2017

Blown to Bits Project

David Schmidt Ph.D.
Fort Hays State University, dschmidt@fhsu.edu

Blown to Bits Project
David Schmidt, Ph. D.

I needed supplementary materials for an introductory course called Management Information Systems 101, since renamed Informatics 101. The course has two main objectives, skilled use of Microsoft Office and Google Apps (and other application software) and understanding central issues involved with the use of digital technology. I looked for resources on the web that I could incorporate into the course and found a very good book called *Blown to Bits*. Fortunately this book has a Creative Commons license (Attribution-Noncommercial-Share Alike) that permits it to be used in its entirely for my course and other courses like it. Because I could not cover all of the topics in the book I picked the chapters I wanted to use in the course, and I worked with the content in those chapters. I wrote notes for each chapter that summarizes selected topics from the chapters and I added an assignment with a rubric for each chapters. Since the book was copyrighted in 2008 there have been advances in technology, and in some cases I added information to take that into account. The appendix in the *Blown to Bits* book adds some technical information. I like going into a bit more detail in the course, so I added material to supplement what was in the appendix.

I am licensing this work with the same Creative Commons license (Attribution-Noncommercial-Share Alike) license.[1]

Blown to Bits Chapter One Issues and Questions

1. The new digital world has changed what is possible to know and to do while at the same time testing regulatory laws and principles.

- The Tanya Rider case illustrates the fact that phone companies now have location information available to them that was not available to them a short time ago, and yet that information cannot be given out to the police or to the public except in very constrained circumstances.
- By GPS and by triangulation the cell phone companies can know or approximate the location of phones, but giving out that information is highly regulated.
- In this case Tanya's right to privacy prevented others from finding her more quickly.
- Observation: there is no simple answer to changing the regulations and laws because the right to privacy remains important in spite of the fact that looser regulations could have helped in this case.

2. New technology has brought with it the potential for great disruption.

- Posting photos to Facebook or sharing photos on Google Drive or Microsoft's Onedrive can have unexpected consequences. For example, because the photos often have data showing time and location, someone with an ulterior motive can use the information against the person in the photo.

- Governor Elliot Spitzer's affair with a prostitute was discovered when the bank discovered patterns of payments – all part of an effort by the government to track money launderers.
- Court cases, traffic tickets, medical records, and other digital information is more public now than ever. When interviewing for a job, the interviewer may locate information about you that did not think was available.
- People no longer get their news from the same authoritative sources. In large part because of the use of the Internet (as well as other television alternatives) people choose the news sources they follow. This has resulted in a fragmentation of news and the demise of shared experiences and shared sources. This can result in a more polarized society. Those who watch Fox news have less in common over time with those who watch the traditional sources (NBC, CBS, or ABC).

3. Koan #1: It's all just bits.
    - The Naral case: Verizon initially did not allow Naral the right to send texts to those who wished to opt in to receive texts from Naral. Verizon apparently thought that allowing a group that promoted unpopular (in some quarters) political views on abortion should not be allowed. Ultimately, they did allow it, but they still reserve the right to refuse service if they choose to do so. Government regulations still permit this.
    - Phone calls (which now are handled with digital technology and are regulated as a common carrier, meaning that practically all types of phone calls are allowed) have different laws from text services (digital technology too but not considered a common carrier in this case) which allows Verizon the right to refuse service. The same technology (or bits) underlie both services, so it is a bit puzzling that laws vary.

4. Koan #2: The perfection of bits.
    - When teenagers would copy songs by making tapes of tapes the quality degraded and the music industry was not threatened.
    - Now when music (or movies) are digitized the music industry (and the movie industry) is threatened because the copies are just as good as the originals.

5. Koan #3: There is want in the midst of plenty.
    - If the records have not been digitized "they don't exist." For example, if some past medical records are not available in digital form to a new doctor that you are seeing, they "don't exist" for that doctor.
    - Also, there is the problem of obsolescence. Even if some records have been digitized, if there is not current technology that can access those records, they are useless.

6. Koan #4: Processing is power.
    - Because of Moore's law, that processing power doubles about every eighteen months,

computer chips can now handle and process huge amounts of data.

- This can make things qualitatively different. Whereas facial recognition technology required too much processing power in the past, now it can be done rather quickly making surveillance possible.

7. Koan #5: More of the same can be a whole new thing.
   - Digital photography started slowly because cameras were bulky and memory was costly.
   - However, processing power kept increasing, the size of the processors and memory chips kept getting smaller and eventually cameras appeared in cell phones.
   - Still cameras and motion picture cameras that relied on film were rapidly replaced and a once-vibrant film industry essentially died.

8. Koan #6: Nothing goes away.
   - Because storage is now cheap, billions of transactions are stored.
   - A hotel gives clients key cards. With the key cards and other records the hotel can know exactly when people left and entered the room, what food was ordered, what items were purchased, type of car driven, etc. This data is retained, and it can be aggregated with other data.
   - If it ever gets out, then it is often stored on other databases. It seems to exist forever, and it is hard to expunge.

9. Koan #7: Bits move faster than thought.
   - Dialing for service in local companies might go to India, and the response is just as fast.
   - Sending X-Rays to be analyzed might be sent across the world, and the analysis faster than in a local hospital.
   - All of this causes disruptions to the marketplace. Perhaps it is creative destruction as Joseph Shumpeter says. In any case it is disruption.

10. Technology is neither good nor bad.
    - The same technology that can be used for targeted marketing can be used for blackmail.
    - The same technology that can be used to provide online courses to poor nations can be used to distribute copyrighted materials.
    - Encryption is used to protect our financial transactions, but it is also used by terrorists to escape detection.
    - The challenge is to find the proper regulation of technology while still encouraging new development.

11. New technologies bring risks and opportunities.

- Facebook and Twitter have brought about a tremendous amount of sharing of information. Along with the freedom to share information has arisen the issue of fake news. Some "news" stories take the internet by storm but later turn out to be false. How can this be mitigated?
- Live streaming video from Facebook has resulted in some graphically violent video being disseminated across the web.
- The fast Internet technology has also allowed people in isolated places to serve others in more wealthy areas and bring them out of poverty.
- The authors recommend broadening one's horizons and visualizing opportunities even though there are some disruptive forces unleashed by the new technologies.

Case Study: The Case of a Wireless Internet Service Provider

Background Information: You are in charge of a nationwide wireless service that provides Internet access over cell phones to millions of customers. You provide phone service and data services. In particular, you provide a text-message program that allows various political, civic, and other groups to communicate with their membership. Members of those groups opt in to sign up for text messages by sending a message to a five-digit number known as a short code. After opting in the members receive alerts and other communications from the group providing the messages. Many political candidates and advocacy groups use this method to communicate with those interested in these issues. As a wireless service you have the right to refuse service to groups who request it.

Two Requests: You have received a request from NARAL Pro Choice America (a group that advocates reproductive rights for women including the option to have an abortion) and a request from a White Supremacist group for the ability to set up their own text messaging programs.

Will you grant or refuse service to either or both of these groups? Provide reasons or arguments for and against both groups, and then indicate your decision. Upload your document into Blackboard (Module 2). Include at least 80 words or so in each category (reasons for, reasons against).

Reasons for granting the NARAL request.

Reasons against granting the NARAL request.

Your decision.

Reasons for granting the White Supremacist request.

Reasons against granting the White Supremacist group request.

Your decision.

Name:

Save the file as Lastname_Firstname_Casestudy.docx and submit to the instructor.

Rubric NARAL Case Study

Performance Element	**Exemplary**	**Proficient**	**Developing**	**Points Possible**	**Points Earned**
The reasons given for and given against granting the NARAL request are reasonable and well defended	**45 points** (All items nicely done.)	**5 - 30 points** (Points depend on the quality of the reasons.)	**0 points** (Task not completed)	**45**	
The reasons given for and given against granting the White Supremacist request are reasonable and well defended	**45 points** (All items nicely done.)	**5 - 30 points** (Points depend on the quality of the reasons.)	**0 points** (Task not completed)	**45**	
The document has good grammar, spelling, and formatting.	**10 points**	**8 – 1 Points**	**0 points** (Task not completed.)	**10**	
Total Points				**100**	

Blown to Bits Chapter Two Issues and Questions

Bombing in London

On July 7, 2005, there were four explosions caused by suicide bombers in London. 52 people died and 700 more were injured. London has thousands of surveillance cameras, and they were used to document the time that the bombers had used for reconnaissance two weeks before the bombing. After authorities had determined that these were the bombers, pictures of the bombers were instantly sent around the world.

George Orwell's ***1984*** talked about a time of almost universal surveillance and the phrase "Big Brother is Watching You" became famous. Now "cameras are far from the most pervasive of today's tracking techniques." (**Blown to Bits**, p. 20) Other techniques now track our every move (so to speak).

Here is a list of some of those techniques:

1) Cell phone companies know the numbers we call as well as where we have carried our phones (they can use triangulation or use the GPS capabilities in our phones).

