University of Stavanger

DENNIS MALMIN
SUPERVISOR: HANDE ESLEN ZIYA

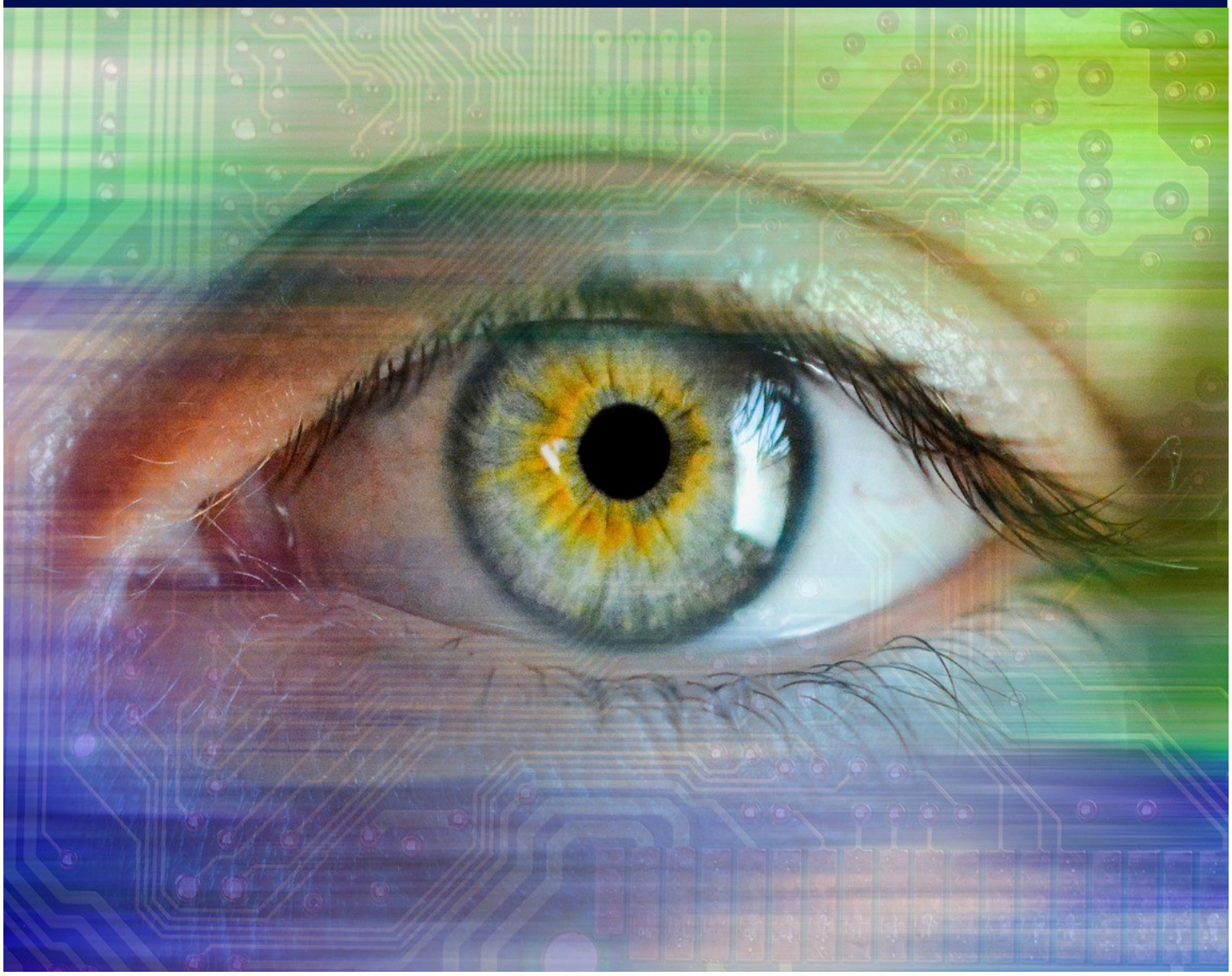
Creating friction within Surveillance Capitalism wit with Free Open Source Software

Bachelor thesis, 2024

Sociology

The Faculty of Social Sciences

Department of Media and Social Studies



Abstract

We have become the raw material for surveillance capitalists. They are relentlessly pursuing an imperative to extract and use our information and behavior for their own profit. Increasing measures are made to be able to develop and increase this extraction, at the same time there is a small subset of developers, programmers, contributors and entrepreneurs, who are pushing back. Development of Free Open Source Software (FOSS) makes it possible for anyone to audit and inspect the source code of programs or applications running on your device. This thesis will examine, if it is possible for FOSS to significantly reduce the possibility for large and small corporations to inject methods to extract human behavior from their users.

