Martin Foucaut

Hidden in plain sight:
Understanding our consent and distrust in the context of capitalist techno-surveillance

_____

A thesis submitted to the Department of Experimental Publishing, Piet Zwart Institute, Willem de Kooning Academy, in partial fulfilment of the requirements for the final examination for the degree of the Master of Arts in Fine Art & Design: Experimental Publishing.

_____

Adviser: Luke Williams
Second Reader: Steve Rushton
Word count: 7958 words

Introduction

> "How can we be devoted to a technology that is marketed as our servant?" (Seymour, 2019, p. 54)

Have you ever been anxiously waiting for feedback on your most recent online publication? Have you ever been relieved to see your notification bar filled with likes and comments? Have you ever felt proud to be followed by someone you admired for so long? Have you ever found yourself passively numb by the infinite flow of text and images displayed to you? Have you ever found yourself almost unconsciously checking the upper right corner of your screen? Have you ever felt envious when confronted by the successful image of your friends and idols? Have you ever felt discriminated by the beauty standards promoted on some platforms? Have you ever felt that your smartphone vibrated when it didn't?

If you have ever felt this way, you may be like me and like some of the other billions of online users who find themselves constantly interacting with technological devices. When being online, even the most innocent action can be invisibly recorded, valued, and translated into informational units, subsequently generating profit for monopolistic tech companies. In an attempt to capitalise on the last remains of our attention, tech firms have gone as far as to create addiction machines by exploiting our deepest desires and biases. And thanks to the tremendous amount of money earned from the data we freely provide every day, this influence continues to take up our time, sleep, bodies, spaces and shape our behaviour, perception, and identities. That being said, the following questions I would like to ask the reader are:

Is being aware of this reality enough to start individually or collectively subverting, bypassing, or boycotting these tools? On the contrary, are we not fully participating to our alienation?

When writing this thesis, I still find myself investigating the effects of tools that I am not yet able to distance myself from. My connected devices, creation software, or social media accounts still appear as important vectors of my daily entertainment, professional practices, and social interactions. This paradoxical posture defines itself as a state of rejection, concern, or disapproval in contradiction with a form of consent, entertainment, and interaction with the tools, allowing this economic surveillance to exist. In a sense, these conflictual feelings could be compared to the drives of some drug addicts or gamblers to get high or bet all their economies with full knowledge of the risks involved.

> "The problem is, widespread knowledge of the dangers of addiction doesn't stop it from happening. Likewise, we know by now that if social industry platforms get us addicted, they are working well. The more they wreck our lives, the better they're functioning. Yet we persist." (Seymour, 2019, p. 58)

To understand this paradox and the dilemmas it leads to, we will first look at the economic model lying between us and the interfaces that we use and, likewise, use us every day.

The first step is to understand the model of surveillance and attention on which many of the tools and services we use are based and to situate this economy within the broader historical framework of the Internet. We will learn how and when this business model emerged, how it evolved, and who we are inside this economy. Finally, as a clue of the widespread datafication and the culture of surveillance that emerged from this economy, we will observe how tech firms tried to legitimise prac-

tices of surveillance and self-surveillance through the promotion of tracking apps and data-driven advertisements.

Secondly, we will investigate the perverse effects of the interfaces built to mobilise our attention, stimulate our interactions, obtain our consent, and create addictions. We will study the implementation of gamification, gambling and lottery systems in various connected devices and online platforms, as well as question their effects on online users. By closely following these companies' expansionist logic, we will also investigate the intrusion of these surveillance tools in our physical environments and our bodies, leading towards an entirely datafied society.

Finally, we will consider other perspectives on the culture of surveillance and self-surveillance that we live in, notably through the exploration of counter-practices, alternative tools, and critical and activist works.

Chapter 1: Homo Data

Have algorithms taken control of our brains? Have we become the willing slaves of platforms, which under the pretext to entertain and educate us, do not hesitate to manipulate us to convert our precious data into dollars?

—

According to some studies, the leading online platforms mobilise our attention for an average of 2.5 hours a day, a figure constantly increasing among all age groups and exceptionally high for the youngest generations. (Stewart, 2016) This realm results from an economic strategy based on mobilising a maximum of users' attention to collect and resell their data. In this attention economy, the tech firms have aimed to develop increasingly addictive and distracting tools, notably by emotionally stimulating us with virtual rewards (likes, thumbs up, badges, followers), making us stay with an endless flow of recommended content and keep us coming back with persistent notifications.

> "(…) they miss you, they love you, they just want to make you laugh: please come back." (Seymour, 2019, p. 20)

Before studying the mechanisms used to maximise our attention online, let's head back two decades. During its first years of existence, between 1998 and 2001, *Google* possessed an already overwhelming amount of data collected from its early users. At the time, as the company publicly positioned itself against the presence of advertisements in its search engine, this information was mainly used to improve the referencing/indexing system. However, later on, this growing quantity of informational units found their true lucrative potential by studying and selling users' behavioural data for advertising purposes.

> "Ironically, it was contempt for advertising (on the part of the founders and chief engineers) that would ultimately pave the way to the company's unrivalled success as an attention merchant. The key was in renegotiating the terms under which the public was asked to tolerate ads. It presented what seemed a reasonable trade-off. So unintrusive was AdWords that some people didn't even realise that *Google* was ad-supported." (Wu, 2016, p. 5)

Thus, by remaining free while subtlety inserting advertisements in its search engine, *Google* would go from gaining almost no financial benefit to outrageous profit until this day. While this business model was already used in some other industries, such as television and printed newspapers (Wu, 2016), the democratisation of the Web and the lack of rules concerning Internet users' privacy allowed *Google*, as well as a handful of other companies (such as *Baidu*, *Facebook*, *Microsoft*, *Twitter*, *Yahoo* or *Verizon*), to acquire a dominant status in their respective sectors.

