Zachary Lineman

Mr. Fritz

AP Computer Science Period 3

1 August 2018

*Blown to Bits Vocabulary*

**Chapter 1:**

Bit: A miniscule amount of data made up of 1s and 0s

Blacklist: Something that blocks someone on the blacklist from using a service

Character: A letter or symbol on a screen

Cyberspace: A land where there are no limits were every can connect and talk to each other as if they were in the same town.

Datacenter: A place where massive amounts of bits are stored where there is tons of storage for everything.

Data: Different statistics or facts about one thing.

Data network: A network of different facts and statistics that can be accessed.

Disk drive: A place where data and bits can be stored for people to access through computers

Intellectual property: A set of bits that someone owns usually something that they made like music, games or movies.

Moore’s Law: The Density of integrated circuits will double every couple of years.

Network: Connects millions of people together sharing data from one person to the next open to almost anyone

Processor: A chip that can do work at lightning fast speeds. Multiple are put onto one chip to speed up the entire chip increasing speeds.

Social networking: A place where people can contact each other and share moments and stories

Whitelist: A list of people who can use a service everyone else not on the list do not have access to the service

**Chapter 2:**

ad hoc: something formed for a specific reason

Database: A giant of data set that can store mass amount of data

data aggregation: a gathering of data usually by a company or government

data mining: Examining large databases to generate new information.

data repository: A destination designated for data storage.

data sources: A source of data

digital detritus: A trail of digital fingerprints and footprints.

Dossier: A folder

EDR: An EDR is an automotive black box for airplanes wich

Encode: To convert into a coded form

Encryption: The Process of encoding a set of data so that it is harder to understand.

IP address: An identifier for every computer or mobile device on the internet.

Metadata: A set if data that give information about other data

Query: A computer language used to receive data from a database

RFID: A form of wireless communication usually used for cards or identifiers

**Chapter 3:**

Algorithm: A method that performs a task

Analog: Information represented by a physical quantity

ASCII: A character encoding standard for electronics

Cloud computing: Using a network of servers on the internet to manage and store data

Cryptography: Writing or solving codes

Digital: A series of 0s and 1s

Digital signal processing: The use of digital processing

Download: The processes of copying one set of information from one computer to another computer.

lossless compression: Algorithms that allow the original data to be reconstructed from compressed data:

Megabyte: One million bytes

Megapixels: One million pixels

Modeling: Representation of a photograph in bits

OCR: Recognition of of printed or written text.

Pixels: an area of illumination on a display

Raster: a rectangular pattern of scanning lines followed by an electron beam on a display

Render: processes of generating photorealistic or not photorealistic image in 3d or 2d

Spam: irrelevant message on the internet

Steganography: Concealing messages and information with text or data

Upload: Transfer data from one computer to another. The data usually goes to a larger remote server

**Chapter 4:**

Background: The color of what is under everything is shown over on a computer display or A priority assigned to an application that is usually in the behind the scenes

Binary: A system of numerical notation with a base of 2. The base language of computers.

Bot: program that endlessly performs the same task.

Cache: A collection of items of the same type.

Firewall: a part of computer or network that is designed to block unauthorized access from outside connection

Foreground: A priority assigned to an application usually the applications the user is currently using.

HTML: A standardized language for web development.

URL: An address on the internet

**Chapter 5:**

AES: Advanced Encryption Standard, Is a new encryption method for anyone to use.

certification authority: Something that can be issued by a company to allow someone to use a product.

Ciphertext: Encoded text

DES: A national standard for encryption

Decryption: To solve an encryption or reverse it

Encryption: To mix a set of bits up to a special code that can be used to decrypt the Encrypted bits.

Packet: Blocks of bits that travels through the internet.

plain text: Text that is not written in written code.