Table of Contents

1. The beginning of Surveillance Capitalism

1.1 A brief history

We have been conditioned to think all advancement in the tech and computer industry is natural and a right for the surveillance capitalist. This is simply not the case, the origins of early surveillance on the world wide web can be traced back to the invention of web-bugs and cookies in 1994 by the software and browser company Netscape. Web-bugs and cookies are extremely small in byte-size and/or invisible graphical elements which are hidden throughout websites and e-mails. These were deliberately developed to be able to collect information and behavior when a user interacts with an e-mail or website. They could gather personal data and extract information from whoever came across them without any discrimination or care, the process is completely automatic and not detectable by the average user of any given internet service or website, unless you have high technical knowledge on how browsers collect, store and transport information (Zuboff, 2020, p. 105). Advertisement firms saw the potential of these small and invisible mechanisms and their ability to gather data from users without their consent.

The Federal Trade Commission (FTC) drafted a proposal to automatically control personal data and privacy laws on the internet. In response the advertisers banded together and demanded to self-regulate instead of the state trying to control what they would call their right to free speech. This is the birth of a cyber-libertarian ideology called *free speech fundamentalism*. In 1996 advertising firms gathered all their experts, from software engineers, scientists and lawyers to craft a spectrum of data collection mechanisms, analytical tools and algorithms into a carefully constructed patent-protected package in the name of free speech (Zuboff, 2020, p. 130). This in turn turned behavioral data into a new market product to be traded, analyzed and transformed. The product of small and large corporations is not to deliver a well manicured service for their users to drive their profit.

Instead the product is a quantitative prediction calculating how likely a user is to click on an advertisement displayed on a website or service. When behavior has turned into a market product we are subject to the forces of the market when we access the internet and it's variety of services, whether we like it or not (Zuboff, 2020, p. 120).

1.2 Discovery of behavioral surplus

In the early days of data collection there was no real logic to the data that was collected through the internet. This is what Zuboff calls *raw material*, it is a collection of random data that users generate when they interact with a website, through it's forms and search boxes. As the internet grew through the early 2000s more users began purchasing products through the internet and used search engines to find content. This is where Amit Patel, a Google engineer saw the potential of these vast amounts of dormant data resources.

The unstructured flood of signals which were generated in the aftermath of any given interaction through a web element or automatic data collection mechanism could actually be constructed to create a detailed history of any user, be it thoughts, feeling or interests (Zuboff, 2020, p. 86). These bi-products of raw material would become known as *data exhaust*. The language of the word itself is carefully constructed through terminology to disguise the actual value of the resource it describes. No individual or entity would care if a company or corporation collects the exhaust produced from a process. It is a purposefully selected word to signal valueless waste (Zuboff, 2020, p. 110).

It is this data exhaust which companies will exploit to further improve and develop their product. This surplus of data exhaust can be considered a *surveillance resource*. Surveillance resources are the main element which creates *surveillance profit* and drives the imperative to constantly extract information from the users to gain as much behavioral data as possible (Zuboff, 2020, p. 93). When the main goal of your profit source is in the collection and extraction of human behavioral surplus it is imperative to find as many supply lines as possible, and these supply lines need to be free from any sort of regulation or friction.

Most online services are now free of charge, all they ask is that you create an account and accept their Terms of Service (TOS). Failure to do so will restrict access to the service or product and render it inoperable or a lesser version of itself (Zuboff, 2020, p. 151). Whenever an entity or state body suggest to regulate an online service they will cry for their freedom, it is this free speech fundamentalism which has driven tech companies to freely navigate and distort the social territories that have yet to be discussed in policy making and law. In the eyes of the tech giants regulation is a negative force which hurts innovation and progress, therefore lawlessness is the required and necessary framework for technological innovation.

Computer and internet technologies are a new phenomenon in our lives, while it has been a point of research since the 1950s it did not become commonplace in homes around the

western world until the early 2000s. The tech companies move faster than what any state or regulatory body could ever comprehend, whenever they try to interfere they have strategies to make any perceived threat to their supply lines waddle and stumble to further restrict and prevent anything and anyone from disrupting the flow of behavioral surplus (Zuboff, 2020, p. 125). This is the essence of surveillance capitalism, to extract all of the data possible from the users who are using their services, applications, programs, operating systems or social media. Analyze said behavior and put it through unknown algorithms and processes which nobody, but the patent holders of the processes themselves have any real knowledge or insight into (Zuboff, 2020, p. 71).