Until the last ten years, when the first real signs of discontent started to grow, it was still considered that these services were aiming to make our lives better, improve our working and living places and connect us. Even for a minority of geeks, journalists, and researchers writing about the subject, such as Soshana Zuboff, their main objective long appeared to be led by the desire to allow users to get what they want, on their terms. (Morozov, 2019)

However, since some events, such as the Cambridge Analytica scandal, the January 6 U.S. Capitol riot, or the recent revelations made by ex-employees of *Facebook* (Slotnik, 2021), we are witnessing a growing mediatisation of the issues related to the services provided by tech giants. Among the long list of topics addressed are notably the political interference linked to the proliferation of false information, the resale of personal data to obscure third parties, the abuse of a dominant position towards concurrent companies, and the significant increase of psychological disorders among social platforms users.

Today, despite growing disillusion and distrust about the real intentions of the tech industry leaders, we come to observe a paradoxical willingness or even enthusiasm from most people to continue using these tools and to share information about themselves. In most cases, people share personal information of their own free will through likes, publications, tweets, comments, photos, and videos, allowing them to build their online alter-ego, publicly confess, and represent themselves to the online world. But this enthusiasm doesn't stop there and can be further exemplified by the emergence of wearable self-tracking devices, which in the last 15 years have allowed users to track themselves and legitimise the datafication and marketisation of the body.

Beyond self-tracking practices and the quantified self (which we will return to later in this essay), some companies also tend to use data-driven methods as a public marketing tool. *Spotify*, for example, has launched an advertising campaign revealing its users' musical habits and personalities in the form of humorous messages. "Dear Person who played "Sorry" 42 times on Valentine's Day – What did you do?" (fig.1) (Kholeif, 2018). While these messages do not necessarily reflect how data mining works, it could be said that this advertising strategy appears to try to normalise monitoring practices in the eyes of society.

fig.1

The emergence of such communication strategies and the globally positive feedback from consumers are the signs of our ambivalent feelings towards these tools, which we seem to worry about as much as we seem to confess and depend on.

—

At around 13 years old (2008), I started engaging in my first forms of online social interaction through conversations on online games, forums and language exchange websites. These allowed me to interact with foreign people I would not have had the chance to meet in my familiar environment and even carry friendships that continue until now. In the middle of that, during my junior high school years (2005-2011), Facebook quickly became very popular and, to put it mildly, quasi-necessary to each person of my generation. For people like me, who weren't yet part of the club, it was like having the feeling of constantly missing out on something that the others would know about. Questions like "Can I add you on Facebook?"; and "Do you have Facebook?" were pervasive. I resisted the temptation for some time, but it wasn't until a few years later, after a failed integration into my new high school, that I decided to become a member. Until today, my profile publicly displays my entry date on the platform on January 1st 2012, a date that sounds like a 10-year-old resolution to re-socialize by the new standards.

Chapter 2: Addiction machines

Have you ever found yourself compulsively checking your phone at random times of the day and night? Have you ever feared missing something when not checking your feed for a long time? Have you been afraid to lose all your online followers forever?

—

In 2021, just over half of the world's population had access to the Internet. A majority (93,33%) had social media account(s). Among some of the most popular ones, 2,9 billion active users are currently registered on *Facebook* [*Meta*], 2,5 billion users on *Youtube* [*Google*], 2 billion on *Whatsapp* [*Meta*], 1,3 billion on *Facebook Messenger*, 1,2 billion on *Instagram* [*Meta*], 1,2 billion on *WeChat* [*Tencent*], 1 billion on *Tik Tok* [*ByteDance*], 740 million on *Linkedin* [*Microsoft*], and 353 million on *Twitter*. (Kemp, 2021) While these numbers could impress, it should be noted that the condition of access to the Internet can be affected by various economic or geopolitical factors within each country/region. As a result of a lack of means or limited access to electricity, various parts of Eastern, Central and Westen Africa, as well as central Asia, do not have regular access to the Internet. In some countries such as China, Cuba, Ethiopia, Iran, Russia, Saudi Arabia or Sudan, governments have sometimes created their own social platforms/messengers or taken over existing ones to apply more governmental control and censorship. (Unesco.org, 2010)

Nowadays, most leading online platforms and tech brands rely on our willingness to share information about ourselves. Given this, one of the central questions of this thesis is to understand how such companies encourage our participation in an economy that, paradoxically, exploits us.

> "Is it possible that in their voluntary communication and expression, in their blogging and social media practices, people are contributing to instead of contesting repressive forces?" (Hardt & Negri, 2012, p. 137)

As argued by Richard Seymour in *The Twittering Machine,* it is first essential to understand that when we do such innocent actions as searching, looking, clicking, scrolling, or purchasing products online, we are collectively writing to the machines. (Seymour, 2019)

> "The nuance added by social industry's platforms is that they don't necessarily have to spy on us. They have created a machine for us to write to. The bait is that we are interacting with other people: our friends, professional colleagues, celebrities, politicians, royals, terrorists, porn actors – anyone we like. We are not interacting with them, however, but with the machine. We write to it, and it passes on the message for us after keeping a record of the data. The machine benefits from the 'network effect': the more people write to it, the more benefits it can offer until it becomes a disadvantage not to be part of it." (Seymour, 2019, p. 10)

Because of this invisible layer, it is mostly unconsciously or unwillingly that we participate in a social industry where platforms take the shape of giant virtual laboratories with millions, if not billions of guinea pigs. At first and all along, our participation is never forced. However, we quickly find ourselves navigating inside interfaces that persuasively stimulate our desires, twist our emotions, and

keep us hooked by any means. While remaining "hidden in plain sight", this invisible layer allows ideologies to pervade "the most quotidian aspects of life." (Debord, 1995, p.138)

As argued by Seymour, social media platforms have become some sort of "rigged lottery systems", (Seymour, 2019, p. 20), giving users/gamblers an impression of constant wins and objective randomness by feeding users with intermittent variable rewards. In reality, the users/gamblers always lose, but their "lost", disguised as "wins", encourage compulsive play and persuasively keep them playing.

> "Something similar happens when we post a tweet or a status or an image, where we have little control over the context in which it will be seen and understood. It's a gamble." (Seymour, 2019, p. 53)

As in many gambling games, the idea remains that supposedly anyone can win big almost instantly, no matter how ephemeral or artificial that fame can be. But as with many types of addiction, it is also essential to consider that absolute pleasure is not necessarily found in the moment of winning (if ever that is possible). Instead, the joy can be found when players dislocate themselves from time, from their bodies, and find themselves numbed only by the idea of winning.

