Università
Ca'Foscari
Venezia

Master's Degree

in Global Development and Entrepreneurship

Final Thesis

Surveillance capitalism

The implications of losing privacy

Supervisor

Ch. Prof. Mario Volpe

Graduand

Sofia Benanchi

891482

Academic Year

2022/2023

Table of contents

Preface

Since the introduction of the World Wide Web in 1989, the digital revolution has made its way, passing through mobile devices, social networks, big data and computing clouds, revolutionizing every environment. The adaptation and proliferation of computers led to the development of more advanced systems that secured a much more comfortable life for many.

As expected, the economic system and relative infrastructure have been greatly revolutionized, especially the relationship between demand and supply.

The dissertation presents surveillance capitalism, as coined by Professor Shoshana Zuboff, the business model through which companies collect and employ personal information of consumers to increase their revenues. From market research and analysis of consumers' trends and preferences, the competition shifted to advanced datasets and surveillance arrangements that threaten people's privacy. The innovation lies in the way supply is brought together with demand: initially, data was collected to maximize the probability to sell, as the production was designed accordingly the information acquired; then, progresses of the surveillance infrastructure were such that it was possible to induce specific conducts in people: it is no longer necessary to predict a behavior if you can instill it and control its development. It's a predatory approach to do business, especially harming those unable to critically engage with the Internet. As we spent a significant part of our days connected, the phenomenon and its consequences are worthy of critical observation.

The first chapter introduces the fundamental characteristics of surveillance capitalism: its accumulation logic carried out by the imperative of extraction; the cycle of dispossession and how its operations are made amenable to consumers; the division of learning and the consequent asymmetries of knowledge that are allowing surveillance capitalists to maintain the status quo. The role of Google as inventor is discussed, together with the set of events that established the growing base of surveillance practices.

In the second chapter it is presented the ubiquitous surveillance infrastructure, what technologies and logics implement it and how it is preserved. Starting with the dystopia of the non-contract and the illusory choice it grants, the essential rendering operations will be discussed, together with the scope economies and economies of action that allow them and the inevitabilist ideology that encourages people to participate.

The third chapter firstly investigates the concept of privacy and the responsibility of protecting it. Then, the impact of culture over the perception of privacy is examined, in particular how differently individualistic and collectivistic countries engage with online

services. The analysis proceeds with the transatlantic clash, the divergence between Europeans, that protects privacy as a matter of dignity, and Americans, for which is foundation of liberty. The focus is kept on the western cultures, presenting and comparing the European and American perceptions of privacy: the addressed issues space from responsibility to trust, the lack of control and understanding of data collection operation and the level of tolerance towards certain surveillance practices.

In the fourth chapter there are listed the main laws and regulations from both the European Union and the United States' systems regarding privacy protection, the discrepancies among the pan-European approach and the State Acts. In particular, it discusses the relevance of the EU's GDPR and its effective action against surveillance operations and how it has impacted the EU-US relationship. It wraps up presenting the EU Digital Decade plan, which is designed to bridge the digital divide towards equality.

The fifth and final chapter examines the way algorithms and AIs take part in everyday's life, in particular their aim to learn how to imitate us. Then, how they are designed to perform radical indifference regarding the consequences of unmonitored contents and the spread of fake information. Finally, the dissertation addresses the automation anxiety caused by the impact of AIs on the job market, how investments should be redirected in order to empower people and not putting them in competition against computers.

Chapter 1 - **Surveillance capitalism**

According to the definition given by Professor Shoshana Zuboff, surveillance capitalism is a new economic order, exploiting the human experience as raw materials for secret commercial practices of extraction, forecasting and selling. It is a mutation of industrial capitalism and represents a challenge to markets' democracy.

Every era is characterized by specific threats that compel people to rediscuss topics such as authority and power. In our case, the phenomenons of digitalisation and computerisation are taking over, altering every aspect of reality with not much time to understand and choose. Will we work for smart machines or will they be the ones used by smart people?

1.1 Introduction

In 2000, a team of scientists and computer engineers from Georgia Institute of Technology (Atlanta, U.S.) collaborated in the Aware Home project. Imagining a symbiosis human-house, they wanted to create a "living laboratory" to study the informatisation of space. It would have been a wireless automated cooperation, between a platform that recorded personal information captured by sensors worn by occupants, and another that collected environmental information from computers around the house. The engineering project was presented as a close circuit: the system would have monitored everything, and the obtained information would have been stored in personal computers of the occupants to guarantee their privacy.

In 2021, the global market of smart home was valued at 68 billion dollars; with a projected annual growth rate of 12.47 per cent from 2022, the market value is expected to reach the value of almost 223 billion by 2027.

Let's consider now a single tool from smart home, the Nest thermostat by Alphabet, a Google's holding. Nest does a lot of what Aware Home imagined: it captures personal and environmental data, learns the occupants' behavior through sensors and can also take data from other connected devices. The resulting datasets from these tools are then uploaded to Google servers.

Every thermostat provides a **privacy policy**, the final user's consent, according to which personal information and sensitive data are shared with other smart devices of the Smart Home and with third parties that will carry out predictive analysis later sold to unspecified subjects. A detailed study over Nest policies by University of London concluded that, in order to acquire and consciously utilize a single thermostat, people would have to analyze around one thousand "contracts". If the client refused such norms, according to terms of service the

functionality and security of the tool would be heavily compromised, and would not be supported by necessary updates anymore.
In 2000, who decided to digitize their life was told that they would have detained exclusive rights over the knowledge derived by personal information recorded. Today, the right of privacy has been taken away without consent.

According to Professor Zuboff analysis, surveillance capitalism employs some data in improving its products and services, but the majority of it becomes private behavioral surplus: this is processed by AI until transformed in prediction products that forecasts users' conducts; these will be then sold in the **behavioral futures market**, into which companies operate in order to understand how to acquire new potential consumers or maintain current ones.
The competitive dynamics of these environments pushed surveillance capitalists to acquire more accurate sources. More precise data are obtained through direct intervention over people' behaviors, bypassing them in engaging the more remunerative actions. The innovation is the exploitation of behavioral data: surveillance capitalism enforced the means of behavior modification, its means of production. People find their data immersed in a computational architecture composed of interconnected smart spaces.
Surveillance capitalism exploits the positive concept of "being connected" and participating in your social surroundings: it is intrinsically parasitic.

Google represents to surveillance capitalism what Ford and General Motors were for managerial capitalism. The company had a pioneering role in financing research and development, in experimenting and implementing innovative practices; surely favored by the lack of concurrence and control laws, it proceeded at a brisk pace. Moreover, it benefited from the historical contingency of September 11, 2001, starting from which the wish of absolute certainty was pursued.
The actions of Google have been covered by ignorance regarding the actual functioning of its technical processes. Its mechanisms became the basic model for the majority of Internet-based businesses.

Products and services of surveillance capitalism are not exchanged as goods, there's no reciprocity relationship between supplier and consumer. In order to gain access to a service, users offer their personal information, which are then extracted and bundled for companies participating in behavioral futures markets. Even if we are the source of their profits, it is

basically impossible to escape from this tie: the digital revolution has pervaded every aspect of human life, we are now addicted to the efficient existence digital devices proved to be able to provide us. Surveillance capitalism operates thanks to information asymmetries: they know everything about us while we can only resign ourselves to being traced and analyzed in exchange for using everyday's services.
Its triumph derives from its unprecedentency: something that's completely new cannot be recognised, the human brain automatically interprets it resorting to familiar categories, hence we conceal its new features. The novelty of surveillance capitalism could be compared to Ford's "horseless carriage".

The logic that surveillance capitalists want to instill is that their practices are inherent to their technologies. In 2009, for the first time people came to know that Google kept users' chronologies for an indefinite time, later confirmed by the company's ex CEO Eric Schmidt. The declaration ended up disguising Google's real intentions: the information was presented as necessary and inevitable commercial operations, while in reality they are projected in detail to achieve success. According to philosopher Max Weber, **technological inevitability** doesn't exist: in a modern capitalistic society, technology only offers appropriate means to achieve its economic objectives. Google algorithms are the expression of its interests.

1.2 Soil for the digital revolution

Apple broke into the music industry during a duel between demand and supply: young people were using Napster and other services of file sharing, asking for a way to consume music "whenever and however they wanted", and the music industry was prosecuting some of the biggest users to protect its activities. Apple was able to build a bridge between the parts through a sustainable solution, both legally and commercially.
The sales of iPods, iTunes and iPhones took off the company's profits: three days after the launch of the iTunes platform compatible with Windows in October 2003, users had already downloaded one million copies of the software and bought almost a million of songs. After a month, they became 5 millions of downloads, 10 after three months and 25 after six months; in January 2007 they were 2 billions of downloads, and Apple substituted Walmart as the biggest music seller in the world. Another fundamental step was to include the iPod's functions into the Iphone's: in 2017, a study about the stock market concluded that Apple generated more profits for investors than any other company from the previous century.

With mass production, Henry Ford set the basis for wealth creation in the 20th century. Digitalisation freed some value propositions from the institutional space in which they were trapped, and set a direct connection with consumers: Apple bypassed the physical production of the product (songs) and its packaging, its stocking, transport and distribution; iTunes allowed people to reconfigure their playlists however they wanted and listen to music whenever they wanted.

Applying the digital revolution to capitalism, Apple was one of the first companies to achieve commercial success intercepting the new and evolving needs of the society. It proposed something completely new and technically inseparable from the digital environment, and their product represented the implicit promise to indulge in their clients' true desires. The digital revolution paved the way to **rational capitalism**, able to connect demand and supply starting from consumers' will and choices.

We could deduce that the dominant form of market becomes more productive when it shapes around actual consumers' needs. According to French philosopher Emile Durkheim, higher productivity is the necessary consequence of the attempt to live efficiently in the conditions of our existence. Capitalism's rationality reflects this alignment with the people and their need to live in their times: Ford's Model T and iPhones/iPods are products of distinct phases of the process of **individualisation**, as called by Professor Zuboff; it is not to be confused with the neoliberal ideology of individualism or the psychological process of individuation (the constant attempt to improve ourselves).

German sociologist Beck-Gernsheim defines as "first modernity" the diffusion of the individualisation of life: every life becomes a non-predetermined reality, there are (too) many ways of living. The industrial society kept many characteristic of the feudal society, visible in the forms of association based on social class, labor, ethnicity and sex, and in the consequent institutions, like corporation, churches, labor unions and political parties: those order and logic guaranteed guidelines and objectives for anyone, hence everyone could decide for themselves, but not totally. You were expected to do what you were supposed to, and little by little you would have found your way; eventual anxieties were coming from the feeling of measuring up with expectations for your role. Ford understood this, and proposed a product that people could have bought with the money they were making.

The generation of the digital revolution is living the "second modernity", child of the first's mentality: the significant shift in requiring the right of autodetermination can lead to a life of uncertainties and stress. Experiences once reserved to elites are now available for more

people: communication, information, consumerism, better living conditions and life expectancy have legitimized the need to form a personal identity over pre-existing social norms. Every aspect of our everyday life can be questioned: this way of thinking and its wants let the Internet enter in our lives. Not having anything pre-set pushed us towards the resources and information that the digital space was offering us, in order to shape the connections we wanted.

The neoliberal habitat

In the 1970s, neoliberal economists were staying in the shadows of the prevalent Keynesian doctrines. Their moment came thanks to the conditions of the postwar economic order, in the US and UK in particular, damaged by inflation, stagnation and economic growth slowdown; politicians found themselves besieged by citizens requesting a change. The doctrine of free market was born in Europe as defense against collectivist and communist ideologies, it aimed to spread the idea of a market able to autoregulate.

Leader of the movement, Friedrich Hayek believed that individuals and the collectivity had to be subjected to market discipline, which was going to substitute the political authority of the State. The disparity in rights and wealth was accepted and even considered a necessary condition to guarantee an advancing system.

Before Hayek, the economic historian Karl Polanyi had proposed the **double movement**, which was going to support the market while anchoring it to society: the auto regulation of a market economy would be destructive without balancing laws and policies in the opposite direction. But while naturally emerged in every European society during the 1850s, in the neoliberal US the double movement was forcibly dismissed: what was implemented by the extreme deregulation program started by at that time President Jimmy Carter in 1978 is considered the starting point for the Reagan and Thatcher eras, and the basis of any other following neoliberal fiscal and social policies.

Despite a decade of digital expansion and the entrance of the Internet in everyday's life, society is still experiencing the legacy of economic growth obtained through neoliberal policies. A significant report by the International Monetary Fund from 2016 displays how inequalities have severely decreased levels and endurance of growth, increasing instability and vulnerability to potential crisis.

> In *Capital in the Twenty-First Century*, French economist Thomas Piketty declares that a market free from regulations releases forces potentially dangerous from democratic society and their funding values. Many scholars are referring to the advent of **neofeudalism**, characterized by the consolidation of inequalities, according to which the opportunities of a person depend on the wealth they inherited and not on their merits. Regarding this tendency, Professor Zuboff states that, for individuals of modern society, with complex experiences and opinions, it is not sustainable to go back to a certain social hierarchy that doesn't belong to our thinking.
>
> Can the capitalism of information create a beneficial condition for all and not for few within this unstable second modernity?

In the 2000s, companies such as Apple, Google and Facebook seemed able to direct digital capitalism towards an improved welfare: information would have freed people from old institutions and let them discover who they truly were.

Apple's innovation represented a production aligned with the real interests of consumers, the possibility to get "a new life" for an affordable price. But the company ended up contradicting the initial vision and lining up to the usual way to do business: Apple was criticized for its exceeding prices, for the delocalisation of its labor force, for exploiting its employees and for the lack of control over their working conditions, and many others violation of the implicit social contract they proposed at the beginning.

Two notable violations of the protection that should be guaranteed to digital consumers are: Gmail, launched in 2004 by Google, which scanned private mails of its users in order to create personalized ads; and Beacon, launched by Facebook in 2007, that allowed advertisers to track the purchases of its users. The latter was shut down in 2010 for the negative reactions to its violations, but Mark Zuckerberg declared that privacy wasn't a social norm anymore and he boasted the fact that he was responsible for the slack of privacy policies of his Facebook.

The infamous requests of "consent to terms of service", the click wraps, are one of the most deceitful sources of danger online. Legal experts call them **general contract conditions**, because they impose "take it or leave it clauses" to users that have to accept them even if disagreeing. Scholars stress the fact that the length and complexity of these digital documents have the purpose to discourage users from actually reading them.

Furthermore, terms of service can be altered at any moment, without the knowledge or consent of the user, changing also the terms of all the many other companies connected with

the one supplying the service. Law scholar Margaret Radin considers these practices as the "moral humiliation of the law"and the institution of the contract": the user has to submit to the legal system chosen by the company in order to actually verify a transaction with it. Digital contracts can be expanded, reproduced, distributed and archived without additional costs.
In 2009, representative of Federal Trade Commision Jon Leibowitz publicly stated that everyone in the business knows that consumers do not read privacy policies. In 2008, two professors from Carnegie Mellon University, Pennsylvania, conducted a study in which they calculated how much time was needed to adequately read these policies, and at that time it resulted in 76 working days; today it would be much more.

The success of iPod and iTunes induced users to be optimistic about digital capitalism, but the belief of digital innovations degenerated in desegregation of the language and in obsession with velocity.
Economist Joseph Schumpeter coined the concept of **creative disruption**, basically what was used to legitimize what Silicon Valley called "innovation without permission". He considered capitalism as an evolution process, even if just a few of its innovations would have been able to be significant for the successive evolution: he defined these rare events as **mutations**, changes that were actually qualitatively lasting and sustainable in capitalistic practices and logics. According to Schumpeter, the mechanism of evolution is carried out by new needs of consumers, and aligning to these creates a sustainable mutation: the capitalist process, not by chance but from within, progressively improves welfare. Mutations belong to rational capitalism, which shapes its relationship with people through democratic institutions; essentially, they direct the system towards those in need.

Google's mission of "organizing all the world's information and making it universally accessible surely changed our lives, but we had to accept that information destined to be forgotten now is recorded to form our digital identity.
On August 9, 2011, inspired by the Los Indignados movement that was protesting the conditions caused by the economic crisis, many people gathered in front of the Spanish Agency for Data Protection in Barcelona, opposing Google and asking for their right to be forgotten. For example, the house of lawyer Mario Costeja Gonzàles had been foreclosed, and even if the situation was resolved, it was still the first information coming up after searching his name on Google, damaging his reputation and his business. The Agency recognised that not all information deserves to be immortal, and Google contested this decision at the Spanish

Supreme Court; the latter selected 90 cases to discuss at the EU Justice Court, which settled the right to be forgotten as one of the fundamental principles of the EU law system in May 2014. This verdict should be dismissed as a delinking of personal data: the Court analysis refused the technological inevitability and recognised that search results are the contingent product of specific economic interests. As stated by law scholars Schwartz and Peifer, the Court recognised the importance of free information without equalizing it to the safeguard of privacy and data protection by European law.

After the announcement of the verdict, the smart money industry asserted that such a situation could have never happened in the US, where Internet companies justify their actions behind the First Amendment. Larry Page defended Google powers, stating that it was better for people that the company held their data and not the Government, "because the company cared for its reputation". Yet, in the same year, Pew Research, a nonpartisan American think tank, found that 93 per cent of Americans cared about controlling whoever was able to obtain personal information.

January 1st, 2015, the **Online Eraser law** was implemented in California, according to which sites, online and mobile services were obliged to remove contents and information of a minor, if the user requested it. A breach was opened.

After the iPod, every research, like or click were claimed as something to track, analyze and sell. Companies justified their violations as necessary to offer free services. Surveillance capitalists exploited the improvements the digital world was able to guarantee us: while satisfying our needs, someone profits from our behavioral data. And we found ourselves unable to counteract new companies led by geniuses apparently able to offer free or cheap innovative services. Surveillance capitalism managed to not be understood and not ask any consent, and neoliberal ideology provided it the adequate habitat to prosper making people accept the logic of exchange: our data for free information and connections.

1.3 Google, the pioneer

Surveillance capitalism was invented by Google, in Silicon Valley, United States.

With the invention of target advertising, Google paved the way for its financial success but also for the discovery of surveillance capitalism: its development required all its operations to be devoted towards absolute control over any information available, with unprecedented social implications.

Founded in 1988 by Larry Page and Sergey Brin, Google embodied the promise of information capitalism as democratic and liberating force. The company was able to impose its mediation over many aspects of human behavior, ending up producing new data based on: keywords, search patterns, spelling, formulation and punctuation of a query, lay off and other data they defined as "waste". This innovative way of studying data highlighted the possibility of reconstructing a detailed story of every user, achieving Larry Page's dream of Google Search, a search engine that becomes an all encompassing artificial intelligence.

Google's engineers understood that this incessant stream of behavioral data was able to transform the search engine in a repeated learning system that could provide constantly improved results. As American journalist Kenneth Cukier stated […] Google exploits byproduct or waste information, traces left by users that are automatically employed to improve Google service or to create brand new products. This scrap data rapidly became the crucial basis for the fast learning process of the company.

In the first phase of development, the feedback loop generated by the improvement of search function set up a balance of powers: Search needed people to learn as much as people needed Search to learn. This symbiosis led to the Page Rank algorithm, which gave a significant advantage to Google in identifying the most popular results for each query. Professor Zuboff calls this stage **reinvestment cycle of behavioral value**: data were only gathered and employed for the benefits of user experience, in order to refine speed, accuracy and relevancy of searches. This cycle emulates the iPod's logic: clients were subjected to the commercial process that promised to align with consumers' requests. The main difference was the absence of a sustainable market transaction: the iPod's cycle was supplied by the sale of a physical product with a high profit margin, while Google was oriented towards the user without any physical goods: it was an interaction, not a transaction with consumers.

Regarding advertisement, Google considered it not meaningful, and built a related team of only four people. When Brin and Page introduced their search engine at the World Wide Web Conference of 1998, they declared that a search engine financed by advertisement would be intrinsically imbalanced towards who pays for it and against the real needs of users, and that instead they aimed for a more transparent service.

In 1999 the company announced that investors of the caliber of Sequoia Capital and Kleiner Perkins were going to buy shares for 25 million dollars: with 7 millions of requests per day to manage and an innovative and self-improving technology, Google was still missing a system to transform investments in gains. Because of the balance of powers, it was risky to ask to pay

for the service, in particular because it meant that the company would have to set a price for information that it was already extracting from consumers without having asked the permission of anyone. From this point of view, even before surveillance mechanisms, Google development appears theft-based. As the New York Times wrote, “Is Google able to create a business model worthy of its technology?”.
In April 2000, the legendary dot-com economy started to sink into recession, as Silicon Valley had to face the so-called **dot-com bubble**: start-ups that a few months before were excessively valued had to shut down, venture capitalists were shocked and didn’t want to risk any more capital. Many Google investors were doubting the company’s ability to survive, even if Google Search was widely regarded the best search engine in the world and the data traffic among the platform kept increasing. This restlessness represented how everything was becoming oriented towards rapid gains: in December 2000, the Wall Street Journal shared the new mantra of Silicon Valley investors, “to count and keep counting something it is not enough to prove to be able to make money, you will need lasting and exponential profits”.