2) Credit card companies know not only where we spent our money, but also what we spend it on. (***Blown to Bits***, p. 20)
3) Banks record our transactions to monitor our account balance but also to notify the government if we make large withdrawals. I believe that this monitoring occurred because the government is interested in tracking money laundering related to drug money as well as in tracking money supporting terrorist organizations.
4) Loyalty cards at various chain stores track our purchases and track the stores that we use for those purchases. For receiving these small discounts we give up our privacy for the use of these loyalty cards. As the authors comment, this is like a privacy tax. If we choose to forego the loyalty cards we pay a "tax" for that right to privacy.
5) The ***Google*** Street View shows the location of our houses, but the cameras also captured whatever was occurring at that location in that moment in time. For example, the cameras show any cars that happened to be parked nearby when the Google contractors took the pictures.
6) Camera metadata. Camera metadata revealed information which permitted tracking the person who took pictures of every page of one of the Harry Potter books, ***Harry Potter and the Deathly Hallows***. This person published those images on the web before the book was released to the public. The metadata included much about the image but also recorded the make, model, and serial number of his camera (***Blown to Bits***, p. 24). Since the camera was registered the identity of the person was found. There are other ways to track it too. If it was purchased with a credit card, or if it was sent in for service the person could be discovered.
7) GPS data.
    - Cell phones track where you are. You can also choose to make yourself discoverable by using the track phone location feature on your ***iPhone*** or other smart phone. Even if you do not make yourself discoverable, the cell phone company knows where you are.
    - Rental cars or transport trucks often have GPS devices. The company you work for or the rental car company can therefore know where you went. So, in cases of dispute, the company can verify where you were.
    - Photos are often stamped with location data based on the use of the phone GPS so your locations can be tracked by looking at the information related to the photos.
8) RFID tags. These are little silicon chips that can transmit information. They are passive devices that respond to transmissions and yield information when prompted. Cattle, pets, passports, and other items often have RFID tags. Because they are tiny, they can easily be put in consumer goods. If a shoe chain would choose to do this they could insert them into the shoes they sell. Then RFID readers would sense when the person is back in the store. Using the database from the store, the clerks could know a lot about their customer – and then offer the customer goods or services based on past purchasing history.
9) Event Data Recorders. Cars now have black boxes similar to devices in airplanes that record events prior to a crash. These recorders log how fast the car was going prior to the crash, whether seat belts were attached, when brakes were applied, whether turn signals were on and other details. The insurance industry uses this information extensively. In this way our driving habits are tracked and recorded at the moment of a crash. This information is now routinely used in court cases.

10) Color printers. Color printers (most) include a secret code on every printed page. This includes the printer serial number, date, and time (***Blown to Bits***, p. 29). The reason for doing this is to identify the printers used in printing counterfeit bills.
11) Parking garage tickets. Some parking garages have two tickets, one that you use for purchasing parking time in the garage and another (unknown to most people) that has a picture of your license plate. If they do not match, then the parking service may delay your exit from the garage. Some people with long parking times and large bills were trying to scam the garages by turning in wrong tickets, so they started to photograph the license plates.
12) Online journals have images (figures) that are high-resolution JPEG images (a requirement of many journals). This can result in using those images for further identification purposes. If, for example, someone would enlarge those JPEG images which display maps containing sensitive data, that data can sometimes be superimposed on housing maps in order to locate individual dwellings. (***Blown to Bits***, p. 47)

Connecting the Dots

Now it is possible to use vast computing power to connect various databases, search various databases, and to link information in many new ways. For example, in the investigation of Enron there were records of thousands of emails. A program was written to display patterns of who was receiving emails from whom, and out of this display of patterns various clusters were found. Certain people typically received a lot of emails from other select people (sometimes people who were scattered across the company), and the program showed the variety of patterns which alerted prosecutors to key individuals to investigate. Similarly, the National Security Administration analyzes phone calls in similar ways. The agency takes note of the patterns of calls. They may not know the content of the calls, but if a pattern of calls is suspicious, then that might warrant looking into why the calls are being made. If the pattern of calls correlates with other events, then that too triggers further investigation.

Even deidentified data can be correlated with other public data to pinpoint individuals because it can be correlated with other public data.

Why We Lost Our Privacy, or Gave It Away

Saving Time

RFID cards can save us time on tollways. The RFID K-Tag card is used to go quickly through the toll line on the Kansas turnpike instead of waiting in line for those wanting to pay in cash. The tradeoff is loss of privacy. The Kansas Turnpike Authority can know exactly when you drove onto the turnpike and exactly when you exited the Turnpike because the K-Tag information is logged. These facts have been used in divorce cases and child custody cases when a spouse has claimed to be at one location when he or she was in another location (a more compromising one) or when someone claims to be home to pick up a child and the records show differently.

Convenience of the Customer

Amazon has algorithms that look at past purchases and suggest additional items that one might like. Amazon typically does a fairly accurate job at targeting the consumer interests. The tradeoff is the fact that Amazon knows a lot about our personal preferences depending on how many purchases we make.

Public Documents are VERY Public

The Federal Election Commission was created to administer the Federal Election Campaign Act. As a result all political contributions are now public information. If we choose we can snoop on our neighbors and see who donates to whom. Also, because real estate tax rolls are online we can see what our neighbors paid for their houses.

For a fee one can get all kinds of information about individuals. There are even services that say they can produce cell phone records for individuals for a fee. Now there is the Telephone records and Privacy Act (2006) designed to prevent this, but some still advertise that they can find this information. Further one can also pose as an "employer" and pay for background information on potential employees to get information on others.

Other Instances:

55% of teenagers and 20% of adults have profiles on social media sites. (***Blown to Bits***, p. 20) Many have no restrictions on who can see those profiles. Much of the social media is for purely social reasons, but there are social media sites that are more professional such as ***LinkedIn*** that also contains a lot of detailed information.

There are other ways for tracking us.

1. We log in to various services, so those services know exactly who we are.
2. The computing service may leave cookies on our computers for later reuse. These cookies are small text files that remain on out computer that allow personalization and tracking. If we realize they are there at all, sometimes we choose to leave them on our computer for purposes of convenience. For example, if I allow Netflix the ability to use cookies I don't have to login each time I want to use Netflix. It "logs me in" automatically. The problem is that if my computer gets hacked, the hacker can get this information and get access to the computing services that use these cookies.
3. The web server knows your IP address. In order to send web pages to me (such as my bank transactions or suggestions for purchases from Amazon), the web server needs to know my IP address. Even though these numbers can change from day to day from my computer, the ISP has records of the IP addresses and logs for every day, and these logs can be subpoenaed.
4. Suppose I use Gmail as my email provider. Google inspects the content of all my emails with a goal of attaching some appropriate advertising. Google could easily build a profile of my preferences and interests on the basis of these emails.
5. If you work for a financial services company your emails typically are all logged in case there is a problem later. In case some issue arises, the company can then search through all of your past emails to see what happened.

Spying Software and Hardware

1. Parental Control Software. Spouses have been known to use parental control software to spy on their spouse. Some individuals have been caught in rather compromising communications with others as a result.

2. Keyloggers. Hardware or software keyloggers can be installed in ATMs, on keyboards, or elsewhere. These devices or appliations do what their name implies; they log keystrokes. So, every keystroke that has been made is logged and saved. In some cases the keystrokes are transmitted wirelessly to someone monitoring the activity. Keyloggers with wireless transmitters have been known to be installed on ATM machines so that usernames and passwords can be captured by someone receiving the transmissions nearby.
3. Cell Phones. Cell phones "can be reprogrammed remotely so that the microphone is always on and the phone is transmitting, even if you think you have powered it off." (***Blown to Bits***, p. 49) Some people now remove the batteries from cell phones to prevent this or they use burner phones that get discarded after use.
4. ***OnStar***. The ***OnStar*** microphones can be remotely activated in cases of emergency by ***OnStar*** operators. What is lesser known, however, is that ***OnStar*** will cooperate with federal authorities so that federal authorities can and have listened to conversations in cars with these systems.
5. The FBI would like to gather biometric data on about everyone it can. As people go through airport security, they would like to give people the option of having a snapshot taken. The idea being that they could then pass through quicker the next time. This information would then be added to the FBI database, and it would cause less political backlash because people would submit to this voluntarily.
6. Big Aggregators. ***Acxiom*** and ***ChoicePoint*** are two big data aggregators. ***Acxiom*** looks at a large part of a billion transactions a day. ***ChoicePoint*** has 100,000 clients. The scale of what they do makes them different. They can search through financial transactions, phone call records, travel tickets, banking transactions, and so on to see if individuals are good risks for various things, to track down terrorists for the government, etc.

In summary we give up a lot of privacy for convenience and for small price breaks. We like the K-Tag because we can get on the toll road quicker. We like the loyalty cards because we get discounts. To some extent we appreciate the suggestions from ***Amazon*** about new books to buy or new items we might like to purchase. On the other hand, when we think about all of the different ways our lives are not public and how companies or investigators can aggregate all of this information, it should give us pause.

Assignment

List 10 ways in which we have given up our digital privacy. Explain in each case how we have lost some privacy. In each case, discuss whether that loss of privacy is desirable giving reasons why it is acceptable to give up our privacy in that way or whether you believe it is not acceptable. In each case discuss how we should minimize that loss of privacy or maintain full privacy (if that is possible).

Rubric Privacy Case Study

Performance Element	**Exemplary**	**Proficient**	**Developing**	**Points Possible**	**Points Earned**
Ten cases involving loss of privacy are cited. Explanations are given for the	**20 points** (All items nicely done.)	**5 - 15 points** (Points depend on the quality	**0 points** (Task not completed)	**20**	

loss of privacy.		of the reasons.)			
Discuss in some detail why the loss of privacy is acceptable or why it is not.	**40 points** (All items nicely done.)	**5 - 30 points** (Points depend on the quality of the reasons.)	**0 points** (Task not completed)	**40**	
Discuss ways of minimizing the loss of privacy for each case.	**40 points**	**5 – 30 Points**	**0 points** (Task not completed)	**40**	
Total Points				**100**	

Blown to Bits Chapter Three Issues and Questions

What You See is Not What the Computer Knows

WYSIWYG or "What you see is what you get" can lead to some unexpected issues and problems. The WYSIWYG interface has been a godsend to office workers. When a person uses the Print Layout view in ***Microsoft Word***, for example, what is shown on the screen is what is printed when the document is sent to the printer. This feature helps a lot in saving paper because changes would have to be made to make it look better when printed. WYSIWYG applications also work well for web pages. In the past, office workers needed to know HTML in order to produce interesting web pages. Now, many applications build the HTML code behind the scenes as the operator uses the application software to place images, format text, and create forms to be filled out on the web. ***Word*** can also be used in the Web Layout View as long as one picks the right option in saving the files.