In some cases, we observe that some of the ways the interfaces work are becoming even more explicitly related to gambling mechanisms. As one of the most prominent examples since the last decade, we have witnessed platforms such as *Facebook* implementing "social media games" (games within social media platforms), allowing users to play for free but also encouraging them to purchase tokens, chips, and items with real money.

The *Instagram* recommendation page also has something very similar to a slot machine. When scrolling up at the top of the home page, the user can automatically refresh the page and display a new set of randomly recommended content as many times as needed. (fig.2)

fig.2

On these platforms, the fact that the most "popular" content and profiles are being highlighted in the recommendation feed actively entertains the fantasy to become popular or even famous. As exposed by Guy Debord already fifty years ago, the post-war consumerist big bang gave birth to a "celebrity culture", "society of the spectacle" (Debord, 2014) or what could even be called a society of self-performance.

> "The status of celebrity offers the promise of being showered with 'all good things that capitalism has to offer. The grotesque display of celebrity lives (and deaths) is the contemporary form of the cult of personality; those 'famous for being famous' hold out the spectacular promise of the complete erosion of an autonomously lived life in return for an apotheosis as an image. The ideological function of celebrity (and lottery systems) is clear - like a modern 'wheel of fortune,' the message is 'all is luck; some are rich, some are poor, that is the way the world is...it could be you! " (Jenkins quoted in Debord, 1995)

Online, the obsession with visibility leads numerous people to adapt their way of interacting and posting depending on the ever-changing algorithm logic. Within this new algorithmic governance, each new update leads communities of users, influencers and content-creators to calibrate their behaviours and contents to a new set of mystified parameters. On *YouTube*, for example, countless videos will guide you through the best ways to get your content displayed on the recommendation pages, often by trying to catch the viewer's attention for as long as possible (fig.3). On *Instagram*, some will suggest you to post, like, and comment daily or during peak traffic hours. On *Spotify*, numerous song-makers are even willing to collaborate with search engine optimisation companies to know which artist, song, or album names and formats would get the best chances to get highlighted by the algorithms. As a symptom of this "fame rush", we are witnessing a limitation of the variety of content being recommended on these platforms, often revealing recurrent patterns among the most popular content. However, making content that achieves significant visibility or feedback (likes, comments, subscriptions, etc.) remains quite unpredictable.

fig.3

By extension, it is also how users consume content, navigate through interfaces or interact with them that become subject to the same limitations. User's behaviours are industrially automated to keep them passively stuck in the loop of watching, scrolling, swiping, watching, liking for as long as possible.

In exchange for their labour, users are rewarded with likes, hearts, comments, responses, followers, subscribers, fans and friends, symbolised by stimulating visual feedback such as hearts, thumbs up, stars, and stats. To be effective, these visual stimuli play with our psychological vulnerabilities by feeding our instinctive need for social validation, self-display and extensively creating the fantasy of accessible and quantifiable fame.

Since its first appearance on the video-sharing site *Vimeo* (2005) and its popularisation on *Facebook* (2009), the "like button" has become one of the best motives for users to log in, be active, interact, and come back on social platforms. In 2015, when the "like button" started to feel too limited for its users, Facebook, in return, implemented additional reaction buttons in the form of emojis, allowing them to express different emotions (heart, sad, happy, angry, supportive, surprised). This update would respond to the user's demand but also allow the company to know more accurately how users react to content and sell such information to third parties. (Tian et al., 2017)

> "Our results show that there is a reliable correlation between Facebook reactions and emoji usage, suggesting that emojis can be used to detect users' sentiments if we take into account contexts where their meanings are modified (used ironically or for politeness). This study also demonstrates that Facebook reactions and comments are a good data source for investigating indicators of user emotional attitudes. " (Tian & al., 2017)

As argued by Adam Atler, author of the book *Iresistible* (2017), another determining factor in how we consume online content and become addicted is the absence of stopping cues in the content feed. With more traditional media such as newspapers, books, television, or radio, contents usually have a transition or a stopping time, naturally leading readers/viewers/listeners to do something else. However, with social and streaming platforms (such as *Netflix, Youtube, TikTok, and Snapchat*), the auto-play is either settled as a default setting (*Youtube, Netflix*) or part of the entire concept of the platform (*TikTok, Instagram*). By doing so, interface designers are appealing to another human cognitive bias commonly referred to as the "default choice", putting users in the middle of an endless stream of recommended content and encouraging their passivity. (Atler, 2017)

> "As if that wasn't enough, in 2014, Youtube introduced the autoplay feature to its main site. Now, instead of having to click on the next cat video, the video will play automatically after a brief countdown. This may seem like a small adjustment, but by creating the autoplay feature, Youtube effectively created a default setting, and because our brain tends to go with the flow, we default right along with it. " (Johnson, & al., 2020)

Stuck inside these feedback loops, it is no surprise that such patterns can lead some users to develop different degrees of addiction and, eventually, suffer from mental health issues. Thus, while links between social media addiction and mental illness are still being intensely studied and debated, symptoms such as depression, anxiety, bipolarity, eating disorders, or attention deficit are increasingly diagnosed. In a research paper from the Journal of Affective Disorders (Mahalingham et al., 2022), some researchers studied potential links between social media use and psychological distress. Ultimately, the research evidenced that heavy social media use may cause problematic mental health consequences among those who experience difficulties with attention control. Among the symptoms experienced by these specific subjects, it has been noticed that the subjects were more susceptible to creating unobtainable ideals and experiencing exacerbated feelings of depression and anxiety.

> "Substantial proportions of individuals report negative impacts on home, social and working lives from digital technology use, with many trying but failing to cut down use. Individuals

with higher DOAT[1] may experience improvements or worsening in self-esteem and other measures of mental well-being when using the Internet for health purposes. From a public health perspective, a greater understanding of risk factors for digital overuse, its impacts on well-being, and how to reasonably limit the use of technology are critical for a successful digital revolution." (Bellis & al., 2020)

While it is often considered that a limited use can also show beneficial effects (Small & al., 2020), users struggle to use such tools with moderation. Faced with this situation, some key questions are: How far are big tech companies willing to go to make us addicted and engaged? Where could this business model extend to? What are some examples of capitalist surveillance practices that apply to the physical world? How do self-tracking practices allow tech firms to gather and sell even more personal information about their users?