At the end of 2000, the stage of emergency of the industry became the excuse to set aside the reciprocity relationship and the hostility towards advertising. Google would have worked through its expanding archive of behavioral data and its technological capabilities to match ads and query. According to this rhetoric, Google would have started to use *only relevant* advertising: ads would have been linked not only to keywords, but customized to a target user; this perfect matching would have provided a valid running service for advertisers. The data waste, the **behavioral surplus**, previously used only to improve the user experience, were now employed to make ads more profitable for Google and its advertisers. 2002 was the watershed year in which Google’s surveillance capitalism found its “lasting and exponential profits”.
The first ads were linked to a research query: Google verified the click-through rate, if people actually clicked on it; investors paid depending on how many people saw the ad. With the scheme expansion, Google created the AdWords system: the research with advertisers’ keywords also included their text box and the link to their page; now prices depend on the location of the ad among the search results. As Bloomberg.com explained in 2006, Google maximized its income ensuring the best resulting position to the advertiser that could pay the most for it, based on estimations of the actual probability that users would click on the ad.

In respect of investments, Google moved from optimizing its service to wide and advanced extraction operations of data: the company was setting the dependence of its revenue over gains of behavioral surplus.

In support of innovation to collect more behavioral surplus, Google registered various patents: those who rose above the law were now asking for official legal protection for their business. The most emblematic being the 2003 *Generating User Information for Use in Targeted Advertising*, which best represents the logic of accumulation and the new mentality oriented towards profit. This innovation was needed to minimize the money wasted in matching the ad with a specific user: for any query typed, the system performed a predictive analysis during its typing and gave back a particular configuration of the ad. This matching operation compiled new data sets called **UPI**, user profile information, which drastically increased the accuracy of the prediction and nullified the waste of advertisement budget.
Regarding the UPI, some data could have been extracted from pre-existing Google databases, which were kept in expansion; but for the majority, UPI was created integrating and analyzing search patterns, personal documents and many other online behaviors, even when information was not given directly.
UPI can be deduced or derived. Some examples of data analyzed for compiling your UPI are visited sites, psychogeography, browsing and previously shown ads, shopping made after visualizing them. Basically, Google invented an automated architecture that works like a one-way mirror, that guarantees access to secret behaviors without caring about awareness: the whole company operates thanks to asymmetries of knowledge and powers, and holds a predictive capability very useful in the low risk market of individual conducts.
An important innovation concerned the price system: the **click-through rate**. As a significant relevance signal, it was used to improve the accuracy of forecasts and the ads matching itself, consequently increasing profits. This logic institutionalized the demand for prediction products, setting the necessity of a scale economy of behavioral surplus' supply. Moreover, the **quality score** concurred in setting the ad price and its specific position in the result page.
Thanks to the winning combination of Google patents and behavioral surplus, profits reached 347 millions of dollars in 2002, a billion and a half in 2004 and 3.2 billions in 2004, the year in which the company entered market listing; in less than 4 years, the discovery of behavioral surplus had made profits growth of 3590 per cent.

If Ford revolutionized the production, Google revolutionized the extraction: professor Zuboff calls it the **extraction imperative**. Users became the way to achieve goals of others: Google reinvested in its service to extract more information, making its users unaware suppliers of raw materials of others' incomes. Behavioral surplus is necessary to profit, as much as secrecy is for abundantly accumulating and illegitimately using it.

Aside from corporate secrecy policies, Google always misled what was really doing through a specific jargon: the behavioral surplus has always been defined as "digital waste, crumbs", something worthless that anyone could take possession of.

In the general context, privacy is not eroded, it is *redistributed*, but among the wrong people, excluding its real owners. Surveillance capitalism appropriates the right to choose what to reveal: the accumulation logic of Google works only if the company is able to take whatever information it needs.

Is surveillance capitalism another form of capitalism?

The behavioral surplus is the fundamental raw material needed to obtain surveillance gains, later transformed into surveillance capital: this logic sets an economic order based on surveillance. The surveillance economy is characterized by subordination and hierarchical relationships.

The means of production are techniques and technologies, the artificial intelligence of machines, in perpetual evolution. In 2017, Beijing researchers for Microsoft's Bing search engine published a study that dealt with the role of the click through rate: even a 0.1 per cent improvement of its accuracy would increase by millions the profits.

The products are forecasts of users' conducts, sold to people that want to sell to them their products in return. Technically, Google doesn't invade privacy: the company doesn't sell personal data, it sells prediction products based on its extraction. Competition between surveillance capitalists pushes them to large accumulation: totality of information leads to certainty, which means lower risks and higher sales on the emerging behavioral future markets. This new system overcomes the classic idea according to which the market is intrinsically unknowable: accurate data allow the possibility to know details about demand and supply of the behavioral futures market.

Aside from the fact that people are not counted as consumers anymore, a meaningful difference between surveillance capitalists and traditional ones is the size of the labor force: this pattern is called **hyperscale**, with very few specialized workers employed in a gigantic economic architecture.

> The historical discontinuity is blatant when comparing the biggest US companies, (even if we are considering a large time range): General Motors with Google and Facebook. At the end of 2016, Google reached a capitalisation of 532 billion dollars, while Facebook of 332 billions: these results while having around 75 thousand and 18 thousand employees. GM reached its maximum capitalisation of 222.15 billion dollars in 1965, while employing 735 thousand people. This means that GM employed more people, even during the Great Depression, than Google and Facebook ever did while at high capitalization on the market.

1.3.1 The withstanding convergence

Television newscaster Douglas Edwards reported that in 2001, during a meeting with founders, Page said that if Google belonged to a category, it would be the one of personal information. According to his vision, people would have generated so much data to be collected that any life experience could have been searchable. This perception perfectly reflects the capitalist appropriation of things external to the market sphere, later made reborn as products to sell.

In his 1944 book *The Great Transformation*, Polanyi describes the appropriation process of an economy able to autoregulate through three fictitious commodities. The first was the capability to subordinate the human experience to market dynamics, transforming it in “labor” to buy and sell; the second was the translation of markets’ nature in “land”; the third was the rebirth of exchange in “money”. In *The Capital*, Marx too described the appropriation of land and labor as the starting point of the modern formation of the capital, money, and defined the process as “original appropriation”.

Philosopher Hannah Arendt elaborated such concepts and stated that the original appropriation is a recurring phase in a running cycle, in which more and more aspects of the natural and social world are subjected to market dynamics; the process must be repeated in order to keep up the accumulation engine of capital.

Page understood that human experience could become Google's raw material to be extracted for free or not much more, and be used as the basis of behavioral data that can become a new class of commodities to be exchanged on the market. Surveillance capitalism grows from this act of digital expropriation, that lifted Google from the crisis and towards high profits. To follow the previous logic, the human experience undergoes the market’s mechanisms, it is translated into data that feed the previsional machines and sold within the behavioral futures market. The exchange is protected by secrecy and competences, and people don’t have any

formal control over it, because they are not needed to make it happen and because it would make the caste crumble.

The responsibility for the settlement of these practices lies with the convergence of political circumstances and active strategies that co-created the adequate habit for this mutation to prosper.

- **The claim**

  The unusual company structure of Google is certainly a factor of their success. When in 2004 Google was publicly traded, Page and Brin firstly introduced a double class structure, according to which they would have controlled the "super B class" that counted 10 share votes, while "A class" counted only one. This sheltered from market and investors' pressures: for externals it was very difficult to scale or influence Google. In 2011, the founders used their majority of 56 per cent to impose a new shareholding structure with three classes, introducing the non-voting share "C class" that would have guaranteed them full control of the company. In 2017, Page and Brin had 83 per cent of the B class shares, which translated into 51 per cent of the overall votes. Many companies' founders of Silicon Valley followed their suit, like Facebook in 2015.

  Many finance experts were trying to understand the consequence of such shareholding structures, and in the meantime founders of Google and Facebook were aggressively working. To stay ahead of the curve they knew they needed the best talents and AIs available regarding augmented reality, deep learning and facial recognition: they paid exorbitant numbers to acquire all the companies indispensable to cover the sectors they needed.

  For example, in 2006 Google bought for 1.65 billion dollars a young start-up, which wasn't earning anything yet and was bombed with copyright infringement lawsuits: Youtube. In 2009, an analyst from Forrester Research declared that Google had accepted to pay that figure because they would have been able to connect to it their knowledge regarding advertising and transfer to their property all the search traffic; in the end, acquiring YouTube would have been worth it.

  Again, Zuckerberg implemented the same strategy, obtaining the augmented reality company Oculus for 2 billion dollars and WhatsApp for 19 billions: Facebook secured to itself a huge flow of personal data.

As stated in the first page of 2013 book *The New Digital Age: Transforming nations, Businesses and Our Lives* by Schmidt, cyberspace is the largest ungoverned space in the world. Google and Facebook made their claims over operational spaces outside political institutions.

Surveillance capitalists are pushed to search for a lawless context because of their own nature: they take a lobby attitude in order to nullify online privacy protection, limiting regulations and weakening laws in favor of privacy. The extraction must be free and available in order to have success with the accumulation logic: laws against it would make the system implode.

The legacy

Under the influence of Hayek, bureaucracy must be repudiated as a form of domain over everyday's life. Against any inclinations towards the totalitarianism and collectivism of the Second World War, the American political thought oriented towards autoregulation, in search of practices in defense of government coercion. A company must decide its own standards, control if they are respected, even judge its own conduct or violations.

This neoliberal legacy had been the manna for surveillance capitalists, that ended up applying a model in which any interference to set any rules would threaten the competition. The AI law expert Frank Pasquale defines the surveillance capitalism ideology as **cyberlibertarian**. Those companies' representatives hide behind the right of freedom of expression from the First Amendment which, as suggested by law scholar Steven Heyman, recently has been used by judges to carry on a conservative-libertarian agenda. US tribunals made many efforts in order to contain excessive government's actions, while being reluctant in recognising potential problems from excessive private power.

Internet companies insist on freedom of speech for business reasons. The US Constitution has been used as a shield for their innovative practices that are actually damaging to the First Amendment's values, directed towards the protection of any person from any abuse of power.

Section 230 of 1996 *Communications Decency Act* from US Congress Acts has been a key ally of surveillance capitalism: it protects site owners from penal consequences of contents generated by their users. According to Section 230, sites are not editors, only intermediates, hence the paradox: the more providers attempted to protect its users

from obscene or damaging contents, the more they could be persecuted for such contents.

The statute perfectly aligns with surveillance capitalism, for which contents are the source of behavioral surplus, just as much its creators' patterns of connection, communication, or the metadata expressed by the emoticon, punctuation or abbreviations used are. Section 230 protects whoever not only hosts contents, but uses them to extract personal information: Facebook, Google and Twitter are recalcitrant in removing any kind of content, and their legal representatives are ready to fight any attempt of eroding the act.

The elective affinity

Before 2001, in respect of the debate about web privacy, the US Federal Trade Commission was in favor of autoregulation, but recognised that it wasn't sufficient to protect the privacy of individual users. More than half of FTC members subscribed to a report directed towards the regulation of online privacy through laws: they gave recommendations regarding how information practices should be clear and abundant, such as it would be consumers to choose how companies could use their personal data; if this report would have led to an official law, at least some elements of surveillance capitalism would have been examined or subjected to public judgment.

But the FTC attempt did not last long: with the terrorist attacks of September 11, 2001, the whole debate moved from privacy to safety. Every agency or institution was requested to break down any wall and mix up their datasets, in order to obtain information and produce complete analysis. As David Lyon said in his 2003 book *Surveillance after September 11*, the suspension of normality was justified by fighting terrorism.

The 9/11 attacks changed the way the government saw Google, the practices they had tried to fight now had become strategic needs. Both institutions wanted accuracy, and their determination in obtaining it sustained their elective affinities and the prosperity of surveillance capitalism mutation. As stated in the 2015 article *How the CIA made Google* by British journalist Nareen Ahmed, US Intelligence acted as an incubator for Google through a combination of direct funds and informal network connections, strictly aligned with US Pentagon's economic interests.

In 2010, ex CEO of US National Security Agency Mike McConnell wrote on The Washington Post the surveillance operation by Google within the extraction, collection

and analysis of personal data were as much coveted as taken for granted: he stressed that en efficient cooperation between the public and the private sectors was necessary in order for the information to move faster when needed.

We can conclude that the exceptionalism of surveillance capitalism, as defined by Professor Zuboff, contributed to direct the evolution of information capitalism, shaping a frame in which Google's operations were needed and not disputed.

The fortresses

What protected Google and other surveillance capitalists afterwards from criticisms and political interferences was based on four key scopes:

- Google competences, undeniably useful during election campaigns

  The company proved that its predictive capabilities generated from behavioral surplus were able to not only enrich surveillance capitalists, but also to help candidates to win elections. According to research by media experts Daniel Kreisler and Philip Howard, during the 2008 Obama campaign information about more than 250 millions of Americans were collected, in particular relational and behavioral data from the official campaign site and from Facebook. The persuasion score identified how much an indecisive person could be actually convinced to vote for Obama.

  The employment of behavioral surplus and its predictive power was kept secret during that period, in order to stay one step ahead of the Republican party.
- Deliberate blending of public and private interests: the company implemented a sophisticated lobbying system at national level to fight any law proposal for privacy improvement or limitations of behavioral surplus' operations.
- The "sliding doors" system created between Google's personnel and Obama administration, based on elective affinities, between 2009 and 2016

  The political web of Google allowed an significant and fast exchange of employees between the power cores of East and West coasts.

  The Google Transparency Project analyzed the staff movements towards the company's affiliates, law firms and the government during Obama's mandate. Before April 16, 2016, 196 people moved from government to affiliated companies, and 61 vice versa; among the latters, 22 officers of the White House had started working for Google and 31 Google managers entered into

federal advisory committees of the White House that also treated cases in which Google was involved.

- The influence campaign over public discourse over academic research, fundamental for shaping public opinion and political perception

  In 2012, the Washington Post published an investigation about the three seminars organized at the Law and economic Center of Mason University, Virginia, about competition over Internet search engines; it was highlighted the expertise of the speakers, but no one was aware of the fact that the main event organizer was Google itself and the speakers were all pro-Google as being for the majority its employees.

  Moreover, in 2017, an article by the Wall Street Journal revealed that since 2009 Google has looked for and fund university professors to carry out research and policy papers to support Google's stand in respect of laws, regulations, competition, patents and more.

The opinion shared among many journalists is that Google is the most influential company in the US.

1.4 The imperative of extraction

Google wants to offer a search engine that understands immediately what the user wants; in order to produce such an experience, the company submits to the imperative of extraction, which requires increasing replenishment. The supply started through Search, then it expanded among new areas, more ambitious than clicks and queries: currently, behavioral surplus' archives include any element of the digital world, such as searches, emails, pictures, chats, videos, preferences, social networks, songs and so on. The global pervasiveness of computers is such that we produce behavioral surplus any time we interact with Google, configuring an **architecture of extraction**.

This process was born online, but it is now expanding in the real world. Google is investing in home automation, and Facebook is developing drones and working on augmented reality; these activities are often praised as visionary investments, but even if they seem uncorrelated with the main core of the company they are all finalized to capture behavioral surplus. The pursuit of new innovative businesses concurs to the expansion of the extraction architecture, to acquire the amount of raw materials necessary to sustain the increasing production of prediction products, crucial to earn new clients.

New forms of provision are constantly assembled and tested, only some become operational; those that produce huge and reliable results, as it was Gmail, are further elaborated and institutionalized.

When the behavioral surplus was discovered, Google Search was the first service of Google to be refurbished as its extractor; those changes were not known. In 2010, Benjamin Edelman_ from Harvard Business School studied which adjustments were made, and discovered the "finer" option of Google Toolbar: this plugin of the Microsoft's Internet Explorer browser allowed to make searches without running google.com; once recorded, it transferred to the company's datasets the URL of any pages examined, including the researches made on search engines by competitors (hence simultaneous theft from users and competitors). This option was very easy to activate but impossible to deactivate: even when the user specifically disabled it and it was appearing as such in the toolbar, the device kept tracking the browser's activities.

Google is still the most used search engine, its many tracking systems and its inevitable cookies, bits of tracking codes inserted in our devices, guarantees scale economies to build its supplying operations.

In 2015, Internet law expert Tim Wu collaborated with Micheal Luca from Harvard Business School and other scientists to study the hidden tools of Google Search: they found that, to expand their collecting operations, the results were systematically infiltrated to favor its contents and derived products. Through the universal search feature, Search is both search engine and content provider, able to intentionally exclude any concurring contents.

These conducts could be considered monopolistic: because of the necessity of constant behavioral surplus, companies are pushed to pursue exclusivity; the extraction imperative requires to possess anything, and to keep expanding to any information that could have been missed. In addition, Google hinders competitors not to gain the power to fix prices, but to protect its main source.

The emblem of the monopolistic attitude of Google is its Android platform, its second source of raw materials. Developed in 2008 and presented as an open and integrated stage for mobile devices, Android was considered the opportunity for Google to compete against Apple within the smartphone market. Google provided for free the android license to mobile devices' producers, in order to force Google Search into users and introduce a mobile system of extraction. In 2011, Bill Gurley, an important venture capitalist of Silicon Valley stated that,

with Android tools, Google was removing any level of separation with consumers, and it was doing that for cheap.
Contrarily to Apple, the Android platform was “open source”, hence more accessible to any app developer. Google collected their apps in Google Play Store: together with the license to pre-install the platform in their devices, producers were obliged to also buy the licenses of Search, Gmail, YouTube, Maps and so on, and set them as exclusive or default options.

Google opposes any limitations to its extraction operations.
In 2009, Motorola replaced Google geolocalization services with those by Skyhook Wireless, considered more precise. A Google’s product manager expressed his concerns regarding the possibility of other producers choosing Skyhook over Google: despite admitting the superiority of the competitive service, reducing the collective operations would have been a disaster, because the company needed information about Wi-Fi location. Skyhook ended up suing both Motorola and Samsung, which didn’t change their product under the press received by Google.
Another legal battle was with Disconnect Inc., founded by two former Google engineers and a privacy lawyer. They developed desktop and mobile apps to protect users’ safety, able to block hidden Internet connections not requested and invisible tracking sites/services suspected to spread malwares. The Disconnect software was banned from the Google Play catalog in 2015.
After many tries of negotiation, Disconnect joined other companies in filing a complaint against Google to the EU, which had already opened an investigation about Android operations in 2016 through the antitrust offices. According to their representatives, Google answers to the requests of its investors for better tracking systems, in order to increase their profits: that’s why giving users the possibility to protect their privacy or shielding themselves from malwares and hidden connections is a threat to their work.

Among the researches regarding the size of Google’s extraction architecture, the Web Privacy Census from Berkeley Law School quantified cookies in 2011, 2012 and 2015, comparing the top 100, 1000 and 25000 sites of those years. In contrast to 2012, in 2015 sites with 100 or more cookies had doubled up, and those with 150 or more had tripled; visiting the 100 sites meant collecting more than 6 thousand cookies, 83 per cent related to third parties uncorrelated to the visited site. The study detected the Google infrastructure in 92 of the top

100 sites and 923 in the top 1000, and concluded that the company's tracking capabilities were unmatched.

In 2017, a Chinese team investigated the secret process through which an app quietly launched other apps in the background of the device. Analyzing 10 thousand apps from the main app stores, they discovered that this crash was particularly present in Android collaborators' space. The top 1000 apps from the most famous Chinese platform, 822 launched on average other 76 apps, and 77 per cent of these were activated by push services to update the apps; the latter has always been offered by Google in the Android context.

According to the 2017 research by the French organization Exodus Privacy, in collaboration with Yale Privacy Lab, there is a whole industry producing tracking software. These trackers could be in any app, spreading when they get downloaded; any app believed "clean" could contain some that are still unidentified, and in the future developers could even directly insert parts of tracking codes in the main algorithm. According to the scheme implemented by the 2003 *Generating User Information for Use in Targeted Advertising* already mentioned, the tracking activities aren't limited by the "consent system" that Android proposes and that should work according to the user's preferences.

1.4.1 The cycle of dispossession

In order to fulfill the expropriation, Google had to fulfill a series of political, social, bureaucratic and technical actions, converging with managerial decisions to set a frame that would have lasted for long. To be properly institutionalized, the expropriation contemplates four phases: incursion, habituation, adaptation and redirection.

The unilateral incursion in an unprotected space, for example one of the digital devices we use everyday, is launched when personal information starts to be collected from outside the market. Google learned to initiate the process and proceed even in front of resistances; there are too many unresolved legal procedures against Google coming from people, companies and even countries, and even more that aren't even publicly known.

The habituation happens because people accept or resign to the incursion; lawsuits and institutional investigations are slow to come off, and Google can keep operating with its fast pace. If some adjustments are required, managers and engineers proceed with superficial but tactically efficient adaptations, to take care of the most urgent matters regarding judicial sentences or the public opinion. Finally, the company implements new gimmicks or features to redirect the contested operations, to adjust them to legal or social obligations.

The first complete cycle was carried out with the introduction of Gmail, when in 2004 the users were shocked to know that contents of their private mails were scanned to get the information around which to build a targeted ad.

1. Incursion

To introduce Street View, in 2007, Google privacy consultant Peter Fleischer stated that people weren't expecting to enjoy the same levels of privacy they had at home while being in public contexts. With the new service and its other mapping apps Maps and Earth, Google wanted to reach and know any corner of the world: the company assured that the big rotating camera, assembled over some funny looking cars, was designed to respect the privacy of those that found themselves on the same street, and that they already had prepared the procedure to follow if someone wanted their image to be removed from the app.

The flack spread fast, but John Hanke, at the time Vice President of Google Maps, dismissed the situation saying that it was just the start of that period in which people are trying to understand something new. He also belittled the formal complaint that the Privacy International charity filed to the British privacy authority, quoting more than 200 people that had asked to stop the service after having been identified on Street View; he stressed that the information obtained through the app was actually useful to the economy and people.

In 2010, the German federal commission for data protection revealed that Street View cars were actually stealing data from private Wi-Fi networks. Google retorted that they were only collecting names of public Wi-Fi networks and IP addresses, but an independent analysis by German experts proved that the company was extracting any non-encrypted information from the private Wi-Fis. Google was then obliged to admit they were extracting "useful cargo", such as mails, URLs and passwords.