Some authors have been deeply embarrassed because they have posted information that was supposed to be secret only to have it exposed. Below is an example of the sort of thing that has been exposed. These authors were fooled by the appearance (the WYSIWYG) because it appeared that the name and account information had been totally eradicated.

Here are some Names: John Doe, Jane Doe
Account Information: jdoe@fhsu.edu, jdoe#45*23
Suppose the information was blacked out and posted on the web like this:
Names: [redacted], Jane Doe
Account Information: jdoe@fhsu.edu, [redacted]
Can you guess how to view the real information?

The WYSIWYG metaphor only goes so far, however, as we have seen above. The computer application program that displays images on the screen converts data from the computer and builds the image on the screen according to the computer instructions built into the particular computer application. How the image is displayed depends on the programming embedded in the application. When the WYSIWYG metaphor is taken too literally, then some serious issues can arise. One incident occurred related to a case when an Italian journalist was wounded and an Italian intelligence agent was killed by American military fire in Baghdad on March 4, 2005. Instead of being given safe passage after being released the Italian journalist was wounded (and others in the car were also harmed) by American soldiers. The Italians investigated the incident and wrote their report. The Americans did the same. The American report exonerated the Americans involved, but this report was highly controversial. The report was posted on the web with sensitive information blacked out. An Italian blogger looked at the report and guessed how the information was blacked out. He surmised that the writer of the document had used the ***Adobe*** highlighter tool to hide the text. Instead of the usual light yellow color, the author of the document had changed the highlighter color to black and then published the document. Downloading the document and then removing the highlighting brought all of the sensitive information to light, and the blogger published the document (***Blown to Bits***, p. 74).

Here is an example done in Word. Go to the Home tab, Font group, Text Highlight Color. Here the highlighter was changed from the usual yellow to [redacted]. The words are blacked out but still available to those who know to remove the highlight color.

The ***New York Times*** did the same thing several years before. The ***New York Times*** ran a story about CIA attempts to overthrow the Iranian government. They obscured the names of the agents with similar black marks using the same highlighting technique. John Young removed the marks and published the document on the web (***Blown to Bits***, p. 75).

This could have been avoided by using encryption which would have not allowed these unauthorized changes. Alternatively, the document could have been printed out with the black bars covering the text, scanned, and then posted to the web. The office workers who posted these documents on the web were reluctant to do that because pdfs can be searched by a computer. The computer recognizes the symbols as text, and it can perform word searches. The scanned image cannot be searched so easily. Also, the scanned images are not easily used by the visually impaired.

Metadata

It is easy to forget the fact that when documents are created, metadata is often associated with those documents. Metadata is information about the particular file. Different computer applications have different types of metadata. Some programs have rather extensive metadata, others have minimal metadata. Information about files can sometimes be very revealing. Although much of the information is innocuous, some of it can reveal more than we expect. We usually have no problem with the fact that a person sees the filename, because we assume that the person will see it so we are careful to name in appropriately. However, we may be embarrassed if we say one thing and the metadata reveals something else. The metadata usually has the name of the owner of the computer, the date that a file was created, the date the file was last modified, file size, number of pages, who modified the file, and other information. Knowing when the file was last modified can be useful information if there are several versions of a file. If we know that time is important, and we know that several people are working on the file, then it becomes important to track the various times. Because many of us rarely look at this information we tend to forget that it is available. So, if we tell our boss that we were working hard on a document over the weekend and the date it was last modified was clearly different, the boss might not be very sympathetic.

Tony Blair found out that metadata had real consequences for his government. His government released documents supporting the U. S. war effort in Iraq. The work had supposedly been done by his Foreign Office, the equivalent of our State Department. Metadata revealed that it had been created by his communications office, an office designed to put the best spin on things (unlike the more impartial Foreign Office). The metadata revealed the real authors in the “created by” portion of the metadata. This did not go down well with Parliament (***Blown to Bits***, p. 79).

A UN prosecutor named Detlev Mehlis released a report on the assassination of former Lebanese Prime Minister Rafik Hariri. Syrian President Bashar al-Assad denied any involvement in this killing in spite of indications to the contrary. A comment was been deleted from the document but later discovered by reporters. The deleted comment accused Assad’s brother Maher of being personally involved in the assassination (***Blown to Bits***, p. 77). The reporters were able to retrieve this information because ***Microsoft Word*** has a “track changes” option. When this is enabled the full history of the document is available. In addition, editors can leave comments for other editors to see. The problem was that this information was not stripped from the document before it was released. Someone forgot to remove all of these notes before the document was shared with the media. In ***Word*** the reviewing pane has to be on before the reader sees the changes. Comments can be viewed to the right, but sometimes they are hidden. So, it is relatively easy to forget to remove all of these elements. In ***Word*** go to Review tab, comments (Show comments), tracking option, show Reviewing Pane in order to see any commentary left by others or revisions made by yourself.

Representation, Reality and Illusion

The authors of ***Blown to Bits*** talk about the treachery of images. They introduce the topic by showing an image of a pipe that is a painting by René Magritte. In the image itself it has the words “This is not a pipe” (in French). Computer images are good examples of things that “at bottom are not what they appear to be.” At bottom computer images are created out of something very different, zeros and ones.

First, let’s consider a different way of representing things, the non-digital way, the analog way. In analog representations the representation resembles in some sense the object it represents. Vinyl records are making something of a comeback. Vinyl records have tracks and a needle oscillates in the track as the record spins. The faster the oscillation the higher the note. Slow oscillations create low notes; fast oscillations create high notes. The greater the oscillation the louder the note. So, in these cases, there is a direct correlation between the oscillations (and the type of oscillation) and the notes (or loudness of the notes) that are produced. This makes it an analog representation because there is a resemblance, an analog, to the thing represented.

In television the colors depend on the wavelengths of light. Some colors have longer wavelengths than others. The electrical signals that transmit the television signal have wavelengths that correlate with the wavelengths of colors. There is a kind of direct representation, a change in one represents a change in the other.

The digital world is very different. Computer chips are based on switches that are on or off. The on or off switches represent bits that represent ones or zeros. Pixels are all created from ones and zeros. In digital photography there is some representation of an image. If you were to be able to look it, it would not appear to be anything but ones and zeros. However, there is an arbitrary way that the representations have been standardized. The photograph is represented by bits, and this is called a model. The representation has bits arbitrarily assigned to be certain colors. If there are enough bits with enough colors then the model has enough complexity to create an image of the thing that has been photographed. The more bits that are used to create the pixels and the better the lens used to create the model, the more realistic the image. If there are few bits, the image is grainy. If millions of pixels are created with a good lens, the image is remarkably good.

Digital music has evolved as the digital world has evolved. Computing chips continue to get faster, smaller, and cheaper. In a similar way (digital) memory has gotten faster, smaller, and cheaper. As computing power has increased, the ability to reproduce music in an accurate way has dramatically increased too. Computing power is important for compressing data and then decompressing it. The more computing power there is, the better the reproduction will be. When computers compress (code) and then decompress (decode) they are said to be using a codec (short for coder/decoder). The better the codec the better the audio and video.

- MP3 – is an early audio coding format that was used to create small file sizes (because memory was expensive and computing processing power was also expensive). It typically would create files 1/10th to 1/12th the original size. It did this by discarding some data and making some inexact approximations. It eliminated some of the highest and lowest frequencies that were thought to be inaudible to humans, and it approximated some of the other data. Also humans don't hear low frequencies in stereo, so they were not reproduced in stereo. This sound was thought to be fairly good at the time.
- CD – an optical disc storage format co-developed by Philips and Sony. This was originally developed to store music, but it was later adapted to store data. When CDs were popular, they stored more data than the typical hard disk drives of computers. The standard CDs can hold roughly 80 minutes of raw, uncompressed audio. Because the audio is uncompressed, it is higher quality than the mp3 files. At least those audiophiles can hear the difference when compared with the MP3s. However, now CDs are losing popularity because compared to other media, they do not have enough storage capacity.
- DVD – these disks were developed to store digital video. They stored much more digital content then the CDs. DVDs use lossy MPEG-2 video coding formats for video compression. Lossy means that shortcuts are taken in reproducing video. Not every detail is retained. If this were not done, the video storage demands would be very large, and for many uses we do not notice the difference.
- Flash drives – as the speed of memory chips increased, the size decreased, and the cost decreased, they too are widely used to store data and music. Music is stored in compressed form because now the huge increase in computing power can be used to process it. The Apple iPod (now SmartPhone) has significant computing power in its small form factor, and it can store vast amounts of music because of the techniques of compression.
- JPEG – an image format that is lossy. As noted above, it does not reproduce all of the detail of an image, but it is very "lean and mean" and it does a very good job at creating accurate images. For example, researchers have found that human eyes are more sensitive to degrees of luminance than they are to degrees of color. So, JPEG images reproduce degrees of luminance more accurately than they do color, and the results are still quite acceptable for most uses. Note that printers too have to be capable of decompressing the various algorithms used to represent images. Printers too need a lot of processing power to handle the various file formats correctly (Adobe).
- Lossless data compression. Researchers have found clever ways to provide lossless data compression, that is, data compression that loses none of the detail of the original. In an image,

for example, there may be a large section of the image that has exactly the same color of red. Instead of reproducing every pixel with the detail color description, a sophisticated program can just encode 330 red pixels for a certain area saving a lot of storage space. In decompressing the video image no detail is lost.

