Ap CSP Summer Assignment

Shaurya Singh

August 26, 2021

Contents

1 Digital Explosion

1.1 Vocabulary

1. Word: bit

   Definition: (n) **bit** (a unit of measurement of information (from binary + digit); the amount of information in a system having two equiprobable states) "there are 8 bits in a byte"

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=bit&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: koan

   Definition: (n) **koan** (a paradoxical anecdote or a riddle that has no solution; used in Zen Buddhism to show the inadequacy of logical reasoning)

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=koan&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

3. Word: ping

   Definition: (v) **ping** (send a message from one computer to another to check whether it is reachable and active) "ping your machine in the office"

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=Ping&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 23 July 2021.

4. Word: benign

   Definition: (adj) **benign** (not dangerous to health; not recurrent or progressive (especially of a tumor))

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=benign&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5. Word: utopian

Definition: (n) **utopian** (an idealistic (but usually impractical) social reformer) "a Utopian believes in the ultimate perfectibility of man"

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=utopian&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

6. Word: err

   Definition: (v) **err**, mistake, slip (to make a mistake or be incorrect)

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=err&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: paradoxically

   Definition: (adv) **paradoxically** (in a paradoxical manner) "paradoxically, ice ages seem to occur when the sun gets hotter"

   (adj) **paradoxical**, self-contradictory (seemingly contradictory but nonetheless possibly true) "it is paradoxical that standing is more tiring than walking"

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=paradoxically&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

8. Word: expunge

   Definition: (v) **expunge** (remove by erasing or crossing out or as if by drawing a line)

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=expunge&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

9. Word: database

   Definition: (n) **database** (an organized body of related information)

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=database&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

10. Word: blacklist

    Definition: (v) **blacklist** (put on a blacklist so as to banish or cause to be boy-cotted) "many books were blacklisted by the Nazis"

    Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=blacklist&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

1.2 Ideas:

1. Companies keep records of cellphone locations (Page 1)

2. "Its all just bits" (Page 5)

3. "In fact, processors have hardly grown faster at all" (Page 8)

4. "By 2011, we may be producing more bits than we can store" (Page 10)

1.3 Journal Entry

1. I support the idea of companies keeping track of cellphone locations, as long as that information is kept private and in the hands of only the government. Cellular locations are incredibly useful for finding missing people, and quickly reacting to emergencies, such as in Tanya's case.

   However, the key term is *as long as that information is kept private and in the hands of the government*. Private companies shouldn't be able to get the locations of users. These locations are often sold to advertising firms. Companies like Cuebiq make money by collecting location data from smartphone users who agree to share their locations for weather or maps, then analyse and sell that data to advertisers and marketers. Location data shouldn't be used to target people, and should be used as a last resort

2. While technically it is all just bits, personally I believe we shouldn't think of it as such. Thinking of computers in terms of bits is like thinking of writing in terms of atoms on a piece of paper. While all handwritten work is technically just graphite on paper, we interpret it as much more than that. We think of writing in terms of words, phrases, paragraphs, and should think of the computer experience in

terms of experiences. Similarly, copyright law is based on text, and so laws pertaining to computers should be based on the end user's experience, not what delivers that experience

3. Considering the next sentence is talking about "multiple processors on the same chip" I assume this statement is talking about the processor cores themselves. However, data shows that the fastest processors today are about 80 times faster in terms of single core performance with the same efficiency. Still, its true that processor cores have increased over the years (from single core chips to server chips with over 128 cores in the span of just 20 years).

   In my opinion we should focus more on processor efficiency and less on raw processor speed. Processor's these days, even budget ones, are more than fast enough for the majority of use cases. The market for large, high end HEDT processors is extremely small compared to the market share of their lower end counterparts. The future is about switching to arm-based processors in laptops, which should give much more performance at the same wattage.

4. I found this statement the most interesting in this chapter. We've made leaps and bounds in storage technology since then, nowadays you can buy tens of terabytes of storage for quite cheap, compared to the expensive "high end" 80gb drives you could get in 2008, back when this textbook released.

   Similar my opinion on processor speed, instead of focusing on storage size and how much data we can store, we should talk about how we store data. Companies are moving to cloud-based centralized storage, and as of 2020 50% of all corporate data is stored in the cloud, up from 30% just 5 years earlier. As more and more people start using cloud services (e.g. OneDrive, iCloud, Google Drive), we should focus on make data transfer to and from those drives quicker and more secure.

