6
Big Idea 5: Impact of Computing

"Outside of a dog, a book is man's best friend. Inside of a dog, it's too dark to read."

—Groucho Marx

Chapter Goals

- The World Wide Web
- Digital divide
- Beneficial and harmful effects
- Computing bias
- Legal and ethical concerns
- Safe computing
- Encryption
- Malware

The World Wide Web

At its origins in the early 1960s, the World Wide Web was intended only for rapid and easy exchange of information within the scientific community. In October 1969, the ARPAnet (original name for the internet) delivered its first message: "LO." It was attempting to send the message "LOGIN," but it crashed.

The internet is a global connection of networks, while the World Wide Web is collection of information that is accessed via the internet. The uses of the internet are changing all the time and have changed forever how we do business and how people communicate.

The internet has created global villages with both positive and negative effects. With a low investment, the internet has allowed users to access large audience via webpages, social media, and message boards. The freedom and rapid growth have had both positive and harmful effects on societies, cultures, and economies.

Internet access varies among different socioeconomic and demographic characteristics as well as among countries.

Digital Divide

The digital divide is the difference in access to technology including access to computers and the internet. Several variables affect the digital divide:

- Infrastructure—Some parts of the world do not have access to the internet.
- Education—A person could have access to the internet but not have the education to use it.
- Indifference—A person could have access to the internet but choose not to use it.
- Cost—The cost of accessing the internet could make using it unaffordable.

Efforts are currently being made to reduce the digital divide. For example, Google X's Project Loon is using balloons traveling at the edge of space to provide internet infrastructure to people living in unserved communities around the world. Some communities are also providing education classes and free Wi-Fi to decrease the digital divide.

An ethical concern about the digital divide is that official governmental policy at the time of this writing is being announced on Twitter that requires internet to access. People with access to the internet and Twitter are receiving policy change, while people without internet access remain in the dark.

The digital divide is why the course AP Computer Science Principles requires teachers to give a minimum of 12 hours of class time to complete the Create Performance Task. By guaranteeing the minimum classroom hours, students without computers or internet access at home can still be successful in this class.

Beneficial and Harmful Effects

A computing innovation can have both a beneficial and a harmful effect on societies, cultures, or economies. An effect may be an impact, a result, or an outcome. Beneficial and/or harmful effects are contextual and interpretive. Identification includes both the classification of the effect as either beneficial or harmful and justification for that classification.

A single effect can be viewed as both beneficial and harmful by different people or even by the same person. For example, GPS in a car can predict the time of arrival during a long car trip by tracking the speed of a car and the distance needed to travel. This can be beneficial to the driver to know his or her time of arrival. However, this same innovation can be harmful to the user if the police gain access to this data and give the driver a speeding ticket.

The way people complete tasks often changes to incorporate new computing innovations. For example, AP exams used to be graded in one place after physically flying in and housing graders from all over the world. Using new video-conferencing technology, AP grading is now being accomplished without the need for all graders to be in one place. This has reduced the cost of grading AP exams.

An Impact Beyond Their Intended Purpose

Although most innovations are created through careful planning, some are simply created by accident. Innovations such as the pacemaker, bubble wrap, X rays, and the microwave have all have been created by accident and have had a lasting impact beyond their intended purposes.

Computing innovations and algorithms can also have unintended impacts. The "greedy algorithm" was developed in 1956 by E. W. Dijkstra to find the shortest path from a starting node to all other nodes in a weighted graph. The purpose of this algorithm has evolved over time and is now commonly used for finding the shortest path to take by navigation systems.

The internet's original purpose was to be used exclusively by academic, government, and scientific communities. Today the internet can be used by anyone who has the tools to access it. Currently, the internet has over 3 billion users. As it has grown in influence, the internet has become a main source of credible news to many.

Innovations in technology have also changed the way that people complete tasks and do their jobs. For example, teachers no longer have to enter hand-calculated grades into a grade book manually. Instead, they use computer innovations to calculate and communicate grades with students and their families through the internet.

A computing innovation includes a program as an integral part of its function. Some examples of modern computing innovations include the following:

Snapchat
Facebook
WhatsApp
GPS systems
Self-driving car (software)
Cloud services
ATMs
Instagram
Twitter
YouTube
Sound Cloud
Uber
Pandora
LetGo
Google Maps
e-commerce (nonphysical computing concepts)
UberEats

Effects can be societal, economic, or cultural and can be connected to a group or individuals. Examples of the internet's effects include but are not limited to the following:

- The impact of social media online access varies in different countries and in different socioeconomic groups.
- Mobile, wireless, and networked computing have an impact on innovation throughout the world.
- The global distribution of computing resources raises issues of equity, access, and power.
- Groups and individuals are affected by the digital divide.
- Networks and infrastructure are supported by both commercial and governmental initiatives.