1.3 Monopolization

There is no territory, both digital or physical which can hinder or try to prevent the never ending collection of information and data. Every territory needs to be annexed for the benefit of producing the behavioral surplus from our human existence (Zuboff, 2020, p. 151). It is specifically after the terrorist attacks on September the 11th which causes this exceptional need for surveillance on every plane of existence. It is not enough to just gather the data and try to find people who are willing to do wrong. Both the surveillance capitalists and state actors were yearning for an excuse to further their surveillance exceptionalism, and it is surveillance capitalisms mutation that enables the lucrative and fruitful territories to be exploited (Zuboff, 2020, p. 137).

There is also a constant race of technology. Large companies are essentially forced by the logic of accumulation to constantly acquire other smaller companies that are developing new advanced technology. Some examples are how Meta and Google since the mid-2000s have been acquiring companies that specialize in technologies such as: facial recognition, deep-learning, augmented and virtual reality (Zuboff, 2020, p. 123). These are not random acquisitions, they are carefully planned out to further establish supply lines for gathering human behavior and further expand their own repertoire of applications and services they can provide to their users. Essentially locking them down into their own walled gardens, and at times not even informing their users in an understandable way that their data is being collected when they are using their services.

2. What is Free Open Source Software?

2.1 Definition of FOSS

In the early days of software development it was customary to share and freely distribute software. The reason? Mainly because there was little standardization of hardware. Instead of being specialized in a certain programming language, the early developers were specialized in architectures of hardware and developing direct interfaces with the central processing unit (CPU).

Secondarily there was no world wide internet yet, software was shared through smaller local area networks (LAN), or through physically sending disks and tapes through land mail (Fogel, 2023, p. 3). This gave rise to a community of like-minded individuals whose ideal was to create code of good quality, the idea that software had any sort of market value was non-existent. It was companies like Xerox, and later Microsoft and Apple who saw the potential of locking down source code for their own profit. This would extend all the way to the late 1990s through the development of the operating system Linux, or Netscape's decision to release the source code (called Mozilla) from their browser (Torvalds & Diamond, 2001, p.231).

The terminology and definition of Free Open Source Software (FOSS) is ideological and has become increasingly hard to describe as understanding of the acronym develops (Fogel, 2023, p. 157). FOSS could be a potential candidate to create actual *trustless* systems which are audited by independent organizations or private companies which have good standing the FOSS community. Trustless in this senses does not refer to the definition adopted by the cryptocurrency community. Trustless refers to the fact that no actor needs to be trusted, the systems themselves are transparent and you can see with your own eyes what sort of code is executed locally on your machine. The current solution for companies to gain positive reputation with privacy conscientious communities is to refer to the fact that they have been audited by independent and trusted third parties. Instead of relying on centralized components to verify open source code many decentralized independent parties can investigate and report if the software is functioning as intended (Fogel, 2023, p. 91). To understand FOSS we first need to understand what copyright is in regards to software, secondly we have to look at the ideological and philosophical reasons why FOSS exists.

2.2 Copyright and DMCA

Copyright is part of what is called intellectual property, a modern phenomenon used to establish monopolies of control in cyberspace (Feller, et al., 2005, p. 351). Copyright and intellectual property have been warped to essentially control code and software. The Digital Millennium Copyright Act (DMCA) was enacted by the 105th United States Congress in 1998 (U.S. Copyright Office, 1998). In the DMCA there is an anti-circumvention provision, which states: it is illegal to develop code, that cracks code, which protects content. Even if the purpose for why you are cracking said code is considered to be fair use and legitimate, it does not matter.

Under U.S. Law the act of cracking code is breaking the law (Feller, et al., 2005, p. 355). FOSS is the complete opposite of any software that has been protected by DMCA or any copyright.

Software is a form of content which defines how cyberspace is constructed. Code can determine how free speech works on the internet, on any given site and service. FOSS software lives in the commons, anyone can look at it, build on it, create a new version, or modify it to a better purpose. It also does not need permission. When software is open source it is transparent. We see the mechanisms, the security, the regulation and the protection it offers.

Closed source software, or software that has been protected by copyright, requires the users to trust the publisher of that code, because there is no way for anyone outside to look at it (Feller, et al., 2005, p. 358 & Fogel, 2023, p. 158). Presently most FOSS code is hosted through services like Github and Gitlab using a variety of licenses mainly the GNU General Public License (GPL). The GPL in effect uses copyright law to do the opposite of the DMCA. If a software product uses any code that has been licensed using GPL, the software developer or publisher must open the source code to interested parties if requested by the original license holder (Feller, et al., 2005, p. 282).