- Streaming video. When streaming high definition video from a satellite transmitter or from a video source like Netflix, there are lossy techniques that work well. When 30 images per second are being streamed, there is a lot of repetition between frames of video. The background often remains the same while there is some movement in the foreground. The sofa and chairs in a room remain the same while a person is walking from one place to the next. In this case, only the changes need to be transmitted if the codec is sophisticated enough. Furthermore, if there is some loss in an image that lasts only 1/30th of a second, that is probably acceptable. Because of the high definition video, that could only occur if the processing power in the satellite code box (or cable codec box) in the living room has enough power to compare two images in real time and reproduce the image on the TV screen. For all of this to happen the algorithms have to be very refined, the computing chips very fast, and the transmissions uninterrupted. As is mentioned in the Blown to Bits book, "decompression algorithms are built into … cable TV boxes, cast in silicon in chips more powerful than the fastest computers of only a few years ago." (***Blown to Bits***, p. 91)

This digital revolution has many ramifications:

- As with all technology, the processing power can be used for good or bad purposes. The digital power to represent reality can be changed by the power of ***Photoshop*** (or digital video editing) to change what is represented. We have seen negative effects of live ***Facebook*** video streams when some killings have been shown live as well as other events.
- Because there is no longer a one-to-one change in the thing being represented as there was when there was the analog form of representation, it can become harder to distinguish reality from what has been artificially created. When it all comes down to algorithms, subtle changes can sometimes make a big difference.
- The digital technologies have created new industries, but they have also destroyed others. Still cameras that used film and motion picture cameras that used film are now obsolete, and the companies that produced them have undergone a lot of restructuring with many people losing their jobs.
- Battles are now fought over file formats, algorithms, and standards. There was a battle among big companies over the format for DVDs, for example. In the Eastern US there was also a battle over the .doc/docx format used by ***Word*** because there were some who advocated ***Open Office*** with an Open Document format over ***Microsoft Office*** with the .doc format.

There are issues with deleting data.

- Data is referenced on hard drives by an index. The index tells the read/write arm of the hard drive which block of data to access. When the delete command is given to delete a file, the file is not really deleted. Rather the index reference is deleted. The data is still there intact in the hard drive. So, social security numbers, bank account numbers, and other sensitive data can still be retrieved unless other measures are taken. If the hard drives are disposed of but not fully erased, others can retrieve the data. Even the format command leaves much of the data unaltered because the format command looks for bad sectors in the disk and removes them from the sectors available for writing.

- Cell phone data has the same problem. The call logs and email messages remain on the phone unless measures are taken.

There are other issues with archiving data.

- When data is saved on a medium there is always a danger that the industry will move to a different medium for saving data, and the techniques for retrieving data from the original medium will be lost.
- With changes in technology the old ways soon become the obsolete ways. Also, there is a danger that the medium will degrade so that the data will become unusable.

Assignment

Part One. Create a document in Word that you will use for collaborating with at least one partner. Find a partner who will work with you online. Email your partner a link to the document you have created so that you can edit it together. Before doing that go to the **Review tab** and **turn Track Changes on**. Also in the Comments section click on **Show Comments**. Use the Comments tab and find a place in the document and add a comment (or two). Save the document on OneDrive. Then share the document with your partner by sending an invitation using email. He or she will receive an invitation to edit the document on OneDrive – and then will be prompted to log in. Then there will be the option to edit it using Word Online or to use the full version of Word. If your partner has the full version of Word, encourage your partner to use that version. Include a request to add comments and to make some changes to the document. Clicking on the Review Tab allows your partner to Show Comments and add comments. There is also the option to Show Edit Activity – that should be clicked as well. When your partner has completed their commentary and changes, then show this work to your instructor by downloading it to your local computer and then uploading it to the learning management system or emailing it to the instructor.

Part Two. Clean up the document so that it will not have the commentary. Accept or reject the changes made by your partner. When you have accepted or rejected the changes, go to the File tab and click on **Info** and then **Inspect Document**. After Word has inspected the document, then you will be given the option to remove all comments. Then submit this cleaned up version of the document to your instructor by the method provided by your instructor.

Rubric Collaboration and Document Cleanup

Performance Element	**Exemplary**	**Proficient**	**Developing**	**Points Possible**	**Points Earned**
A document is created and shared with a colleague.	**20 points** (The document is created and shared.)	**5 - 15 points** (The document is created but not shared properly.)	**0 points** (Task not completed)	**20**	
The document has comments from the author and changes from the colleague.	**40 points** (All items nicely done.)	**5 - 30 points** (Points depend on the quality of the reasons.)	**0 points** (Task not completed)	**40**	

The document is cleaned up so there is no extraneous information in the document.	**40 points**	**5 – 30 Points**	**0 points** (Task not completed)	**40**	
Total Points				**100**	

Chapter 5: Secret Bits
How Codes Became Unbreakable, The Deep Net and the Dark Net

After 9/11 there was a big outcry in congress about the use of secret codes (encryption) that allowed terrorists to communicate with each other in private. Senator Judd Greg wanted to make sure that government had a backdoor to view all encrypted messages. However, after a few weeks he dropped efforts to promote such a bill. Even the USA PATRIOT Act does not address encryption.
What happened? Why was the issue dropped?

The reason is that encryption had become widespread; commerce routinely relies on it. People need to be assured that their transactions over the web are secure. If there were backdoors put in place to allow the government (or anyone else) to decrypt the transactions, then people would quickly move away from electronic commerce. So, Senator Judd Greg not to push the issue.

What is encryption?

"Encryption is the art of encoding messages so they can't be understood by eavesdroppers or adversaries into whose hands the messages might fall. De-scrambling an encrypted message requires knowing the sequence of symbols – the "key"—that was used to encrypt it." (***Blown to Bits***, p. 161) Some of us as children would create "secret codes." We might reverse all of the letters in the words or we might devise simple ways of substituting letters. Then we would share those methods with our friends and send them secret messages. Generals and diplomats do the same sort of thing when sending messages across enemy lines.

Julius Caesar used a cipher (a method of transforming a message into an obscure form) when he communicated with Cicero (among others). His method was simple, he replaced the original letters with a letter four letters over in the alphabet. This is a substitution cipher. In this case, he just shifted the letters to encrypt the message. To decrypt the message, Cicero just reversed the shift. This is known as a substitution cipher because one just substitutes one letter for another. A more sophisticated variation of the substitution cipher randomizes the alphabet and then matches the letters to the randomized alphabet (***Blown to Bits***, p. 166). The key in this case is knowing the form the randomized alphabet takes. If you have been given the randomized key, it is easy to match up the letters.

Why is it important to encrypt text sent over the Internet?

Packets of information are sent over the Internet, with the to and the from address visible to those who would wish to view the packets. The packets usually arrive in the proper sequence, but if those packets are interrupted in transit and arrive scrambled they are reassembled in the proper order at the other end. The TCP portion of TCPIP is the protocol that makes sure the packets are reassembled in the correct way this protocol also regulates the flow of bits across the Internet so that the computers at the receiving end can process them properly. It adjusts streaming to be faster or slower depending on the computing power of the computer receiving the messages.

In addition to the addresses being visible, other messages (such as email and chat messages) are sent in plain text. Encryption is important because the unencrypted messages are sent in plain text. Because the messages are sent in plain text, they can be viewed by anyone intercepting them. The packets of plain text are sent through a variety of routers across the Internet, so anyone with access to those routers could view that plain text.

How does public-key cryptography work?

One form of encryption has become **the** means of encryption in this digital age. It is used in the commercial transactions and it is used by many to share information privately. To become this widespread the creators of this type of encryption had to make it easy to use and very secure. The creators wanted to find a way to meet the following challenge.

Here is the challenge. Two people need to have a way to agree on a secret key without any prior arrangement, "a key known only to the two of them, by using messages between them that are not secret at all." (***Blown to Bits***, p. 179)

"The crucial invention was the concept of a one-way computation—a computation with two important properties: It can be done quickly, but it can't be undone quickly." (***Blown to Bits***, p. 181) Two numbers are used to produce a third number. The algorithm works such that it is easy for the first two numbers to produce the third, but knowing the first and the third, it is very, very difficult to calculate the second. Or if you know the second and the third, it is extremely difficult to calculate (discover) the first. In addition there is a critical property that makes this all work: (x * y) * z always produces the same result as (x * z) * y.

Here is how the scheme works:

1. Alice and Bob each choose a random number. This typically is a rather large number. We'll call Alice's number a and Bob's number b. We'll refer to **a and b** as Alice and Bob's secret keys or **private keys**. Alice and Bob keep their secret keys secret. No one except Alice knows the value of a, and no one except Bob knows the value of b.
2. There is a third value, g, that is public knowledge. Alice calculates g * a and Bob calculates g * b. (Not hard to do.) The results are called their **public keys A and B**, respectively.
3. Alice sends Bob the value of A and Bob sends Alice the value of B. Essentially, they **share their public keys**. It doesn't matter if Eve overhears these communications: A and B are not secret numbers.
4. When she has received Bob's public key B, Alice computes B * a, using her secret key a as well as Bob's public key B. Likewise, when B receives A from Alice, he computes A * b.

It turns out they both compute the same number because Bob computes A * b, that is, (g * a) * b (see Step 2 – A is g * a). Alice computes B * a, that is (g * b) * a. Because of the critically important property of the one-way computation, that number is (g * a) * b once again – the same value, arrived at in a different way! (***Blown to Bits***, pp 181-182)

This results in a shared value (K) that is used for encrypting and decrypting the messages they send and receive. They have a unique value, a shared unique value, that allows them to communicate privately and securely.

What is interesting is that a third party can know A and B because they are public keys. They can even know the value of g. In fact, they can also know the algorithms used to produce the numbers. However, if they don't know a or b they cannot know the value of K – the value used to encrypt the messages. The commercial transactions all use these public keys behind the scenes to create the unique value (K) that is used in encrypting the communications used in the transactions.

Public Keys for Private Messages

The same type of computation can be used to allow others to send a person messages that only that person can decrypt. As before Alice picks a **secret key a** to use for creating a public key A by computing a * g. She publishes this key A in a directory for anyone to use. A person wanting to send a private message to Alice share his or her public key with Alice too (the public key is b * g). This person then uses Alice's public key A from the directory to compute an encryption key K just as with the key-agreement protocol: K = A * b. The person uses K as a key to encrypt a message to Alice, and he sends Alice the ciphertext, along with B.