People create computing innovations. A programmer cannot possibly consider all the ways a computing innovation can be used. Responsible programmers try to consider the unintended ways their computing innovation can be used and the potential beneficial and harmful effects of these new uses. However, it is not possible to consider all the ways a computing innovation can be used. Computing innovations have often had unintended beneficial and harmful effects by leading to advances in other fields.

The rapid sharing of a program or running a program with many users can result in significant impacts beyond the intended purpose or control of the programmer. For example, a social platform may be designed to give people the power to build a community and bring the world closer together. However, with such a large community, the control over the information shared is hard to police. The resulting misinformation can lead to negative impacts on societies, economies, and cultures.

Example One

One **beneficial effect** GoFundMe has on society is that the website facilitates fund-raising for the needy. GoFundMe allows organizations to raise money for donations to charities.

For example, organizations can raise money for victims of violence or disasters. This benefits society because it improves the status of the needy by providing them with money for recovery. For example, fund-raisers like Equality Florida raised money to benefit victims of the Pulse Nightclub shooting. According to the *Orlando Sentinel*, "The largest GoFundMe page for Pulse Nightclub shooting fallout and victims has broken records on the website, nearing $5 million on Thursday."[2] GoFundMe allowed donations for the victims to break records.

One **harmful effect** of GoFundMe on society is that the fund-raising site can facilitate the growth of fraudulent organizations. Because money is transferred online, users cannot confirm their money is going to legitimate causes. GoFundMe is unable to prevent fraud effectively. The growth of fraudulent organizations harms society because it prevents money from going to those with true need. For example, individuals can set up accounts claiming to donate to a charity but instead use the money for themselves. This happened in the case of donations collected for Justin Owens's funeral. His friend, Justin Racine, created the account and likely kept the money for himself. According to *The Denver Channel*, "It was very easy for him to set up this bogus account with GoFundMe and then be able to take all the grieving friends' money, not to mention the grieving parents." [1]

Example One References

1. Allen, Jaclyn. "Family Alleges GoFundMe Account Fraud after $3,500 Meant to Pay for Funeral Disappeared." *The Denver Channel*. N.p., 15 June 2016. Web. 18 Oct. 2016. <http://www.thedenverchannel.com/news/local-news/family-alleges-gofundme-account-fraud-after-3500-meant-to-pay-for-funeral-disappeared>
2. Brinkmann, Paul. "Pulse Fund on GoFundMe Nears $5M, Breaks Records." *Orlando Sentinel*. N.p., 16 June 2016. Web. 17 Oct. 2016. <http://www.orlandosentinel.com/ business/brinkmann-on-business/os-fundraising-gofundme-record-20160616-story.html>

Example Two

One **beneficial effect** that Twitter can have on society is that it can help spread awareness of an issue or a cause. It is an easy way for groups to reach millions of people, and making an account is free. An example of this is when the Memphis Veterans Administration (VA) was concerned with the number of veterans committing suicide, and it started a Twitter campaign using the hashtag #BeThere on Twitter.[1] With this campaign, the VA was able to reach out to the community and help stop suicides thanks to Twitter's service. This not only helped veterans but also helped to create a more caring, concerned, and charitable society.

A **harmful effect** that Twitter can have on society is that it makes it easy for terror groups to spread their message. If spreading a good message is easy, it is almost equally as easy to spread a bad message. So far, Twitter has suspended 360,000 terror-related Twitter accounts in 2019 alone. Many similar Twitter accounts are popping up every day.[2] The ability for terrorists to spread their message and recruit new members is alarming, especially because of just how easy Twitter makes it. These messages also make law-abiding people feel afraid for their safety and well-being.

Example Two References

1. McKenzie, Kevin. "Memphis VA Promotes Suicide Prevention with Comedy, Fashion." The Commercial Appeal. *USA Today*, 7 Sept. 2016. Web. 9 Sept. 2016.
2. Rutkin, Aviva. "Extremists Are Turning Twitter and Facebook into Theatres of War." *New Scientist*, 7 Sept. 2016. Web. 9 Sept. 2016.

Human Bias

Computing innovations can reflect existing human bias. Algorithms are helping people make decisions that can have extreme ramifications. An algorithm can determine where to place police resources; it may decide who gets into a college or who will get a job. To avoid negatively impacting people or groups of people, care must be taken in not only the development of algorithms but also in determining what data the algorithms can access. Algorithms can be intentionally or unintentionally biased. Algorithms can be used to determine starting salaries for large companies. One of the variables might be salary history. Given the well-documented concern of sexism in salaries, however, including salary history would import gender bias into starting salary calculations.

