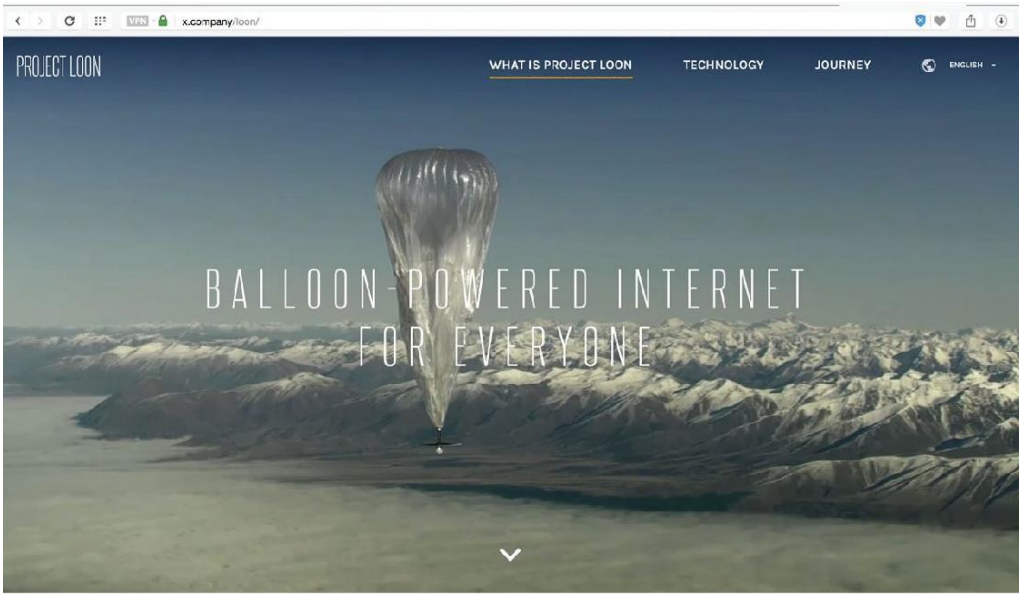
E-waste refers to discarded digital electronics devices and components. The Environmental Protection Agency estimates that 400,000 tons of e-waste is sent to recycling centers each year. Much of that waste contains dangerous contaminants such as lead, cadmium, and beryllium as well as brominate flame retardants. There is concern that digital electronics are being discarded at a rate that will soon overflow our landfills. There is also a concern about recycling practices that are hazardous to those involved and to the environment. Roughly 80% of recycled e-waste is shipped (often illegally) to poorer, developing areas such as Guiyu, China, and Lagos, Nigeria. Working for pennies an hour, workers dismantle, burn, or give acid baths to components to salvage valuable metals such as copper and gold, often at the cost of their health and the health of their environment. Children are exposed to dioxins, soil is poisoned with heavy metals, and the water becomes undrinkable.

Computer manufacturers are working hard to reduce the amount of dangerous contaminants in their products and are implementing take-back programs to assist customers with recycling.

Computer manufacturers are also working to avoid the use of conflict materials—natural resources that are extracted in conflict zones and sold to perpetuate the fighting. For example, cassiterite (for tin), wolframite (for tungsten), coltan (for tantalum), and gold ore are extracted from eastern Congo and used to manufacture consumer electronics. Electronics companies like Intel are avoiding the use of these minerals in order to help end conflict in the Congo.

Reading: Digital Divide

Digital Divide



Authored by: Courtesy of Project Loon, License: Fair Use

The **digital divide** refers to the social and economic gap between those who have access to computers and the Internet and those who do not.

Why This Matters

The digital divide highlights the issue of access and the difference in opportunities between the “haves” and the “have-nots.” Most agree that those without access to digital technologies are seriously disenfranchised in today’s world. The have-nots in this scenario may be unable to access technology due to a physical disability, financial limitations, geographic isolation, or political or social repression. There are digital divides based on gender, ethnicity, race, age, income, location, and disability.

Essential Information

Although a significant concern, the economic digital divide in the United States has been shrinking since the turn of the millennium. The number of Internet users in the low-income range (earning less than $25,000 per year) has soared, making them the fastest-growing segment of Internet users.

The global digital divide provides a greater social and ethical challenge. The World Economic Forum website states that countries need developed Information and Computing Technologies (ICT) systems to allow new models of collaboration, increase efficiency and boost productivity. The lack of skills in these areas leaves these populations with poor educational systems that do not support the new age of entrepreneurship and innovation enjoyed by the rest of the globe.

Several organizations and companies are working to bring computing and the Internet to everyone on earth. Intel is working with the Chinese government to provide Chinese university students with low-priced laptops. An international consortium, including Indian and American companies as well as the World Bank, is building thousands of rural Internet centers in India. Each center connects to the Internet by land lines or satellite links and includes five to ten inexpensive, thin client PCs to provide access to government, banking, and education services in isolated villages. Google has launched Project Loon, which delivers Internet access to remote areas of the globe via large weather balloons. Facebook, Nokia,

Samsung, Qualcomm, and others have created a global partnership to bring Internet access to unserved populations around the world via drone aircraft.

If humans are to utilize the Internet to build a global community, it is clear that the more affluent "neighborhoods" in this community cannot ignore the needs of the less fortunate. Those seeking to assist developing nations believe that societies must move from "divide" to "include" as the central organizing principle of their analysis and actions. Passing out PCs and providing Internet access is the first step; providing education is the next step; and including all humans in the information economy is the important last step.

Bridging global digital divides requires extensive commitment and organization. Many feel that it is an important investment worth the expense and effort. Although the information and communication technology revolution offers genuine potential, there is a risk that a significant portion of the world will lose out if humans do not take a global perspective. As technology reaches out to the world with fiber-optic, wireless, and high-speed connections, the world must be able to respond and participate. The Internet has created a seemingly smaller world and, in so doing, has called attention to social and economic problems. It is up to developed nations to recognize these problems and help develop solutions. However, if countries adopt a self-serving and opportunistic approach to technology, the digital divide will grow, as will global unrest.