2 Naked in the Sunlight

2.1 Vocabulary

1. Word: pervasive

   Definition: per·va·sive | pər□vāsiv | adjective (especially of an unwelcome influence or physical effect) spreading widely throughout an area or a group of people: ageism is pervasive and entrenched in our society.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
pervasive&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=
&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: cleric

Definition: cler·ic | ˈklerik | noun a priest or religious leader, especially a Christian
or Muslim one.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
cleric&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
&o4=&h=. Accessed 18 July 2021.

3. Word: disseminate

Definition: dis·sem·i·nate | dəˈseməˌnāt | verb [with object] spread (something,
especially information) widely: health authorities should foster good practice by
disseminating information.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
disseminate&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=
&o3=&o4=&h=. Accessed 23 July 2021.

4. Word: encode

Definition: en·code | inˈkōd, enˈkōd | verb [with object] convert into a coded
form: using this technique makes it possible to encode and transmit recorded
video information.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
encode&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
&o4=&h=0000000. Accessed 23 July 2021.

5. Word: RFID

Definition: RFID **(abbreviation)** radio frequency identification, denoting tech-
nologies that use radio waves to identify people or objects carrying encoded mi-
crochips.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
RFID&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
&o4=&h=0000000. Accessed 23 July 2021.

6. Word: exonerate

Definition: ex·on·er·ate | i⬚⬚zänə⬚rāt | verb [with object] 1 (especially of an official body) absolve (someone) from blame for a fault or wrongdoing, especially after due consideration of the case: they should exonerate these men from this crime

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=exonerate&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: discourse

Definition: noun | ⬚dis⬚kôrs | written or spoken communication or debate: an imagined discourse between two people traveling in France.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=discourse&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

8. Word: profilerate

Definition: (v) **profilerate** increase rapidly in numbers; multiply.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=profilerate&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

9. Word: prodigious

Definition: pro·di·gious | prə⬚dijəs | adjective, remarkably or impressively great in extent, size, or degree: the stove consumed a prodigious amount of fuel.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=prodigious&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

10. Word: clairvoyant

Definition: clair·voy·ant | ⬚kler⬚voiənt | noun a person who claims to have a super-natural ability to perceive events in the future or beyond normal sensory contact

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=clairvoyant&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

2.2 Ideas:

1. The notion of privacy has become fuzzier at the same time as the secrecy-enhancing technology of encryption has become widespread (Page 21)

2. His car had a black box-an EDR, that captured every detail about what was going on before the crash (page 27)

3. Bits mediate our daily lives. It is almost as hard to avoid leaving digital footprints as it is to avoid touching the ground when we walk

4. "There is no patient confidentiality" said Dr. Joseph Heyman. "It's gone"

2.3 Journal Entry

1. I agree with the notion that privacy has become fuzzier over time. As encryption and security technologies are becoming more widespread, it seems people are caring less and less about their privacy when really they should be caring more. Companies give us a false sense of privacy, when really they are breaching it more than ever.

   The greatest example of this is google. When you open up www.google.com, you can see multiple mentions of privacy. In reality, google is notorious for using user information to target ads and search results. They have multiple analytics and adsense services that companies can purchase.

2. I agree with the idea of having tracking devices in cars. If most people are given the choice between getting an expensive ticket and facing criminal charges or lying, most people will choose to lie. Devices like the EDR ensure we can make a conclusion based on actual data rather than from the victims point of view.

   However, similar to the issue with cellphone locations the key term is *as long as that information is kept private and in the hands of the government*. Private companies shouldn't be able to get the locations of users and use it when it isn't needed. Examples of this can be determining how to price billboard advertising, requiring cars to be serviced ever *x* miles. There can be certain exceptions (e.g. An insurance company trying to determine who is at fault), but for the most part this information should be for the government, and even then only for when the government absolutely requires it

3. Its true that now its extremely difficult to do anything without leaving digital traces

everywhere. I personally think this issue is linked to idea #1, people value convenience over privacy. Companies create a false sense of privacy, and justify all the analytics with improved convenience.

Most people don't want to put effort into maintaining their privacy, or resist changes to their workflow and life, and unless you make privacy more convenient, that won't change.

4. As I stated in the previous two responses, I agree with this, and the issue is not many people care about it. The solution is to raise awareness and make privacy the default, instead of having to have users change it themselves.