When Alice receives Bob's encrypted message, she takes the B that came with the message, together with her secret key a, and computes the same value K by taking B * a. Alice now uses K as the key for decrypting the message. Others can't decrypt it because they don't know the linked secret keys. (***Blown to Bits***, p. 183)

The result is that anyone can send encrypted messages in the open, public Internet.

Why would one need Certificates and Certification Authorities?

So far, we are able to be sure that the message we are receiving is private and not able to be read by anyone else besides the sender. However, how can we be sure the sender is who she or he says she or he is? One way is to use a trusted authority to vouch for the other individual. Alice could go to a trusted authority and present her public key and a proof of her identity. Then the trusted authority can digitally sign her key. This then is a certificate. To communicate with another she produces her certificate. If we want to be certain it is Alice we then check on the authenticity of the certificate. If the certificate comes from an authority that we trust, then we can be certain that it is Alice. That is, we can be as certain as we are certain of the certification authority.

Cryptography for Everyone

When we pay for something using PayPal, do a banking transaction, or buy from Amazon, we are using public key cryptography. The sign that we are using encryption is the "s" in **https**. The "s" stands for the word "secure" in hypertext transfer protocol secure. What is little known is that public key cryptography is being used in the transaction. When our computer contacts Amazon, for example, the Amazon site presents a certificate signed by a Certification authority. The operating system in our computer has been configured to recognize that certificate. New keys are generated and shared with each transaction. So, now we individuals have powerful encryption at our fingertips, encryption that the NSA cannot break.

Phil Zimmerman worked on producing encryption software for the people. He did it to counter the ability of government to conduct widespread surveillance over computer communications by the public. He believed that it was just too easy for the government to scan plain text emails for a variety of keywords in a wholesale way without having to make much effort to go to the court to get permission to do surveillance on specific persons. So, he set out to create software to allow individuals to keep their privacy. Zimmerman named his software “Pretty Good Privacy” taking a cue from Garrison Keillor’s Pretty Good Groceries.

The State of Cryptography Today

All banking transactions are encrypted. There are also free email programs that use PGP.
However very little email is actually encrypted today. Gmail messages are scanned by Google so that Google can send relevant advertisements our way. Court orders may require Google to turn over emails to the government which further undermines privacy. Passwords provide some protection so that others cannot get to our email on the email server. But the emails pass through many routers, wires, fiberoptic cables, and satellite transfers. They can easily be monitored. Satellite traffic is monitored for key words by the international ECHELON system.

To use encrypted email, you need to use nonstandard software. This can be a problem because the people you communicate with need software that can decrypt the messages, and this may not often be the case. Corporations and companies typically do not want your email to be private because they may be required to monitor it in various ways.

Skype communications are encrypted, but much chat software is plain text. A company named Signal has come out with a product that is encrypted.

The Dark Net and the Deep Net

There is an important distinction between the Deep Net and the Dark Net. We use the Deep Net everyday because we login to various services as well as using the secure services mentioned above. The Deep Net is not searchable by Google or Bing because most of the information is not public because it is protected by logins that authenticate users. There are also unpublished blogs and some content on Web pages that are not linked to other public pages. Web pages that are generated on the fly such as Amazon pages that are created when you search for various items are not available for Google’s indexing techniques. Photos on Facebook that you mark as private are not indexed. Google’s spiders follow links to go from site to site when indexing that data. Some subscription websites (magazines, newspapers) are not fully indexed. Also, if there are public webpages that require the user to use a search field to find information, that is not indexed by Google. If there is a “pay wall” then Google will not index the information behind the pay wall. There is a lot of raw science data that is not searched by Google either.

So, perhaps it is not as surprising to find that some estimate that only 4% of the content on the web is indexed by (searchable by) Google.

What is the difference between the Deep Net and the Dark Net? What was the Silk Road?

Some sites require special browsers in order to view the site. Google does not index those sites. The most famous special browser is called the Tor browser. The word Tor stands for the onion browser. The dark web is hosted by anonymous sites so you do not know who you are dealing with when you access those sites.

The Tor browser is a specially configured kind of browser. It is an altered version of the Firefox browser that can navigate the Dark Net without leaving a trail of where it has been. The Tor browser and the Tor system was created by the U. S. Navy in order to allow people in non-democratic nations to communicate without being watched by their governments.

The ordinary browsers use TCPIP which means that the address being sought and the address of the seeker is open to the routers to see. The Tor browser is like using a proxy server to access a variety of sites. At FHSU we use proxy servers in a number of ways. To access certain library sites, student and faculty browsers contact a proxy server and the proxy server then accesses the library site. So, from the point of view of the site contacted, it is the proxy server that is seeking the service. This is done because some of the library sites need special licenses. Since FHSU students and faculty have paid to access some of these services, they access the proxy after logging in to the FHSU website. In that way access to certain paid databases is controlled. The difference between proxy servers and Tor relays is that proxy servers are not truly anonymous. Logs are kept of who is accessing the library services, and those logs could be turned over to authorities if there were subpoenas.

The Tor browsers is configured to access a variety of relays (computers) that are randomly selected. People may volunteer to use their computers as relays to help increase the scope of the Tor network. Then the content of the message is encrypted and a "first layer of the onion" is decrypted so that the Tor browser knows which randomly selected relay (suppose it is G) to access. Then after arriving at G, a second layer of the onion is decrypted and the Tor browser moves on to the next relay (suppose it is F). After arriving at F then the process continues until the final relay is reached. It is called the exit node. Then everything is decrypted and access to the web service occurs. The web service only sees the exit node, so it thinks that the exit node is the node requesting the service. Then the message travels in reverse back to the originating site. What makes this network different is that the origin of the message is untraceable. Also, the path to the destination site is untraceable. Both the sender of the information and the receiving website are anonymous. Neither knows who the other is. Encryption keeps everything secret. The following website explains onion routing, http://www.makeuseof.com/tag/what-is-onion-routing-exactly-makeuseof-explains/.

Server administrators can choose to add their server to the Tor network by configuring it in a certain way to keep it anonymous too. In this way the server is kept away from prying eyes.
One more element is necessary to add secrecy, the ability to do financial transactions without the money being tracked to an individual's bank account. This was solved by the use of bitcoins.

What Are Bitcoins?

> Bitcoins are electronic currency, otherwise known as 'cryptocurrency'. Bitcoins are a form of digital public money that is created by painstaking mathematical computations and policed by millions of computer users called 'miners'.
>
> Bitcoins are, in essence, electricity converted into long strings of code that have money value…

> How Bitcoins Work
>
> Bitcoins are completely virtual coins designed to be 'self-contained' for their value, with no need for banks to move and store the money.
>
> Once you own bitcoins, they behave like physical gold coins: they possess value and trade just as if they were nuggets of gold in your pocket. You can use your bitcoins to purchase goods and services online, or you can tuck them away and hope that their value increases over the years.
>
> Bitcoins are traded from one personal 'wallet' to another.
>
> A wallet is a small personal database that you store on your computer drive, on your smartphone, on your tablet, or somewhere in the cloud.
>
> For all intents, bitcoins are forgery-resistant. It is so computationally-intensive to create a bitcoin, it isn't financially worth it for counterfeiters to manipulate the system. ("What are Bitcoins? How do Bitcoins work?," https://www.lifewire.com/what-are-bitcoins-2483146, Paul Gil, May 26, 2017)

Bitcoins can be purchased at various bitcoin exchanges. They then reside in personal "wallets." As noted above this means that they are stored on one's hard drive or in the cloud. In fact one hard drive with bitcoins worth $9,000,000 was thrown in the trash in England. Even though bitcoins are traded from one personal wallet to another and even though there is a public record of the bitcoins, there are no personal identifiers on the wallets or on the transactions. There is no central bank or government guaranteeing the transactions. Transactions are not reversible. The value of a bitcoin is market-driven.

The Silk Road

Since the Tor network is completely anonymous and Bitcoins can also be used anonymously, the stage was set for someone to take full advantage of this. For the full story go to https://www.wired.com/2015/04/silk-road-1/.

The architect of what became the Silk Road was a young person named Ross Ulbricht. He grew up in Austin, Texas, attending the University of Texas at Dallas and then went on to Penn State in Physics. He got bored with the lab work there and worked at managing the inventory of a book selling web site. This inventory management gave him the skills to handle what became a huge inventory of drugs. While at Penn State he started reading works from the Libertarian economist Ludwig von Mises. He graduated and moved back to Austin. He tried day trading stocks, but that was not successful. However, he learned about bitcoin while doing these trades. As a libertarian he believed that individuals had the right to use drugs of their choice.

According to an account in Wired he dreamed of a website where people could buy whatever they wanted anonymously with no trail leading back to them. (Wired, The Untold Story of Silk Road, https://www.wired.com/2015/04/silk-road-1/, Joshua Bearman & Tomer Hanuka, May, 2015) He programmed the site and created a business model to make it work financially. Using the Tor network he created instructions giving advice to sellers on how to ship the products, usually through the US Postal Service, how to get paid, how to get onto the system, etc. He became a very vocal mouthpiece of the service and of various libertarian views and used the persona of Dread Pirate Roberts. He talked about the new digital economy that no longer needed the state with its rules. Freedom would be maximized.