Since computing innovations are created by people, the innovations created can reflect bias that the programmers bring with them. Programmers should take action to reduce biases at all levels of software development. Variables such as age are appropriate in some calculations, such as life insurance and auto insurance, but inappropriate in other calculations, such as hiring and mortgage lending. Based on information bought from social media, neighborhoods could be denied opportunities determined by demographics alone.

Crowdsourcing

Crowdsourcing is the practice of obtaining input or information from many people via the internet. For example, the United Kingdom looked to crowdsourcing to name one of their state-of-the-art boats for the Natural Environment Research Council. Around 120,000 people voted for the name *Boaty McBoatface*. Another example involves the Create Performance Task required for this class. Coding hints can be found on websites such as Stack Overflow, which crowdsources questions and answers on coding tips. You could ask the "crowd" for feedback, and anyone with access could provide answers. The accuracy of the answers can vary, but make sure you give credit in your code. The use of material created by someone other than you should always be cited.

Crowdsourcing offers new models for connecting business with funding. For example, Uber connects drivers with people who need rides. Crowdsourcing can also connect social causes with funding. In New York City (NYC), a crowdsourcing site funds local community gardens. Crowdsourcing exposed people who never thought of growing a garden in NYC to the idea; the thought of walking through a garden and enjoying nature motivated donations. Anyone can raise money for almost any cause. However, with the ease of posting legitimate crowdsourcing causes, it is equally easy to post false causes.

Citizen Science

Citizen science is scientific research using public participation in scientific research. The research is conducted in whole or part by distributed individuals, many of whom may or may not be scientists. They contribute relevant data to research using their own computing devices. Since many of the contributors might not have scientific training, usually the data collected, although vast, are not necessarily technical.

For example, citizen science could be used to calculate the firefly population on the east coast of the United States. Firefly counting needs lots of people but not a lot of technical skills or expensive equipment. An example of an experiment not suited for citizen science is testing a vaccine on human volunteers. When testing on humans, a trained professional scientist is needed.

Legal and Ethical Concerns

Material created on a computer is the intellectual property of the creator or organization. Ease of access and distribution of digitized information raises intellectual property concerns regarding ownership, value, and use. Algorithms on legitimate sharing sites have an obligation to safeguard intellectual property. Sites do this by scanning for content that matches intellectual property and removing the illegally shared content from their site.

The use of material created by someone else without permission and presented as one's own is plagiarism and may have legal consequences. Sites, such as Napster, that did not protect intellectual property have been shut down and heavily fined.

Materials created by someone else can be used legally in certain situations. The following are a few examples.

- Creative Commons is an American nonprofit organization that is dedicated to expanding the range of creative works available for others to build upon and share legally. The Creative Commons license is a public copyright license that allows for free distribution of copyrighted work. Creative Commons is used to give people the right to use, share, and build upon an author's work. These licenses allow creators to communicate which rights they reserve and which rights they waive for the benefit of recipients or other creators. Creative Commons licenses can vary from letting others copy, distribute, display, and perform only original copies of work while not allowing modification without the author's permission to allowing for modification if credit is given to the author. There are six different levels of this license. Creative Commons licenses are common in education where teachers share their work in the hope that someone will add to their lessons and help other teachers. This is not used when seeking profit from the work. However, Creative Commons can increase exposure to the author, which might eventually lead to financial gain for him or her.
- Open source are programs that are made freely available and may be redistributed and modified.
- Open access is online research output free of all restrictions on access and free of many restrictions on use, such as copyright or license restrictions.

Creative Commons, open source, and open access have enabled broad access to digital information. As with any technology or medium, information from computing innovations can harm individuals. Malicious information can disguise itself as legitimate information, making it

hard to figure out what is real. In combination with the role computing plays in social and political issues, the possibility of malicious information raises legal and ethical concerns.

Computing innovations can also raise legal and ethical concerns. Some examples of these innovations include:

- The development of software that allows access to digital media downloads and streaming
- The development of algorithms that include bias
- The existence of computing devices that collect and analyze data by continuously monitoring activities

Safe Computing

Security is needed to protect the confidentiality, integrity, and availability of information. Security protects that data from cyber attacks and hacking. Privacy is the right to control data generated by one's usage of computing innovations and restrict the flow of that data to third parties.