Router: Computer that steers packets across the internet

**Chapter 6:**

centralized systems: Centralized systems collect data at a central computer for people to download

Commons: A system of sharing that reduces the need for heavy property restrictions

DRAM: Dynamic Random Access Memory

DRM: Distributing content with control information that restricts its use. Digital Rights Management

Flooding: Every computer in a file sharing network has a list of other computers in the network. When one person wants a file they ask everyone on their list until someone has the file and if no one has it everyone who was asked asks everyone else on there lists until the file is found and the transfered.

Gigabyte: One billion bits

peer to peer architecture: A central directory tells where the files are on one computer and then other computers can pass this file onto others

Piracy: An unauthorized use of another's personal data

sealed storage: A encryption that can only be decrypted on certain whitelisted computers

TPM: A chip in most consumer computers called a Trusted Platform Module.

**Double-Entry Journal (Chapter 1)**

Chapter 1: Digital Explosion: Why Is It Happening, and What Is at Stake? of Blown to Bits makes the point that today everything is digital –that is, everything is represented by binary digits or bits. It provides some provocative examples of societal implications of this digital explosion.

Read Chapter 1 to learn more about how digital our world has become. As you read, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# Moore's laws works for multiple things. One of these is the processor which double every two or so years. Another is the disk which follows its own sort of Moore's Law**

I think that Moore's Law should not be accepted as completely true or even a basis of knowledge and understanding. I think that it is mostly just a coincidence that processors and disks double every two or so years. I feel that it is just a general statement.

**# The internet has completely shifted the way the world works changing businesses and communication.**

I believe that without the internet small businesses would not be able to compete with name brands. This is because they would only be able to advertise in there general area and not across the entire globe.

**# Social Networking has helped and not helped many people causing problems but also helping a lot of people vastly**

Social Networking is neither good nor bad. Some people have found love or great friends over the internet but for some it has not been as good. Social networking needs some restrictions or ways to stop people from getting hurt but in most ways social networking has helped people for the greater good.

**# Products get into consumers hands much faster then before the digital age.**

Consumers are throwing away products much faster then they were years ago. Technology from 2016 is seen as old and people are only wanting technology that is considered new.

**Double-Entry Journal (Chapter 2)**

Chapter 2: Naked in the Sunlight: Privacy Lost, Privacy Abandoned of Blown to Bits focuses on the issue of how the digital explosion affects our privacy. This is an especially important issue for today’s mobile computing generations. Our smartphones and tablets can not only track our electronic correspondence, they can track our whereabouts, opening whole new areas of potential privacy infringements. What’s especially interesting about the privacy question is that, for the most part, Americans seem to be willing to trade privacy for convenience. We don’t mind letting the supermarket track our purchases if that brings us discounts. And we don’t seem to mind letting mobile apps know and record our whereabouts in exchange for some service we like.

Visit the website http://aboutmyinfo.org/ and enter your date of birth, gender, and zip code. Why might you be easily identifiable by this information? (HINT: Estimate the number of people in your zip code and the number of unique combinations of birth date and gender. See the About page of the website for more information.)

Read Chapter 2 to learn about some of the ways our electronic devices impinge on our privacy – some of the stories will surely surprise you. As you read, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# “Ironically, the notion of privacy has become fuzzier at the same time as the secrecy-enhancing technology of encryption has become widespread. Indeed, it is remarkable that we no longer blink at intrusions that a decade ago would have seemed shocking”(21).**

This shows that we care less and less about what we want private. I feel that as a species we have started to feel that we have no control over what people know about us. We really don't care what information we give out.

**# “EVER READ THOSE “I AGREE” DOCUMENTS?**

**Companies can do almost anything they want with your information, as long**

**as you agree”(67)**

Most people don't care for what is written in the I Agree documents. I would say 99% of people actually read what they say. Also I believe that most people don’t realize what companies can do with their information once they click the I Agree button. Most people just see that button as an extra step to signing up for an account at any site on the vast internet.