The "Spy-Fi" scandal was the first event after a long time that many believed would be the one actually damaging Google. German politicians reacted to the investigation proposing to the Parliament to fine Google for disposing of private properties without any consent, followed by Switzerland, Canada, France and the Netherlands.

Google defined the privacy violation of Street View as a mistake by a single engineer while experimenting with coding. Schmidt admitted to the Financial Times that the company "made a mess", and that the engineer had been subjected to internal scrutiny. A 2012 investigation by the US Federal Communications Commission stated that the event originated from a deliberate decision taken regarding the app design: the

engineer had been selected for his unique expertise in localizing Wi-Fi networks while moving, *Wi-Fi wardriving* as defined by Denis Howe. Data traffic and users' position would then be cataloged as offline information to use for other scopes. The FCC investigation also included the communications between the employee and his project leader, which proved that he knew Street View was collecting personal data. Despite finding such evidence about the attempt of Google to find a scapegoat, representative engineers denied being aware of the privacy violations.

2. Habituation

From 2010, the FCC asked Google to collaborate in the investigation. The various responses were characterized by incomplete information and elusive statements: Google hinted that they were having a bad time in researching or verifying what the FCC was asking. The agency requested an affidavit five times, and Google agreed only after September 2011 because they were threatened by a subpoena; the engineer refused to speak with detectives, quoting the right of no auto-incrimination from the Fifth Amendment. Eventually, the FCC commanded a 25 thousand dollars for investigation obstruction: Google was able to avoid any consequence because there were no significant laws to protect citizens from its practices.

We can observe the habituation tactic from the scapegoat trick, but especially from the fact that Google kept Street View active during the whole investigation: starting from the first incursion in 2007, through the 2010 outbreak of the scandal and the 2012 and 2013 closures of both the FCC and German investigations (the latter obtained very little results compared to the efforts made).

Between 2008 and 2010 Google illegally collected 600 billion bytes of personal data from all over the world; the company has declared that they got rid of the archive, with no one to check if it's true.

3. Adaptation

In October 2010, just before receiving the first FCC communication, the Senior Vice President of the Engineering&Research department announced that tighter privacy controls would have been applied, as a consequence of the mistake they admitted (which was still presented as involuntary). The post, published on the official corporate blog, assured the public the company was also referring to external bodies of

control in order to set eventual policy improvements. They were “mortified” for what happened but sure about the positive impact of these structural changes.

Still, apart from these promises, Google had to adjust to governmental requests from all the countries that sued Street View, such as Australia, Belgium, Israel, Poland, and many more. For example, to satisfy the almost 250 thousand Germans that requested for their houses to not appear in any shot, Google had to hire 200 programmers. The data protection supervisor that firstly observed the illicit operations by Street View fined Google for 145 thousand euros: despite being the highest fine ever imposed in Europe for privacy matters, it was nothing compared to the company’s income. In 2011, Google closed the German Street View project, keeping up the shots already processed but stopping to update them.

4. Redirection

Despite the apology declaration, the implicit message was that any Street View adjustments won’t have canceled any data already captured. Google didn’t want to give up on its accumulation logic or slow down the app’s operations, also there was not much to do to guarantee privacy.

After two years of actions to restore Google’s reputation regarding privacy, in 2012, an ex detective of the Street View investigation identified the “bad engineer”, Marius Milner, a famous hacker and specialist of wardriving. It became clear that nothing really changed: despite being officially accused by Google to have committed serious violations, he was still working for the company, in the Hanke’s team working on a feature of Ingress, a new game (which would become the trial version for the basic concepts of the successful Pokémon Go).

Thanks to the experience built with Street View, Google learned to sustain even the most controversial expropriation attempts, if necessary to get new behavioral data.

Emblematic is Google Glass, which combined informatics, communication, photography, GPS, audiovisive recordings and data capture in a pair of glasses, a wearable device; any personal information was then sent to Google servers and converged in the big behavioral surplus storage.

Google Glass was considered the precursor of any extraction wearable device. Hanke said that the shape chosen to introduce such innovative technology was the traditional one of glasses to reduce the sense of disorientation derived from something completely new.

Of course, the continuous (but not identifiable) recordings by the device while walking cut out any privacy expectancy, in particular considering the software of facial recognition provided in any device . In 2013, a caucus of the US Congress requested Page reassurance regarding privacy protection; in 2014, a Pew Research survey revealed that 53 per cent of American men and 59 per cent of American women viewed wearable devices negatively. Google would have resisted any criticism (confiding in people's habituation), and Brian made it clear when in 2013 he mockingly declared that "people are naturally adverse to innovation".

The adaptation phase started in 2015: still not recognising any public rejection, Google announced that the glasses would not be available anymore, but just because they were developing improved versions of them. Schmidt, now Google CEO, stressed that the platform was fundamental for the company, they just wanted to prepare the public to what it would have inspired as pioneers of their wearable innovations.

Finally, the redirection phase became official with the introduction of Glass Enterprise Edition. Instead of public space, the platform would have been used in those work spaces where it is easier to normalize invasive technologies, such as the manufacturing and logistic sectors, or health care; in the presentation, it was highlighted how useful to get information and other resources while doing such jobs that "keep your hands busy".

Google Glass represents how, to keep following the extraction imperative, new ways are built to get around any obstacle.

1.5 The division of learning

If once "doing a good job" referred to physical tasks with raw materials and equipment, today it has to do with the ability to analyze data and employ algorithms in order to decide the next step in business. As stated by Professor Zuboff, the ordering principle of the workplace went from division of labor to division of learning.

According to a Brooklyn Institution report, the fast spreading of digitalisation is cutting off average workers from job opportunities: it is stressed that companies should urgently invest in improving the computer skills of future employers, being the crucial element of increased productivity.

The decision to employ "smart" machines instead of "smart" people is defined **work polarization**, with the separation between high skills and low skills jobs and machines doing the majority of those jobs in the middle. Despite many business leaders, economists or tech experts state that this is the inevitable consequence of the use of computers, academic research proves that the division of learning reflects (neoliberal) political ideology; in fact, in

Europe, where some elements of the double movement survived, the polarization is tempered by significant investments in education of the labor force.

In the 20th century, Adam Smith defined the division of labor as the most efficient principle of industrial organization, through which increasing productivity and therefore profits. Durkheim recognised productivity as an economic imperative of industrial capitalism, but focused on the social transformation it was carrying on: specialization was becoming very prominent. He speculated that the objective of the division of labor was connecting people of the modern industrial society in a perspective of solidarity, understanding each others' needs in respect of the new conditions of human existence. In his 1893 dissertation *The Division of Labour in Society*, the sociologist stated that division of labor was establishing a new moral and social order. The worst and most dangerous drift was labor specialization, that would have produced a disaggregated and confrontational society: the consequent inequality would have set an extreme asymmetry of powers, which would have kept people unable to fight for their role as active people of their community.
For us people of the second modernity, division of learning represents the same dangers.

Professor Zuboff theorises that surveillance capitalism control over the division of learning starts from what she calls the **two texts problem**. The first text is produced through the data we release online, both in what we research and the contents we publish on social media. The second text is the shadow of the first, so Zuboff defines it as the shadow text: every information on the first text is taken as raw material for the second, like a confidential communication for surveillance capitalist we are unable to not produce and share. Google, Facebook and any other surveillance capitalist has algorithms that select and order our data to be sent to companies that want us as clients.
According to the logic and the dynamics of surveillance capitalism, the shadow text must remain secret and must keep increasing. The asymmetries in knowledge and within the Internet architecture are what keep the mechanism going.

A double movement is missing in linking capitalism of information and people's interests. Surveillance capitalism arrived in the US in a pretty much lawless context, then it spread to Europe and keeps doing so all over the world thanks to a relative absence of contrasting regulations. The concentration of knowledge has produced such asymmetries that Zuboff

defines as unauthorized privatization of society's division of learning: it means that powerful private interests control the social order of our times.

1.6 The competition

The ascendancy of Google through surveillance mechanisms started a war over extraction constantly escalating. The first was Facebook, still today the main competitor, that rapidly learned how to master the dispossession cycle.

One of its first tools was the like button, introduced in 2010 as a way to keep in contact with friends. It didn't take long for privacy doctoral student Arnold Roosendal to publish his research about how that button installed cookies in users' PCs even when it hadn't been clicked on: it captured the behavioral surplus and was actually able to track even people that weren't Facebook users and therefore it could potentially connect the company to any Internet user. Zuckerberg had already defined all the violations his company was accused of as oversights, so he kept the act on defining "bug" Roosendal's discovery.

A year later, Australian hacker Nik Cubrilovic disclosed that the app kept tracking its users even after they logged out. In response, Facebook announced that they would have fixed the glitch, but even if some cookies were wrongly tracking users, this function couldn't be totally deactivated for "safety and performance" reasons. In addition, just three days before Cubrilovic's statements, journalists discovered that Facebook had patented some techniques to track down users on web domains: such procedures allow to trace personal profiles based on social media presence, collect feedback from third parties sites and put everything together to produce targeted ads. The company denied the relevance attributed to the patent and any other accusation, gaining time to institutionalize the phase of habituation.

In 2011, during the adaptation phase, an FTC investigation started in 2009 settled with a resolution according to which the company could no longer lie about their privacy treatment, and users would have had to give their explicit consent; moreover, a general programme about privacy was imposed, to be submitted to external judgment every two years for 20 years.

Then, the redirection phase began. In 2012 Facebook announced that it would have sent targeted ads based on the apps used, in collaboration with Datalogix (now Oracle Advertising) to define how many online ads actually translated into offline shopping. Advertisers got access to data such as mail addresses, phone numbers, visited sites and private messages, plus all the like buttons automatically activated in respect to shared links. The general privacy

programme requested by FTC informed users through few adjustments on their traditional long and complex terms of service, and still no opt-out option was given.
Facebook income grew greatly. In 2017, the Financial Times praised the company, its capitalisation of almost 500 million dollars and a monthly average of two billion active users; advertising, mobile one in particular, made up almost the totality of the profit, 9.2 billion over 9.3, with a growth rate of 47 per cent in respect of 2016.
In 2017, in her article *Google and Facebook Bring in One-Fifth of Global Ad Revenue* for The Guardian, Julia Kollewe stated that, compared to 2012, the two companies were responsible for the 90 per cent increase of ad expenses in 2016, making them indispensable for any other company.

Among the other major Internet companies, it was clear that Microsoft had lost many opportunities to compete with Google and develop something regarding targeted ads. The 2014 CEO Satya Nadella publicly admitted that their search engine Bing couldn't compete with Google because it wasn't able to obtain the behavioral surplus quantity necessary to carry out scale operations; not having enough data meant less accurate and relevant ads. Search engines are evaluated in respect of their ability to collect data, not their efficiency. Nadella commissioned an investigation regarding marketing intelligence, and announced that the company would have swerved towards competition over data collecting: his initiatives aimed to catch up with other surveillance capitalists and use behavioral surplus to improve their means of production. In 2015, with Satori, a Bing learning system able to collect an amount of data comparable to what was contained in 28 thousands dvds, Microsoft closed in profit, thanks to the proceeds made with advertisements.
Another extracting strategy with Bing engine was implemented in 2015 through Cortana, the digital assistant. As reported, even if four out of five queries go to Google through the browser, with the Windows 10 taskbar (to access Cortana) Bing received five out of five queries. Moreover, apart from the data obtained through research, it was suggested that Cortana would have worked better if people signed in a personal account and connected to other related services. Just as the automatism of Google, Cortana was able to learn about its users: this feature was described as "progressive", not "automatic", in order to not scare people with their devices taking over their life. According to Nadella's vision, Cortana will become a platform to have casual conversation with, delivering to databases an enormous amount of personal information.

An Ars Technica investigation revealed that users were pushed towards the *express install* function that activated the default settings needed to send the maximum flux of information to the company's servers; even when such set timings weren't activated or Cortana was disabled, the system would keep sending information to Microsoft.

In 2016, Microsoft acquired LinkedIn for 26.2 billion dollars: it would have allowed it to collect the so-called *social graph* from the 450 million users, their behavioral data from social networks. Hence, together with Cortana, Microsoft was now able to build a complete profile of its users and increase the accuracy of targeted ads, even in relation to their professional career.

Nadella and Microsoft have been rewarded for their breakthrough towards surveillance capitalism: in January 2017, the company's capitalisation was over 500 billion dollars for the first time since 2000, and its shares were valued 65.64 dollars each.

Chapter 2 - **The enabling structure**

If and when practices of surveillance capitalism are known, they are definitely not accepted. So how could this form of market have so much success?

1. During the first raids of Google, Facebook and other surveillance capitalists, the innovative practices and proposals intrigued everyone and didn't cause the anxiety it should've.
2. The system developed under the zeitgeist of neoliberalism, which favored autoregulation and preserved the lack of necessary control legislation. Moreover, after 2001 the US government relied on the elective affinities with Google and its technologies: the war on terrorism allowed the company to escape controls and furtherly develop.
3. Google, Facebook and others' services answer latent needs of today's society: the means of social participation end up matching the means of behaviors' prediction.
4. We are assisting the diffuse institutionalization of a network of allies towards the surveillance capitals: the key locations of the market are characterized by low risks, dynamicity and high profits; furthermore, the concepts of AI seem so distant that trying to control its expansion seems impossible.
5. The spread of surveillance capitalism set a sort of dictatorship of lack of alternatives: we are showered in the rhetoric of inevitability of technological progress, which discourse by companies and its leaders was built to leave us feeling powerless and ignorant.
6. Surveillance capitalism is characterized by unprecedented speed of growth, such that both academic learning and legal systems aren't able to keep up with its innovations.

Discussions regarding data property, encryption and other tools to protect privacy are much needed to consciously and actively participate in the surveillance economy.

2.1 The infrastructure

The capability of the world to produce information has largely upraised its ability to process and store it. In 1986, only one per cent of the world information was digitalised; in 2000, it became the 25 per cent; in 2013, the digitalisation and datafication processes, together with storage technologies, allowed the digitalisation of the 98 per cent of world information.

The power of Google, gained from the political and social context previously presented, couldn't perform without the gigantic material infrastructure the company built with its revenues.

Hyperscale operations are performed through data centers, which require millions of “virtual servers” to exponentially increase the extraction ability without needing further physical space, electric energy or cooling time. Google is the pioneer of them: according to 2016 estimation, its system includes customized data centers in 15 locations, with 2.5 million servers in four continents; Google power depends for the 80 per cent on its infrastructure, its means of production.
Google is known as a full stack AI company, of which domain is reinforced by the fact that its algorithms can exercise and learn thanks to the available data; and as we know, no one has more data than Google.

In 2013, they understood that the direction in which AI development was going would have significantly increased the needs of computational capabilities, and consequently required the doubling of data centers. If the company would have tried to process the kind and quantity of information they wanted with their traditional CPUs, they would have needed to exponentially increase their entire footprint.
In 2016, Google announced the development of their **Tensor Processing Unit**, a new chip for high learning inferences. The TPU would have greatly expanded the capabilities of Google’s AI while consuming much less energy than the already employed processors, hence reducing the operational budget while learning much faster. It was expected a 56 times increase in the company’s revenue from AI products and services, from 644 million dollars in 2016 to 36 billions in 2025.

To properly exploit the opportunity represented by this material infrastructure, an arms race started between tech companies, to get experts from all over the world and gain the necessary knowledge to actually transform the colossal amount of data they will collect into actual profit. Between 2014 and 2016, Google acquired nine AI companies, twice as much as Apple.
The concentration of AI experts between Google's employees reflects a larger tendency: it was estimated that in 2017 American companies spent 650 million dollars to get the best AI talents, and of course the main Internet companies can count on much more money available to realize it. In the UK, academics define it as the lost generation of data scientists: these big salaries attract professionals to gather such knowledge in only a few companies instead of spreading it among the society, like start-ups, universities, companies from other sectors or in developing countries.

2.2 The ubiquitous computation

In 2015, at the World Economic Forum in Davos, Switzerland, Schmidt was asked about the future of the Internet: he declared that it would soon disappear, because the increasing presence of digital devices, sensors and wearable interactive tools would merge it to human existence.

This statement reflects the 1991 article *The Computer for the 21th Century* by computer scientist Mark Weiser, in which the ubiquitous computation was introduced: according to him, the deepest technologies are able to disappear because they bind to the human context until they result indistinguishable. Weiser stated that the virtual world is just the shadow of the real one, despite absorbing its data: it is just a simulation of the latter and it doesn't add anything to the reality, while the ubiquitous computation would have merged a universally interconnected system into it. This is defined as computational environments, with unlimited knowledge and possibility to also perform retroactive analysis.

Surveillance capitalists cannot allow the end of the Internet, nor its liberation from digital devices. Their profits depend on their competitive position among the behavioral futures markets: even performing the best conversion processes, the accuracy of the prediction products depends on the raw materials used; therefore, they need the most reliable behavioral surplus. Such urgency forces the **imperative of prediction**.

The first wave of prediction products led to online targeted advertisement: the competition to obtain behavioral surplus in scale quantities is ruled by the imperative of extraction; however, the development of surveillance capitalism made behavioral surplus necessary but not sufficient to be successful: now the competition is based on the quality of prediction products. The prediction imperative pushes towards prediction products approximable to the actual observed reality, that's why the disappearance of the Internet is so sought after.

In order to improve their predictions, surveillance capitalists understood that they needed to diversify and enlarge their extraction architecture: procurement operations would be performed through the traditional scale economy, joined by intense scope and action economies.

To implement scope economies, behavioral surplus has to be huge and varied. Such variety must be developed within two dimensions: the extent of extraction operations, passing from the virtual to the real world; the depth of the research, based on the idea according to which the most predictive behavioral surplus comes from the most intimate and private dynamics.

The objectives of the extraction are our mood, emotions or reactions to events and conversations from our everyday's life.

Still, just as scale economies, also scope economies are necessary but not enough to create prediction products that would guarantee a permanent advantage over the behavioral futures markets. Surely, the best way to predict a behavior is to intervene at the source through economies of action: the machines' intelligence is configured to participate in the reality and increase the accuracy of things to happen.

The binomial scope-action, as defined by Professor Zuboff, increases the intrusiveness of extraction operation, actualising Weiser's vision of ubiquitous and automated computational processes merged to everydays' life: Zuboff calls it the **reality business**. There are many expressions trying to hide the economic interests behind such practices, for example Internet of Things (**IOT**), but the logic behind the system is always that of surveillance capitalism.

The action economies required matching the extraction architecture (the one that knows) with the execution architecture (the one that does): together, they force "secret" business objectives onto many behaviors. Surveillance capitalism imperatives and its infrastructures implement extraction and execution operations and end up creating the **means of behavioral modification**, whose aim is not to force a certain conduct but to induce a reliable behavior that leads to certain commercial outcomes.

As stated by Gartner research manager, mastering the IOT will secure the transformation of any business from guaranteed levels of performance to *guaranteed results*.

Professor Zuboff stresses that while it is possible to imagine the IOT without surveillance capitalism, it is not possible to imagine surveillance capitalism without the IOT: the new system reflects the prediction imperative and the compulsive attitude of achieving accuracy.

2.2.1 The human flock

Telemetry technology combines biology, physics and electronic engineering, providing the long distance transmission of computer data. In 1964, it was used by R. Stuart MacKay and his team during their international expedition to Galapagos. He was interested in the key feature of the compact transmitters they were using, which allowed them to collect behavioral data of the animals in their natural habitat, not interfering with their psychological and physiological conditions.

From the resulting publications, it emerged the capability of telemetry to capture huge datasets and combine them to study correlations between the whole fauna. So, the first generation of wearable technologies allowed to study wild animals, unaware of any incursion.

Moreover, MacKey affirmed that data transmission and monitoring could also work in reverse: he theorized a counter telestimulation able to both capture behavioral data and reveal how to optimize it.
The farsighted theories of MacKay have been actualised in the digital era: satellites, the exponential growth of computer capabilities, advanced sensors and Internet networks produced extraordinary prediction systems applicable to whole populations.
The need of large and deep scope economies reflects the intention to collect detailed information about people, while the inverse telestimulation revives in action economies that tickle a conduct just to increase its predictability.

MacKey's legacy is relieved by Professor Joseph Paradiso from MIT Media Lab, where surveillance mechanisms such as data mining and wearable technologies are designed. His team of scientists is working through datafication, browsing, indexing and research, in order to create the ubiquitous sensors necessary to actually build a ubiquitous environment.
They developed an inertial sensor that tracks complex movements and perceptive fibers that should bring electronics in any malleable thing: these are electronic components that attach directly to the skin, while wrists are used to capture fingers' movements even without the hands moving.
Paradiso and his teams found themselves dealing with proliferate sensors in basically any environment but with the relative difficulty of integrating many data in order to produce significant analysis. Hence, they created *DoppelLab*, a digital platform that combines and visually represents data from sensors: the goal is to transform any physical space in a browseable environment in which any data will be constantly collected through sensors. Paradiso affirmed that when we enter the wearable devices' era, information will flow directly to our ears and eyes. He says that the next tech challenge will be the aggregation of contexts, the assembling of the huge amount of data coming from sensors of all the new apps.

This vision of an uninterrupted nervous system of the society seems to not be aware of surveillance capitalism, its imperatives and what such technologies would mean for it. The competition to become the "new Google" of the new extraction and execution architecture already began. According to an International Business Machines Corporation report, we are witnessing the liquefaction of the physical world: thanks to the IOT, physical goods are easily indexed, researched and traded, so they are becoming part of the digital world in real time.