3 Ghosts in the Machine

3.1 Vocabulary

1. Word: metadata

   Definition: noun Data that describes other data, as in describing the origin, structure, or characteristics of computer files,

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=metadata&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: open source software

   Definition: Programs for which the source code is freely available and freely redistributable, with no commercial strings attached.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=open-source-software&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

3. Word: ascii

   Definition: noun (computer science) a code for information exchange between computers made by different companies; a string of 7 binary

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=

ascii&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
&o4=&h=. Accessed 23 July 2021.

4. Word: steganography

   Definition: noun The deliberate concealment of data within other data, as by em-
   bedding digitized text in a digitized image.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
   steganography&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=
   &o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5. Word: blocks

   Definition: noun (Computer Science) a block is a segment of a large area that can
   be used to assign data

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
   block&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
   &o4=&h=0000000. Accessed 23 July 2021.

6. Word: algorithm

   Definition: noun A finite set of unambiguous instructions that, given some set of
   initial conditions, can be performed in a prescribed

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
   algorithm&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=
   &o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: pixel

   Definition: noun One of the tiny dots that make up the representation of an image
   in a computer's memory.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
   pixel&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
   &o4=&h=0000000. Accessed 23 July 2021.

8. Word: raster

   Definition: (v) noun A bitmap image, consisting of a grid of pixels, stored as a
   sequence of lines.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
raster&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
&o4=&h=0000000. Accessed 23 July 2021.

9. Word: render

   Definition: transitive verb (Computers) To convert (graphics) from a file into visual
   form, as on a video display.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=
   render&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=
   &o4=&h=0000000. Accessed 23 July 2021.

10. Word: spam

    Definition: noun Unsolicited e-mail, often of a commercial nature, sent indiscrim-
    inately to multiple mailing lists, individuals, or

    Ref: WordNet Search - 3.1.

http://wordnetweb.princeton.edu/perl/webwn?s=spam&sub=Search+WordNet&o2=&o0=
1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

3.2 Ideas:

1. Metadata can help or refute claims (Page 78)

2. With some clever programming, the process could be made unnoticeable, but
   so far neither Microsoft nor Apple has made the necessary software investment
   (Page 102)

3. Free software is a matter of the users freedom to run, copy, distribute, study,
   change, and improve the software (page 94)

4. If google holds your documents, they are accessible from anywhere the internet
   reaches

3.3 Journal Entry

1. As the text after that statement mentioned, metadata can be easily altered to match a criminals statement. Although most people won't know about metadata and how to alter it, this makes it ineffective for most purposes.

   Personally, I think we should remove most metadata. It ends up doing more harm than good, especially in the case of images, where metadata can help trace the location where the image was taken. In the case of documents, it provides easily forge-able data that serves no purpose.

2. In my opinion, there isn't a need to zero all abandoned blocks by default. This is for several reasons. Firstly, the majority of people have no intention to sell their storage. The majority of laptops nowadays have storage soldered down, which would make those drives impossible to resell. Secondly, those who care about their privacy will likely have other methods to zero their storage anyways.

   Additionally, making this zero-ing behavior the default will bring performance implications as mentioned in the textbook. It's a slow process writing to all of the abandoned blocks. The author mentions this issue could be solved "with some clever programming," but programming isn't magic, in the end to properly erase these blocks you will have to write to then. A better solution would be to incorporate this behavior into the filesystem itself, prioritizing writing to abandoned blocks before free ones. This system increases drive longevity, reduces the chance of abandoned blocks, and is already incorporated in many filesystems today

3. I support the Free and Open Source movement. Open source software gives power to the users. With the open source model come better security, more features, and more support for users. Compared to commercial (paid) software, users can not only identify and report bugs, but also fix those bugs themselves. Since the source code for open source applications is available, you can clone the repository, change the insecure code, and submit your changes. On the other hand, with commercial software, you will have to wait until the company updates the application.

   Additionally, you can add features to open source software. If Microsoft Word is missing a feature, you can only request Microsoft to add it. However, if there is an open source editor missing a feature, you can simply fork it and add the feature yourself. Likewise, most open source editors will never die, since there is always a community of people working on it, whereas most commercial software is dependant on the future of the company producing it.

However, there are also drawbacks with open source software. Since there is no financial backing for most projects, maintainers don't have an incentive to keep working. Similarly, since coders aren't paid the quality work may not be as good as that of a commercial project.