—

While writing this thesis, the course of my thoughts can often be interrupted by a desire to glance at my social platform feed, reply to a message/mail, or check my phone. In this sense, my writing work can often be disturbed by the attention mechanisms I am trying to study. As an example, because of the few amount of interactions I have on Facebook, the platform randomly notifies me with messages such as: "You have a new friend suggestion:" "This person shared a link", "This person shared an event that might interest you", or "you might like this page". While such information has no significant importance, I still find myself checking my home page with remarkable consistency every day, as if out of a fear of missing out.

---

[1] DOAT: Digital Overuse and Addictive Traits, "DOAT was measured using self-reported questions adapted from a social media addiction scale (failure to cut down use, restlessness when not using, and impact on job/studies and home/social life in the last year), combined into a single DOAT score" (Bellis & al., 2020)

Chapter 3: Self-empowerment

Have you ever felt comforted by the possibility of checking your daily step counts, your heartbeat and your followers daily? Have you ever adapted your actions/behaviour on behalf of this data? Have you ever felt that you could have disappointed a machine? Have you ever felt like your body was a device? Have you ever wondered who else could access your information and for what purpose? Have you ever tried to delete or suspend a social media account before ultimately reactivating it?

—

"To make people believe is to make them act." (Certeau, 1984)

In his book *Discipline and Punish: The Birth of the Prison* (1977), Michel Foucault describes the rise, from the 16th century onwards, of a new type of power applied to people, the population, and no longer exclusively to land and countries. For that, this power will be interested in what should be the life, the body, and will use new techniques centred around the discipline. Biopolitics aims to control the deepest corners of the individual, to integrate the living into politics. In short, to control more and more intimate parts of people to achieve its goals. The metaphor that Foucault uses to represent this is the panopticon (1977, p.95), a building invented by the philosopher Jeremy Bentham at the end of the 18th century, with the goal of better controlling prisoners. (fig. 4)

fig.4
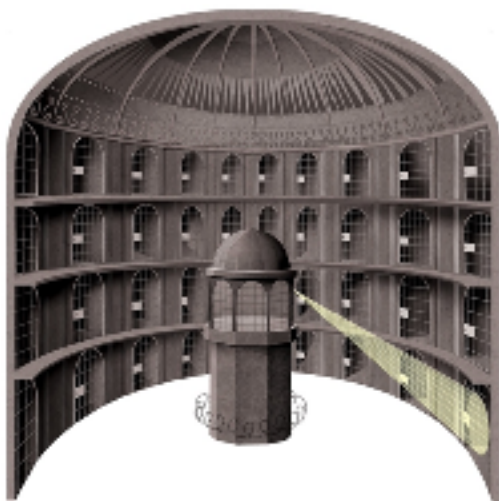
The overseer, hidden in the centre of this building, cannot be seen but instead can see everyone's actions without knowing who and when she/he is looking. Since the prisoners cannot know when they are being watched, they will constantly act as if they are under surveillance, eventually changing their behaviour from day to day in a more desired way. Bentham, at the time, was inventing this as part of his utilitarian view of life, aiming to maximise utility and the amount of happiness produced.

This example illustrates what Foucault describes as a modern power. This power observes its population with permanent measurements through biopolitical techniques such as statistics, allowing, for

example, to know the birth rate, the age pyramid or to determine social groups inside a population. This relationship of power that shifted from visible > invisible to invisible > visible, thus, can serve all sorts of political or economic purposes. In this realm, the population is segmented into different groups on which a piece of knowledge is created. This behavioural model will make it possible to identify and punish individuals who do not behave according to the expected norm. Therefore, this knowledge aims to control each body and gesture with the minimum of means necessary for its application and maximum coordination.

As one means to apply control on the masses, Foucault quotes four technologies such as the technology of production, sign systems, or power and what he calls the "technology of the self". As it can be understood, the "technology of the self" is a form of power that is not necessarily only applied from one subject to another subject but also by the subject toward himself. In Foucault's disciplinary society, the subject internalises its own position. It develops knowledge about itself based on another behavioural model, which will affect its own behaviour. In that context, humans can operate their own surveillance and self-regulation.

> " (…) technologies of the self, which permit individuals to effect by their own means or with the help of others a certain number of operations on their own bodies and souls, thoughts, conduct, and way of being, so as to transform themselves in order to attain a certain state of happiness, purity, wisdom, perfection, or immortality." (Foucault, 1982)

Beyond applying this model in the military, prisons, factories or corporations, the form of power described by Michel Foucault over 40 years ago is now widely applied to humans through the Internet, where tech companies can now afford to achieve a degree of omniscience and influence that no kingdom, government or organisation could ever have achieved before. Also, as evoked earlier with the example of wearables, tech firms even encourage people to contribute to their own surveillance, track their bodies and transform the last remains of their existences into data.

> " The recent proliferation of wearable self-tracking devices intended to regulate and measure the body has brought contingent questions about controlling, accessing, and interpreting personal data. Given a socio-technical context in which individuals are no longer the most authoritative source of data about themselves, wearable self-tracking technologies reflect the simultaneous commodification and knowledge-making that occurs between data and bodies." (Crawford, et al., 2015)

In order to encourage people to these practices, all kinds of pretexts can be highlighted, such as public safety, healthiness, well-being, and self-management. All these pretexts reinforce the idea of the human being an entrepreneur of their own life and draw towards the concept of a "society of self-performance". Sport and health apps have been some of the first to promote the visualisation and public sharing of daily performance to the mass market. Doing so would allow humans to regulate their behaviour based on their data and encourage them to give away some of their most private information, which could then be sold to third parties such as advertisers and insurers. (Bernard, 2015).