**# “The meaning of privacy has changed, and we do not have a good way of describing it.”(68)**

This quote almost perfectly sums up what is happening now in the digital world. People are still trying to figure out what power they have and where that power is affective. People have no idea what there privacy truly means and frankly not many people really care.

**# “Many 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”(49)**

The Fact that phones can have there microphones turned on remotely to be used to spy on anyone. People believe that just because they turn there mics of they are safe people don't pay attention to what it really means when they accept the “\_\_\_\_\_ app wants to use your microphone”.

**Double-Entry Journal (Chapter 3)**

Chapter 3: Ghosts in the Machine: Secrets and Surprises of Electronic Documents of Blown to Bits describes how digital documents, including images and sounds, are represented by sequences of bits. Why do you think this chapter is called “Ghost in the Machine”?

As you learned in a previous chapter and as shown in the diagram, the first step in representing an image is to convert it into a sequence of bits. This is known as modeling. The model is an abstract representation of the original image.

Read Chapter 3 to discover what’s hidden in electronic documents. As you read, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# “The users of the computers had for the most part done what they thought they were supposed to do they deleted their files or formatted their disks” “that by dumping them on eBay, they might be releasing personal information into the digital environment” (100)**

People don't realize that there data can be taken from there old discs that they don't clear correctly. People think that throwing away drives will just get rid of the data and they won't have to worry about there data getting stolen ever.

**# “But mass emails are so cheap that getting one person out of a million to respond is enough to make the spammer financially successful”(95).**

Since there is always one person who falls for the scam the scammers can make thousands. There is really no way to stop scammers because the emails cost so little and one person can make as many emails as they want

**# “A researcher bought ten cell phones on eBay and recovered bank account numbers and passwords, corporate strategy plans, and an email exchange between a woman and her married boyfriend, whose wife was getting suspicious”(103)**

The fact the people don't completely wipe there phones and leave there data in a state that can be recovered. If someone throws away there phone and doesnt completely wipe it they can get there bank accounts stolen or other personal information.

**# “Sometimes electronic records become unavailable quite quickly, in spite of**

**best efforts to save them permanently”(105).**

Some things that could get deleted could be very devastating. If something that is needed or is a massive part of history gets deleted and can no longer be found a piece of history has just disappeared .

**Double-Entry Journal (Chapter 4)**

In Chapter 4: Needles in the Haystack, Google and Other Brokers in the Bits Bazaar, you will learn about how search engines control how users obtain information on the web, how search engines work and how search engines can be exploited. As you read Chapter 4, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# “Second, the Web has gotten so big and so unstructured that it is not**

**humanly possible to split it up into neat categories”(111).**

Finding one piece of information that you may have found months before but dont remember how you found it can be very hard and near impossible with the shear size of the internet. If the internet was split into categories it probably would not help at all even in the slightest because the categories would have to be broad and there would probably still bhe thousands of sites in each category

**# “We have given search engines control over where we get reliable information—the same control we used to assign to authoritative sources, such as encyclopedias and “newspapers of record.” If we place absolute trust in a search engine to find things for us, we are giving the search engine the power to make it hard or impossible for us to know things”(112)**

We have given pure trust into search engines to find the most reliable sources for us to find information out if a search engine wanted a site to disappear they could just make a few changes to there search algorithm and completely block out the site or sites that they do not like, restricting information for anyone who uses that search engine.

**# “But you might not be willing to pay the price of mentioning the competition on Abelson’s page. On the other hand, if you just put the word “Bloomingdale’s” in white text on a white background”(149)**

Knowing that websites might be hiding text to get better search traffic. The fact that people are willing to hide text from regular people to get better traction seems very scammy and not something you should do as a web developers.

**#“Search engine companies can store everything you look for, and everything you click on” (156)**

With unlimited storage available to search engine companies why would they not store all of your data they can sell the data to other companies. The companies can also use the data to give better search results.