In parallel to the rhetoric of waste data from the first phase of surveillance capitalism, the term **dark data** refers to those unstructured data collected by companies, hard to codify or datafy because they cannot be included in functioning circuits for data circulation: these information cannot be used until rendered as a behavior and transformed into observable data. Basically, dark data are those detected behavior or conditions not conceived to be public: those that wants to get rich through surveillance methods consider dark data as remunerative and indispensable, but only if they are able to process them and include them into their prediction products, or else they must be treated as the unknown to cut out.
IBM invested in Watson, introduced as the "IOT brain": they want to make the most out of its learning capabilities to translate ubiquitous data and dark data into ubiquitous actions.
The new tools of surveillance capitalism are projected to render any bit of action or situation from all over the world to a huge behavioral flow: in the current totalitarian conception of the market, any living or inanimate entity share the same existential state, it is processed as something objective, measurable and browsable.

2.2.2 The implementation

Hal Varian, Chief Economist at Google, wrote about transactions via computer, and the way these happen: data extraction and analysis, new contractual forms, customisation and continuous experimentations.
Data extraction and analysis is what everyone refers to when we talk about "big data", the raw materials of surveillance capitalism. "Extraction" refers to social and material infrastructure with which the company imposes its authority over data, to obtain significant quantities of it and be able to sustain a scale economy. "Analysis" refers to the specialized computational systems, basically the artificial intelligence of the machines, that convert raw data into lucrative algorithms able to predict the consumers' behavior. This transaction reflects the importance of extraction imperative for surveillance capitalism.
Varian stated that the following three ways would have become even more important than data extraction and analysis over time, and the time arrived. Any transaction is mediated by computers, therefore now it is possible to observe certain conducts not discoverable before and use them as contract basis.
He uses as an example the vehicle monitoring systems, thanks to which insurance companies today are able to check how their clients drive and choose how to manage their insurance plan. Such computer mediation in the context of insurance companies depends fully on

connective devices that allow scope economies, and even action ones if it was possible to make the car unfunctional if the owner didn't pay the monthly installments.

The prediction imperative moved the actions within the real world, and suppliers of goods and services uncorrelated to Silicon Valley are now interested in surveillance revenues too.
For example, automotive insurers seem to agree with the vision of Varian and the telematics of MacKay: they have known the correlation between risk and behavior since forever, but only today's long distance monitoring systems enable to know our and our cars' state. Telematics produces data that can substitute the traditional demographics employed to estimate the risk: through the approach of behavior coverage, insurers can minimize their risks. Even small companies that do not have much capital to invest can use mobile apps for the same purpose, cutting out the expensive hardware and data transmission expenses.
The economies of action pictured by Varian are not that unattainable. For example, Spireon is a telematic company of the automotive industry specialized in localizing and monitoring of vehicles on behalf of insurers or renters: its system of "rent with collateral management" alert driver when they are late in their payments, deactivate the car after a certain period and localize it for the distraint.
Thanks to telematics, insurance companies can now apply specific behavior parameters, transformed into algorithms that monitor and evaluate the drivers' conducts in real time. According to Sprireon's patents, the aim is to optimize insurance plans' prices based on how much the drivers' conduct adhere to parameters set by the company, also assigning prizes or penalties accordingly; from the behavioral surplus collected, companies will also derive prediction products for advertisers, that will connect to drivers directly through mobile ads.
The future value of the IOT applied to the smart car will be revealed only when the change in conducts of drivers will be evaluated after receiving feedback from their devices.

According to Deloitte Center surveys, the majority of consumers reject telematics for privacy reasons. It is then suggested that significant savings would help to get over such resistance, and if not enough, companies should present the monitoring as funny or interactive, something that would differentiate who uses it from the average of insured: this approach is called **gamification**, which encourages people to take part in incentive-based challenges.
If it is still not enough, Deloitte suggests to induce a sense of inevitability in their clients: they have to internalize that the great number of technologies monitoring driving, the surveillance and the geolocation by now are part of daily life.

Co-marketing

Beyond the beneficial and efficient system that the automotive insurance industry is employing, they could earn even more. Data used for online ads are treated also in the real world, setting behavioral futures markets where prediction products are exchanged.

Cloud service provider Covisint suggests monetizing through automotive telematics, moving investments from target ads to target apps. Data used for your targeted advertisement will send information to your mobile apps regarding potential experience you could have while being in the place you are in that moment, according to what surveillance systems learnt about your preferences. The implementation of co-marketing refers to many services, such as road assistance, mechanical workshops, car washes, restaurants and shops; the owners of those businesses will be ready to pay for such promotion.

McKinsey consultants stated that insurers could use the IOT to expand in new areas: they could carry out telematics scale operations teaming up with Internet companies.

Among the many examples there is the 2016 IBM and General Motors agreement, through which they introduced OnStar Go, their platform of cognitive mobility for the automotive industry. Moreover, Dell and Microsoft launched IOT accelerators for the insurance industry: Dell proposes tools and services to analyze and predict risk levels, while Microsoft teamed up with American Family Insurance to develop a start-up for domestic automation.

With Maps, Google can already offer a telemetric geolocator to app developers. According to a Capgemini consulting company's report, 40 per cent of insurance companies see Google as a potential threat to their business and their data management operations.

A very famous example of co-marketing is Pokémon Go. The business model already contemplated collaborations: Niantic knew that many business owners would have paid in order for their locations to be included in the mapping system and therefore be sponsored by the game.

The non-contract

The example of insurance companies is simple but meaningful. Behavioral data from drivers' experience are processed and sent in two directions: to drivers as economies of action, to modify their conducts and make them more predictable and remunerative; into behavioral futures markets, where third parties' speculation become prices, incentives or monitoring regime. With digitalisation, it is now possible to observe behaviors and complete transactions

previously inaccessible: hence, new contractual forms are constituted, which bind in ways that would not be possible without the dispossession operations of surveillance capitalism.

The incursion we are undergoing represents the annihilation of the traditional contract as resolution of a relationship. Professor Zuboff calls this innovation the non-contract, with unilateral execution: fundamental for surveillance capitalism, it is the largest and more complex of its means of behavioral modification; it uses the behavioral surplus to implement economies of action, actualising the determinism of surveillance processes and obtaining prediction products approximable to reality.
The asymmetries of knowledge that characterize surveillance capitalism make it possible to use a non-contract to bypass social relations in favor of automated computerized processes.

The non-contract aims to realize what economist Oliver Williamson defined as *the utopia of the contract*, a condition in which perfectly rational people are perfectly informed and therefore act always according to the contract. But, as stated by Williamson, complex contracts are inevitably incomplete, because they will have to confront the necessity of adapting to any unattended event. But the surveillance economy applies the imperative of prediction, hence any human, legal and economic risk is adapted into a monitored, designed and maintained business plan, in order to secure the profit. This is more a *dystopia of the contract.*

The inevitabilism

The transaction to ubiquitous computation is told with what the tech community knows as the inevitabilist ideology. Its supporters posit a revolutionary phase change that will reassemble the society according to a new system. The rise of such a model is introduced using solemn words or historical metaphors: this contextualisation carries on the idea of how useless it is to oppose the settlement of the ubiquity.
Silicon Valley is at the center of the faith on inevitabilism: among high-tech leaders, scholars and experts there seems to be unanimous consent about the future and the fact that anything will be connected, known and processed.
Although the inevitabilism has strong foundations, within the context of the scientific community there is a evident lack of critical analysis: the concept of digital omniscience is taken for granted without analyzing its links to politics or market forces, and issues regarding individual autonomy, moral or social norms and the right to choose are set aside. Paradiso

suggested that laws should guarantee the property and the control over data in your proximity, so you could choose to encrypt or limit their accessibility: he's imagining a society in which individuals must protect themselves from ubiquitous computational systems.

The theme of supposed autonomy of technology has been treated by political theorist Langdon Winner: he stressed that modern life is characterized by the quiet acceptance of technological presence and evolution. This tech drift is defined as "accumulation of unexpected consequences": we surrender to technological determinism for society's sake, also because considering rationally the social implications is viewed as a retrograde attitude.
Google and the other surveillance capitalists want us to accept the realpolitik behind their automated processes. The inevitabilist ideology excludes voluntary participation, it distracts from the surveillance economic aìmbitions and their dispossession operation.

The battlefield

Surveillance capitalism domains, its dynamics and its tools are combined in a public space for people, in which its business can bloom: the city.
Cisco Systems, a multinational digital communications corporation, owns 12 **smart cities** all over the world, some of which adopted Cisco Kinetic, a cloud based platform that helps clients to extract, process and send data from digital devices to IOT apps. "To bring the right data to the right app at the right moment", while performing policies in support of privacy, property and data security.
This basically legitimates the concept of city for-profit.

In 2015, after the reorganization of Google in its Alphabet holding, Sidewalk Labs was introduced, and with it the term "Google city". Its public implementation started from the installation of many free Internet cafés in New York, to fight the digital inequalities. These places were data sources to further equip with sensors, in order to get information about hyperlocal conditions of the city.
In 2016, the US Department Of Transport announced a partnership with Sidewalk, to send data towards city authorities. The DOT organized a contest with a 40 million dollars prize pool: the winners would have worked with Sidewalk to include its technologies in city activities and develop Flow, Sidewalk's traffic management system. Flow employed Google Maps, Street View cars and machines' intelligence to get data from drivers and public spaces;

moreover, there are some algorithms set on specific conducts to manage the data flux, in order to monitor anything.

Columbus, Ohio, won the competition and started a three-year project with Sidewalk. From the collaboration, the resulting documents published by The Guardian, report ideas such the optimization of parking lots or the marketplace of shared mobility; the city administration was requested to invest a lot on the tech platform by Sidewalk: the company wanted the city to share data from public transportation with car sharing services, so Uber could send its cars to crowded bus stop.
The Flow Transit System merges information and payments from basically any transportation tracked by Google Maps, and any transit or parking service has to be paid through the mobile payment system by Sidewalk.

It is clear that Google city is a market operation guided by the prediction imperative. When Sidewalk announced its collaboration with 16 other cities, its CEO defined such projects as "inevitable".
The Wall Street Journal wrote that it was obscure how Google/Alphabet was able to get all the money necessary to execute such a large-scale operation, and that Sidewalk was trying to be independent from the city regulations.

2.3 The rendering

The expropriation of human experience is not only abstract: as defined by Professor Zuboff, the rendering is the set of practices that dataifies our information and activates the ubiquitous apparatus. The verb "render" refers to something that takes form from something else, hence the causal action of transformation; the same verb is also synonymous with surrendering. Such a term also belongs to the vocabulary of digital technologies: in fact, a rendering engine translates the contents of a html page in order to show and print them.
Technologies of surveillance capitalism render our experience and translate it into data without us being aware of it, but simultaneously we let our information available to such rendering operations any time we use an online platform.
Aware Home, only one year older than surveillance capitalism, was projected according to very different terms: people could choose which data to leave to render, data had to improve life conditions and people could also how and with whom data could be shared. Aware Home

proves that rendering can exist without surveillance capitalism, while surveillance capitalism cannot exist without rendering.

The market for smart house devices is proof that any kind of product can be reinvented to respond to surveillance needs.
The 2017 autonomous vacuum cleaner Roomba by iRobot was designed to capture the house plans of its customers, which sales were expected to be great; it was provided with a camera, sensors and mapping functions. According to the privacy policy, deactivating Wi-Fi or Bluetooth of the device, data would be sent only to the internal cloud, connected to the mobile app of the owner; of course, rejecting the full data processing meant to lose the majority of the tool's functions, such as remote activation or some deep cleaning features. Therefore, even if the data sharing is facultative, who rejects the render has to accept a demoted product.
Another example of unfair "contract" is the one related to Sleep Number bed and its Sleep IQ app for sleep tracking. Every bed is customizable thanks to sensors that change its slope and even its softness according to the preferences set; other sensors capture our body's activity during the night, such as the breathing frequency or the heartbeat. Every morning the app produces a report that gives suggestions regarding the improvement of your sleep; also, the company suggests connecting the device to a fitness app or the thermostat in your room, to automatically adjust the temperature accordingly.
The twelve pages of privacy policies inform about the consequent data sharing with third parties, even the creation of your profile on Google Analytics, to maximize the app's efficiency. Again, not accepting such conditions implies giving up certain features.
The distribution of biometric data or sensible images from inside the house has been recognised as dangerous, but courts have always declared that such companies are not actionable because it doesn't sustain a noticeable loss for the consumer.
Despite reaching disturbing developments, the smart house market is growing and becoming more profitable, offering devices such as cyborg bugs that collect sounds around the house or wearable baby monitors.
Increasing the environmental intelligence is the first phase of rendering, which in turn is the first phase of the composition of the shadow text; these practices set aside any discussion regarding consent or opt in/out options,

2.3.1 Body rendering

Having a smartphone always with us makes us traceable to anyone.

Location data are extracted from the information automatically recorded from photos or videos in which we appear. This is called *geofencing*, the report of a geographic area in which we are located and the consequent notices sent to our smartphones. Then, *geotargeting* is the ultimate form of mobile advertising, which can push to impulsive shopping just through notifications. *Life pattern marketing* provides localized data collection and similar through mobile phones, sensors or satellites, in order to crack the conduct of someone and foresee their future behavior. Market actors of these industries know the impact of these operations in their consumers' psychology.
We could deactivate GPS on our smartphone, but the majority of people don't do it to keep the full functions of their phones. In their 2014 research, computer scientists Arvind Narayanan and Edward Felton from Princeton stated that there's no known (efficient) way to make anonymous your location data, nor any certainties that it is actually possible.

Aside from location data, wearable technologies and their applications have an important role in body rendering.
A 2017 report presents a new generation of devices with more sensors and algorithms for biometric monitoring, even the daily mood of the person. Google developed connecting fabrics, hence moving away from electronics and turning simple everyday's materials into interactive tools; this has already happened through a partnership with Levi, which resulted in an interactive denim for the 2017 Jacquard jacket.
Future wearable devices will be able to capture data regarding the context around the user, their health and their mood, that will be used in highly accurate targeted ads.

Already in 2002, the market analysis indicated that wireless telemedicine represented potential huge revenues, in respect of monitoring of the elderly or the introduction of sanitary services in areas difficult to reach. At the beginning, the designed system was closed, a direct link between the patient, the hospital and the doctors. Just like Aware Home, these services assumed that the collected data had to only be reinvested in the improvement of the product in benefit of the consumers.
Some researchers theorize a context of *smart health*, which offers medical services through the hospital's network; there will be apps or sensors that will execute an accurate biometric analysis of physiological processes and keep us safe and informed.
In 2016, Google Android and Apple iOS were offering more than 100 thousand health and fitness apps, double the amount in respect of 2014. In the US, the majority of these apps

aren't subjected to any health privacy laws, it is expected that they autoregulate according to FTC and other governmental entities' guidelines.

Zuckerberg has a significant advantage in respect of biometrics: in 2017, Facebook reported to have two billion users per month, who uploaded an average of 350 million pictures per day. In 2018, the company announced to be able to recognise faces with an accuracy of 97.35 per cent, almost comparable to the human capability.
They declared their intention to use facial recognition to realize the most efficient targeted advertisements possible, because the deep learning abilities of their machines would have paved the way to infinite market opportunities.
In 2016, US National Telecommunication and Information Administration published its recommendation regarding the employment of facial recognition in respect of privacy: according to their guidelines, whoever wants to use such technologies should make sure that their consumers have control over it. Jurist Alvaro Bedoya nipped such a recommendation, being "a parody" of information principles and unable to offer any kind of real protection.

2.3.2 Deep rendering

The third transaction via computer that Varian presented is personalisation/customisation. Google Now, first digital assistant of the company, had to know what we wanted even before asking; Varian encouraged people to open up more to the app in order to explore all of its feature: he believe that second modernity individuals will entirely accept rendering operations in exchange for the promise of a more efficient and less stressful life. But at the basis of a doctor-patient relationship there must be mutual trust, instead surveillance capitalism mechanisms have unilateral effects.
According to Varian, many business opportunities come from observing how rich people live their life, because once discovered, normal/poor people will want it too; hence, while rich people have assistants, Google can make money introducing a personal digital assistant for anyone with Internet access and a digital device,
Varian asserted that customisation is the new necessary good for busy people, too worried about money and feeling ignored by public institutions; being sustained by a digital assistance means to have a more functioning life. Google Now combined any previous system by Google, regarding neural networking and voice search: the unprecedented intelligence built a "knowledge graphic" with all the data captured from email, agenda, apps, location and social

media contents; it was able not just of assembling a prediction product, but also learn about the kind of information you could have needed depending on the situation.

Any requirement is anticipated through notification on mobile phones. Google uses an enormous amount of computing power and behavioral surplus to assist people during the day because Google Now paved the way to the development of a new stock of prediction product.
Google Now combines the ubiquitous apparatus (that is already expanding to real life) with new operations of *life crawling*, that render, anticipate and modify our conducts.
For surveillance capitalism, digital assistance is like a Trojan Horse, looming over any aspect of the everyday's life. Google and the other surveillance capitalists pushed the conversation as a means of interaction between people and the system: the more informal chatting we do with the digital assistant, the more we give it our experience to render.
An interface who talks to you answers to the basic joy of people, and it is very easy for it to transform a word into an action. Referring to Alexa, a senior Vice President reported that selling an Amazon device meant also to sell clothes: "online shopping is good for businesses and benefits future business". Talking with a digital device is easier than speaking with a salesperson, it creates a situation that you feel you can control; those words that could be considered confidential are let out freely, transformed into **vocal behavioral surplus** related to *what* we say and *how* we say it: vocabulary, cadence, dialect, …
Any market reaction to such surplus is associated with voice activation, voice recognition and the consequent answer, which in turn are calibrated according to global archives of words pronounced all over the world. Machines learn from vocal surplus, hence the commercial value of our chatting would be useless without their learning system.
Algorithms of the vocal systems are improved through audio analysis of fragments of conversations captured from smartphones and messaging apps; the correlation level between the reviews audio and the texts initially processed is then estimated. Companies insist that it is not possible for their commercial partners to link a voice to a person, but a journalist that applied as an analyst of these recordings revealed that she heard people booking a doctor appointment, or pronouncing the whole name of another person to call them.

Samsung is another company investing a lot in smart devices "to connect homes to the online life of its owners"; its devices work through the Android platform. In 2015 it came out that the SmartTV recorded anything said in its proximity and sent everything to Nuance Communications to be transcripted. As usual, Samsung rejected any responsibilities: it was

suggested to read the privacy policy, because it should have been clear that any word captured while vocal recognition was active would be sent to third parties.
In 2017, the general attorney of New Jersey reported the activities of Vizio, one of the biggest producers of SmartTVs. The detective found out that Vizio was collecting some pixels from tv screens and compared them to tv programs included in a database of tv contents: such operations were covered under the nominative of *Smart Interactivity*, introduced as a feature that suggested movies or shows to watch in line with your preferences. In reality, they were selling the chronologies and IPs to third parties, which then associated such information with consumers' addresses and were able to build a profile to help them produce targeted ads.
FTC imposed a fine of 2.2 million dollars; this decision is important, because it implies that watching tv should be included in those private activities that FTC should protect.

Deep rendering reached even toys. One of these disturbing spy toys is My Friend Cayla, which supervised children and parents' smartphones without any real protection over privacy. Produced by Genesis Toys, these dolls were paired to mobile apps in order to activate the understanding of what the child was saying, so the doll could answer. At the same time, it resulted that the system was connected to other mobile apps unrelated to the toys, like camera and contacts list.
The conversations with the child were recorded and sent to Nuance Communications (again), to be uploaded on the company's servers, analysìzed and saved, to become vocal surplus.
Similarly, Barbie's Dream House by Mattel uses a system of vocal activation to fastly answer any command, like "switch on the disco ball" or "down with the lift": these technologies are not even that slowly normalizing the presence of ubiquity in intimate spaces.
In 2017, German Federal Network Agency forbade sales of the Cayla doll and invited it to destroy it, being an illegal surveillance device; the US FTC has still to wrap up with Genesis Toys. Also, the 2017 Mattel project of the Smart Room was heavily hindered by parents, hence it was shelved.

In this race for supremacy between Google, Samsung, Microsoft and Amazon, it seems that is the latter to be winning. Alexa, together with its related line of devices such as Echo hub or Dot, has the fastest learning system and has established many connections with producers of smart home devices. In 2018, Amazon agreed with some house constructors for the installments of Dot in the ceilings, and to power up door locks or safety systems through

Alexa. If it wasn't enough, in 2015 it was announced the sale of Alexa as a service under the name of Amazon Lex, so any company could include this system in their product.
Any Alexa expansion increases the amount of vocal surplus Amazon possesses, which is directly sent to Alexa itself in order to learn and further improve. Lucan Matney, Apple's Siri co-creator and Samsung's Viv developer (another voice system), said that the smart home market and all the related devices are gonna be the next challenge for the big 5, because speaking to people allows you to make them do things.

2.4 Rendering the abyss

Facebook's strategy changed since 2010, when a team composed by German and American scientists applied the 5 factors personality model on a sample of users and discovered that Facebook profiles reflected the real personality of them, not an idealization of it. Consequently, in 2011 three Maryland University researchers developed a method to accurately define users' personality based on information and contents published on Facebook: observing how much individuals were down to opening up about themselves, the team started to collect and analyze **metadata** (or mid-level metrics), the amount of information revealed. Internal Facebook analytics and metadata analysis led them to be able to predict a personality trait with only one-tenth error.
Being able to infer any user's personality allows to adjust any interface of social media, e-commerce sites or advertisements according to that person's preference, increasing their receptivity. It is even possible to highlight only reviews of a product that contains words that the user uses most, or that reveal a personality similar to the user: any person would then trust more that review and would be more prone to buy that product.