> "With the innovation of wearables, this belief has come to a new dimension. Now, it is not only the individual relating to its own numbers, but the bodily self-regulation through the aggregation of the data of many individuals." (Crawford, et al., 2015)

Far from the unfriendly interfaces of financial stock markets or military devices, regular people's use and sharing of complex information have also been made possible thanks to the embellishment of

the data, mainly done through UI (User Interface), UX (User Experience) and graphic design (fig.5). Uncluttered interfaces, minimalist symbols, pastel colours and rounded shapes give this self-monitoring practice an innocent and appealing aspect. Moreover, with the example of wearables, we also understand that biopolitical power can once again be exercised through incentive mechanisms, such as rewards, badges, data sharing features, and gamification of life and labour.

fig.5

In parallel to its emergence, the self-monitoring practice has also seen the birth of the *Quantified Self* movement, a community of people who systematically collect and share their most personal body data to control and improve their lives. (Quantified Self, 2012) Of course, it should be remembered that some of these tools can help people with diabetes, obesity, or other health problems. However, the issue is to underline that these tools induce a philosophy in which only quantifiable things count.

Furthermore, the example of wearables illustrates how the power of tech firms can extend far beyond our screens, namely to our bodies and physical environments such as our cities, cars, homes, public spaces, etc. Through the Internet and connected devices, wherever we are and whatever we do can be transformed into information and marketed.

> "Individual finds itself permanently communicating, interfacing and engaging with technological devices." (Katrin Fritsch cited in Crary, 2014)

This reality tells about the long-term effort from major tech firms to extend their monitoring practices in an always more considerable array of contexts, such as with satellite and street photography

(*Google Earth, Street View*), geolocation systems, simulated three-dimensional environments (augmented reality, virtual reality, metaverse), facial/vocal recognition systems or extensions of our bodies, homes, and cities (wearable devices, vocal assistants, smart cities).

Thus, with smart cities, we move from the subject of the self-regulation and discipline of the bodies to the regulation of the people, assets, resources and services inside urban spaces. Thanks to sensors, video surveillance, facial/vocal recognition, machine learning, and algorithms, many major cities worldwide try to regulate traffic, collect waste, prevent crimes, and autonomously save energy. For example, China, which counts almost one billion urban residents, has, with smart cities, made a major socio-economic issue to control population, and pollution and ensure the country's constant economic growth. In the United States, Canada and India, some algorithms, which keep a record of all crimes, police units, addresses, and accidents, can speculate and designate the location of potential future crimes for police patrols. As another form of algorithmic surveillance, some cameras equipped with facial recognition and behavioural analysis can alert local authorities when detecting suspicious behaviours. (Yuval Noah Harari, 2018)

The last two decades have seen a rapid development of biometric technologies, which are now ubiquitous in many people's daily lives and work. While the use of biometrics can have real benefits for public safety and practical reasons, the intrusiveness and accuracy of this technology raise several privacy and human rights concerns. Since the 2001 9/11 terrorist attacks, which have opened the way to a new era of governmental surveillance, biometric techniques have also made their way into private sectors, such as the smartphone industry, the advertising industry and the shopping industry, with different levels of complexity.

> "Biometrics may be divided in various ways, one of them being 'strong', 'weak', and 'soft' identifiers. Strong identifiers allow or confirm the unique identification of a natural person, e.g. fingerprints, iris, and retina. Weak biometrics are features that are 'less unique' or 'less stable', e.g. body shape, behavioural patterns, voice, and body sounds. Soft biometrics comprises features that are generic in nature and not uniquely associated with a person, e.g. gender or age." (Mordini et al., 2012)

While some biometric techniques are now regulated through fundamental rights and data protection laws in some countries, the public health concerns related to the coronavirus pandemic have been high enough for many governments to expand their surveillance infrastructures. Some countries and locations still benefit from exceptional authorisations to use such technologies. For example, facial recognition is used in many airports across China to speed up security checks. In Shanghai Hongqiao International Airport, this service is even fully automated, allowing passengers to check-in their flights in a flawless way. (The Independant, 2018)

Moreover, despite restrictions, biometric techniques are still subject to considerable improvements (Policy Department for Citizens' Rights and Constitutional Affairs, 2021), with the upcoming possibility of capturing bio-signals such as heartbeats and brain waves, measuring neurons activity, and translating brain activity into machine-readable input. Thus, the current technical progress only reinforces concerns about the intrusion of these technologies in our lives, on the human body and into the human mind, allowing discrimination and violations of some of our most fundamental human rights.

—

More than ten years ago, it was still unusual to see animated ads in public spaces. I remember that while passing in some corridors or while waiting for the train, I often had no other choice than to have these ads in my field of vision. When I looked closer, one particular element caught my attention. Many panels had a sensor somewhat similar to a webcam. By studying the issue more closely, I understood that these screens could often be equipped with sensors, cameras and microphones, allowing some companies to collect, study and resell a maximum of biometric data for advertising purposes. This was one of the first times I became aware of the intrusion of surveillance devices (for capitalist purposes) into physical spaces.

Chapter 4: Agree and continue?

>"We must not confuse surveillance capitalism with digital technologies, which are merely its instruments. It is possible to imagine and build a society with the Internet without this logic of surveillance." (Morozov, 2019)

When Tim Berners Lee invented the World Wide Web in 1989-1990, its original idea was to create a space of freedom, free from any owner, national borders, control or economic logic. Over the last few decades, this ideal has been gradually eroded to benefit a handful of companies and to the detriment of our human freedoms. Today, our use of online tools often limits itself to a few services whose purposes are not as much to connect us to people rather than to connect us to them.

Nevertheless, the notion of privacy is not dead. According to the Economist Intelligence Unit, 93% of online users cite privacy and security as one of their top concerns. (Economist Intelligence Unit, 2018). In this context, everyone is concerned and has a role to play, from the industries that design these technologies, the public authorities responsible for regulating their use, and the consumers, who can choose to imagine or support infrastructures in which other economic policies can reside.