4. I support the idea of using cloud-based storage solutions. As of 2020 50% of all corporate data is stored in the cloud, up from 30% just 5 years earlier. As more and more people start using cloud services, we should focus on make data transfer to and from those drives quicker and more secure. Otherwise, cloud storage is superior to offline storage except for solutions which require speed (e.g. boot drives) or high security.

4 Needles in the Haystack

4.1 Vocabulary

1. Word: bot

   Definition: noun A software program, such as a spider, that performs automated tasks on the Internet.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=metadata&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: cache

   Definition: noun A fast storage buffer in the central processing unit of a computer.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=open-source-software&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

3. Word: HTML

   Definition: The HyperText Markup Language, or HTML is the standard markup language for documents designed to be displayed in a web browser. It can be assisted by technologies such as Cascading Style Sheets and scripting languages such as JavaScript

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=ascii&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 23 July 2021.

4. Word: URL

Definition: the address of a resource (such as a document or website) on the Internet that consists of a communications protocol followed by the name or address of a computer on the network and that often includes additional locating information (such as directory and file names)

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=steganography&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5. Word: firewall

Definition: noun Computers A software program or hardware device that restricts communication between a private network or computer system and outside networks.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=block&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

6. Word: Web 2.0

Definition: Web 2.0 refers to websites that emphasize user-generated content, ease of use, participatory culture and interoperability for end users.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=algorithm&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: index

Definition: noun Computers A list of keywords associated with a record or document, used especially as an aid in searching for information.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=pixel&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

8. Word: background

Definition: noun Computers The environment in which programs operate that the user does not engage with directly.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= raster&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=0000000. Accessed 23 July 2021.

9. Word: foreground

Definition: noun computing the application the user is currently interacting with; the application window that appears in front of all others.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= render&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=0000000. Accessed 23 July 2021.

10. Word: spider/web crawler

Definition: noun A program that automatically retrieves webpages and follows the links on them to retrieve more webpages. Spiders are used by search engines to retrieve publicly accessible webpages for indexing, and they can also be used to check for links to webpages that no longer exist.

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= spam&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=0000000. Accessed 23 July 2021.

4.2 Ideas:

1. If you try another search engine instead of Google, you'll get different results. Which is right? Which is better? Which is more authoritative? (page 114)

2. Web 2.0 sites—Facebook and Wikipedia, for example—exploit what economists call "network effects." (Page 110)

3. Free software is a matter of the users freedom to run, copy, distribute, study, change, and improve the software (page 94)

4. If google holds your documents, they are accessible from anywhere the internet reaches

4.3 Journal Entry

1. The reason google is so ahead in the search engine space is because of data. Google is known to collect enormous amounts of data on their users, and this is both a good and a bad thing. Although there are many privacy issues surrounding the use of this data, google can use this data to predict what each user likes, and can also tune the search engine's results to match that users preference.

   Other search engines such as DDG can't provide you "accurate" search engine results, because they don't have the data google has. Neither result is more accurate, or better, just calculated differently. If you were to disable google's analytics, log out of gmail, and open an incognito tab, chances are you would get different results than the ones you would get when logged in.

2. I dislike the shift to Web 2.0 sites, and specifically the excessive use of Javascript. Javascript originally started off as a scripting language, but with the V8 engine, was performant enough to be usable elsewhere. Suddenly. everyone started using Javascript, even when it wasn't required. While there are benefits to using Javascript, its still quite slow and in most cases can be substituted for Html5 + CSS

   Static, read-only sites (Web 1.0) get a bad reputation for their bland look, and their issues with ease-of-use. However, css solved many of these issues, and you can still design user-friendly Web 1.0 sites, which perform much better than their Web 2.0 counterparts. Web 1.0 sites also have the benefits and drawbacks of being read-only. For websites like articles, that means there are no comment sections or request popups. Lastly, javascript isn't a bad language by nature, people are just using it for the wrong purpose. When used tastefully, it can still vastly improve websites.

3. My favorite part of free software is that users can improve the software as they please. If a piece of software that someone like, but doesn't have a feature they need, the user is free to modify the software as they please, and submit they're code upstream (back to the source of the software) if they wish to. On the other hand, with commercial (paid) software, you are stuck with requesting the company to update the application.