This field was investigated also by Cambridge researcher Michael Kosinski and vice direction of Cambridge Psychometrics David Stillwell: when their first 2012 study warned that it was very simple to derive their whole personality just from their contents, Zuckerberg asserted that the unilateral management of users' data had already been considered social norm for a long time, so they were gonna keep their ground on privacy.
The team tried again, and their 2013 research reported how Facebook likes could accurately estimate many personal characteristics that would be generally considered private, such as sexual orientation or political and religious beliefs.
It was clear that these kinds of automated predictive engines were able to track millions of profiles without any consent or awareness of any people involved. Traditional mechanisms to

analyze personalities are very expensive, both in terms of money and time, and they cannot capture private information without the user's consent. Therefore, according to a market logic, the true progress of the intelligence of the machines was being able to obtain behavioral abysses in scale quantities and employ them as automated assessment tools, both cheap to create and efficient. It seems impossible to actually control what information we are revealing online.

Google, Facebook, Microsoft, Snapchat and many others are able to access data that scientists would never dream of. Based on colors, composition, demographics and expression of a Twitter profile picture; on face texture and makeup of a selfie; on style, saturation or luminosity of an Instagram picture, data scientists get the surplus necessary to apply the 5 factor model and extract the user's personality. Starting from messages exchanged on Facebook, it is possible to predict the degree of satisfaction that will derive from a certain ad. In a 2015 interview, Kosinski stated that any interaction is digitally mediated and recorded, and that his job was actually "pretty disturbing"; he concluded that, even in presence of such significant asymmetries between companies and users, being able to perform such violations doesn't mean that it should be done, especially without any consent. But, as an evolution of capitalism, surveillance capitalism follows the rule "latent demand creates producers and products".

In 2015, IBM introduced their Watson Personality Service, which AI systems were much more impressive and invasive than the usual. Aside from the 5 factor model, IBM implemented a twelve categories system to classify people: structure, stability, love, challenge, harmony, self expression, enthusiasm, practicality, curiosity, freedom, ideal and closeness. Moreover, they set the identification of factors influencing decision-behavior in five dimensions: openness to change/enthusiasm, self-reliance/help from others, self-improvement/achievement of success, self-preservation/traditionalism, hedonism/enjoying life.

With these technologies, IBM is able to perform unlimited surplus collection and study in depth their clients. These operations are first tested over employees (habituation phase), to get the first data over which test any personality correlations and gain some predictions on clients' reaction.

Social media contents and how we act while using them can be transformed into data, used to gain through targeted operations. Any approach by advertisers, from travel agents to brokers, can be adjusted to the individual personality. The interactions are then observed in real time

and through scale monitoring, to learn what attitudes keep and what delete in respect to market results; a little improvement in conversion rate greatly raises revenues.
The value of micro behavioral targeting is hence significant in rendering operations.

The machines' intelligence of Facebook is incomparable, exactly what is needed to satisfy all the businesses that lean on the company to gain on behavioral futures markets. The spine of Facebook AI is the FBLearner Flow platform. Processing billions of data everyday and training many models (in real time and offline), the system is able to present only the more relevant contents according to the personality extracted, hence is what makes it possible to create actual customized experiences. Since its implementation, Facebook is able to realize 6 million predictions per second.
The service *loyalty prediction* is proposed as analysis of the behavior surplus and consequent prediction of what individuals could stop supporting a brand.

2.4.1 Mechanics of feelings

In 2015, former start up Realeyes won a 3.6 million euros fund by EU Commission for their SEWA project: Automatic Sentiment Analysis in the Wild, which aim was to develop an automated technology able to read the emotions of a person while consuming a content, how much they were appreciating it.
This technology was seen as revolutionary for video marketing, for machines' learning systems related to analysis of ads impact over consumers. SEWA paved the way to a new segment of rendering, ***affective computing***, which led personalisation even closer to our private lives.
SEWA devices employ specific softwares to read gestures, faces and bodies through biometric sensors, often combined with "discreet" cameras. The machines' intelligence is trained to capture the most intimate and blurred attitudes: they can estimate age, ethnicity and gender, understand what you are looking at, interpret micro-expressions and perceive when you are lying; of course, they are facilitated by the omnipresent cameras of our mobile smart devices.
Again, the quality of behavior surplus depends on the quantity of data captured: Realeyes stated that their databases included more than 5.5 million single frames from around 7 thousand people from all over the world.

The human unconscious has been the object of propaganda and advertisement since a long time ago; before the development of computational capabilities, approximations and experts' intuition were the basis to produce mass communications.
The idea that feelings are translatable into observable behavioral data set during the 1960s, thanks to the work of California University Professor Paul Elkman: there are certain non-verbal behaviors that reveal things a person could be trying to hide. Following this concept, in 1978 Elkman and his collaborator Wallace Friesen published *Facial Action Coding System*, which proposed a scheme to categorize facial movements in 27 *action units*; the six basic emotions (anger, sadness, fear, joy, surprise and disgust) were used as reference for any other expression produced. FACS and the 6 emotions model became the principal paradigm to study facial expressions.
The new field of computer sciences related to emotional rendering was called affective computing by MIT Professor Rosalind Picard, the first to understand that devices could automatise the analysis of micro-expressions according to Elkman's studies and connect them to which emotions caused them. The goal was to combine any behavior signal that could be measured, such as facial expressions and the tone of voice.
In 1996 she published *Affective Computing*, in which she explained how some emotions are shown consciously while others only through indirect signals (for example, you could say that you are scared out loud, but it could be also clear if you start to sweat or your jaw clenches). The affective computing would have rendered both conscious and unconscious behaviors: once understood the pattern, the device would have codified any emotion. Again, Picard was imagining softwares and sensors that would have improved our life, for example able to analyze the behaviors of students and produce teaching modules appropriate for their preferences or capabilities. From her book we perceive that she was conscious about the importance of privacy protection, she even brings up her fear of a potential dystopian future in which an evil government rises to control and manipulate feelings.
She also imagined wearable technologies that would have captured information useful for us, but she stressed the importance of having control over them.

In 2014, Facebook patented its system of emotions' detection. Through some softwares, it would have detected an ambitiously long list of expressions and feelings, such as: joy, exaltation, smiles, astonishment, irony, pouts, sadness, surprise, jealousy, confusion, disappointment, boredom, anger, indifference, pain or depression. In 2017, the affective computing market was expected to grow to 53.98 billion dollars in 2021, with an annual

growth rate of almost 35 per cent; according to Marketsandmarkets researches, in the post-Covid scenario, the market is projected to reach 140 billion dollars in 2025, with a increased growth rate of 37.4 per cent. This expansion is due to the mounting demand of emotions' mapping from marketing and advertising sectors.

To participate in this "economy of feelings", EmoShape developed a microchip able to classify 12 emotions with 98 per cent of accuracy; they define such technology as "the first engine for emotional synthesis on the market". The automated emotion scanning would be taken for granted just as any cookie tracking our online browsing: showing contents designed to make us satisfied will make any consumer happy, and happy clients can be more easily involved in commercial operations.

The science of emotions was redirected towards surveillance capitalism aims: any time the direction is lost, it becomes habituation, and after it is normalized it will be legitimized.

2.4.2 Economies of action

The new capability of the machines' intelligence is to become activators: beyond ubiquitous computation, the objective is now modified in real time people's actions. Economies of action represent the completion of the new means of behavioral modification, which can change people's conducts with almost the same ease they control the features of a device.

Professor Zuboff defined three approaches to action economies: tuning, herding and conditioning. Consequent strategies vary depending on the combination of these approaches and which one prevails.

- **Tuning**

  It can be applied in many ways, for example it can instill a series of behaviors (based on previous analysis) in a precise moment, in order to maximize the influence of the action economy. Another kind of tuning is the so-called *nudge*, any feature of the architecture of a choice that ends up altering the conduct in a predictable way. The denomination "architecture of a choice" refers to the way events are already structured to perform an action; these could also be intentionally designed to perform a specific behavior, without the object of the chosen conduct being aware of it: an example could be the chairs' placement in a classroom, forcing students to look at their teacher.

  According to the majority of behavioral economists, people tend to make irrational choices because their mind is fragile and cannot comprehend the actual array of alternatives; Thaler and Sustein suggested governments should actively nudge citizens towards options aligned with welfare.

Not surprisingly, surveillance capitalists absorbed such knowledge and digitally nudged consumers towards choices that benefit their businesses, hence in favor of the architecture rather than the individual, which ultimately loses part of their self-control. Even if these tactics work over only the 5 per cent of people, it means that some company has full control over some people's actions anyway.
Facebook is an example of tuning via suggestions, which proved to be very efficient for scale telestimulations.

- **Herding**

  Based on controlling the key elements of the context in which the person is inserted, herding allows to direct the behavior towards a route over which is possible to make predictions much more accurate; this technique cuts out the alternatives and increases the possibility to control conduct from distance.
  Some examples of herding approach are the TV telling you to sleep because you have been watching it for too many hours, or blocking the car because it senses that you need to rest.

- **Conditioning**

  To set his **reinforcement model** of stimulus/reaction, Harvard Behaviorist B.F. Skinner observed some behaviors performed freely by wild animals, then reinforced the specific **operating action** that he wanted the animals to perform again; these reinforcing schemes could produce a full routine of precise behaviors. He then defined the employment of reinforcement to instill specific conducts as **operating conditioning**.
  The main project of *behavioral engineering* aimed to induce behaviors in a way that some actions were amplified at the expense of others. He also imagined a behavioral technology, applicable to the whole of humanity.

  Scale conditioning is fundamental for the current surveillance capitalism. Companies can manage a wide reinforcement model thanks to any signal coming from the monitoring activities of smartphones and wearable devices. We could imagine a fitness app reporting suggestions regarding exercising or eating healthier, but surveillance capitalism removes the close feedback or the reinvestment cycle in favor

of people: it is not about what devices can do, but how it is useful according to the political orientation and the economic interests.
A behavior that has already been predicted, modified and directed towards secure earning is the most valuable.

The last computer mediation praised by Varian was continuous experimentation. Google engineers and data scientists constantly work over many A/B tests, based on randomisation and control of users' reaction to any variation performed over the results' page. If once they could only measure correlations and not causality, after years of testing the enormous amount of data collected and improving their mechanisms, now they gained the causal knowledge. Moreover, when the experimentation can be automated, closing the gap between prediction and observation is even easier.
Varian stated that surveillance capitalists are experimenters, but this role has been gained exploiting asymmetries of knowledge and inducing their will upon unaware customers.

2.5 Instrumentarianism

Scale operations of behavioral modification integrate data extraction, ubiquitous rendering and economies of action within supply chains of prediction products. To achieve certain predictions, surveillance capitalists pushed us in their businesses, participating as literal warrantors of their powers, being under the influence of means of behavioral modification. Such ability has been defined as **instrumentarian power** by Professor Zuboff: this allows to structure and exploit behaviors in order to modify and predict it, and later monetise and control it.
Social conformism is not enough, any totalitarian power must affect the inner life of people, claim it and reduce any free space in which it could freely develop. While totalitarianisms use violence, the instrumentarian power uses its means of behavioral modification: it does not aim to force new principles or to conform us to an ideology, it works through measurable actions, therefore it only cares if its rendering, modification and monetisation can access our conducts. Instrumentarian power is a market project converging with the digital space to create its innovative domain over society.

In his 1976 book *About Behaviourism*, Skinner recovered such current stating that the hate it received depended on its (considered) founder's words. According to John Watson, behaviorism conceives psychology as an experimental and objective field of natural sciences,

aiming to predict and control human behavior without necessarily considering any personal introspection; basically, under behaviorist lenses, there was no difference between a man and a brute.
After harshly criticizing Watson, Skinner proposed Max Meyer's research as a new starting point. Despite not being well known, through the translation of the teachings of his supervisor Max Planck, he was able to award scientific status to psychology as a field of research. Planck, one of the most renowned physicists of all time, stated that it was possible to study and know anything of the physical world through the mathematical analysis of the quantum of action (which handed him a Nobel Prize in 1918) alone. "The external world is totally independent from human kind, therefore researching law that can explain and be applied to such an absolute entity is the most sublime achievement that can be attempted".

Among Meyer's publications, Skinner praised his 1921 book *Psychology of the Other-One* as the basis of modern behaviorism: according to Meyer, the only behaviors that must be considered while studying the psychology of any person were the ones objectively observable and related to the previously occupied environments. It is crucial to see any human as "just" another organism among all the other organisms: despite being much more complex than animals or vegetables, according to Planck's theory inside any human there are particles of the universe, therefore we are inevitably conditioned by our surroundings. Psychology then becomes the study of people' social behaviors: observing such performances in their usual environment provides data needed to understand any human behavior. The soul or consciousness, the "subjective" experience of an individual does not have scientific value, because it is not observable or measurable. Human societies spring from natural laws, and can be studied as norms among a group of organisms. And this shift from "human as soul" to "human as organism" was, according to Meyer, the necessary step towards democracy. When science takes over civilization, the human kind recognizes the common status of organisms: social divisions based on class, richness or race become ridiculous, differences are supplanted by similarities and it doesn't make sense anymore to slip society into groups.
According to Planck, Meyer and Skinner, freedom is ignorance: when actually investigated, those gaps that we consider free will offer explanations regarding a certain behavior. Personal exemption from determinism is a psychological defense from being aware that your behavior is entirely predictable. The notions of freedom and chance lose importance with the development of computational measures that explain and allow the prediction and control of behaviors.

In his 1953 book *Science and Human Behavior*, Skinner anticipated the modern rendering operations. There are events that happen privately and how the organism/person reacts is significant: public and private lives are not sharply separated, and further technological development will nullify any privacy level until any behavior will be known, understood and explained. Surveillance capitalism represents a threat to the free human experience, which seems to be a bothersome illusion for surveillance capitalists.

Totalitarianism as represented in George Orwell's *1984* shows the intention to possess every person from the inside, not just as an anonymous entity among the others. The Big Brother is a pervasive consciousness, with its tenacious operations it aims to convert its oppositors and make them take its side.

In his 1948 dystopian novel *Walden Two*, Skinner presents another form of totalitarianism: through his own behaviorist theories, with no democratic practices or elected government involvement, people were controlled in any aspect of the everyday's life; in order to provide and enjoy the "good, comfortable life", any liberal ideals such as freedom, privacy or the right of self-determination must set aside. Skinner described a sly system in which, pursuing and repeating the right operations (behavioral engineering) for a long time, compulsion can spring without any violent encouragement.

Behavioral futures markets now have surveillance tools and mechanisms to implement behavioral technologies into daily tasks; the goal is to deprive any conduct from its thoughtful meaning: automation of people, consequent automation of society, which means certain revenues to someone else.

The instrumentarian society

From human behavior we can derive any detail regarding the various domains of social interactions. Reality mining is feasible through the direct channel of the omnipresent mobile phones, hence combining data coming from these wearable monitoring devices. The resulting sociometrics present a layered society, not according to race, gender or job but instead to behavioral patterns: these identify behavioral subgroups and a sorta new behavioral demographics; the accuracy of measurements over a sample organized in this way can only increase further.

A society arbitrated by computers works according to the "hive logic": mutual observation of the other becomes a habit, social patterns based on imitation spring and can be manipulated to obtain confluence of the behaviors.

In his 2014 *Social Physics*, computer scientist Alex Pentland presented what he theorized could be an instrumentarian society. A collective intelligence, shared through a capillary nervous system, coordinates everyone towards achieving the greater good, defined by universal social values. A "special" group of planners exercise strict control over society, just because it is necessary for the correct functioning of the community. Collecting everybody's data allows them to predict any behavior, which can be modified in order to maintain optimized performance of the super-organism.
The aggregate pressures the individual to follow shared patterns, identity is submitted to synchrony. As Skinner stated, we live under the control of a social context built by millions of other people.

Living in the hive

theworldUNPLUGGED international project aims to investigate the consequences of disconnecting from media for 24 hours; it brings up emotional issues such as addiction, inability to disconnect, boredom, confusion, distress and isolation: the sudden parting from news and social media caused needs and moods typically associated with clinical depression. Economists and technology experts define this domain of social media as the *network effect*, the resulting anxiety from being aware that any logistical, communication and informational requirement depend on devices connected to the Web. As students reported, a young person cannot afford to not be active on social media, since it became the main form of social participation: teenagers and young adults are naturally prone to turn to others, seeking rewards such as acknowledgement, acceptance, membership and social inclusion. Furthermore, the failure of institutions in answering the requests of the new society highlighted the role of digital connectivity as a fundamental means of social presence.
Social media and any other digital interface have been projected to have engaging user-experience designs for a long time, making the most of the worrying 2018 Pew Research statistics according to which 40 per cent of people between 18 and 29 years old and 36 per cent of those between 26 and 49 years old state to be online "almost constantly". Moreover, in order to better fit into the alluring platforms' designs, users experience the so-called chilling effect: to maximize their profiles' engagement (hence their value into the "existential market"), people take constant care of contents and comments published. Online presence is deeply influenced by the realization that what we share could hint how we live offline: the chilling effect extends, and the fear of disappointing this imaginary public pushes everyone to self-censorship.

Surveillance capitalism pushes people towards the hive. Considering the neoliberal values from which the system benefited from, such collectivist orientation is an unexpected development. Professor Zuboff talks about scientific application of **radical indifference**: the learning model is soundly asocial, contents are evaluated on anonymous criteria such as clicks, likes, lengths, volumes and variety, on how much behavioral surplus they can get from it. The indifference excuses surveillance capitalists: their aims for expansion and innovation cancel out any moral difference between potential outputs of their practices.

Chapter 3 - **Privacy in the digital era**

Life all over the world has gone digital, and many of our approaches to daily tasks depend directly and indirectly on the devices we use.

As for any fundamental change, the digitization of many services has its pros and cons. First, one of the most useful outcomes is convenience: saving time and effort by being able to run many errands from the comfort of your own home. Then, digitization has increased the availability of facilities for people who live in remote areas, have disabilities or simply encounter difficulties in reaching services. Finally, when it comes to businesses, digitization enables personalization of the customer experience. As discussed in the previous chapter, collecting data on purchasing habits allows companies to customize and offer products that directly reflect individual needs.

Moving to the cons, with easy access to digital services anytime, anywhere, people can become addicted to them and spend more time online than they actually need. Of course, as the ability to analyze and store personal data continues to increase, privacy is constantly at risk from both unauthorized third parties and cyber frauds. Digitization has only exacerbated the polarization of society: those who do not have the access or skills to use high-quality equipment are cut out from the same opportunities that others have, and this situation will only get worse as technology advances and becomes more specialized. Ultimately, digitization led to the emergence of the gig economy. The (forced) increase in labor flexibility contributed to labor instability and general precariousness.

To reap the real benefits of digitization, we need to consider key issues and ensure a sustainable transition for all.

3.1 The philosophy of privacy

The digital transition is not a choice: one's involvement can be reduced by not participating in social media or not using IOT devices, but in the end we are actively living during the digital era. According to political analysts, the **digital divide** is composed of all those material conditions that are preventing the most poor, uneducated and geographically isolated populations from accessing tools and devices that are fully incorporated in others' everyday's life.

Still, even the most destitutes aren't “able” to escape digital life: for example, in 2018, in the Indian region Chhattisgarh, the Prime Minister Raman Singh announced the 71 million dollars worth program to distribute mobile phones among the 26 million people living in the 7 thousand villages of the area. The project aimed to bridge the digital gaps in one of the most

densely populated countries in the world, and secondly to influence voters during the election campaign. Another permeation is represented by the 2009 Aadhaar card: through its system, Indian citizens and residents can be uniquely identified by a 12-digit number, while using digital devices or for any offline verification. Upon completion of an official (voluntary) request, demographic information is collected through iris and fingerprint scanners. The goal is to have a biometric ID to access all public and government services.

According to Professor Anita L. Allen, the development of the digital life raises conceptual questions that need to be debated by philosophers, in the same way biomedical innovations raise questions about their ethical enforcement. One of her most discussed topics is data protection, especially in the context of data protection. Such concerns are internationally recognized and taken into account, forming the basis of a new branch of academic philosophy in Europe and North America: the philosophy of privacy. Its goal is to provide an explanatory theory about the meaning, value, politics, and purpose of privacy. The project aims to engage and interact with other disciplines such as psychology, economics, sociology and law, to provide realistic and applicable contributions.

Professor Allen's 1988 book *Uneasy access* is the first long study about privacy by an American author, but there are many canonical philosophical works that dealt with today's issues.

In Plato's tale *Ring of Gyges* from Book II of *The Republic*, the underlined statement was that people act fairly and ethically only when they believe to be observed; the power to spy on others is dangerous.

If people voluntarily renounce their privacy, according to Aristotle they lack modesty and humility, while according to Kant they lack self-respect: such ways of thinking associate privacy ethics to respect your own dignity.

Part I and II of Rousseau's *Discourse on Inequalit*y describe humans in their natural state as lonely but happy, led to live in societies in order to achieve comforts and deal with difficulties. This community lifestyle induced the interior need of shelter, secrecy and control, and the tendency to make comparisons between one another: in modern societies, having privacy to build and protect your reputation is highly valued, in order to rest from constant external judgment.

Utilitarians Bentham and Mill both contributed to the philosophy of privacy. In his 1787 book *Panopticon*, Bentham proposed an “inspection house”, which structure could inspire those who had to build specific buildings in which many people were to be kept under strict

surveillance; the author influenced today's surveillance buildings' designs. In Mill's *On Liberty*, the author firmly affirms that private life should be free from governmental intervention, differentiating between decisional privacy and informational privacy; his works were the basis to enforce the liberal agenda in respect of many topics related to the rights of privacy, such abortion, same-sex relationships, drugs, suicide and prostitution.