2.3 FOSS Hierarchies

Many FOSS projects have contributors and maintainers who are not getting monetary compensation for their work. Some projects establish companies, hire developers and maintainers to further their software. The main motivation for contributors who are not monetarily compensated the expected return can be described as a *balance value flow*.

The main motivation individuals value and contribute to FOSS is pragmatically because it is an opportunity to learn. Developers and programmers also report they take more value out of the project than they themselves give. It is not out of pure altruism developers decide to contribute to FOSS projects. It is an open learning environment where you can gain skills and experience collaborating with others (Feller, et al., 2005, p. 33 & 34). We can further analyze the hierarchy of the sociological model of FOSS.

- *Methodological gurus:* These individuals write and spread the word of FOSS. It can be through personal blogs they themselves maintain, or it could be through participating in organizations like the Open Source Initiative or Free Software Foundation to gain influence.
- *Product gurus:* You can also call this group the maintainers or arbiters of a given project. They decide what code needs to be merged in order to achieve the goal that has been set out to be produced.
- *Contributors:* This group are the programmers who contribute to the ever increasing repertoire of free open source software. If their product becomes successful enough they can become product gurus.
- *Readers:* As the word suggest, they read, criticize and analyze code. They propose changes, find faults in the code. The open source community is heavily reliant on this group at the bottom of the hierarchy. They help with reliability and security in the products (Feller, et al., 2005, p. 87).

It is also worth noting that not *everyone* possesses the necessary skills or knowledge of any given programming language found in a FOSS project. For non-programmers it is a technical impossibility to read and understand code. Even for trained programmers it can be an extraneous exercise to read and understand code that someone else has written. Regular users therefore have to trust that the contributors and readers of an open source project are competent. Is there really any significant difference between trusting code that you can see but not understand, and code you can never see (Feller, et al., 2005, p. 89)?

2.4 Philosophy

One of the leading figures in the philosophy regarding the freedom to use software is the founder of the Free Software Foundation, Richard Michael Stallman (RMS). RMS constantly

states that the word *free* in FOSS does not mean that the software does not have a price, it is about the freedom of said software. It is the destruction and restriction that software can impose on an individual which he takes issues with. This is generally through forcing users to use a certain program, by which the company owns the program and there is no other alternative which is able to provide a support system. With FOSS you are free to either edit the source code itself to meet your needs and requirements, or hire an individual or company who possesses the technical skill or knowledge to fit your needs (Stallman, et al., 2002, p. 38).

Suppose you have a copy of some software, and your neighbor does not. Should a person not be able to freely distribute or make further copies of something that is already a copy of original source code? If a project or piece of software is FOSS whoever owns the copy can freely distribute it to whomever they so choose, if the software is protected by DMCA there are digital rights management (DRM) implementations that prevent any user from seeing or modifying the source code, and making a copy of the already distributed copy is considered illegal. The only person who benefits from this sort of distribution would be the copyright holder. The two neighbors are unable to share the software among themselves, and they are also unable to modify it to suit their needs if the need to do so ever arises (Stallman, et al., 2002, p. 121).

A simple demonstration is just to show what source code looks like:

```
fn calculate_price_of_apples(quantity: u32) → u32 {
    if quantity > 40 {
    quantity * 1
} else {
quantity * 2
}
```

The same code, but at the executable level:

```
1314258944   -232267772   -231844864   1634862
1411907592   -231844736   2159150      1420296208
```

It might not be impossible to gain some meaning or understanding from the above code, but it is much more abstracted and foreign than the original source code. With OSS you can verify that there are no unwanted functions or processes which you might not want on your

computer. With programs that are not open source you have to trust and rely on the developers and publishers of said code to actually not inject or enable nefarious programs when you execute the program. Even when a publisher of a program has promised to disable tracking or other ways of collecting data it has been shown that the program does still track the user, instead of being honest about it, the process runs in the background and essentially becomes invisible to the user (Zuboff, 2020, p. 154).

3 Methodology

3.1 Restatement

In the new digital world it is important to understand how we arrived at this point. The rise of surveillance capitalism did not happen by pure chance or randomness, it is a carefully constructed and designed phenomenon guided by highly rationalized practices which have been enabled by institutions and organizations created before the age of surveillance capitalism ever begun (Zuboff, 2020, p. 101).