Privacy and security are concerns with any interaction on the internet. Once a company's security or privacy has been compromised, it takes years, if ever, for customers to trust that company again. Target, Ashley Madison, AOL, Yahoo, and Facebook are examples of large companies that have had their data compromised, with some of those companies never recovering consumers' trust.

Personally, identifiable information (PII) is information about an individual that identifies, links, relates, or describes that person. Examples of PII include the following:

- Social security number
- Age
- Race
- Phone numbers
- Medical information
- Financial information
- Biometric data

PII can be analyzed and processed by businesses and shared with other companies. The information collected has enabled companies to gain insight into how to interact with customers better. PII and other information can be used to enhance a user's online experience. PII can also be used to simplify making online purchases.

PII has monetary value. The entire business model for some computing innovations is to sell user information to targeted advertisers. As a result, concerns have been raised over how companies handle the sensitive information of their consumers.

Information placed online can be used in ways that were not intended and that may have a harmful impact. For example, an email message may be forwarded, tweets can be retweeted, and social media posts can be viewed by potential employers.

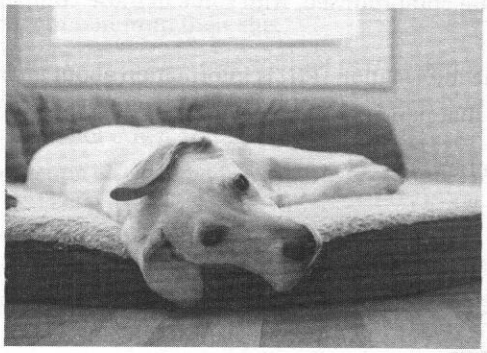
Once information is online, it is difficult to delete. Information posted to social media services can be used by others. Combining information posted on social media and other sources can be used to deduce private information about you.

Cyber criminals are creative in their methods for stealing PII data. One such data breach was an app developed to use on Facebook that was a personality quiz. The app was designed to take the information from those who volunteered to give access to their data for the quiz. This quiz generated more data when the quiz was shared with friends and family. The data were then sold to the political consulting firm Cambridge Analytica, which used the data for targeted ads during the 2016 presidential election campaign. Facebook was fined $5 billion by the Federal Trade Commission for violating consumers' privacy rights.

Technology enables the collection, use, and exploitation of information about, by, and for individuals, groups, and instructions. For example:

- Search engines can record and maintain a history of searches made by users.
- Websites can record and maintain a history of individuals who have viewed their pages.
- Devices, websites, and networks can collect information about a user's location.

A computing innovation generates metadata that can have the effect of reducing the privacy of the user. Metadata can include geolocation, time, date, filename, and so on. This rapid sharing of user data can often have significant impacts beyond the intended purpose or control of the programmer.



For example, user data can be sold to targeted marketing companies. Marketers can use large data sets to target audiences who are likely to buy their products. For example, the author of this text adopted a puppy named Lilygoose. Soon after the adoption, the author received an advertisement for puppy products. This advertisement included the dog's name, breed, and color. (A picture of Lilygoose is provided above for reference.)

The same open standards that fueled the growth of the internet have, at the same time, left users open to malware. Antivirus software and firewalls can help avoid malware. However, some cyber criminals hide malware in antiviral software! Users must always be aware of who they trust.

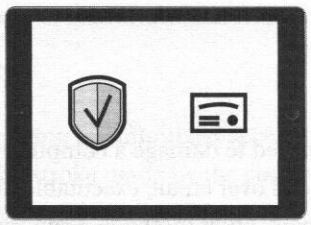
Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include passwords and multifactor authentication. A strong password should be easy to remember but difficult for someone else to guess. A weak password would be something that PII data can predict. Combinations of your birthday and your elementary school would be easy to guess if cyber criminals have your PII data.

Multifactor authentication is a method of computer access control in which a user is granted access only after successfully presenting several pieces of evidence to an authentication mechanism, typically in at least two of the following categories:

- Knowledge—something the user knows
- Possession—something the user has
- Inherence—something the user is

Multifactor authentication requires at least two steps to unlock protected information. Each step adds a new layer of security that must be broken to gain unauthorized access.

Digital certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.