Modern feminist philosophers, like Martha Nussbaum, deal with the impact of privacy policies over property, power and subordination: women, girls and the LGBT community are faced with specific dangers in the digital era, such as revenge porn and anonymous cruelty while in cyberspace.

Despite a rich tradition to draw on, a philosophy of privacy not contextualized or related to other disciplines has limited value. Addressing global issues such as data breaches, non-consensual profiling, political manipulation, and algorithmic discrimination against content creators requires extending that practice to public philosophy.

A philosophy of privacy could help us meet the contemporary challenges politics are facing. In 2018, EU Data Protection Guarantor Giovanni Butarelli continued a 20-year tradition of analyzing trends and impacts on society in terms of dignity, freedom and democracy: ahead of the introduction of new EU General Data Protection Regulation (GDPR), he convened the Ethics Advisory Group, headed by the German philosopher J. Peter Burgess. Their resulting final report concluded that traditional European values such as dignity, personhood and democracy need to be rethought in order to preserve them effectively in everyday occurrences in the digital age.

Philosophy can undoubtedly influence public order and, in turn, law. Previously introduced, the program enacted by the Aadhaar Act was widely challenged in Indian courts. There were concerns about government surveillance and profiling, lack of choice in sharing biometrics, physical integrity, potential identity theft, and risks in the big data economy.

In 2017, in the case of *Puttaswamy v. Union of India*, the Supreme Court ruled that Indians have the "constitutional right to privacy as a fundamental part of the legal framework protecting human dignity, which is an integral part of the Indian Constitution". The Court held that the protection of dignity should be the end of all laws and the means of justice. The apparent public's indifference to privacy in India does not justify the Aadhaar Act violating Indians' fundamental rights.

A following comprehensive comparative legal analysis included a number of considerations and quoted the opinions of various international scientists and lawyers. Maybe for the first

time, privacy was discussed keeping a broader view, as a core value beyond national issues: one of the positive outcomes was that, on September 6 2018, the Supreme Court of India overturned *Section 377* of the Indian Penal Code, which criminalized consensual same-sex acts by adults. This was a long-awaited event for the country's LGBT community.

While proposing a "complete" philosophy of privacy, Professor Allen elaborated its four necessary components, in the USA legal context:

1. Meaning and definition

   Despite being easier, defining privacy for one of its many specific and narrow purposes wouldn't lead to an exhaustive comprehension of the concept.

   According to Professor Allen, privacy can be related to three conceptual clusters:

   - physical group, referred to isolation;
   - informational group, referred to secrecy, anonymity and confidentiality;
   - decisional group, referred to freedom, choices, personhood and limited governmental intervention.

   Such conceptual groups are then reflected in laws and ethics:

   - physical privacy, provided by illicit common law doctrines;
   - informational privacy, provided by constitutional rights' doctrines, hence 1st to 5th, 14th and 21th Amendments;
   - decisional privacy, provided by statutory laws.

   In addition, they are protected by international standards and agreements.

   A global philosophy of privacy must deal with debates about definition, how terms change the regulatory spaces and powers. For example, in her influential Yale Law Journal 1980 article *Privacy and the Limits of Law*, professor Ruth Gavison stressed how misleading it is to view privacy in the same way when considering protection against governmental control over abortions and against violations of medical confidentiality. There are also many debates about the need to redefine privacy in the Internet world. As he states in his 2018 book *Privacy as Trust*, Professor Ari Waldman argues that traditional spatial and physical methods of understanding privacy in the information age can be dangerous. If we understand privacy to be keeping away strangers' prying eyes from our homes, the extraction of personal data can continue unhindered.

Privacy theory and the laws and policies that go along with it need to update the concept to reflect today's situation.

2. Ethics and values

   A complete philosophical theory of privacy should provide a report in which its values are presented in all its possible forms. According to European tradition, the rights to privacy and data protection are related to the individual right to dignity: privacy as freedom of choice over personal life is the basis of the inalienable right to dignity. But many academics state that this broad definition doesn't support the emerging needs of the digital society, and push jurists and legal courts to produce appropriate policies and regulations that, in today's context, will eventually guarantee privacy and dignity.

3. Politics

   To be an adequate legislation of privacy, it should investigate all of its particular forms, which laws protect them and who benefits more from those regulations. As politics should provide a shelter for everyone, the discourse should especially focus on the evolution of the relation between privacy, privilege and subordination: a key example would be how privacy was used to explain how authorities shouldn't interfere when a man beat his wife in their private home.

   Legislations on privacy are challenging: positive outcomes can be negatively impacted by demographic and sociocultural differences between populations. In addition, culture establishes social groups and how they are viewed and treated by society: even when laws are expected to apply equally to all, disadvantaged social groups such as minorities, poor and women are always treated differently.

4. Application

   According to the *intractable vagueness of privacy* theory, the concept of privacy cannot be applied unambiguously. For legal applications, privacy must be reconsidered and contextualized on a case-by-case basis.

To effectively translate data protection philosophy into digital regulation, the discipline needs to be understood outside of its economic functionalities. Policies and politics should protect the integrity of people's rights in all circumstances and not create loopholes for surveillance capitalists to exploit their private lives. Therefore, public philosophies should be incorporated

into STEM prescriptions to humanize them and contribute to improving people's living conditions, not making them an inaccessible privilege for some.

In the digital age, whenever we simply use a digitized service, such as logging on to social media, doing research on Google, or buying something with a credit card on Amazon, we contribute to the Big Data Economy. Certainly we all have a moral responsibility to protect our privacy, but protecting it is also an unavoidable duty of governments and corporations. Politicians need to be concerned with regulating the unexplored internet spaces and platforms in which the majority of people live their daily lives in many ways.

3.1.1 Cultural aspects influencing the perception of privacy

The majority of technologies and social media are available across the globe, yet the cultural differences in behaviors and approaches persist while using them. Consequently, users with different backgrounds manage their privacy differently: investigating such variety could help orient the design of privacy policies towards a more efficient and inclusive application of them.

Privacy regulations are present in basically every culture, but the psychological and behavioral mechanisms people engage in to set and protect their privacy are unique. Even only considering privacy in its physical dimension, academic researches proved how different populations enforced specific protection processes in order to make their private spaces less accessible to others, depending on the historical period, the geographical areas they set in, or the religious activities they carried out.
In the digital era, when personal data are often too easily accessible, such distinct approaches are still present in the interactions users have with modern technologies. With the European Union enforcing its General Data Protection Regulation, users have more control over their information than ever before, protected by tougher sanctions against companies that don't follow the practice. As a result, many companies had to update their policies and features. Therefore, multinational companies that provide online services to consumers around the world should consider the diversity that consumers may display and expand their privacy governance accordingly, letting go of the one-size-fits-all approach.

Culture is the collective program that influences the mentality and morality applied in everyday’s reality and its perception. Since the 1960s, social psychologist Geert Hofstede has

developed a framework to identify the most important cultural aspects; this model has been refined and validated by many scientists. The latest models provide the following features:

- *Power distance* (PDI), the extent to which the most disadvantaged members of society expect an unequal distribution of power. High PDI values reflect people accepting hierarchical order.
- *Individualism* (IND), the degree to which individuals prefer a social environment in which they are expected to care only about themselves and their immediate family. Low IND scores are found in collectivist cultures, where membership binds people to specific responsibilities to the group.
- *Masculinity* (MAS), the degree of preference towards a competitive society that emphasizes heroism, assertiveness, and material recognition. A low MAS score indicates a certain feminine energy that celebrates humility, cooperation, and consideration for the disadvantages.
- Long-Term Orientation (LTO), which measures how connected a society is to its past, and how that memory influences the relationship between the present and the future challenges it faces.
- Uncertainty avoidance (UAI), the level of discomfort felt by society and its members towards ambiguity.
- Indulgence (IDL), the level of social tolerance towards individual gratification, allowing people to enjoy life and pleasures. A low IDL reflects a modest society.

Individualism, associated with a strong sense of independence and a desire to protect personal space, may also be associated with uncertainty avoidance: people who tend to avoid ambiguity and maintain control over their online personality perceive greater risks in sharing confidential information online.

high risk perceived - high IND score - high UAI score

Regardless of what approach researchers apply to study culture, a society's most salient feature is its position on the spectrum of the dichotomy between individualism and collectivism. Collectivists understand their identity in terms of their roles and efforts to maintain harmony in social relationships. Confidence is built through social interaction, which makes them more likely to trust others. Individualists seek uniqueness and personal fulfillment, place greater emphasis on immediate family relationships, and expect greater freedom to choose the groups they wish to join. Collectivists value relational and contextual

information, whereas individualists tend to underestimate the impact of context in explaining specific behaviors.

Over the past decade, social media has become a global phenomenon. Facebook, Twitter and Instagram reach users from all over the world, actively impacting their social life. People with different backgrounds, experiences and expectations are in contact and share their contents; online platforms' providers should invest in inclusive privacy management.
According to previous research, individualistic cultures appear to care more about their privacy in respect to information shared online: for example, American citizens seem to be more aware of the extraction processes of their data and use self-censorship on social media to protect themselves. Instead, collectivistic users are much less worried, they share more about their personal life, encouraged by the feeling of reciprocity in online communities: if high levels of intimacy are established among the group, users will feel the responsibility to participate in such dynamics, and they will be open and honest.
Countries presenting a high UAI score, like South Korea or Germany, report severe worrings regarding privacy and awareness about their data protection: national users will negatively perceive the consequences of sharing information on social media.
Still, collectivists tend to be more cautious in sharing information with weak links: according to an investigation carried out in the US, China and North Korea, collectivists tend to not disclose information regarding their relationships with people from different social groups, while individualists share much easily what they assume will benefit their reputation online. These statements are confirmed by other investigations, which reports how collectivists are the ones more controlling over the levels of privacy they keep with the different groups they interact with. They use social media to carry out existing relationships with people they are already intimate with and spend time with offline: the higher level of trust in social media reported is therefore due to the fact that strangers or acquaintances have less possibilities to access their personal information online.
Furthermore, collectivists care more about the privacy of the group and its members than individualists. They are prone to perceive others' sensibility and be concerned regarding their reaction to the contents they share: feeling as part of the whole, they relate their own wellness to that of the group, therefore they tend to apply cooperative privacy management strategies. Instead, individualists choose personal remedial strategies to prevent losing control of their privacy.

A common functionality among social media is to enable their users to control who, among their contacts or other users of the platform, is able to access the information they shared on their page.
Still, the majority of control functions aren't differentiated among cultures: as previously mentioned, in collectivistic ones people would prefer to enforce more strict control over their privacy levels with weak links, so social media providers should invest in providing this service to this share of their consumers.
Instead, individualists are comfortable sharing personal information with people in the same social group, so the platforms could be designed to provide the opportunity to enlarge their network, for example recommending online groups that share the same interests. Moreover, future privacy management systems should allow them to exercise even more control over what and with whom they share information, also letting them modify the contents even after being made public or even removing their personal information from others' shared contents.
Privacy management systems in collectivistic countries should invest in collaborative administration, in order to coordinate online experiences of users. In individualistic countries, platform designs should include notification systems to inform users of potential data breaches so that users can correct their behavior faster.

Services are digitized on a global scale, raising privacy concerns. Each country has its own regulations regarding the use of your personal data. However, in a global economy where data is collected and transmitted across borders, privacy policies must be designed to work within an international framework.
A recent study explored specific cross-cultural differences in attitudes toward disclosure of information to companies and organizations. The online poll was shared across 8 countries. Participants were presented with different data collection scenarios and informed about who collected the data, why the data was collected, how the extraction process was performed, and the benefits they would gain from completing the survey.

Factors that affect the acceptability of a data collection process	*Individualistic countries*	*Collectivistic countries*
Entities	Paid service Existing relationship	Government
Usage purpose	Customization	Customization Autonomously make decisions

Collection methods	Through computer	Through mobile
Value exchanged	Saving time or money Unique or compelling value	Saving time or money Unique or compelling value Benefit for the community
Attitude	Acceptability increased if the potential third party takes accountability for data collection	Acceptability decreased if the potential third party disclose its accountability

- People in collectivist cultures are more likely to accept data extraction procedures when governments and political bodies perform them, whereas people in individualistic countries are more likely to pay for them, or prefer to participate if they already know the entity carrying them out.
- Data collection for personalization purposes is permitted in all countries. Also, collectivist cultures embrace data extraction to automate platform functionality, while individualistic cultures value autonomy.
- Respondents were asked about their willingness to share sensitive information such as bank account numbers, medical history, and ID cards. Individualist countries tended to use computers, while collectivist countries preferred mobile phones. This deviation may depend on how well the device is deemed suitable for controlling disclosure.
- “Time and money savings” and “unique and compelling value” appeared to be valuable in both individualistic and collectivistic countries, but only the latter took into account the impact of the process on communities.
- Individualistic societies are more likely to accept data extraction when a third party is formally responsible. This is probably because they feel protected by contract-based relationships. Instead, in collectivistic countries, an increased perception of the third party decreases the acceptance towards the data collection.

In order to integrate culture into the privacy management system, the platforms could detect the user's IP address and even approximate its geographic location, so that it can redirect the user towards the most suitable design.

Nonetheless, even within the same country, some individuals may exhibit characteristics opposite to the dichotomy, especially between different generations and ethnicities. Furthermore, the type and amount of data shared on social media will vary depending on the platform itself, the age of the user and, in particular, the geographic region considered. For example, Snapchat is used by teenagers for everyday conversations, including conversations with strangers, and is primarily used only in the United States.

Research into cross-cultural differences in Internet platform use and personal information disclosure needs to keep up with the pace of technological innovation.

3.2 Dignity and liberty

Concerns about the unpredictable consequences of uncontrolled intrusions into privacy have been growing for some time, but their potential extensions pose great difficulties for professionals and legal practitioners when designing protective management procedures.

Differing interpretations and expectations of what should be confidential don't contribute to finding a common definition on which to base common legal regulation. Privacy is considered a basic human right, as outside intrusions are intuitively perceived as damaging for our personhood. However, privacy concerns not only differ between ancient and modern cultures, but also between Western cultures. American attorney James Q. Whitman defined this "disagreement" as a **transatlantic clash**.

European and American sensibilities differ on many issues. For example, Europeans are embarrassed by Americans' habit of discussing salaries without discretion, as they could even ask their interlocutors what their annual income is. Meanwhile, there have been numerous documented incidents of European tourists being reported to police for lying topless on American beaches.

But it's not just everyday behavior, there are many aspects of the continental law that confuse Americans. An example is the power to decide what names are allowed for children given to governments in 1996 by the European Court of Human Rights (although the relevant laws have changed since and eased over time). On the other hand, Europeans find it unacceptable how easily tolerated is the highly invasive American credit reporting process, especially when it concerns someone who has never defaulted.

As mentioned earlier, the need for privacy is the same, so differences in privacy perceptions should not be taken lightly. A proper comparative analysis of data protection laws will reveal many points of contact and many differences between Western systems; what must be acknowledged is that different privacy laws have been produced due to different cultures and histories.

Raw intuitions of privacy are shaped by the dominant values of an evolving society. What ultimately becomes law reflects the principles that society follows. The fundamental contrast in the two conceptions of the transatlantic scene has been identified by legal academic Robert Post: privacy as an aspect of dignity and as an aspect of liberty.

In Western cultures, the concept of **personhood** as the integrity of the person is rooted in the respective backgrounds: one in which dignity, honor and preserving your position in society are highly valued, the other that has always been suspicious about authorities' impositions.
Continental practices aim to safeguard the right to respect and to personal dignity, over one's image, name and reputation; in German law is defined as *informationelle Selbstbestimmung*, the right to informational self-determination, to control what information about yourself disclose. People are shielded from unwanted public exposure, as the main threat to privacy is perceived to be the media, whose internal mechanisms are not calibrated around the preservation of human dignity.
The American right to privacy protects the jurisdiction over one's private property, the liberty from intrusions of the state in your own home. So, in their view, undressing is like losing the walls of your home and losing your privacy. But what European law wants to protect is the right to undress if we wish.
Europeans perceive the procedure to access American credit histories as an invasion of privacy. As a result, such information is less readily available in Europe, which may have contributed to slow progress in credit card usage. Good credit reporting practices can make a big difference to the system, but market efficiency is secondary to preserving the image of an individual's financial history.

Privacy isn't the only thing continental law protects people from "losing face". Legal protection for interpersonal respect is similar to American norms against hate speech towards minorities, but it goes beyond them and it applies to everyone. For example, the law protects the right of workers to be treated with respect by their colleagues and superiors. In addition to moral harassment and insulting remarks, imposing degrading duties falls into the crime of mobbing too.
The culture of dignity that permeates European law is not just a reaction to the atrocities of Nazism and Fascism: modern European society descended from societies in which class order and its privileges were contested in the name of class equality. Modern continental law is the product of centuries of sociological and political processes and reflects an ongoing commitment to extending the right to dignity to all.
Similar contradictions are found in Western approaches to data protection. US policymakers are much slower to draft appropriate regulations and much more tolerant of market self-regulatory mechanisms: extracting and analyzing consumer data is beneficial, reduces research costs, and connects sellers and buyers. European law permits the collection of data

for limited purposes and for a limited period of time under state supervision and only with the explicit consent of the data subject. Americans may find it strange that Europeans are more willing to share sensitive information with governments than independent businesses, but as expected from continental traditions, free market mechanisms are not entrusted with the protection of individual dignity.

Although the attitudes towards the problem are (and will probably remain) clearly divergent, making generalizations about the systems is wrong; also the differences among them are comparative, not absolute.

The more prominent effort to accost American laws to the continental style, as stated by jurist Harry Kalven, has been “the most influential law relies article of all” Warren and Brandeis's *The Right to Privacy*. They attempted this introduction knowing that an extensive application of European procedures was impossible in the established American system.

If the American founding documents were meant to adapt to times and future unknown technologies, and if the Declaration of Independence and the Constitution talk about the inalienable rights to liberty and to pursue happiness, then there must be laws to protect them. The authors argued that the copyright law of the time (1890) was outdated and not adequate to protect personal writings and any other intellectual product; moreover, any individual has the inherent right to be left alone, hence to privacy. Laws must be flexible and adapt to the evolving needs of society. They set out to identify four types of privacy violations that media can cause: intrusion in private life and affairs, public disclosure of embarrassing private facts, unwanted publicity and misappropriation of a name to get financial advantages.

Then, they proposed what could have been a potential basis for an adequate privacy protection legislation: privileged communications were the domain of libel; gossip and oral communications weren't protected by privacy rights; consent to publication was an outright defense; truth and malice were irrelevant to a breach of privacy action.

Any attempt to enforce rights to privacy was outclassed by the right of free speech and freedom of the Press: today's public figures are forced to proceed legally if they disagree with the disclosure of their private lives by paparazzi.

It must be said that American law provides protection for one's image: the right of publicity contemplates that each person has ownership over their image, and can sue whoever misappropriates it. Yet, as argued by lawyer Melville Nimmer, the image is protected as a commercial commodity, not as part of the personhood that must be honored. In American tradition, the main defense against the main enemy, the nation, is the home. Looking at how

public nudity is perceived, it follows that an invasion of privacy occurs when the problem can be compared to breaking into a home, or even a body. Of course, some will wonder why the recent abortion ban in 14 states and relative investigation aren't viewed as such.

Just as there are no universal data protection values, a universal privacy regime won't be efficient. Nevertheless, national laws can meet the challenges of the digital age and function adequately, as long as they embody the social commitments in which citizens recognize themselves too.

3.2.1 European perception

The information below is taken from *Cultural and generational influences on privacy concerns: a qualitative study in seven European countries*, a 2014 article by Professors Caroline Lancelot Miltgen and Dominique Peyrat-Guillard, published in the European Journal of Information System.

The investigation concluded that culture is more impacting over privacy concerns and disclosing attitudes, while age influences the protecting behaviors.

The research follows a qualitative approach, with focus groups discussing:

- What issues do people perceive to be more threatening to their privacy? What factors are considered when deciding what information to share online?
- How does culture affect privacy issues? And what actions will be triggered?
- How does age affect people's attitudes towards privacy, and what behaviors does it provoke?

As mentioned earlier, the dichotomy between individualism and collectivism is the most investigated when it comes to cultural dimensions. The first hypothesis (H1) states that *people coming from different European countries report discrepancies in respect to the anxieties they claim feeling about privacy; in particular, people from collectivistic cultures tend to share personal information less reluctantly than those from individualistic societies.*

The second factor studied is age. Young people tend to consider themselves Internet experts and are the largest population participating in online interactions explicitly designed to increase the amount of personal information shared. The second hypothesis (H2) is that *people from different age ranges have different approaches and concerns regarding privacy; younger people see such issues under a more positive light than older people.*

The authors organized 14 focus groups in seven European countries, each counting between 8 and 12 participants, divided according to the information received from demographic surveys previously conducted; the average duration of a discussion was 90 minutes.

To sufficiently get both cultural similarities and differences, Europe was divided into four blocks, as:

1. NORTH EUROPE (Denmark, Finland, Sweden, Estonia, Latvia, Lithuania);
2. EAST EUROPE (Bulgarian, Czech Republic, Hungary, Poland, Romania, Slovakia, Slovenia);
3. WESTERN EUROPE (Austria, Belgium, France, Germany Ireland, Luxembourg, The Netherlands, UK);
4. SOUTH EUROPE (Ciprus, Italy, Greece, Portugal, Spain, Malta).