It is the Neo-liberal roots of self-regulation which ultimately gave the new tech companies and corporations the power to be able to skirt regulations from state bodies, specifically in the United States where there were attempts from the FCC, to regulate the early forms of surveillance tools like cookies and web bugs. The FCC ultimately failed to cull the rise of self regulated private entities that could pick and choose how these technologies should be used.

While most state laws prevent states from performing overt surveillance on its populace, there are not similar laws preventing intelligence agencies from cooperating and colluding with private entities to gather information and knowledge. This incentivizes cooperation between private business to collect, surveil and generate information (Zuboff, 2020, p. 140). This essentially breaks the barrier between the democratic limitations that are set upon state actors, and is a way for the state to dodge judicial control and operate in secrecy instead (Zuboff, 2020, p. 141).

Free open source software would be the natural counter to the problem of large companies and corporations doing unregulated surveillance on virtually everyone in the world who uses their services. Free open source software has a myriad of issues itself, like the need for technical knowledge or third party auditing of software. This is by no means a trustless system, you still need to trust actors to report the truth when they analyze the code (Feller, et al., 2005, 127).

This essentially is a verification by majority, if a large amount of independent programmers and code writers report the same results it weighs heavier than a company that has exposed its source code to a third party in a closed environment.

3.2 Data Collection

Some of the books which are referenced in this paper have been personally bought by myself. While some books and papers are freely accessible from the internet. I have also confirmed that the books that have been available for free are licensed to be freely used and are either lacking in copyright. This is naturally true for most of the books and papers relating to the FOSS community. They are freely accessible from their sources and such websites will also be referenced in the ending of this paper in the references list.

3.3 Purposeful analysis

This paper is designed to give a purposeful insight into the world of informational technologies and how they are impacting our lives without leaving a trace. Surveillance capitalists have designed their applications, programs and data collection methods to be leave no trace, and to reduce friction between the user and the products they use. Due to patents and secrecy closely guarded by the large corporations who deal in surveillance capitalism, it is hard to find actual empirical data on how, when and why they collect the data they do.

This is why the insights and research from Shoshana Zuboff are of great importance to understand the phenomenon of surveillance capitalism. She has categorized and theorized the various methods these corporations and companies use to establish their profit margins and the pursuit of ever increasing surveillance dividends.

The FOSS component of the research was finding direct sources often written works from themselves. This includes individuals like Richard Michael Stallman (RMS), who is considered to be the father of the FOSS movement, and the developer of the GNU Compiler Collection and the GNU operating system packages. Linus Torvalds is the creator of the Linux operating system and the version control system Git. RMS is considered the more radical of the two in sense of philosophy, together with Lawrence Lessig they developed the GPL, which is the license which gives a lot of FOSS software a lot of power.

3.4 Qualitative Component

The qualitative component involves a critical discourse analysis of academic literature, industry reports, and policy documents related to FOSS and surveillance capitalism. This analysis aims to unpack the conceptual underpinnings, key debates.

The findings of this study are expected to contribute to the ongoing scholarly discourse on the role of FOSS in resisting the extractive and exploitative practices of

surveillance capitalism. The insights generated may also inform policy recommendations and community-driven initiatives aimed at promoting user autonomy, data sovereignty, and ethical technology development.

4 Theoretical framework

4.1 Terms

Raw material is the collected data used by the surveillance capitalists to generate their predictions of human behavior, and is required for this new form of product processing. It is human nature that is being scraped to be used as a commercial product (Zuboff, 2020, p.114).

Extraction imperative is the process of gathering and categorizing data so they can be further analyzed and processed through algorithms that are not known to the general public, but held secret by the surveillance capitalists who are benefiting from the said extraction. The users are not the goal, but they are the means for other people to enable their goals (Zuboff, 2020, p. 107).

Extraction architecture began under the internet. It was considered to be exclusive to the internet, data was extracted there, analyzed, and used for unknown means by the surveillance capitalists. As technology become an integral part of our lives this architecture has expanded to encapsulate almost every space we occupy. An example would be the inclusion of accelerometers in our phones, global positioning systems, thermometers in our homes that are connected to the internet and also autonomous vacuums (Zuboff, 2020, p. 266). All of these devices are connected to the internet and relay the information from their sensors to a server owned by the company which produces these products. Not only do we have to pay for the product, but we are also being monitored by the very products we use in our homes (Zuboff, 2020, p. 152).

One way mirror is an asymmetrical distribution of power and knowledge when we are talking about surveillance capitalism. The surveillance capitalists have access to all of our data, all of our behavior on the internet and our user profile indexes (UPIs). We on the other hand have no access to how they use the data and why. This is also a form of forceful social relation where the user has no choice but to comply to the means of the surveillance capitalist (Zuboff, 2020, p. 100).