> The site was modeled, sensibly, on Amazon and eBay. And that's what it looked like: a well-organized community marketplace, complete with profiles, listings, and transaction reviews. Everything was anonymous, and shipments often went through the regular old postal service. No need for fake names—you put your real address, and if anyone asks, you just say you didn't order all that heroin! (Wired, The Untold Story of Silk Road, https://www.wired.com/2015/04/silk-road-1/, Joshua Bearman & Tomer Hanuka, May, 2015)

He broke up with his girlfriend and moved to Australia. At that time he was making about $25,000 a month and had programmed and managed the site himself. To prevent people from scamming others with fake goods, he created an escrow account (a center of trust) where money would be held until the transaction went through and the goods were delivered. This allowed the Silk Road to flourish as a business. At its height the Silk Road was very big business. Once he had an offer to buy the business and he countered with a demand for one billion dollars. However as the Wired authors state that "number might have been low; the scale of Silk Road commissions over the next year would in fact qualify DPR as one of the biggest entrepreneurs of the second Internet boom." (Wired, May, 2015) He moved to San Francisco and led a double life. He appeared to be just a regular guy, and his friends and acquaintances had no idea that he was Dread Pirate Roberts.

To manage the project he eventually had to hire an associate and other workers. After some time a variety of federal authorities learned about Silk Road and Homeland Security, the FBI, and others attempted to learn the identity of Dread Pirate Roberts. By appearing to be people wanting to help Dread Pirate Roberts with his business, one of them gained his trust. To make a long story short, Ross panicked at one point and talked about using force to control one of his employees. The infiltrator pretended to kill one of the employees at the request of Ross and sent fake videos to him. The FBI spent a lot of resources trying to track down the server used by Ross. They caught a break when they saw a message stating the Ross's address was vulnerable. Ross had been warned to increase security precautions, but he was under too much stress from running the operation and he was not a trained computer professional so he ignored the warnings. Eventually the FBI tracked down the server address and they broke in and made a duplicate of the information on the server (which happened to be in Iceland) which then allowed them to understand the layout of the whole Silk Road network.

Finally, they found a log with a non-Tor IP address. The fact that it was a non-Tor IP address was significant because that meant it could be traced. It led to a location in San Francisco, to the apartment he rented there. After watching him, the FBI eventually found a way to physically remove his laptop while he was logged in and to detain him. Because the FBI had such overwhelming evidence based on the duplicated server data, and because of other forensic computer information Ross was convicted.

Other Uses of the Tor Network

The story of Silk Road is certainly a cautionary tale, but there are other quite legitimate uses of the Tor Network. The Navy created it for oppressed peoples, and those who need to communicate in oppressive countries certainly use it to avoid surveillance. There is a Torchat service where one can communicate secretly, for example. Many whistle blowers who fear retribution use it to communicate with news sources, government officials, attorneys, or others. There is also a Library Freedom Project that has now aligned itself with Tor to create Tor exit relays in libraries (https://libraryfreedomproject.org/torexitpilotphase1/). The rationale for the project is to avoid government surveillance and corporate access to one's private information. The Library Freedom Project allows people access to many services anonymously. Major newspapers and news organizations encourage people to use encrypted means, including the Tor browser, to share information (leak information) to them. Without such means many people who would be willing to share information are very reluctant to send normal emails or use common chat services, because those emails and chats can be traced back to them. People who are strongly opposed to government surveillance and the constant data mining of companies like Google, Microsoft, Insurance Companies, and others appreciate the ability to hide their searches and other transactions by using the Tor Network.

Assignment

Try to provide a convincing case FOR using the Tor Network and a convincing case AGAINST using the Tor Network. The quality of reasons giving for and against are more important than the quantity of reasons for and against. In doing this assignment you might do more research about the Library Freedom Project or do more reading about the Silk Road.

Rubric Privacy Case Study

Performance Element	Exemplary	Proficient	Developing	Points Possible	Points Earned
A convincing case is made for using the Tor Network.	**40 points** The reasons given and the examples given are well-selected.	**10 - 30 points** The points given depend on the quality of the reasons and examples.	**0 points** (Task not completed)	**40**	
A convincing case is made for not using the Tor Network.	**40 points** The reasons given and the examples given are well-selected.	**5 - 30 points** The points given depend on the quality of the reasons and examples.	**0 points** (Task not completed)	**40**	
The document is well-formatted and professionally done.	**20 points** The document has good grammar, good spelling, and nice formatting.	**5 – 15 Points** Points are subtracted for bad grammar, spelling, and formatting.	**0 points** (Task not completed)	**20**	
Total Points				**100**	

Legal Minefields on the Web

Chapter 7: You Can't Say That on the Internet

Controlling Predators on the Internet

Representative Judy Biggert of Illinois co-sponsored the Deleting online Predators Act (DOPA), 2006. Basically, the idea was to cut funding/regulate agencies getting federal funds – Libraries – etc. if they allowed underage kids to see the wrong things on the Internet.
This happened after Katherine Lester, a 16 year old honors student from Fairgrove, Michigan, went missing in June, 2006.

- The parents called the police.
- Federal authorities then got involved.
- She was found, safe, in Amman, Jordan.

She met a guy online, a Jordanian named Jimzawi who got plane tickets for her. She tricked her parents into getting her a passport.U. S. authorities met her plane in Amman, and she returned home.
But – Katherine still insisted she wanted to marry Jimzawi. Jimzawi said he was in love with her, and he wanted her to tell her parents before she took off, but she refused.

Later when she turned 18 she took off to Jordan to meet Jimzawi.

- All of this was televised on Dr. Phil.
- But shortly later they broke up.

How should laws be shaped? What are the right metaphors, the right comparisons?
In the pre-web world there are different laws regulating telephone service (common carrier), book publishing (defamation could affect the publisher as well as the author), radio broadcasts (stricter standards of what could be said), TV broadcasts (again fairly strict standards on what could be said), transporting goods across state lines, etc.

Web 1.0 featured basically static websites. One can ask is this like publishing a book?
Web 2.0 features sites that get input from viewers – social media sites – crowd-sourced sites like Wikipedia and other sites that are more participatory. One can ask of these sites is this like placing a conference call?

When a person publishes a book, an intermediary between the author and the reader is the publisher. In some cases, publishers can be held liable for what is published. So, perhaps the **social media companies** (*MySpace, Facebook, Twitter*, etc.) should have some liability. There was a case of predatory behavior, and the parents **sued MySpace** for $30 million. A man named Pete Solis contacted and then assaulted a 14-year-old girl. The parents held that MySpace helped enable the assault. (Blown to Bits, p. 232). Another type of entity that could be sued is the **ISP (Internet Service Provider)** that carried the bits across the Internet. The ISPs are companies like Verizon, Nex-Tech, AT&T, Cox, etc.
As noted between the authors and readers are the publishers. They are intermediaries. Even lecturers require the lecture halls, and whoever provide them is an intermediary.

What about the Internet? The source has an ISP (perhaps Cox, NexTech) and the destination has an ISP (perhaps Cox, Verizon, AT&T, Google Fiber). Then there are fiber optic cables, many routers, satellites, etc. There could be many owners of these. We can designate these connections as the cloud. (This is different than some uses of this word. In this case it stands for the many unknown intermediaries.)

Whom do you regulate?

The source – this could be the person speaking, writing, blogging, and creating the content.

- One could try to criminalize certain kinds of speech.
- However, this will not work if the speaker is not in the same country as the listener.
- Different countries have very different kinds of laws. Some protect free speech far more than others.

The ISPs – these are close to the source and destination.
The Cloud – holding these responsible seems almost impossible.
The Destination -- this is the recipient.

One could try to control the listener, by prohibiting possession of certain kinds of materials.

- In the US possession of copyrighted software w/o an appropriate license is illegal, and it is illegal to possess material with the intent to profit from it by redistributing it.
- The main problem from the point of view of enforcement is that citizens have reasonable privacy rights.
- So, it is hard for the government to know what its citizens possess.
- In the U. S. it would be difficult for the government to do one-at-a-time prosecutions.

The Intermediaries

The government can try to control the intermediaries.

Physical World

Intermediaries between the speaker and the listener sometimes share responsibility with the speaker – and sometimes not. If someone is defamed in a publication the author may be sued AND the publisher may be sued. The publisher may have known that what was said was false. However, truckers who transport the books probably will not be sued.

So, the question is -- are the electronic intermediaries more like truckers or like publishers?

Publisher or Distributor?

The first court ruling when CompuServe was sued for defamation for material posted by one of its subscribers was that CompuServe was just a distributor and not a publisher. The court considered CompuServe as “an electronic for-profit-library.” (Blown to Bits, p. 235) In this ruling CompuServe was considered to be like the truckers. It was not considered liable. The electronic intermediaries felt a great sense of relief because they feared being held liable for content.

The Prodigy Case

Prodigy was a company that decided to market itself as family-friendly. Worried about sexual content, bad language, and other offensive materials Prodigy said it would monitor content and remove the offensive content on its many bulletin boards.

One of the bulletin boards was called “Money Talk.” Someone anonymous posted criticism of an investment firm Stratton Oakmont. This person said the President of the company would soon to be proven a criminal. Stratton Oakmont sued Prodigy for libel claiming that Prodigy was the publisher. Prodigy claimed it had zero responsibility for what its clients said.

A New York court ruled that since it had exercised editorial control for its family-friendly image, it became a publisher (Blown to Bits, p. 136). The problem, however, was that it is relatively easy to monitor for sexual information and bad language. It is quite another thing to monitor for truthfulness.

So, the message from the courts to these kinds of services is do not monitor or modify any content unless you want to open yourself up to lawsuits. Rather, pass all the information through to the public -- publish it all.

Many felt this was a very bad ruling. Defamers and liars would continue to publish. The general public would tend to stay away from all bulletin boards.

The Nastiest Place on Earth

In the US, the First Amendment protects authors and speakers from **government** interference: Congress shall make no law … abridging the freedom of speech, or of the press. But First Amendment protections are not absolute. No one has the right to publish obscene materials.

The Supreme Court uses the Miller test. The average person applies contemporary community standards to determine what is obscene. This means there is no national standards. Community standards are the litmus test.