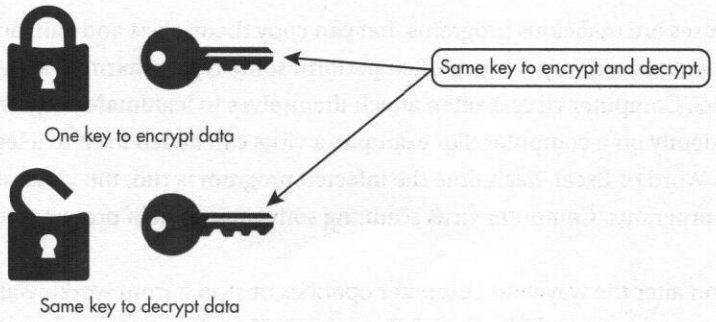


Digital Certificate

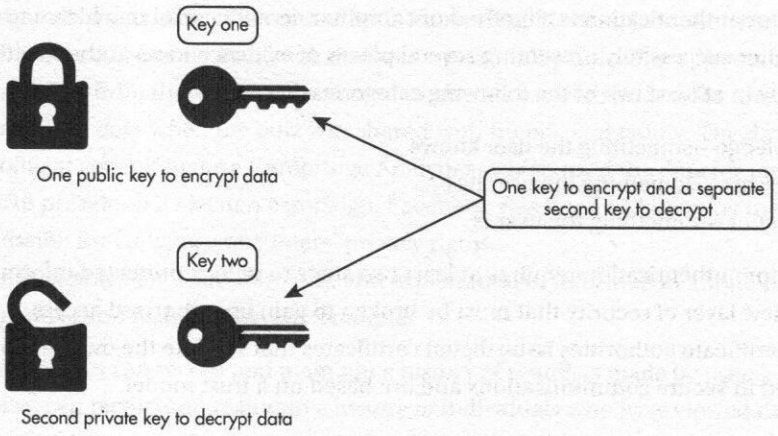
Encryption

To increase security, encryption is used. Encryption uses cryptographic algorithms to encrypt data. Encryption is the process of encoding data to prevent unauthorized access. Decryption is the process of decoding the data.

Symmetric key encryption uses the same key for both encryption and decryption. The one key is a shared secret and relies on both sides keeping their key secret.



Public key encryption (also called asymmetric encryption) uses two keys—one private and one public. Anyone with the public key can encrypt data, and the public key is public. To decrypt, a second key, which is private, is needed.



Malware

Malware is malicious software intended to damage a computing system or take partial control or its operations. Malware can be spread over email, executable files, instant messaging, social media, freeware, shareware, and many other methods. Even mobile phones are vulnerable to attack. Malware scanning software can help protect a computer against infection.

Malware has caused billions in damage and have been used as cyber weapons. For example, Stuxnet is malware that was built by the United States with the intention of obstructing nuclear weapons from being built in Iran. Stuxnet was spread by a USB thumb drive and targeted software controlling a facility in Iran that held uranium.

Real-world systems have errors or design flaws that can be exploited to compromise those systems. Malware looks for outdated software with unpatched security flaws to infect. Regular software updates help fix errors that could compromise a computing system.

Computer Viruses

Computer viruses are malicious programs that can copy themselves and gain access to a computer in an unauthorized way. Viruses often perform some type of harmful activity on infected host computers. Computer viruses often attach themselves to legitimate programs and start running independently on a computer. For example, a virus can attach itself to a legitimate program, such as Word or Excel. Each time the infected program is run, the virus runs and attaches itself to other programs. Computer virus scanning software can help protect a computer against infection.

Viruses can alter the way your computer operates or stop it from working altogether. Computer viruses currently cause billions of dollars' worth of economic damage each year. Some viruses such as REvil encrypt data on infected machines and hold that data until a ransom is paid.

Phishing

Unauthorized access can be gained to computers in several ways. One method is phishing. Phishing is a technique that directs users to unrelated sites that trick the user into giving personal data. Phishing is a technique used by cyber criminals posing as a legitimate institution to lure individuals into providing sensitive data, such as PII, banking and credit card details, and passwords. This personal information can then be used to access sensitive online resources, such as bank accounts and emails.

Scammers often update their tactics, so phishing attacks can be hard to identify. A common phishing scam involves a malicious link that is disguised on a webpage or in an email message, directing the user to a site that the user identifies as a trusted site. However, the site is not the trusted site but, instead, is a site designed to just look like the trusted site. The spoofed site prompts users to download freeware or shareware that contain malware.

Keylogging

Keylogging is another method involving unauthorized access to a computer. Keylogging is the use of a program to record every keystroke made by the computer user in order to gain fraudulent access to passwords and other confidential information. Keylogging monitors and records every password and credit card number the user types and then sends this information to cyber criminals who make use of this sensitive data. Some keyloggers are hardware. The physical hardware is installed between the keyboard and the computer. Security software cannot detect hardware keyloggers.

Rogue Access Point

Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point. A rogue access point is a wireless access point that gives unauthorized access to secure networks.