   However, there are also drawbacks with open source software. Since there is no financial backing for most projects, maintainers don't have an incentive to keep working. Similarly, since coders aren't paid the quality work may not be as good as that of a commercial project.

4. If google holds your documents, they are accessible from anywhere the internet

reaches.

This is why I like cloud storage over local storage. With local storage you have to deal with organizing files, keeping storage down, and most importantly you have to deal with sharing files with others, and making sure your assignments are accessible elsewhere when you need them. Additionally, when you share files with others, you need to keep track of changes others do

With google drive, everything is instantly organized and searchable. You don't have to deal much with keeping storage down, as cloud storage is extremely cheap. Most importantly, all your files are available as long as you have an internet connection, and collaborative work is much easier, as google keeps track of changes, and everything is in one document

5 Secret Bits

5.1 Vocabulary

1. Word: Cipher

   Definition: noun a secret or disguised way of writing; a code

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=metadata&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: decryption

   Definition: noun a text that has been decoded

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=open-source-software&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

3. Word: encryption

   Definition: the process of converting information or data into a code, especially to prevent unauthorized access.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=

ascii&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=. Accessed 23 July 2021.

4. Word: packet

   Definition: a block of data transmitted across a network.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= steganography&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9= &o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5. Word: router

   Definition: a device which forwards data packets to the appropriate parts of a computer network.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= block&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=0000000. Accessed 23 July 2021.

6. Word: plain text

   Definition: text that is not computationally tagged, specially formatted, or written in code.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= algorithm&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6= &o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: RSA

   Definition: An algorithm used in public key cryptography, commonly used in various protocols for secure online transmission of data.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s= pixel&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3= &o4=&h=0000000. Accessed 23 July 2021.

8. Word: private key

   Definition: a cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (the private key).

Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=raster&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

9. Word: digital signature

   Definition: a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=render&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

10. Word: one-time pad

    Definition: In cryptography, the one-time pad (OTP) is an encryption technique that cannot be cracked, but requires the use of a single-use pre-shared key that is no smaller than the message being sent.

    Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=spam&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5.2 Ideas:

1. If you try another search engine instead of Google, you'll get different results. Which is right? Which is better? Which is more authoritative? (page 114)

2. Having a good system doesn't mean people will use it (Page 175)

3. Today, electronic mail is gradually replacing conventional paper mail, and is soon to be the norm for everyone, not the novelty it is today (page 189)

4. Overall, the public seems unconcerned about the privacy of communication today, and the privacy fervor that permeated the crypto wards a decade ago is nowhere to be seen

5.3 Journal Entry

1. The reason google is so ahead in the search engine space is because of data. Google is known to collect enormous amounts of data on their users, and this is both a good and a bad thing. Although there are many privacy issues surrounding the use of this data, google can use this data to predict what each user likes, and can also tune the search engine's results to match that users preference.

   Other search engines such as DDG can't provide you "accurate" search engine results, because they don't have the data google has. Neither result is more accurate, or better, just calculated differently. If you were to disable google's analytics, log out of gmail, and open an incognito tab, chances are you would get different results than the ones you would get when logged in.

2. I agree with this statement. The largest issue with creating new technologies is that many people are reluctant to switch from the old ones. Every new idea seems to follow the same cycle. A new technology is created, adopted, and then either replaced by a newer one or deprecated and left unmaintained.

   The issue is when you create a new technology, no one depends on it. You are free to modify it to your liking. After others start to adopt a new technology, you can't create breaking changes. This limitation creates a lack of innovation, until another technology comes along and replaces it. With so many new technologies popping up and fading away, sometimes within the same year, it makes sense if people are more reluctant to switch.

3. This statement aged very well. Over time, email has replaced almost all physical mail, and is used for communication around the world. Not only is it secure, but its dependable, and a standard format that works just as well with ancient technology and modern web browsers. Email's biggest benefit and drawback is its standardized tried-and-true method of sending information. While this means that you use several different email clients which all work perfectly with each other, it also becomes impractical to use email for things like instant messaging.

4. Its true that now its extremely difficult to do anything without leaving digital traces everywhere. I personally think this issue is linked to idea #1, people value convenience over privacy. Companies create a false sense of privacy, and justify all the analytics with improved convenience.

   Most people don't want to put effort into maintaining their privacy, or resist changes to their workflow and life, and unless you make privacy more convenient, that won't change.