Cyberspace poses a problem for community standards. What is a “community” in cyberspace? What is OK in San Francisco is not OK in Tennessee typically. A bulletin board advertising itself as “the nastiest place on earth” was available on the web. A jury trial held in Memphis determined that content on a that bulletin board based in Milpitas, California, violated the standards of persons living in in Memphis, Tennessee (Blown to Bits, p. 238).

Mass Speech

Senator Exon, worried about porn on the web, sponsored a bill called the Communications Decency Act. It was signed into law by President Clinton. It prohibited making offensive images and indecent materials available to a person under 18.

This bill was challenged, and it was declared unconstitutional. The ruling stated that the government can only regulate free speech for a compelling reason and in the least restrictive manner. It would chill discourse unacceptably to demand age verification over the Internet.

TV and radio laws (FCC) are more restrictive than for print media (and these laws were the bases for the lawsuit), and so free speech is more limited in this arena. These kinds of rules should not apply to the Internet said the judge.

The judge apparently wanted to protect the Internet's promise as a lively marketplace of ideas. So, the burden of blocking unwanted communications moves from source ISPs to the destination. So that is why there is some pressure on libraries and schools to monitor content.

Protecting Good Samaritans – and a Few Bad Ones

In 1995 the Stratton Oakmont v. Prodigy decision discouraged ISPs from exercising any editorial judgment. This decision helped spur passage of the Communications Decency Act which was intended to protect children from Internet pornography. Because the lawmakers knew that ISPs and other service providers would not exercise any judgment and control, they added a "Good Samaritan" provision to the Communications Decency Act.

The "Good Samaritan" provision said there is no liability in the case of ISPs if they acted in good faith to filter out "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material. And it said ISPs should NOT be thought of as publishers or as sources. So no there were no more Stratton Oakmont v Prodigy provisions.

The U.S. Supreme Court struck down the CDA in 1996, but it allowed the Good Samaritan clause to stand. That remains the law today. ISPs can do as much as they want to filter or censor their content, without any risk that they will assume publishers' liabilities in the process.

The Good Samaritan clause makes it clear that ISPs are not publishers but they can filter content. Publishers are liable for the content that they publish. They can be held liable for slander or obscenity if that exists in their publications. After this decision ISPs are exempt from this liability in spite of the fact that they exercise control over content.

But things get muddy.

There was a service that was a roommate matching service. It was sued on the grounds of discrimination, women (or men) only roommates could be sought, for example. First it was considered not guilty because ISPs are not publishers. Later, that was reversed and they were considered guilty because this matching service could not filter everything as it wished. It could not filter for racial preference, for example. So, in this case they were found liable.

There is a problem with the Good Samaritan clause. It protects certain publishing-style activities when, arguably, they should not be protected. Illustrating the nature of the problem is a case involving an American On Line bulletin board. There was false information on AOL targeting an individual who supposedly was selling t-shirts making fun of the Oklahoma City bombing. AOL was informed it was false, and the person targeted got all kinds of harassing phone calls. When taken to court AOL was ruled to have no liability because the Good Samaritan clause said services like AOL should not be treated as a publisher. So, in this case someone harassing another person was protected by this clause. This is probably an unintended consequence of the law since the point of the law was to protect providers who tried to act in the best interests of their customers.

There was another case where some lewd pictures of a young man were spread on the Internet by an AOL chat room. Apparently the young man (age 11) had been lured into a setting where he was sexually abused. Then the abuser posted lewd pictures online. AOL was told about this. AOL reserved the right to terminate service, and yet they did not terminate this service. AOL was sued by the young man's mother, but she lost due to the Good Samaritan clause. One dissenting opinion argued that it is not enough to say that AOL is not a publisher. They are more like distributors. And **distributors do have some responsibility.** If a trucker knows he is hauling child pornography and if he is getting some of the profits, he has **some** complicity. So, the argument goes, this service too should have some liability.

There is an anti-cyber stalking law in California which served as a model for a national law. One conviction occurred when a 28-year old woman entered a chat room geared to sexual fantasies. She said she longed to be assaulted, and invited men reading this email to come make the fantasy a reality. She said she wanted men to "break down my door and rape me." She then gave an address and instructions on how to get bypass the security system. Nine men came. She sent each one away. Then she would post an email appeared stating that rejecting them was part of her fantasy.

The reality of this was that Gary Dellapenta, a 50 year old security guard, was posing as this woman. He was rebuffed by this woman. He took revenge by pretending to be her and posting these messages to the chat room. The lady did not even own a computer. This resulted in a conviction which was very unusual, but the conviction was made possible because of the cyberstalking law.

There is another kind of case that resulted in a conviction. Anti-abortion groups suggested stalking doctors who performed abortions. They listed names, addresses, and license plate numbers of those doctors. The web site grayed out names of those who had been wounded and crossed off those who had been murdered. A civil suit found the group liable because "**true threats of violence were made with the intent to intimidate**." (p. 151) Based on this decision, there are some legitimate limits to free speech on the web.

Now consider the general question, what about the right to free speech?

Many scholars emphasize that free speech is the cornerstone of democracy. In the long run free speech protects everyone. This right does sometimes interfere with someone's safety – as seen above. Still, many consider it the right that makes all of the other rights possible.

Yet there are issues. *Barron's* (a New York based company) published an article suggesting that Australian businessman Joseph Gutnick was involved in money-laundering and tax evasion. Gutnick sued in an Australian court arguing that *Barron's* was available in Australia for a fee, so it was published there. He sued in Australia because laws protecting free speech are much weaker there than in America. *Barron's* argued the place of publication was New Jersey. *Barron's* lost.

The implications of this are staggering. Americans on American soil expect to speak out freely. However, now the community standards make Australian law applicable to American web publications. So, it could happen that the freedom of the Internet press is largely curtailed because companies need to consider court decisions in many different countries. The temptation for the various companies is to make the content acceptable to all of these different countries, and thereby water down the content in the articles that they are publishing.

The American press fights hard for its right to publish the truth. The problem is that there are global corporations that are not in the news business, and they will tend to do what will make a profit. The Union of French Jewish Students took Yahoo to a French court demanding that it stop allowing Nazi paraphernalia to be sold on their website. The French court said that Yahoo had to make sure no one in France would view such items. Yahoo removed it from the yahoo.fr site. But then the Jewish students discovered the French people could find them on the US site, and they demanded that the paraphernalia be removed also from the US site. A first ruling in US courts found against the French saying it would have a chilling effect on free speech in the US. But a court of appeals reversed this decision. So, Yahoo had to give in and remove the items from all of their websites.

The danger is that information liberty will tend to fall by the wayside by domestic child protection laws and to international money-making opportunities. Flickr removed photos to conform with orders from Singapore, Germany, Hong Kong, and Korea. Google complied with requests from China to limit materials available to its search engine. Business tends to be business.

Assignment

The right to free speech is the right to say or to write things that are objectionable to some people. There are also some limits to free speech because not everything should be allowable. Cite three examples of what you consider to be acceptable forms of free speech even though others would think the speech is objectionable. Provide reasons why you think this kind of speech should be protected. Cite three examples of speech that you think should be prohibited.

Performance Element	**Exemplary**	**Proficient**	**Developing**	**Points Possible**	**Points Earned**
Three examples are given of free speech that some people consider objectionable. Give plausible reasons why these examples should be protected.	**40 points** The examples given are well-selected and good reasons are given for protecting this kind of speech.	**10 - 30 points** The points given depend on the quality of the examples and reasons given.	**0 points** (Task not completed)	**40**	
Three examples are given of free speech that should be prohibited.	**40 points** The examples given are well-selected and the reasons for prohibiting this kind of speech are plausible.	**5 - 30 points** The points given depend on the quality of the reasons and examples.	**0 points** (Task not completed)	**40**	
The document is well-formatted and professionally done.	**20 points** The document has good grammar, good spelling, and nice formatting.	**5 – 15 Points** Points are subtracted for bad grammar, spelling, and formatting.	**0 points** (Task not completed)	**20**	
Total Points				**100**	

Supplementary Material for the Blown to Bits Appendix

Understanding Binary, Hexadecimal, and Dotted Base 10

First, review how the **base 10** system works.

- The first location is the ones. (Ten to the zero power is 1.)
- The second location is the tens. (Ten to the first power is 10.)
- The third location is the one hundreds. (Ten to the second power is 100.)
- The fourth location is the thousands. (Ten to the third power is 1,000.)

10^4 10^3 10^2 10^1 10^0
1 0 0 0 0

Twenty is 2 10's and 0 1's, for example.

Three hundred is 3 100's and 0 tens and 0 ones.

Next, consider the same scenario for **base 2.**

- The first location is the ones. (Two to the zero power is 1.)
- The second location is the twos. (Two the first power is 2.)
- The third location is the fours. (Two to the second power is 4.)
- The fourth location is the eights. (Two to the third power is 8.)
- The fifth location is the sixteens. (Two to the fourth power is 16.)

2^4 2^3 2^2 2^1 2^0
1 0 0 0 0 is 16 in decimal.
1 is 1 in decimal.

1 0 is 2 in decimal.
1 0 0 0 is 8 in decimal.
1 0 0 1 is 9 in decimal.

Doing simple math in binary.
Addition/Counting

Suppose you have a number (in binary) like 1110. How would one add one to that number? As you might expect since the last number is a 0 you would replace that 0 with a 1 so that you have 1111. If you started with a number like 1010 you do the same thing. Since the last number is a 0, replace it with a 1.

Suppose you have a number like the following: 111. Then if you add one, what do you do? The rule is to reset all of the 1's to 0's and put a one in the left-most place like this 1000. Note that the first number is 1+2+4 = 7. 1000 = the number 8.

You could practice by counting to 7. The first number would be 0, then 1, then 10, then 11, then 100, then 101, then 110, then 111.

Higher numbers work the same way.   Adding 1 to 11111 (31 in base 10) yields 100000 (32 or 2^5).