From each block, two countries were selected to maintain variety both within and across blocks:

1. Estonia was chosen because of its high levels of available e-government, yet low access and usage;
2. Poland and Romania report very different levels of e-development in respect of block 1;
3. France and Germany were representing their block as European leaders;
4. Spain has similar IT development to France but different cultural and geographical background, while Greece has a much lower IT development rate than Spain.

Moreover, the Internet usage rates of the chosen countries significantly diverge from one another:

- low in Romania and Greece (30 and 31 per cent);
- moderate in Poland, Spain, Estonia and France (48, 51, 58 and 62 per cent);
- high in Germany (75 per cent).

The European average of Internet usage is 57.2 per cent, while the average of the chosen countries is 54.6 per cent, therefore the sample was appropriately selected.

For each country, authors considered age ranges as young adults (15 to 24 years old) and adults (27 to 70 years old); later, they were able to furtherly divide them as:

- 15 to 18 years old
- 19 to 24 years old
- 25 to 44 years old
- 45 to 60 years old
- 61+ years old

The following results relate to opinions that emerged from focus group interviews that the authors considered most appropriate for their report.

The first issue considered was the *management of personal data*: most participants find data collection intrusive.

- 15-18

  (Germany, M) *Compulsion*: disclosure of data is basically mandatory, being required to obtain any online service.

- 19-24

  (Poland, F) *Pseudo-anonymity*: personal emails aside, lying about yourself reinforces the perceived individual control.

  (Greece, M) *Benefit*: disclosure of data may offer advantages with respect to commercial advertising and information about companies.

  (Greece, F) *Sensitivity*: we prefer to only share non-confidential data and only with known or trusted individuals and organizations.

- 25-44

  (France, F) *Constraints*: basic information such as name and address should be provided without being paranoid about the consequences.

- 61+

  (Germany, M) *Trade-off*: different levels of disclosure may be acceptable depending on the circumstances; only disclosing personal information allows us to gain real benefits from Internet usage.

The second topic was *privacy and control*: most participants perceive data disclosure as a loss of control or even an invasion of privacy; many were already thinking about future risks that are difficult to predict.

- 19-24

  (Greece, F) *Function-creep*: Anxiety arises from uncertainty about the actual purpose of the information collected. (France, France, F) *Loss of control*: once the data reaches the Internet, the user loses complete control over it.

- 45-60

  (France, F) *Privacy breach*: the constant advancement of technology and the digitization of services inevitably lead to invasion of privacy and, consequently, dictatorship.

(France, M) *Future risks*: the actual negative effects of social media will come later, but young people are still unaware of the dangers.

- 61+

  (Poland, M) *Misuse*: risks arise from accidental or unanticipated misuse of data and are therefore difficult to predict.

The third theme considered was *protection and regulation*. Participants expressed their outrage at the perceived imbalance of power and wanted efficient and safe regulation to ensure their rights were respected, beyond from self-defensive behavior.

- 15-18

  (Germany, M) *Power imbalance*: privacy agreement forms are always designed to insure the organization, proved by the fact that privacy concerns only increased despite such contracts.

- 19-24

  (France, M) *No security*: using special Internet protections does not protect users from invasion of privacy.

  (Estonia, M) *Self-protection*: the best protection available is to not create an account on the online platform and therefore not register for the service.

- 25-44

  (Germany, M) *Need for regulation*: very eloquent and clear guidelines are expected (when using surveillance cameras).

  (Greece, F) *Redress*: the right to change disclosure settings while using the service must be guaranteed. Organizations must not be able to obtain additional data if users are dissatisfied with the service.

The fourth theme considered was *trust*: participants feel safe sharing their data if they see no risks associated with their usage and if the company is known or reputable.

- 19-24

  (Poland, F) *No perceived risk*: disclosure of certain types of information does not imply access to other information (knowing your bank account number does not give you access to the bank account itself).

  (Greece, F) *Trust, experience, reputation*: disclosure of certain information is more tolerable when dealing with professionals whose services have already been utilized and evaluated.

The fifth item considered was *responsibility*. Concerns involve participants, the companies that receive the data and states that need to protect their citizens; furthermore, it was added that parents have the responsibility to protect their children from invasion of privacy.

- 15-18

  (Germany, M) *Companies*: statal involvement is not always possible, as data management is primarily the responsibility of service providers.

  (Germany, F) *State*: government protections apply when data is made public, but users are still the primary controllers.

- 19-24

  (France, M) *Self*: you are responsible for what content is ultimately shared on your online platform and who you engage with.

- 45-50

  (France, F) *Parents*: young people are so much influenced by the internet that they cannot be exempted from parental intervention when necessary.

The research prosecuted with the analysis of pronounced vocabulary: for each country, the authors reported the prevalence of specific semantic areas emphasized when discussing the topic.

Data disclosure concerns every country involved except for Estonia, which appears to focus more on which information could be made public. Concerns regarding protection and regulations appear in every country. The specific word “trust” is used only by the Southern European countries, while “responsibility” is mentioned only by Germany and France, rich countries with an extensive history.

Germany	**France**	**Greece**	**Spain**	**Poland**	**Romania**	**Estonia**
Data disclosure 20%	Data disclosure 16 %	Data disclosure 21%	Trust & Control 12%	Control & Regulation 70%	Privacy & Relationship 15%	Data usage & Risks 11%
Protection & Responsibility 13%	Responsibility 15%	Data usage & Protection & Redress 24%	Mandatory disclosure & Regulation 11%	Data disclosure 22%	Data access & Consent 13%	Anonymity 14%
Conditions of data disclosure	Risks &	Data usage &	Social networking	Authentication &	Monitoring &	Protection strategies

23%	Dangers 26%	Consent 11%	9%	Security 8%	Regulation 22%	18%
Security & Monitoring 44%	Privacy invasion 43%	Trust & Control 12%	Virtuality 33%		Data disclosure 50%	Experience & Trust 24%
		Identification 32%	Monitoring & Privacy invasion 35%			Public data 19%
						Passwords 14%

The lack of individual control over sensitive information is universal, still the discrepancy emerged reflects the various socio-political experiences of the countries involved. The main differentiating factors are the IT development level and the perception about security governance.

Regarding the topic of responsibility, it is interesting to focus on the fact that France highly values it, while for Greece it is correlated to trust. This difference can be associated with the one in respect of Internet usage level: Greece's one is lower (31 per cent), hence an inexperienced person would probably prefer to rely on trusted processes, while the France's one (62 per cent) reflect the higher competence of users, which must be aware of their own responsibilities. This north-south divide reflects that people in northern Europe feel the need to disclose their data, while people in southern Europe feel they can choose to do so.

Back to H1 on the spectrum of individualism and collectivism. According to Ivana Nasinovich Blaje's 2019 survey, Greece has an IND score of 35, while France has IND = 71. Greece is more collectivist than France: supporting the authors' hypothesis, the first country appeared to be more trusting of personal data and more willing to share personal data with companies they knew, whereas the second country’s attitude reflected more discretion.

The authors also analyzed which words were more commonly pronounced by different age groups. This research on the generational divide finally supported their second hypothesis H2. According to their results, people belonging to the oldest age ranges view negatively the disclosure of data, as they perceive too many potential unpreventable risks; instead, the youngest (15-18 and 19-24 years old) are optimistic about their data management capabilities:

to participate in the Internet everyone has to respect its mechanisms and its rules. Finally, young adults (25-44 years old range) kept a neutral attitude, hoping for more transparency regarding the responsibility of data extraction processes.
Moreover, it appears that younger people rely a lot on self-censorship when it comes to social media participation, as they feel that anonymity or a fake-persona can shield them from privacy invasions; as the relationship with their contacts develops, they become more willing to be honest about who they are.
The relative competence younger people have makes them more relaxed about Internet usage; also, despite the common idea according to which younger people are careless, they resulted to be more attentive in their privacy management. The authors define this attitude as a paradox: young people trust more their own abilities and the efficiency of legal protections, so they are less worried about privacy breaches; yet, their level of awareness about Internet mechanisms push them to employ much more privacy protection strategies.

3.2.2 America perception

The information below is taken from *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Personal Information*, a 2019 article by Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erika Turner, from Pew Research Center.
The surveys were conducted from June 3 to June 17, 2019, by the American Trends Panel of Pew Research Center; participants were 4272 American adults.

The survey focused on public perceptions of how some entities use sensitive information. Personally identifiable information is collected by government agencies such as the Internal Revenue Service, Census Bureau, Post Office and social care departments. However, it is complicated to determine how much information they and third parties have access to. Areas where they can obtain information include financial and career information, physical characteristics, living conditions, property status, insurance plans, etc. However, there are some restrictions on what government agencies can communicate to the public and other similar organizations.
Organizations such as the National Security Agency monitor cell phone usage and personal displacements. Under certain court orders, police or similar agencies may access personal devices, online chronologies, email records, or social media activities. Access is granted as part of a transparency declaration that all service providers are required to submit.

Americans' privacy concerns regard entities that extract their data, both corporate and governmental. A common feeling is that you have no control over sensitive information and how it is actually used by third parties. As services become increasingly digital, 70 per cent of those surveyed say their data protection controls must address far more threats today than in the past.

% of US adults perceiving - regarding data collection by - :	Companies	The government
1 - Lack of control	81%	84%
2 - Risks outweigh benefits	81%	66%
3 - Concerns over data usage	79%	64%
4 - Lack of understanding about data usage	59%	78%

US adults who say privacy breaches are **more likely to happen** than in the past	70%
White	73%
Black	61%
Hispanic	65%
18 - 49	67%
50+	73%

1 - *Lack of control*

The majority of Americans feel little to no control, compared to the minority of respondents who believe they have control over potential privacy breaches. In particular, personal information that people are more concerned about is obtained through Internet operations, such as purchases made with a personal card or web chronology or. Although any personal social media profile is highly customizable, less than a third of the respondents feel safe about who can access their content.

% US adults feeling - control over of who can access:	A lot	A little	No
Physical location	18%	54%	28%
Activities on social media	16%	50%	35%
Private conversation	13%	49%	37%

(online/text messages)			
Online/offline purchases	12%	43%	45%
Websites visited	10%	44%	41%
Search terms used online	9%	39%	48%

Considering the age of the respondents, older Americans reported feeling the least in comparison to any other age range, especially when it comes to Internet activity. An analysis of responses from 30-64 year olds found similar levels of control, yet defined by a decreasing tendency. Predictably, young people feel they have the most control, especially when it comes to their physical location and social media participation.

% US adults feeling **in control** of who can access:	18 - 29	30 - 49	50 - 64	65+
Physical location	83%	74%	68%	60%
Activities on social media	74%	68%	60%	56%
Private conversation (online/text messages)	73%	66%	60%	52%
Online/offline purchases	64%	60%	50%	44%
Websites visited	67%	56%	51%	37%
Search terms used online	59%	55%	42%	37%

In respect of ethnicity, white people feel less in control than black and hispanic ones (50, 69, and 66 per cent, respectively) when it comes to protecting information about online and offline purchases.

2 – *Risks outweigh benefits*

While the majority of Americans don't believe in the benefits of data extraction by businesses and governments, almost half of those surveyed admit to be aware of at least some of it. Only one-third of respondents said government data collection is beneficial and not a risk, and only 17 per cent said the same for businesses.

%US adults				

benefitting from data extraction operations by:	A great deal	Some	Very little	None
Companies	5%	23%	49%	23%
Government	4%	19%	42%	34%

More or less a third of respondents aged 18 to 49 agree that there is no real benefit to data collection by governments or companies. For older Americans, the sense of gain is even lower.

% US adults benefitting **a great deal or some** from data extraction operations by:	18 - 29	30 - 49	50 - 64	65+
Companies	29%	31%	29%	19%
Government	32%	24%	20%	17%

Black and hispanic Americans are more likely to find government (32 per cent and 29 per cent) and corporate data collection (38 per cent and 39 per cent, respectively) beneficial. Instead, only 19 per cent of white people believe government data extraction is beneficial, and slightly more (23 per cent) companies' operations.

3 – *Concerns about data usage*

Traces of our activities and preferences remain both online and offline. Respondents were asked about how their data could be accessed and used by third parties. In particular, nearly 8 in 10 Americans are very or somewhat concerned about how social media and website providers, advertisers and companies they buy from use their personal information. The least threatening entities (albeit still important) eventually resulted being the police, employers, and finally friends and family.

%US adults concerned - about how much information - might know about them	A lot	A little
Social media/sites used	40%	46%
Advertisers	39%	44%
Companies from which they buy from	30%	50%
Law enforcement	26%	36%
Their employer	19%	39%

(among who is employed)		
Friends and family	9%	34%

Overall, concerns are more pronounced among minorities, especially when it comes to offline relationships. Black people were most concerned about their information, especially what law enforcement would know about them; a similar trend exists among hispanics.

%US adults concerned **a lot and a little** about how much information - may know about them	Law enforcement	Employer	Friends and family
US adults	61%	58%	43%
White	56%	51%	35%
Black	73%	71%	61%
Hispanic	67%	64%	52%

A consistent percentage of Americans (72 per cent) believe their online or mobile activity is tracked by companies, with 31 per cent of them believing the same will happen for their offline activities. Potential governmental tracking rates are lower, but vary by ethnicity and age.

Black people are the most likely to feel tracked online and offline, followed by hispanics who are less concerned about their offline activities.

Respondents between the ages of 18 and 29 are twice as likely as Americans over the age of 65 to believe their governments track their online activity, and the same pattern emerges when asked about their offline activity.

	Online/mobile phone	Offline
US adults who say they believe **the government** is tracking their activities	47%	24%
White	43%	19%
Black	60%	47%
Hispanic	56%	28%
18 - 29	59%	30%
30 - 49	53%	26%
50 - 64	44%	23%
65+	30%	16%

4 - *Lack of understanding about data usage*

Even if the majority of Americans believe that their activities are being tracked, only the smallest share is confident about how much they understand how their data is being used. In particular, 53 per cent of the interviewees admit to getting very little of what the government could do; in general, governmental operations are less understood than corporate ones.

%US adults understanding - what is being done with their data	A great deal	Some	Very little	Nothing
Companies	6%	34%	48%	11%
Government	4%	17%	53%	25%

Despite being worried about personal digital privacy, 97 per cent of the participants admitted that they don't really pay attention when asked regularly to accept the terms of service they are presented with while using an online service before agreeing to it:

- 9 per cent always read the privacy policy;
- 13 per cent often does;
- 38 per cent does sometimes;
- 36 per cent never do.

Moreover, among those who claim to read it, only 22 per cent actually read its entirety. Regarding policy understanding, 63 per cent of Americans understand little to none of the current protection laws on data privacy.

Data collection for specific purposes

The study also explores the debate about which objectives of data collection and sharing are more acceptable. The most tolerated operations concern improving educational outcomes and preventing terrorist threats. Fitness tracking apps were the ones that split the most public opinion. Finally, the most unacceptable activities were social media companies monitoring personal content and smart speaker providers sharing personal recordings with law enforcement agencies.

% of US adults perceiving:	Not acceptable	Acceptable	Not sure
Poorly performing schools sharing data with organization seeking to improve educational outcomes	27%	49%	24%
The government collecting			

data about all citizens to assess potential terrorist threats	31%	49%	19%
DNA testing companies sharing customers' genetic data with law enforcement to help solve crimes	33%	48%	18%
Fitness tracking app makers sharing users' data with medical researchers to investigate the link between exercise and diseases	35%	41%	22%
Social media companies monitoring users' posts to identify signs of self-harm and connect them with counselors	45%	27%	27%
Smart speaker makers sharing users' audio recordings with law enforcement to help with criminal investigations	49%	25%	25%

Also when considering the age variable, previously recognized patterns are confirmed. The most unacceptable invasions of privacy are social media surveillance activities (especially among Americans over 65) and sharing of personal recordings by smart speaker providers according to people aged 30 to 49).

The biggest difference is how much older people are more tolerant of governments extracting counter-terrorism data and distributing genetic data to aid in criminal investigations compared to young people.

The attitude regarding school sharing students' data to improve their performance is pretty similar among the age ranges.

% US adults **accepting**:	18 - 29	30 - 49	50 - 64	65+
Poorly performing schools sharing data with organization seeking to improve educational outcomes	47%	52%	48%	44%
The government collecting data about all citizens to assess potential terrorist threats	42%	47%	55%	58%
DNA testing companies sharing customers' genetic data with law enforcement to help	39%	43%	54%	58%

solve crimes				
Fitness tracking app makers sharing users' data with medical researchers to investigate the link between exercise and diseases	52%	44%	34%	35%
Social media companies monitoring users' posts to identify signs of self-harm and connect them with counselors	42%	29%	20%	18%
Smart speaker makers sharing users' audio recordings with law enforcement to help with criminal investigations	22%	21%	26%	32%

Accountability issues

As previously reported, the majority of Americans admitted to not reading carefully (if not at all) the terms of service, and those who do it have trouble really comprehending it. At the basis of data extraction and privacy protection systems there's the idea that users are given notice and give explicit consent on their data usage, yet the majority of participants said to be not too much or not confident at all in companies following their own privacy policies.

% of US adults confident that companies will:	Very	Somewhat	Not too much	Not at all
Publicly admit mistakes and take responsibility when they misuse users' data	3%	18%	46%	32%
Be held accountable by the government if they misuse data	4%	21%	43%	32%
Usa personal information in ways users would feel comfortable with	4%	27%	47%	22%
Promptly notify users if their data has been misused or compromised	5%	30%	41%	24%

Follow what their privacy policies say to manage users' data	5%	37%	40%	17%

Depending on the purpose, Americans vary their perception:

- 57 per cent are very or somewhat comfortable if data are used to improve the company's fraud prevention system;
- 64 per cent would be uncomfortable if data are shared with third parties, even if they are doing researches to improve society;
- when it comes to companies using data to develop new products, the public opinion is evenly split.

Other interesting remarks from interviewees:

- In the twelve months prior to the survey, 28 per cent said they had dealt with identity theft issues:
    - 21 per cent related to fraudulent debit/credit card charges;
    - 8 per cent related to social media or email account appropriation;
    - 6 per cent associated with name theft.

% US adults that dealt with _ twelve months prior the survey	White	Black	Hispanic
Social media/email breaches	6%	7%	20%
Name theft to open a line of credit or apply for a loan	4%	7%	12%

- 57 per cent say they check privacy-related messages very closely (11 per cent) or fairly closely (46 per cent) privacy related news, while 10 per cent admit to not checking them at all.

  White people are more likely to ask about this topic than black or hispanic ones, although the percentages are fairly similar. In addition, it was found that the willingness to dedicate yourself to the theme increased as the age increased.

US adults that follow very or somewhat closely privacy related news	57%
White	58%
Black	55%

Hispanic	53%
18 - 29	45%
30 - 49	53%
50 - 64	63%
65+	66%

Variables among groups

> age

Surveillance topics are perceived differently by different ages.

- Compared to people between the ages of 18 and 29, Americans over the age of 65 say they have far less control over who can access their location, private conversations, or online and offline purchases. Additionally, only 17 percent of people over 65 years old think government data collection efforts are beneficial, and only 19 percent think the same about business.
- Young people are more open to the idea of social media providers monitoring user content or fitness tracking apps sharing data with medical researchers. Older Americans are more open to law enforcement reaching DNA and smart speaker companies for data collection to solve criminal investigations; also, they tend more to condone data extraction for terrorism prevention.
- While 66 per cent of older people declare to follow privacy news somehow closely, just 45 per cent of those younger do the same.

> race and ethnicity

- In comparison to 40 per cent of white Americans, 60 per cent of black Americans are more likely to say they think that their online activities are tracked by the government; such discrepancy is reflected also in relation to offline activities: 47 per cent of black adults and just 19 per cent of white ones.
- Black and hispanic adults are more likely to admit they are worried about what security officials, employers, friends and family know about them.
- Regarding identity theft issues, in particular social media or email accounts intrusions, just 6 per cent of white adults declare they have been a victim of it, followed by only 7 per cent of hispanic adults, unlike 20 per cent of black interviewees. Furthermore,

black folks are more likely to say that they experienced name theft than white and hispanic people.

- Compared with 69 and 66 per cent of black and hispanic adults, only 50 per cent of white ones feel in control over who can access their online/offline purchases information.

Finally, opinions were divided when people were asked to choose between better consumer tools and stricter privacy laws: 55 per cent want tools in place and direct control over their data, while others would prefer the enforcement of specific stricter laws on companies, both in data use and transparency of activities, as they would be more effective.

To actualise a philosophy of privacy, in order for it to be effective as a public philosophy, its four components should take into account the impact culture has on people's perception. In general, the broader conceptualisation should be always legalized, in order to derive specific definitions when they are needed. The potential philosophy should have the most broad application possible, as privacy and integrity of the personhood are universal needs, just beholden differently. Control should be provided over any functionality of a platform, in order for each person to customize their experience according to their preferences; it should be cheaper than having to design different platforms or policies depending on the country.

Comparing the two context, the dichotomy of individualism and collectivism is more prominent in EU: during the continental history, each country both cultivated their individual culture and came in contact with one another and left their traces in one another; also, within the European Union every member maintains its sovereignty, they can have their own laws, they just have to be compliant with the pan-European principles. Although Europe has become ethnically diverse too, in the US the levels of ethnic integration have always been higher. It is important to take into account what the survey has revealed about the sense of discrimination these “minorities” feel when it comes to their privacy, inevitably understandable considering the blatant racist propaganda perpetuated by the former US President and how since then some people feel entitled to speak and act disrespectfully. Racism and “not directly” harmful discrimination is present also in Europe, but it seems that in the US people are resigned to it, which has a significant impact over their perception of their own privacy.