From a legal point of view, we are witnessing an increasing number of legal actions against the few leaders of this industry and towards more user privacy online. In the USA, several trials have been started with the explicit goal to regulate these companies' business models. However, the sharp division in the political landscape has not allowed applying any significant regulations to date. (Kang & al., 2029). In the European Union, a bit more was done, such as with the introduction of the General Data Protection Regulation[2] (GDPR) in 2018 and upcoming laws such as the Digital Markets Acts[3] and the Digital Services Act[4] (DSA) in 2023. In some cases, civilians can also participate in collective initiatives to promote new laws. For example, *Protect your Face* is a 'European Citizens Initiative' (ECI) calling for the European Parliament for an end to the abusive use of biometric surveillance techniques.

Beyond legal actions, some challenges remain to inform consumers that power resides in their hands and imagination. The current context of techno surveillance already pushes civilians, communities of programmers, hackers, activists, and artists to be involved with alternative tools, counter-practices and imaginative possibilities.

We can imagine infrastructures that would not be centralised around a single company but distributed between smaller, independent entities. We can imagine infrastructures where the data would belong to the citizens and not the owners. We can imagine infrastructures that would not try to hook our attention without considering the risks to humans and societies. We can imagine infrastructure that could be federated, distributed rather than centralised.

---

[2] Protection Regulation (GDPR): a regulation requiring Web platforms to seek consent from their users when using their data

[3] Digital Markets Acts willing to prevent GAFAM companies from abusing their monopolistic status)

[4] Digital Services Act (DSA) (meant to fight against online discrimination, hate or discrimination speeches) in 2023

As far as tools are concerned, some of the examples presented below attempt to demonstrate that digital tools and platforms are not limited to what the handful of ultra-dominant companies can offer us. On the contrary, the hegemonic tools only camouflage a much greater diversity of alternatives than one might imagine. This chapter will introduce examples of creative challenges to big tech media. It is far from comprehensive but wishes to provide some coordinates for imagining and making alternative realities.

Fediverse is an Open-source online network of federated publishers who stand as alternatives to some of the most hegemonic online platforms, audio/video streaming websites, blogs and microblogs on the Web. In this ensemble, we can find *Mastodon*, a popular alternative to *Twitter*; *Mobilizon*; which allows event planning outside of *Facebook*; *Funkwhale* for music streaming; *PeerTube* to upload and watch videos; *Pixelfield* as an alternative to *Instagram*; as well as about thirty other platforms which can communicate between them by using the same protocols. While different rules can apply to each tool, the great variety of existing instances should theoretically allow each user to find a place that best suits their needs. Another essential factor in the economic model of these platforms is that they do not necessarily rely on advertising revenues. Thus, although these companies are far from the profits made by GAFAM (Google, Amazon, Facebook, Apple, Microsoft) and sometimes struggle to survive, their tools can often be supported through donations and funding.

Interestingly, the military context in which some surveillance and communication tools were created also inspired the governmental support of alternatives, allowing people to compute and communicate with more privacy. *Signal* is an encrypted messaging application partly founded via the *Open Technology Fund*, a US governmental program. Today, this tool presents itself as a solid alternative to *WhatsApp* [*Meta*] by intending to "Develop open-source privacy technology that protects free expression and enables secure global communication." (Signal, 2014)

As another example, *Tor* or the "Onion Router", was developed by the United States Naval Research Laboratory only a few years after the invention of the Internet. Tor is an open-source software aiming to allow people to browse the Internet anonymously by hiding the IP address from the visited websites. As a complement to *Tor*, VPNs (Virtual Privacy Networks) have taken off among the general public, supposedly allowing users to create a secure connection from another private network located somewhere else in the world.

Web users can also choose between various privacy-oriented search engines, which will ensure that their online activity will not be monitored and sold back to third parties. This is the case for *DuckDuckGo* or *Qwant*, two of the most popular alternatives to *Google* [*Alphabet*] or *Bing* [*Microsoft*]. Another option is *SearX*, a free and Open-source metasearch engine that allows anyone to build or join custom instances and combine the results from various other search engines.

The previous examples are a few of the hundreds of other tools available on the Web. Indeed, the monopoly situation of some Web tools would almost make us forget the diversity of existing alternatives. Next to the techno-solutions are the imaginative possibilities allowing a non-specialist audience to measure the stakes of the datafication of our world. As Katrin Fritsch argues, to bring the topic into the public debate more forcefully, it should be possible to dismantle the technological mysticism of these systems and propose artistic works that speak to everyone.

"In a technologically connected society in which datafication and the capitalisation of the social and the body affect everyone, an activist response should be understandable and accessible by every single individual of this society — and not only by a technologically literate community." (Fritsch, 2016)

Fairly intelligent (2021) is the demo of a supposedly "fair" artificial intelligence designed by the artist and game designer A.M. Darke. In order to access and contribute to the algorithm, the visitor has to answer a few questions and follow some instructions. As the survey progresses, the questions become more unexpected and our choices more limited. In the end, the *Fairly Intelligent* system analyses the collected data to establish whether or not the visitor can contribute to the project. However, no matter what answers can be given, it is impossible to be trusted by the algorithm. By rejecting visitors' access, this work highlights tech companies' cynic promises and the discrimination politics underlying their products.

With *Unfit-bits* (2016), Tega Brain and Surya Mattu invite the *Fit-bit* owners to attach their connected bracelets to objects unrelated to the human body. By encouraging them to make a counter-use of this device, the two artists wish to dismantle the social imaginary upon which technology brings truth and objectiveness. Indeed, the understanding made by this technology mainly depends on our willingness to use these devices as expected. Thus, we acknowledge that imaginative uses can easily fool such tools.

In the installation *Data Production Labour* (2018), the artist and activist Manuel Beltran created an installation inviting visitors to scroll on a Facebook page for a limited time while being intensely tracked by some cameras and sensors. At the end of their shift, the visitor (as a worker) receives a receipt ticket with information about their behaviour and the money created from their labour. In this installation, Manuel Beltran exposes Web users as producers of valuable intellectual work for the benefit of the tech firms. By suggesting that the receipt can be used to ask Facebook for payment, he also offers different perspectives on data production and ownership.