Hexadecimal Numbers

The hexadecimal (base 16) system is also important in computing. Often computer printouts contain a lot of hexadecimal notation. The principle is the same. The first position is 16 to the 0 power or 16^o. The second position is 16 to the first power 16^1, the next is 16 to the second power 16^2, etc. In base 16, 11 = 16 + 1 because the first position is the 1's position and the second position is the 16's position. Addition/counting works the same way.

What is different in hexadecimal notion is the fact that there are 15 unique symbols. 1 through 9 are familiar but the following symbols are not: 10 is A, 11 is B, 12 is C, 13 is D, 14 is F, and 15 is G. So the numbers are written in the following way 123456789ABCDEF. It may take getting used to adding 1 to A to get B as in 1A (in Hex) becomes 1B when you add one. Adding 1 to FFFF becomes 10000 (because F is the maximum value before going to the next place).

In computer printouts you may see a string of numbers like, 100, 10F, AAC, C8B23, and so on. Below you will see how hexadecimal numbers are used to represent the new generation of IP addresses. Here is a chart comparing the three notations.

Binary	Decimal	Hexadecimal
0	0	0
1	1	1
10	2	2
11	3	3
100	4	4
101	5	5
110	6	6
111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

10000	16	10

ASCII

The importance of binary can be seen in the ASCII code. The ASCII code is used to represent the characters, numbers, and special symbols in the various alphabets. Here is a short table. This helps to illustrate the importance of the binary system for computing.

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001

IP Addresses

IP addresses are used to uniquely identify devices. Every device on the Internet has an IP address. In the classic format (IPv4) the IP addresses are written in dotted decimal notation such as 111.10.128.6. There are always four sets of numbers. Each device has a unique number. Because of the possible combinations available using this format IPv4 numbers provide over 4 billion unique IP addresses (2^{32}).

Even though this is a large amount of unique addresses, it turns out that this number of addresses is too small. Because of this a new scheme was devised to produce an almost unlimited set of numbers. This new format is called IPv6 and it represents numbers in hexadecimal. So, in this format you will see numbers like 3ffe:1900:4545:3:200:f8ff:fe21:67cf. This new format allows for a vastly increased number for the IP addresses needed for the Internet of things. IPv6 supports a whopping 340 *trillion, trillion, trillion* addresses (2^{128}).

Networking

TCP/IP (Some Basics of Transmission Control Protocol Internet Protocol)

1) Each device/computer has a number. When people talk about the Internet of Things you should think of the fact that each device is connected on the Internet. The way they connect is by reference to a number that identifies them.

The number will look something like this (for Internet Protocol version 4): 130.103.140.12 (called dotted decimal notation – using base 10 numbers).

There are always four sets of numbers (three possible in each) separated by periods. Another example of a legitimate number is 100.0.0.1. Home routers that connect your devices to the Internet often have the following numbers: 192.168.0.1 or 10.0.0.1.

For many purposes, your computer will also have a name to make it easier for humans to remember. You could name your computer Samantha's Apple. However for another device to communicate with it requires translation of that name into a number. There is a specific service on the Internet that does this, and it is called **Domain Name Service** (System or Server). The DNS takes the name, "Samantha's Apple", and translates it into a number like 130.205.150.213 (the corresponding IP address). The DNS is said to resolve names and domain names such as amazon.com or fhsu.edu to its respective IP address.
2) For one computer (John's PC) to communicate with another computer (Samantha's Apple) it must know its number (IP address).

The Internet Protocol proves a systematic way of addressing all devices. The Internet Protocol needs to know the receiving device's address in order to send the information (the information is divided into manageable packets) across the Internet to that specific device (and "location" on the Internet).

Note that the packets are sent across the network to a specific address in a **best effort** manner. That is, there is no guarantee that they will all arrive at the destination, but the IP service picks the best route across the network and sends the packets on their way. Using TCP/IP each packet has the originating address in plain text and the destination address also in plain text.

3) There are some problems with this:

- Packets may not arrive at all (there is no acknowledgement sent back across the network to tell the sending computer they have arrived)
- Packets may arrive out of order.
- There is no flow control. That is, they may be arriving too fast for the receiver to process them with the result that many packets are dropped.
- This is a **best-effort kind of scenario** – not a guaranteed success kind of scenario. So, even though it may work much of the time, there are times that the transmissions are unsuccessful.

4) The Transmission Control Protocol (TCP) was designed to correct these problems.

a) When TCP breaks the data into packets it numbers them.
b) If the packets arrive out of order, then TCP reassembles them into the proper order.
c) If they arrive too fast to be processed TCP slows down the transmission (it buffers the data so data arrive at a slower pace). Because of this TCP can handle streams of data, such as that created by Netflix.
d) If some packets are lost, TCP sends a message to get them retransmitted because it knows the address of the sender and of the receiver (which in many cases is the address of the client and the address of the server).
e) These features change the nature of the service from a best effort service into a much more reliable service.

5) The genius of the TCP/IP protocol was that it was well designed and that it was an open system and not tied to any particular company or proprietary system. It was supported by the federal government for communications over its network. Over time all of the major computing companies adopted it and so it became a part of the operating systems for Apple, IBM, HP, Compaq, Dell and others. When people refer to smart devices, they typically mean that the device has an IP address and can interact with other devices on the network. Smart devices also typically use or supply data to be used by other devices in what is now called the Internet of Things. Lights, thermostats, webcams, and many other devices now can be controlled by other devices because they are part of the TCP/IP network. Because a thermostat is part of the network, it can be controlled by smartphones at a distance.

Switches

Ethernet switches work with local area networks, networks where computers and connected devices are in the same physical location. They transmit packets to specific addresses, called **MAC addresses**. The MAC address stands for media access control and is the physical address of the device. If a PC, Apple Mac, or other device connects to a LAN via a wired ethernet connection, a network interface card (NIC) is used. The address is a 6 byte address with the last 3 bytes containing the serial number of the NIC itself.   Switches need to know the physical address in order to send information to the correct device. Switches basically direct traffic in the network to the intended physical addresses. The switch has a lookup table that contains the MAC addresses on the network. The packets that are sent have headers with the MAC address of the intended recipient. Even Fitbit scales that connect wirelessly to the Internet have (physical) MAC addresses.

Routers

Routers work at a different level in the network, a level called layer three, the network layer. In this layer routers connect networks. Software in the routers do not use the MAC address. Rather, they use a different address, the IP address discussed earlier, to communicate with devices on the network. Routers use different methods (algorithms) to connect devices than switches do. To send data to devices on the network, the packets must include the address (IP address) of the destination.

Windows computers obtain their IP address typically by using DHCP (dynamic host configuration protocol). The IP address used by your home computer to request services over the Internet is assigned to your computer after a server receives the request for the IP address (this is what makes it dynamic, not static). If you have a cable (or satellite) service, a server at the cable company assigns your computer an IP address from a pool of addresses. This address can be used for a specific time (sometimes up to five days) before it expires and a new one must be sought. The cable company keeps a record (logs the IP address) of what IP address was assigned at the time in case there is a need to trace the transaction between devices later.

Wireless Access Points

Wireless access points connect to a wired network and transmit information wirelessly. In business locations, the wireless access points are separate devices that handle many different wireless devices simultaneously. In a home location, often the wireless access point is part of a switch/wireless router combination unit. Wireless access points are routers that have names. When you search for wireless networks with your phone or computer you may see lists of names like Wildcat, Jayhawk, Superfan, Starbucks1, Hilton, or more cryptic identifiers such as ATT9Hdyh5. These are called SSIDs or service set identifiers. Often you are prompted for a password if you attempt to access one of these SSIDs.

Ports

Hardware Ports

Hardware ports are connections on computers that attach to peripherals. A serial, parallel, usb, firewall, or ethernet port allows external devices to interact with computers. These ports are distinct from TCP/IP-based software ports which provide services. The network interface card (NIC) is one such port, and it is used to send communications across the local area network (LAN).

TCP/IP Ports

When transmissions are sent over the Internet to various servers or other devices, how are those transmissions parsed? That is, how does the processor receiving them know what to do with them? TCP/IP has created a variant of standardized ways to handle these software transmissions and software requests. These are "doors" or ports that open up for specific computer applications and protocols. Your web browser uses an (hypertext) http: protocol – a rule-based way of speaking to a web server. Secure HTTPS users a different port. Email and File Transfer protocol use different ports. Some of most popular ports are listed below:

1) HTTP is on port 80. This is used to send or receive web pages.
2) HTTPS is on port 443. So a web browser knows to send a message to port 443 and to receive the response on the same port. The S at the end of HTTP is significant. It stands for secure and provides a more secure connection across the Internet because the content is encrypted.
3) If you are downloading a music or video file your file transfer software often uses file transfer protocol – ftp – and contacts Port 20 (or 21).
4) Email uses POP and SMTP (simple mail transfer protocol).
5) DHCP uses ports 67 and 68.
6) Apple Quicktime uses port 458.
7) The Domain Name System uses port 53. (This translates the human readable names to the numbered sequences.)

TCP establishes a socket – a connection that remains during transmissions.

Each Socket: has the IP address of the server, the IP address of the client, the port number of the server, and the port number of the client.

Routers

- Move packets from one network to another – from your local home network, for example, to the Internet.
- They are more sophisticated than switches.
- They look into the packets – find the destination address and send it to that destination address – moving data from a local area network to a wide area network (Internet) – switches can't do that.

Switches

In a LAN switches can move messages/data directly to another computer on the network.

Firewalls

- Prevents receipt of certain kinds of network messages.
- For example: a firewall might allow all http traffic (browser traffic) but prohibit any ftp (file transfer) traffic. Or a firewall might allow only http traffic and email traffic.
- A firewall might have **a whitelist for certain computers – always allow all traffic and all protocols from computers x, y, and z.**
- A firewall might have **a blacklist for other computers** – disallow any traffic from computer x, y, and z.
- A firewall might inspect packets looking for various signatures – various patterns that indicate viruses and worms.