Accumulation logic is a new law of motion where information and knowledge has become the new material for rapid growth. Surveillance capitalism has established a new economic form to get new connections and information which can be used to further enormous growth and profit in the economic world. This new logic did not suddenly appear, it has been fostered by the Neo-liberal institutions which has efficiently established surveillance capitalism. Any attempt to dismantle or undermine this new logic will be met with long established institutions which are incentivized to keep this new market form alive (Zuboff, 2020 p. 70).

Surveillance logic is a result of the accumulation logic and collection imperative which is the main drivers for keeping surveillance capitalism secret and hidden from its users. The commercial potential is the cause and logic of the aggressive extraction and storage of data (Zuboff, 2020, p. 108). Ever since Google discovered the behavioral surplus it has been important for all surveillance capitalists to continue the secrecy, because they are extracting something from their users without asking for their consent or permission (Zuboff, 2020, p. 109).

Surveillance in this theory can be boiled down to four points.

1. Extraction and analysis of data
2. New contractual forms because of surveillance (eg. ToS)
3. Personalization and adaptation
4. Experimentation

Firstly the whole purpose of surveillance is to gather information and knowledge to be used for some unknown purpose, afterwards it is analyzed. Secondly we can see new forms of contracts being established whenever we use any sort of website, these contracts are purposefully written with such language that any user will never read it fully, or fully comprehend it. Thirdly, the content of websites adapt to your personality, content is developed and procured based upon the data which has been collected and analyzed by the corporation delivering the service. Lastly, new services and technologies constantly pop up within surveillance capitalism. The main goal is to try to find the supply line which will deliver the most growth and profit (Zuboff, 2020, p. 83).

4.2 Interconnection

When a human interacts with any system connected to the internet, a vast amount of information is generated, both from the actual interaction, but also from data points which are not as visible to users. This can range from anything from:

- How long did a user hover over any given element on the web page?
- What website did the user come from, and what was the next website they visited?
- Location, date and time-related information
- How long did they scroll until they found relevant information or links?
- What link did they click on when they found the content they were looking for?

These information at first might seem random, but it's through the use of algorithms and data processes these data are eventually given a new life (Zuboff, 2020, p. 93). When a user has generated enough information for a system a new category is generated called the *user profile index* (UPI). This process establishes the ability for surveillance capitalists to better predict how any user will act on a site and is the main source of revenue companies that deliver or auction off ads will earn their profit from. It is not merely the ads themselves that are the product it is the prediction that can be produced when UPI is processed through a myriad of algorithms and machine learning processes which is the product of surveillance capitalists. Not only are these data gathered from the services and products they deliver, but third parties are also selling information from their own services and connecting them to their own existing users. This is what Zuboff calls *interconnection* (Zuboff, 2020, p. 97). This is where exclusivity and monopolization kicks in again. It is important for the services and products which surveillance capitalists provide to be as user friendly and convenient to the user as possible. This is mainly to reduce the social friction, this friction arises when a user does not freely contribute information about themselves, and these companies need to "outsource" the data that they can gather.

4.3 Supply and Demand

We have become the marketplace for large surveillance capitalists. We are no longer the consumers or buyers, we are the raw material for their unknowable and secret processes. In the electronic and technological marketplace you can constantly see new announcements of new services and how new technology will make our lives easier and to relieve our burdens.

Currently the newest fad, which scientists have tried to accomplish since the 1980s is the rise of generative pre-trained transformers, also known as GPTs. The tech world has cried of its usefulness across all sectors and how it will transform how we do work, teach and learn. What they always fail to mention is that GPT models are trained on data they have collected openly on the internet through application programming interfaces (API) and the prompts that users ask the GPT.

While services like ChatGPT, Gemini or Meta Llama 3 might seem useful on the surface the main goal of such a service is to find out as much as possible about you. It is no surprise it is using a chat format for its user interface (UI) and has pleasant user experience (UX). It wants to break the barrier between human and machine, it wants the conversation to be casual and easy, with fast replies. It will only be a matter of time until this technology is incorporated into every application, operating system and chat system. Of course users will want to use this technology because it can actually be quite useful when the outputs are correct, but the main selling point for surveillance capitalists are the actual fact of the matter that this is the newest and most efficient form for them to collect information, which in turn creates behavioral surplus which they can use to further their predictions (Zuboff, 2020, p. 152).