(*Fairly intelligent,* 2021)
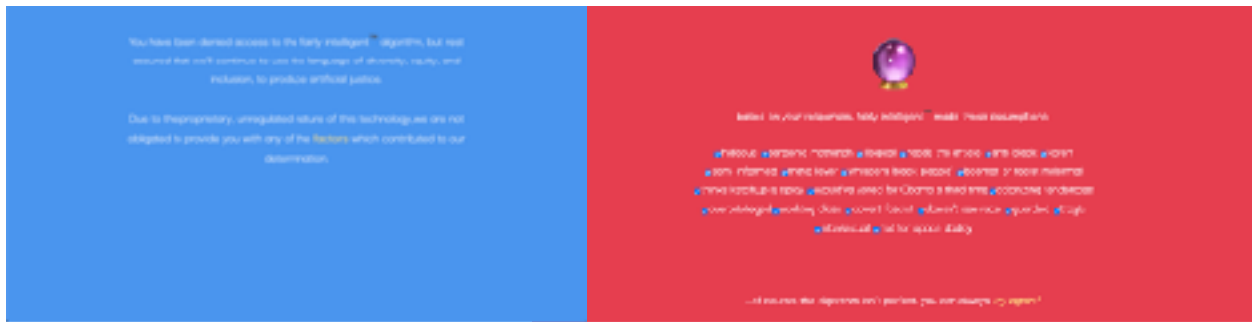
(*Unfit-bits,* 2016)

(*Data Production Labour,* V2 Lab for the Unstable Media, 2018)

Conclusion

As an introduction to this thesis, I quoted Seymour, who asked: "How can we be devoted to a technology that is marketed as our servant?". While elaborating on this issue, I also wanted to ask what the steps can be to emancipate ourselves from this situation.

Big data and artificial intelligence have become easy scapegoats for many of society's ills. However, awareness of the toxicity of these technologies is not enough. Over the last decade, the general mistrust and commitment toward intrusive and persuasive digital tools have increased simultaneously, leading to a dichotomy that became one of the motives of this thesis. Indeed, while most people surveyed declare their online privacy at the top of their concern, attention-greedy platforms, intrusive intelligent devices, and self-tracking tools still benefit from massive popularity. With this thesis, we understand that such contradictions are partly the result of the economic exploitation of human vulnerabilities and our deepest desires for approval, visibility, information, entertainment, control and self-control.

One of the first phenomena described in this text is the commodification of user data, which has encouraged the emergence of an attention economy specifically applied to the Web. Over time, this economy has been progressively refined and industrialised to give birth to authentic addiction machines, turning billions of people into free producers of wealth at the expense of their health and privacy. Furthermore, thanks to modern surveillance techniques implemented in our daily physical and virtual environments, everything we do can now be turned into valuable informational units. Consequently, humans only need to exist, breathe, act and move to produce gold. Likewise, the distinctions between online vs offline spaces, private vs public information, physical vs virtual environments, and labour vs entertainment have become more challenging to distinguish.

The first step addressed here is to demystify these technologies and make the reader understand how this realm extends its influence into every aspect of our lives. However, the assumptions and principles discussed in this thesis cannot provide a complete understanding of this area nor pretend to give real solutions. Instead, I wish to provide access to a field of information and enact different interpretations of a still widely opaque and misunderstood industry. The point here is to avoid being fooled, to finally become free.

The second step of this thesis is to encourage consumers to progressively wean off these addictive devices by showing curiosity toward more open, benevolent, diversified, and imaginative alternatives. In the same way, these writings also encourage artists and designers to not only denounce the realm of capitalist techno-surveillance but also to make propositional, speculative and imaginative works.

To continue to enrich the debate around alternatives to the realms of surveillance and attention capitalism, I wish to emphasise the open nature of this publication. To this end, this publication will be (almost) exclusively produced and published using Open Source software. Additionally, by putting the content of this publication under the Creative Commons Zero License, I wish to allow the right to use, study, make and distribute copies, make changes and improvements, and distribute derivative works.

Following on from this thesis, I am developing a 'data collection installation' that discusses the various pretexts for which we freely contribute to big data business, whether public or private health, well-being, self-management, shopping, entertainment, creativity, etc. Beyond the pretexts are also the contexts in which these surveillance and attention systems operate. By tracking humans' behaviours, I will emphasise the datafication and marketisation of our bodies, a major topic of my thesis. Finally, it will also be a question of activating different perspectives on the subject of the production, ownership and redistribution of personal data or the wealth obtained from the resale of the latter. Transparency between the mechanism and the user is pivotal to achieving a new perspective on this realm. The addiction mechanisms are not an underlying "side effect" but the core premise of experiencing and understanding the installation. Indeed, users will be encouraged to stay as long as possible and generate as much profit as needed. Paradoxically, the installation, disguised as a product of its time, makes the big data business's goal become the visitor's goal.

Bibliography

Alter, A., (2017). *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked*, 1st edition, London, England: Penguin Press Illustrated edition.

Bellis, M., Sharp, C., Hughes, K. and Davies, A., (2021). *Digital Overuse and Addictive Traits and Their Relationship With Mental Well-Being and Socio-Demographic Factors: A National Population Survey for Wales.* Front. Public Health. [online] Available at: https://pubmed.ncbi.nlm.nih.gov. [Accessed 3 Apr. 2022].

Bernard, T.S., (2015). *Giving Out Private Data for Discount in Insurance.* The New York Times. [online] 8 Apr. Available at: https://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html [Accessed 3 Apr. 2022].

Brain, T., Mattu, S., (2015). *Unfit Bits.* Somerset House, London, England.

Beltran*, B.,* (2018). *Data Production Labour*, V2 Lab for the Unstable Media, Rotterdam, The Netherlands.

Certeau, M., (1984*). The practice of everyday life*, Berkeley, USA: University of California Press. p. 148

Crary, J., (2001). *Suspensions of Perception: Attention, Spectacle, and Modern Culture*, Cambridge, USA, The MIT Press.

Couldry., N., Powell, A., (2014). *Big Data from the bottom up*, Big Data & Society [e-journal] Available at: https://journals.sagepub.com [Accessed March 11 2022].

Crawford, K., Lingel, J., Karppi, T., (2015). *Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device*, European Journal of Cultural Studies [e-journal] Available at: https://www.dhi.ac.uk com [Accessed March 11 2022].