6 Balance Toppled

6.1 Vocabulary

1. Word: driftnet

   Definition: noun Driftnet is a program which listens to network traffic and picks out images from TCP streams it observes.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=metadata&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

2. Word: copyright infringement

   Definition: noun The unauthorized use of copyrighted material in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works that build upon it.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=open-source-software&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 18 July 2021.

3. Word: centralized systems

   Definition: A system where decisions for the system goal are made in a central mechanism and transmitted to executive components

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=ascii&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=. Accessed 23 July 2021.

4. Word: DRAM

   Definition: DRAM is a type of RAM that stores each bit of data on a separate capacitor. This is an efficient way to store data in memory, because it requires less physical space to store the same amount of data than if it was stored statically.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=steganography&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

5. Word: digital rights management (DRM)

   Definition: Digital rights management tools or technological protection measures are a set of access control technologies for restricting the use of proprietary hardware and copyrighted works. DRM technologies try to control the use, modification, and distribution of copyrighted works, as well as systems within devices that enforce these policies.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=block&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

6. Word: DMCA

   Definition: The Digital Millennium Copyright Act is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=algorithm&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

7. Word: copyright

   Definition: The legal right granted to an author, composer, playwright, publisher, or distributor to exclusive publication, production, sale, or distribution of a literary, musical, dramatic, or artistic work.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=pixel&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

8. Word: creative commons

   Definition: Creative Commons licenses are free copyright licenses that creators can use to indicate how they'd like their work to be used. Creators can choose from a set of six licenses with varying permissions, from the most open license to the least open license.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=raster&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

9. Word: digital signature

   Definition: A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents.

   Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=render&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

10. Word: SHA-256

    Definition: Secure Hash Algorithm 256, also known as SHA-256, is a one-way function designed to secure digital information. The function uses a complex mathematical process that converts text of any length into 256 bit (64-character long) string of letters and numbers. SHA-256 is called a one-way function since it is not possible (or very difficult) to determine the original input based on the output.

    Ref: WordNet Search - 3.1. http://wordnetweb.princeton.edu/perl/webwn?s=spam&sub=Search+WordNet&o2=&o0=1&o8=1&o1=1&o7=&o5=&o9=&o6=&o3=&o4=&h=0000000. Accessed 23 July 2021.

6.2 Ideas:

1. The answer is to build a chip into every computer that checks the operating system each time the system has been modified, the computer will not boot. (211)

2. A third DRM difficulty is that, in the name of security and virus protection, we could easily slip into an unwinnable arms race if increase technology lock-down that provides no real gain for content owners (Page 175)

3. What is wrong is that we have invented the technology to eliminate scarcity, but we are deliberately throwing it away to benefit those who profit from scarcity (page 222)

4. Universal has been talking to Sony and other labels about a subscription service, where users would pay a fixed fee and then get as much music as they would like. (page 224)

6.3 Journal Entry

1. The main purpose of a TPM chip is to generate RSA keys, SHA-256/SHA-1 hashes, as well as general purpose signatures. However, TPM's don't have a very strong track record. With the ROCA vulnerability, it was found you could easily derive a private key from the public key.

   That isn't to say the idea is bad. Apples implementation (via the T2 chip, and later build into their own chip) a 256-bit AES is generated and burnt into the chip. No one has access to this key, and theoretically no one can get access to this key. The key is then used to encrypt the storage. The idea of TPM is good, its just the implementation isn't.

2. This issue with DRM is already occurring, companies are adding more and more complicated DRM to their products, while providing no real gain for content owners. Those who want to pirate their content usually find a way to circumvent this DRM regardless.

   In the case of video games, some reviewer found that a pirated (and therefore DRM-free) version of the game ran 5-6% faster than a legally purchased copy. DRM isn't only *not* helping consumers, its harming them as well.

3. The issue is that companies are still stuck in the 20th century business model. They produce millions of copies of movies, sell years old music for over 2$ each, and then wonder why people want to get it for free. They *need* that scarcity to survive, because thats the only way their business model works. As soon as the entertainment industry moves to subscription services (which has already happened for the most part, e.g. disney+) , most of these issues with piracy will resolve themselves.

4. I thought it was interesting how this turned out. Only a few years after that, we saw the launch of music subscriptions (especially apple music and spotify at the time), which proved that if you give consumers a cheap and convenient way to enjoy content, the need to pirate content goes away.