If a service or technology fails however they are easily discarded. If they do not meet the quota for knowledge or information gathered the large corporations can easily swallow the cost of research and development if it means that some other technology or software can take its place. You can also see this practice when large companies constantly buy smaller companies which have some sort of prospective technology (Zuboff, 2020, p. 123).

4.4 Prediction Imperative

Through algorithms and data processes it is possible for surveillance capitalists to generate predictions which are based on the behavioral surplus they have access through the extraction of raw material from its users. These prediction processes are not only used to predict the behavior of humans, they are also used to further affect the actual behavior of the users who interact with content generated by the services and mediums which are hosted by the companies and corporations. This attempt at predicting and controlling behavioral influence is steering all other operations in the direction of total information and control which will inevitably create an instrumentarial power which has no precedence to no state, government or ideology (Zuboff, 2020, p. 85).

Due to the miniaturization of electronic chips the start of the 21st century saw an increase in wearable electronic devices. This definition extends to watches, phones, earphones and headphones.

4.5 Bridging the Gap

Due to the miniaturization of electronic chips the start of the 21st century saw an increase in wearable electronic devices. This definition extends to watches, phones, earphones and headphones and the interconnection is especially evident when it comes to technologies such as Google Maps and Street View. Google The success of Pokemon Go, which was a joint collaborration between Niantic Labs and Google (Zuboff, 2020, p. 352). Led to the discovery that you could place virtual Pokemon in an augmented reality (AR) world, which would naturally bring excited players to physically move to those place to catch their personal favorite or rare Pokemon. This phenomenon is defined as *footfall*, this is considered an economy of action. A business or public place can buy what is known as a “PokeStop”. A PokeStop is essentially a token that does not exist in the physical world in a conventional sense. The PokeStop can represent a statue, a park or a business. The function of the PokeStop in the game is that a player can gain items if they are in proximity to the PokeStop, and it also generates more Pokemon to be revealed in the game if you are closer to it (Zuboff, 2020, p. 354). Businesses started to see that they could buy

5 Discussion

5.1 Closed Source vs. FOSS

Every electronic device which touts the moniker “smart” are typically filled to the brim with methods to communicate with hidden servers, which are difficult to track for the average person. They can extract anything from sounds, user inputs, the users clipboard, pictures on the phone, calendar events etc. and send that information to said server. Of course the user has to give permission to the application to gain access to this information, but if you choose to deny said access, the application will not function, or it will limit its capabilities to give you a lesser experience when using the application (Zuboff, 2020, p. 269).

On the other side FOSS applications are usually run locally on your device. If they connect to an external server or require another service to function it is explicitly shown in the source code of the application or program. Independent individuals can report to the

community of said software or development team about what sort of information is being extracted by executing the program. This does not however mean that reporting to the community is a guaranteed way of informing the users of the operational methods the corporation uses to extract data from them (Gwebu & Wang, 2010, p. 2289). They are of course legally required to inform the users in their ToS about any data they are extracting. It has although been shown that these companies still use secret extraction methods even when they explicitly tell their users that the feature will be disabled if they so choose (Zuboff, 2020, p. 125).

This also goes back into the effectiveness of FOSS. While the source code might be visible and public for anyone to see, there might still be "in-house" code that runs on the *backend* of the servers that are communicating with the software locally on your computer. Swiftly explained the backend is considered the background processes of software usually executed on an external server. When you connect to a website what you see is the front-end, the visual elements, the animations, images. The backend on the other hand is somewhat invisible to the regular user. Databases, information gathered from forms, login credentials and encryption are considered backend.

5.2 Disruption

It is hard for anyone to determine what kind of software is running on the backend of a server. If a company or corporation is using FOSS it might be changed locally in their environment to better suit their needs (This also depends on the kind of license of the FOSS). One way to achieve this is to run your own firewall which can detect the domain name system (DNS) calls on your network. Most routers and modems in modern homes has this functionality but it is often hidden behind complicated interfaces on the routers' hosted website, and has to be set up manually.

Certain software also has the ability to block DNS calls on your network, like Portmaster which is a free open source software program which runs locally on your device and tracks every DNS call made on your system. Every modern browser has the ability to manually set its own DNS server which can have built-in filters for advertisements, malware, trackers or fake websites.

It is convenience of the default browser configuration, default router and modem, default search engine, default operating system which makes us ignorant to the processes that

are performed on our data and information. The rights to a private space has been violated, and we have become helpless and resigned about the topic of being private on the internet, on the services, social medias and chat applications (Zuboff, 2020, p. 114).