Darke, A.M., (2021) *Fairly intelligent*, [online] Available at: https://fairlyintelligent.tech/ [Accessed March 11 2022].

David, C., (2022). *Signal Revenue & Usage Statistics.* Business of Apps. [online] Available at: https://www.businessofapps.com/data/signal-statistics/ [Accessed March 11 2022].

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., (2010). *Access Controlled - The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, USA: MIT Press p. 16

Debord, G., (2009). *The Society of the spectacle.* Eastbourne: Soul Bay Press.

Debord, G., (2014). The Society of the Spectacle, Translated from French by Knabb, A., 4th edition, Berkeley, USA: Bureau of Public Secrets

europarl.europa.eu (2021). *Biometric Recognition and Behavioural Detection*. European Parliament. [online] Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/ IPOL_STU(2021)696968_EN.pdf [Accessed 3 Apr. 2022].

Foucault, M., (1982). *Technologies of the Self*. [online] Available at: https://www.foucault.info/documents/foucault.technologiesOfSelf.en/ [Accessed March 29 2022].

Foucault, M., (1977). *Discipline and Punish: The Birth of the Prison*, 1st English edition, Translated from French by Sheridan, A., New York City, USA: Pantheon Books.

Fritsch, K., (2018). *Towards an emancipatory understanding of widespread datafication* [online] Available at: https://medium.com/ [Accessed March 11 2022].

Greenwald, G., (2015). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Republication, New York City, USA: Picador.

Hardt, M., Negri, A., (2012). *Declaration*. 1st ed, New York, Argo Navis.

Impact.economist.com (2018). *What the Internet of Things means for consumer privacy*. [online] The Economist Intelligence Unit. Available at: https://impact.economist.com/perspectives/sites/default/files/EIU_ForgeRock%20-%20What%20the%20Internet%20of%20Things%20means%20-for%20consumer%20privacy.pdf [Accessed 3 Apr. 2022].

Johnson, M., Ghuman, P., (2020). *Blindsight: The (Mostly) Hidden Ways Marketing Reshapes Our Brains*. 1st ed. [ebook] Dallas, TX, U.S. BenBella Books. Available at: https://www.goodreads.com [Accessed March 29 2022].

Kang, C., (2019*). Tech Giants Amass a Lobbying Army for an Epic Washington Battle*. [online] Available at: https://www.nytimes.com/2019/06/05/us/politics/amazon-apple-facebook-google-lobbying.html [Accessed March 30 2022].

Kemp, S. (2021). *Digital 2021 April Statshot Report*. [online] DataReportal – Global Digital Insights. Available at: https://datareportal.com/reports/digital-2021-april-global-statshot. [Accessed March 13 2022].

Kholeif, O., (2018). *Goodbye, World! — Looking at Art in the Digital Age*. 1st ed, Berlin, Germany: Sternberg Press pp.183-184

Mahalingam, T. and Howell, J. and Clarke, P., (2022). *Attention control moderates the relationship between social media use and psychological distress*, School of Population Health, Curtin University, [e-journal] Available through: https://www.sciencedirect.com [Accessed March 13 2022].

Mordini, E., Tzovaras, D., Ashton, H., (2012). *Second Generation Biometrics: The Ethical, Legal and Social Context*. 1st ed, Berlin, Germany: Springer, p.7

Morozov, E., (2019). *Capitalism's New Clothes*. The Baffler [e-journal] Available through: https://thebaffler.com [Accessed March 11 2022].

Quantified Self. (2012). *What is Quantified Self? - Quantified Self*. [online] Available at: https://quantifiedself.com/about/what-is-quantified-self/ [Accessed March 11 2022].

Seymour, R., (2019). *The Twittering Machine*. 1st ed. London, England: The Indigo Press.

Signalfoundation.org (2014). Signal Foundation. [online] Available at: https://signalfoundation.org/ [Accessed March 11 2022].

Slotnik, D., (2021). *Whistle-Blower Unites Democrats and Republicans in Calling for Regulation of Facebook*. New York Times. [e-journal] Available through: https://www.nytimes.com/ [Accessed March 11 2022].

Small, G., Lee, J., Kaufman, A., Jalil, J., Siddarth, P., Gaddipati, H., Moody, T. and Bookheimer, S. (2020). *Brain health consequences of digital technology use*. Dialogues Clin Neurocsci. Available at: https://pubmed.ncbi.nlm.nih.gov/. [Accessed March 11 2022].

Spotify. Com (2021). *The Wait Is Over. Your Spotify 2021 Wrapped Is Here* — [online] Available at: https://newsroom.spotify.com/ [Accessed March 11 2022].

Stewart, J., (2016). *Facebook Has 50 Minutes of Your Time Each Day. It Wants More*. New York Times. [e-journal] Available through: https://www.nytimes.com/ [Accessed March 11 2022].

Tian, Y., Thiago, Dulcinati, G., Galery, Molimpakis, E. and Sun, C. (2017). *Facebook sentiment: Reactions and Emojis*. [online] Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media. Association for Computational Linguistics, pp.11–16. Available at: https://www.researchgate.net/ [Accessed Jan. 12 2022].

The Independent. (2018). *At this Chinese airport, people have been replaced by machines*. [online] Available at: https://www.independent.co.uk/travel/news-and-advice/shanghai-airport-facial-recognition-security-clearance-system-china-a8587871.html [Accessed 13 Apr. 2022].

Unesco.org. (2010). *Freedom of connection, freedom of expression: the changing legal and regulatory ecology shaping the Internet* [online] Available at: http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/freedom-of-connection-freedom-of-expression-the-changing-legal-and-regulatory-ecology-shaping-the-internet/. [Accessed 3 Apr. 2022].

Wu, T., (2016). *The Attention Merchants: The Epic Scramble to Get Inside Our Heads*. 1st edition. New York City, USA: Knopf.

Yuval Noah Harari (2018). *Yuval Noah Harari on Why Technology Favors Tyranny*. [online] The Atlantic. Available at: https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/

Zuboff, S., (2019). *The age of surveillance capitalism*. London, England: Profile Books.