**Double-Entry Journal (Chapter 5)**

Read Chapter 5: Secret Bits: How Codes Became Unbreakable to learn about encryption and cryptography and how they work. As you read, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# ““that we had the capability to break most codes because of our sophistication.” No more. “The technology has outstripped the code breakers,””(161)**

The fact that encryption has gotten to the point that even governments can’t crack the code to decrypt data is kinda scary. If something happens that threatens a countrie and data is found to find out who did it but it is encrypted and they can’t crack the code that is a big problem.

**# “In other words, as long as Alice and Bob can communicate with each other, they can establish a secret key. It does not matter if Eve or anyone else can hear everything they say Alice and Bob can come to a consensus on a secret key, and there is no way for Eve to use what she overhears to figure out what that secret key is”(179)**

Encryption that can make it so other people can't figure out what your saying even if they intercept the messages they can figure out the secret code used. This is also a very basic way to explain encryption.

**# “In 1999, an encryption standard known as WEP (Wired Equivalent Privacy) was introduced for home and office wireless connections. In 2001, however, WEP was found to have serious flaws that made it easy to eavesdrop on wireless networks, a fact that became widely known in the security community.In 1999, an encryption standard known as WEP (Wired Equivalent Privacy) was introduced for home and office wireless connections. In 2001, however, WEP was found to have serious flaws that made it easy to eavesdrop on wireless networks, a fact that became widely known in the security community”(176).**

The fact that security measures that become mainstream have their exploits found quickly. This means that these methods are no longer valid for keeping people's privacy. The more methods that are introduced the more exploits will be found and these privacy and encryption processes will become obsolete and we will need to make more of them.

**# “It is not just email and credit card numbers that might be encrypted. Instant Messaging and VoIP telephone conversations are just packets flowing through the Internet that can be encrypted like anything else”(192).**

It's one good thing to know that our instant messages and telephone communications are encrypted. And that most people aren't able to intercept messages from one person to another.

**Double-Entry Journal (Chapter 6)**

Chapter 6: Balance Toppled: Who Owns the Bits? focuses on the question of use and ownership of digital media, including copyrighted media. It describes how file sharing algorithms should work and discusses some of the sensational cases in the battle between large media companies and users who use file sharing sites to share music and other media. Some of the topics covered include: Copyright, Peer-to-peer architecture/network, Digital Millennium Copyright Act (DMCA), and Open access and creative commons. As you read, write down four ideas from this chapter that you believe are critically important to this topic. You can quote the authors or summarize them. Include the page number. Then write your reaction to the idea.

**The Text (Quote or Summary) Page**

**# “It’s also an error-prone form of justice. Matching names to IP addresses is unreliable”(197).**

It is kind of a problem that people can get mistaken for the wrong person and get fined just because people mess up with who actually pirated the stuff. I feel that a more precise system should be made to detect people who have pirated stuff so that people are falsely accused

**# “The 4,000-song contents of a 20GB iPod would be grounds for minimum damages of $3 million—a thousand times the cost of purchasing those songs on iTunes”(197)**

The fact that 4,000 songs that could be pirated and the person could be sued for 3 million dollars. Also, the fact that people would risk the cost of a thousand times the cost of purchasing the songs legally.

**# “The three companies responded that they had no control over the users’ actions. Moreover, their software was only one piece of the infrastructure that enabled file-sharing, and there were many other pieces”(206)**

Since companies can say that there file sharing platforms are not for pirating even tho that is their only purpose and the only thing that their users use the platform for is pirating.

**# “Going further, computers cannot display images on the screen without copying them to a special part of memory called a display buffer. Does this mean that, even if you purchase a computer graphic image, you can’t view the image without explicit permission from the copyright holder each time”(209).**

Loopholes in the law like this can cause problems for lots of people and creators of content. If someone can sue you for opening a file for just copying it to a seperate disk that is yours because they could just say that it is for someone else and you would have no way of saying it wasn't.