The market also tried to provide services which would ease the mind of its consumers, virtual private networks (VPN) is not a new technology and was frequently used in enterprise and corporations. It quickly became marketed as the saving grace from getting the prying eyes of large corporations, your internet service providers and trackers. The main claim most VPN providers showcase is the fact that they do not log the activity when you crawl through the web using their services. This of course relies on the trust of a third party as mentioned earlier, there is no way of knowing if a VPN provider keeps logs from their users activity, only their word. While this seems to be an efficient way to create friction between the users and surveillance capitalism the case is that if you log in to any service or social media with your regular account, there are mechanisms and algorithms that can easily track you even if you are using an encrypted VPN (Zhou & Huang, 2021, p. 3) . The encryption and anonymity a VPN provides only works if you never log in or authenticate yourself with a user account on services.

Zuboff in her book calls for friction. Make it as hard as possible for the surveillance capitalists to extract data from you. This can be as simple as deactivating your account, or just not using the service or social media all together. The problem is also that a lot of our friends, family, work life and acquaintances are using these services to connect to each other. The most mainstream are run by surveillance capitalist corporations like Meta, Google, X, Reddit or Snap. The FOSS space is still young in this area, while there are a plentiful of encrypted chat applications, there are few that can replace services like Facebook, Instagram or Snapchat.

The social media called Threads by Meta has support for the protocol called ActivityPub. The protocol is a proposed standard by the World Wide Web Consortium (W3C) from 2018 and has been adopted by FOSS activist and turned into what is called the *Fediverse*. The Fediverse is a social media connection system that uses decentralized instances to provide similar services like X and Reddit. Recently Meta announced they would connect Threads to the Fediverse and would add a centralized component to the instances. This was met with calls to *defederate* from Threads, meaning no user in an instance which has defederated can view, create or contact users on Threads and vice-versa (Webber, 2018).

This was also a showcase of the FOSS community creating friction between a large surveillance corporation from trying to extract data from them. Users on Fediverse sites often refer to themselves as “refugees” from the other mainstream social medias.

Another form of being friction would be using an anonymous e-mail when you sign up to a service, or using a different first and last name, address etc. This is called *data poisoning*, and is one way to combat the collection of data and the generation of UPI (Steinhardt, et al., 2017).

If we want to maintain the control of our digital lives we need to begin making certain sacrifices regarding our use of large services and social medias on the internet. To meaningfully battle surveillance capitalism you need to become friction, disrupt the flow of information which is being extracted, analyzed and processed every day. Using FOSS alternatives to popular software will remove you from the pool of individuals who are getting their data and information taken from them.

6 Summary

There is no question our data is being extracted by large companies and corporations in the name of profit and the potential to establish economies of action and predicting and influencing human behavior, based upon digital behavior when we search, navigate and supply content to various services on the internet. An option to combat these methods deployed by surveillance capitalists is to use alternative software, specifically free and open source software where members of the community can report and inform users independently about the processes and mechanisms that exist in the code.

More research needs to be done on FOSS projects and how they disrupt or even supplement the other services from surveillance capitalists. There has been a surge the last few years of privacy focused software that promises its consumers to take back control of their own data.

7 References

Feller, J., Fitzgerald, B., Hissam, A., S., Lakhani, R., Karim. (2005) *Perspectives on Free and Open Source Software*. MIT Press.

Fogel, K. (2023) Producing Open Source Software: How to Run a Successful Free Software Project (2nd Ed.).

Gwebu, K., L., & Wang, J. (2009). *Seeing eye to eye? An exploratory study of free open source software users' perceptions.* The Journal of Systems and Software.

Stallman, M., R., Lessig, L., Gay, J. (2002). *Free Software, Free Society: Selected Essays of Richard M. Stallman.* GNU Press.

Steinhardt, J., Koh, W., P., Liang, P. (2017). *Certified Defenses for Data Poisoning Attacks.* Stanford University.

Torvalds, L., & Diamond, D. (2001). *Just for FUN: The story of an accidental revolutionary.* Harper Collins Publishers.

Zuboff, S. (2020). *Overvåkingskapitalismens tidsalder: Kampen for en menneskelig framtid ved maktens nye frontlinjer.* Spartacus Forlag.

Webber, C., L. (2018, Jan 23). *Victory for libre networks: ActivityPub is now a W3C recommended standard.* *https://www.fsf.org/blogs/community/victory-for-libre-networks-activitypub-is-now-a-w3c-recommended-standard*

Zhou, Z., & Huang, T. (2021). *Open VPN Application in COVID-19 Pandemic*. Journal of Physics