In both EU and US emerged a positive attitude towards practices that are not immediately perceived as remunerative for the provider. In the digital era, surveillance operations and the relative infrastructure could be incredibly useful to many, but they inevitably induce a sense of powerlessness and anxiety and consequently end up being demonized: the majority of them are designed with the specific purpose to be profitable only for those investing in them, there's no redistribution of wealth and benefits. It's a waste of potential.

Chapter 4 - **Privacy Regulation and Protection**

Although both European Union and United States regulations protect our privacy over sensitive information as a fundamental right, laws and their designs differ a lot. Through the 95/46/CE *Safe Harbour* directive, the EU was one of the first jurisdictions to introduce privacy laws: the measure was adopted to harmonize the various regulations, guarantee a free flow of data and increase the level of protection towards fundamental rights to any European citizens.

Compared to the EU, US regulations for privacy protection are much more fragmented: there's no federal privacy protection law, just some state laws that deal with sensitive information management.

4.1 EU data protection

As stated in *Article 8* of the Charter of Fundamental Rights, everyone has the right to privacy over personal data, to access what has been collected, and to rectify it. Each EU member constitution has been designed and adapted to protect the fundamental rights mentioned in the Charter, therefore national laws must be enforced accordingly.

To carefully insert the EU in the digital era, a bundle of measures directed towards privacy protection was introduced in May 2016: the *General Data Protection Regulation* 2016/679 (GDPR) replaced the Safe Harbour for the protection of personhood concerning personal data processing and its free movement. This act was fundamental to strengthening individual rights when confronted with businesses participating in the unified digital market. Since its enforcement on May 25, 2018, it has been dealing with the fragmentation of national systems and superfluous administrative burdens.

Both the GDPR and the Safe Harbour have been designed according to the 1980 OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (updated in 2013). According to its precepts, people must be informed when and what kind of data is being collected; such operations must happen within the limits of a specific purpose, and only with explicit consent. Data cannot be shared without consent or unless there are legal reasons; people in charge of privacy protection should be held accountable in case of law breaches.

Compared to Safe Harbour and the OECD principles, the GDPR extends individual rights with the right to oblivion, to rectify, and to know the purpose of data usage and other control operations. Another significant difference between GDPR and previous measures is that it doesn't list recommendations that can be enforced voluntarily: being a European regulation, it

must be fully applied at the European level, also providing a fine to issue in case of certain violations.

Generally, GDPR compliance belongs to the jurisdiction of national Data Protection Authorities (DPA), internally appointed by each EU member state. The DPA manages any violations reported by a company, mediates access requests, and provides recommendations on how to interpret the GDPR. In the case of international investigations, DPAs should collaborate to define who among them has the authority to deal with it.
Recent observations on DPAs showed that West European members are more likely to issue fines, which also resulted to be higher and more frequent than in East Europe: this tendency is due to more efficient regulatory capabilities and having to deal with more multinational companies under their jurisdictions. Moreover, while Western DPAs have often investigated non-national entities, the majority of fines issued by Eastern European DPAs are against national-level companies and small and governmental organizations.
Moving to US companies, some of those which received huge fines, such as Google and Marriott, declared to have the intention to appeal against them. With no prior cases of GDPR appeals, usually, the enforcement of the sanction is paused until a judicial court issues its sentence. To appeal DPAs or any EU court's decisions, people must refer to the European Justice Court; still, its powers are limited, because they can control only the way the authorities reached the decision, not the decision itself or the relative fine assigned.

Flanking the GDPR, EU directive 2016/680 protects natural people when authorities collect their data to prevent or while investigating privacy-related crimes; in particular, sensitive information of victims, witnesses, and even suspects will be protected if participating in international operations.

Every EU member has its national authority responsible for the protection of personal data, as expected from *Article 8.3* of the Charter of Fundamental Rights. Moreover, once enforced, the GDPR led to the establishment of the European Data Protection Board (EDPB), an independent authority that guarantees the homogenous application of privacy protection norms all over the EU.
The entity must provide guidelines regarding the enforcement of the basic principles of GDPR and the directive 2016/680; furthermore, it has to update the European Commission regarding potential new privacy-related controversies or issues and take part in national authorities'

disputes. The European Commission takes part in EDPB's activities and board of directors' meetings with no right to vote.

The EDPB is composed of all the representatives of national authorities for privacy protection, plus the European Data Protection Supervisor (EDPS). The latter was enforced by the EU regulation 2018/1725, which conforms to GDPR and directive 2018/680 and defines which norms can be applied by institutions and European authorities while managing personal data.

The EDPS is an independent entity, responsible for monitoring the appliance of privacy protection norms within the EU and eventual fines. It collaborates with the EDPB and executes its functions according to the instructions given by it.

Finally, the European Commission appointed a Data Protection Officer (DPO), an independent entity that ensures the correct internal enforcement of privacy provisions, in collaboration with the EDPS. The DPO also provides public recordings of all the data operations carried out by the Commission.

Key aspect of the General Data Protection Regulation

According to the regulation, personal data is information that can directly identify a natural person, from the first name to gray areas such as the IP address.

Being EU-based, any resident or entity that participates in the local market has to comply with the GDPR, enlarging the territorial jurisdiction: it is then required that any non-EU business processing EU citizens' data will appoint a representative in the EU.

The GDPR distinguishes between data controllers, who define the purpose of data operations, and data processors, those who execute those operations on behalf of the controller. The distinction is necessary to define the responsibilities: the controller is accountable for extracting data without consent or to modify the accessibility of the processor if the consent has been revoked. On the other hand, processors must provide sufficient guarantees to be chosen by the controller, to implement an appropriate organization in compliance with the GDPR requirements.

Both the data controller and the processor can be fined under GDPR, which also provides the amount to which the companies could be subjected; compared to previous provisions, the penalties have increased, and larger companies end up being penalized because the system is designed to issue a fine proportional to the size of turnover of the organization.

The legislation is consumer-centric, and furtherly controls the way companies can manage sensitive information. The right to be forgotten is outlined in Article 17: if the data is no longer relevant and not of public interest, any subject can ask data controllers to erase their personal information and third parties to stop processing them, removing them from their databases. For even more transparency, data controllers must notify individuals if their data is being processed, where and for what purpose; the organizations must then be ready for consequent requests by the now-aware users. Article 33 gives instructions on how to manage data breaches: it indicates timing, which authorities to notify (Article 55), how to report the event, and how to adapt the companies to prevent future similar occurrences.

A peculiar provision of the GDPR is the requirement for companies that process specific kinds of data (genetic, health, related to religious beliefs, and other sensitive information) to appoint a DPO.

Since the enforcement, many once-legal activities are now banned: companies were pushed to review their plans to comply with the GDPR, in particular regarding their privacy policies and how they were getting explicit consent from their users.

According to the latest reports, authorities have issued 2.3 billion euros of fines. In 2022, the priorities on which they focused were the 50 percent increase in the total GDPR fines issued and the treatment of ad-tech and behavioral advertising. The results were accomplished: what was the biggest fine in history (50 million euros to Google in 2020) has been surpassed by fines received by Amazon and Meta.

Among EU members, the highest fines recorded were issued by The Netherlands to Amazon and by Ireland to Meta.

For violating the GDPR, the biggest fine amounts to 746 million euros: in July 2021, the Luxembourg National Commission for Data Protection issued the fine after receiving a complaint from 10 thousand people against Amazon, being the culprit of processing personal data to target advertisements without proper consent of its users.

In September 2022 and January 2023, the Ireland Data Protection Commission issued fines to Meta, respectively worth 405 and 390 million euros. The first investigation focused on how Instagram accounts automatically showed the personal contact information of minors publicly; the second was about Meta forcing users to accept their new terms of service to still

access the service: by forcing the consent, the consequent behavioral advertising would have been considered conform to GDPR obligations.

Apart from the GDPR, the EU has enforced the *Digital Services Act* (DSA): online platforms will be forced to remove mischievous and illicit content if they don't comply with certain required standards. DSA provisions have already been put into practice since 2022, until the regulation will be fully effective from February 2024.
The interested parties are large platforms (defined as such when they reach more than 10 per cent of European consumers), online platforms that make supply and demand meet, hosting services, and network infrastructure providers (intermediary services).
Very large platforms must produce crisis management protocols and cooperate with authorities when they occur; adhere to their official codes of conduct and refer to external independent bodies of control, to take full responsibility for their activities; allow their users to opt-out from profiling operations and the consequently targeted advertising; share the extracted data with authorities and researchers.
Other provisions refer to both very large platforms and online platforms: they must guarantee full transparency of their advertising practices and recommendations systems, which cannot involve children and users' special interests; a complaint and redress mechanism must be available for users, also one against spams and abusive notifications; if the platform is an online marketplace, personal information of suppliers must be checked, to guarantee their compliance to certain standards.
Going on, hosting services, online, and very large platforms are required to declare any criminal activity and to design a tool for users that reports potentially dangerous content the company should consider removing.
The DSA imposes the four mentioned businesses to cooperate with national authorities, update and adapt their terms of service to guarantee the fundamental rights as intended by the European Union and make an effort to increase the transparency of their reporting and monitoring operations. For any violation committed, the company will be fined up to 6 per cent of their annual income of the previous year; for any informational violation, the maximum sanction amounts to 1 per cent of the previous year's turnover.

The 2022/1925 EU regulation, the *Digital Markets Act* (DMA) affects the gatekeepers, those large digital platforms which can set unfair standards against their smaller competitors: the regulation acts like an arbiter and restrain the competitiveness of big companies such as

Facebook, Google or Amazon. For example, under the DMA, it is forbidden for Amazon to put its products on top of competitors' alternatives on the results page.
A business is identified as a gatekeeper if it has a strong position in EU markets and many EU state members; it is a strong intermediary between consumers and companies; it has or will have a significant market role thanks to its good financial performance in the last three years.
Some of the many duties the gatekeepers must fulfill: price transparency must be guaranteed when intermediary advertising is provided; it is forbidden to track users outside the platform to collect data for targeted advertising; users' data cannot be employed in operations for which explicit consent hasn't been given; the platform's design must be user-friendly, the disclosed information must be easily modified and it must be easy to de-install the software; no registration must be requested to access additional services related to the platform; non-public data of competitors cannot be used to compete with them.

A very awaited measure is the EU's *e-Privacy Regulation* (ePR), which was projected to be enforced together with the GDPR but it is still stuck; on March 2022 the European Council reached an agreement, yet the ePR is not expected until 2023, and even if it will be effective during this year, companies will be given time to adjust to its standards until 2025.
An effective ePR would strengthen the privacy levels of contents of online communications, including metadata, the information from which other data can be disclosed when collected. Service and network providers would have to get explicit consent from users before extracting and processing metadata.
Moreover, ePR would simplify cookie management. Users would accept or reject cookie trackers at the browser level, to deal only with non-invasive cookies, those necessary for the functioning of the platform, and not privacy intruders. Users would be asked once per year to reconfirm their consent on data extraction operations.

4.2 US data protection

Differently from the European Union, US privacy legislation is fragmented, and enforced at different levels. Pending the approval of the *American Data Privacy Protection Act* (ADPPA), which represents the first actual comprehensive federal law, other laws that deal with data invasion at the federal level are:

- the C*hildren's Online Privacy Protection Act* (COPPA)

Enforced in 1998, the law dictates how online services providers must manage children's data; in particular, they must acquire explicit consent from the parents of children under 13 years old for collecting, using, and sharing their information.

- the *Health Insurance Portability and Accounting Act* (HIPAA)
  Enforced in 1996, the law aims to improve the continuity and portability of health insurance coverage, in particular, to challenge frauds in medical services and promote the subscription to long-term plans to access care services.
- the *Gramm Leach Bliley Act* (GLBA)
  Enacted in 1999, the act demands financial institutions to provide records of their activities related to data collection and sharing, and their protocols to shelter their clients' sensitive information.
- the *Family Educational Rights and Privacy Act* (FERPA)
  Since 1974, the law regulates the disclosure of education records of students under 18 years old, limiting access to third parties such as potential employers or foreign governments (excluding parents).

At the state level, there are many sector-specific privacy laws, which provision is under the control of State general attorneys; the appliance could refer to governmental or private (or both) entities. Some of the issues dealt with are data collection and protection, how information must be archived and disposed of, how to notify users in case of privacy violations, and so on. Policymakers have been pushed by consumers and even by companies to provide for such forms of legislation; in particular, the lack of a comprehensive federal law represents significant costs for business: instead of hiring lawyers or experts, it would be more efficient (and cheaper) complying to a single law and adapting internal policies to its precepts. California, Colorado, Connecticut, Virginia, and Utah were the first states to enact laws with a national impact; currently, many states are considering following their steps, in particular Michigan, Ohio, Pennsylvania, and New Jersey.

The *California Privacy Rights Act* (CPRA) was the first and still is the most comprehensive state privacy legislation. It was eforced in 2023 and substitutes the previous *California Privacy Protection Act* (CPPA). It swells significant duties for those collecting data of California residents: users must be informed when and how data is being extracted, to give them the possibility to opt-out from the operation or access, correct or simply delete some information; in addition, data transfers between businesses have been severely limited.

The CPPA already provided the right to rectification (modify inaccurate information), restriction (modify the disclosure of information), and special protections for sensitive information.

The CPRA improved its predecessor by increasing fines related to children's privacy violations; limiting for how long a company can retain data; imposing companies to contractually mandate to third parties they collaborate with to comply with the same privacy standards; expanding the definition of a breach to furtherly protect any information that could allow the access to users' accounts. Moreover, the CPRA was the first act to establish a new regulator. Usually, privacy cases are handled by the Federal Trade Commission (FTC), which has the authority to impose sanctions against several kinds of practices, for example in the case of non-transparent privacy policies or misleading advertisements. From July 1, 2023, the California Privacy Protection Agency will have the power to issue fines, give suggestions regarding privacy guidelines and manage judicial cases related to privacy violations.

Effective on January 1, 2023, Virginia's *Consumer Data Protection Act* (CDPA) protects consumers' data and dictates how companies can employ and share them. It applies to any working business targeted to Virginia residents, but also to organizations that process data of 100 thousand or more people, or that process data of at least 25 thousand consumers and earn half of their revenue by selling such information. Similarly to the EU's GDPR and CPRA, the CDPA forces companies to get explicit consent for processing sensitive data; to notify users when data is collected and sold and allow them to opt out; to provide a transparent privacy policy; to enable consumers to opt-out from targeted advertising.

On July 1, 2023, the *Colorado Privacy Act* (CPA) will be effective. It protects residents' data and sets responsibilities for collectors, as the previously mentioned legislations do. In particular, compared to the CDPA, the CPA applies to organizations that process data of 100 thousand or more people, or that process data of at least 25 thousand consumers and earn revenue by selling such information.

The *Utah Consumer Privacy Ac*t (UCPA) will take effect on December 31, 2023. It doesn't apply to governmental entities or other third parties that manage information protected by HIPAA or by related regulations; also, it doesn't apply to financial institutions subject to GLBA. Compared to the CDPA, the UCPA applies to organizations that earn over 25 million dollars per year, that process data of 100 thousand or more people, or that process data of at least 25 thousand consumers and earn half of their revenue by selling such information. Consumers still gain the right to be notified about their data when processed, to obtain their

data in a more accessible format, and to opt out of targeted advertising, but they cannot opt out of profiling operations or correct their information.
Together with the CPA, *Connecticut's Data Privacy Law* (CTDPA) will be effective in July 2023. It also draws from the CDPA, applying to organizations that process data of 100 thousand or more Connecticut residents or that process data of at least 25 thousand consumers and earn half of their revenue by selling such information; still, it excludes data needed to complete a payment processed by small businesses (such as restaurants). Until December 31, 2024, the CTDPA grants 60 days to fix violations committed.

Other relevant regulations about privacy are the 2021 Chinese *Personal Information Protection Law* (PIPL), which broadly draws from EU's GDPR but guarantees fewer rights, sets harsher criteria for consent, and contemplates greater sanctions; 2020 Brazilian *Lei Geral de Proteção de Dados Pessoais* (LGPD), which provisions are very similar to the GDPR; 2009 Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA), which was retained progressive at the time but is now overshadowed by GDPR's standards.

4.3 EU - US relationship

Both within the European Union and the United States there are several laws governing data usage and companies' behaviors regarding their consumers' rights. The relationship between the two entities has grown through the years, not only on the commercial side but as previously discussed, the attitude towards privacy regulations is very different, influenced by cultural and historical development. Just like their affiliation, the systems managing data exchange between the EU and the US have evolved and adapted to the respective regulations, to keep guaranteeing fundamental rights to the populations involved.

As already stated, the EU *Safe Harbour* directive was one of the first introductions to comprehensive privacy governance, intended to manage data transfers between the EU (and Switzerland) and the US according to seven key principles, still very relevant in today's laws.
First, under the principle of notice, users had to be informed about when their data were collected, how they would have been employed, and how to reach the responsible for the operations without any doubt. The choice precept imposed that any user would have the possibility to opt-out and eventually transfer their information to other third parties; these organizations had still to comply with the shared data protection standards, as set by the onward transfer principle. The security precept pushed to make adequate efforts to shelter

data from theft or loss, and the integrity guaranteed that any data employment would have been adequate to the original purpose of the extraction. According to the access principle, users had to be allowed to access, modify or delete any personal information. Finally, the last principle of enforcement required efficient tools to make others effective.

On October 6, 2015, the *Safe Harbour* was officially invalidated by the European Court of Justice. **Maximilian Schrems**, at the time a law student and today activist for digital rights, declared in an Austrian court that the current European regulation wasn't protecting his rights, because while using Facebook his data was transferred to the US. After Facebook argued that Austrian courts did not have the competencies to deal with the case because Facebook's European activities were carried out in Ireland, the debate moved at first there, then it was brought to the European Court of Justice in Luxembourg. In the end, it was declared that the surveillance practices carried out while users were simply using the platforms didn't protect privacy: as Schrems pointed out, tools such as Google Analytics or Facebook Connect were not necessary to run the webpage, and the user should have the possibility to deactivate them. The Court ruled in Schrems' favor and the 1995 directive was invalidated.

Still, data exchange between the EU and the US wasn't going to stop, an alternative governance was rapidly needed. To find alternatives, *Article 29 Data Protection Working Party* (WP29) was questioned; the body's name came from the 29th article of the Safe Harbour (free data movement and protection from unknown processing). They recommended binding corporate rules: all the companies that were working under Safe Harbour had to refer to or create **standard contractual clauses** (SCCs) with each of their data partners, and they were given a couple of months to put them in place.

On December 1, 2015, Schrems filed another complaint regarding how these tools were still inefficient in protecting privacy, as Facebook kept sharing data with the US venues.

Soon the *EU-US Privacy Shield* was agreed upon and formally adopted on July 12, 2016. It promoted the same principles and invigorated the certification obligations that companies had to comply with to legitimately participate in international data exchanges. The Swiss-specific regulations were aligned with the new framework in April 2017. In the meantime, the GDPR came into effect in 2018 and it doesn't mention the Privacy Shield.

Schrems II ended on July 16, 2020, when the European Court of Justice declared the 2016 Privacy Shield invalid too, yet upholding the legitimacy of SSCs. Regarding the latter, it was then declared that data processors and controllers relying on them would have been obliged to verify their adequacy on a case-by-case basis, and if necessary provide additional sheltering

measures to comply with the GDPR: the SSCs are now the only legal tool governing international data transfers between EU and US.
On October 7, 2022, US President Biden requested a revision over sheltering provisions against surveillance activities: the new EU-US Privacy Shield may have found its basis. The framework will provide enhanced safety measures and mechanisms for both EU and US citizens that will want to file complaints in case of privacy intrusions; moreover, intelligence agencies are requested to review and adapt their surveillance protocols.

On December 13, 2022, the European Commission initiated the procedure to adopt an adequacy decision regarding the US proposal. The Commission's draft of adequacy stated that the protection provided to EU citizens is essentially the same under the GDPR. The significant improvements of the framework have been recognized, yet various concerns arose: the lack of transparency of certain procedures could undermine the capability of users to access and modify their data; the lack of independence of the responsible bodies is such that the US President would still be able to overrule their operations; mass data extractions are permitted in certain cases and safeguards could be inefficient.
In a non-binding resolution on May 11, 2023, The European Parliament called on the European Commission to not adopt the adequacy decision until adequate proceedings are enforced; this decision relies also on the non-binding one by the EDPB (ex WP29), which on February 28 expressed its concerns regarding the sufficiency of the framework. Additionally, it was requested to provide a legal framework that can withstand potential legal challenges, as the Schrems cases have been; this call is especially relevant considering the escalated worries about surveillance practices that emerged during and after the pandemic.

4.4 Bridging the digital divide towards equality

Since January 1, 2016, the list of seventeen Sustainable Development Goals (SDGs) has been introduced, aiming to promote initiatives in all social venues and economic sectors to create a fairer and healthier world by 2030. The initial wave of optimism has muffled down as the time is running out, but comprehensive positive results could be obtained if the focus would move towards SDG 9C, universal and accessible Internet networks, and devices for the least developed countries in the world. The digital divide takes part in worsening the living conditions of developing countries, preventing people from accessing those goods and services that would enable the achievement of SDGs; its surge must then be fought by governments and big organizations.

The pandemic highlighted how fast broadband is fundamental for society, businesses, and economic systems' advance. Health care, workplaces, education, and all the other essential services lean on digital infrastructures: enforcing ubiquitous access to them would improve the everyday life of many more people.
Despite the increased awareness of the issue, the progress to resolve it proceeds slowly. The International Telecommunication Union reports that one-third of the globe does not have access to the Internet: some of the most trivial everyday online activities cannot then be taken for granted. The possibilities to live a comfortable life decrease with no access to remote learning, online banking, or remote work interviews; also, the ability to face and resist global challenges is severely undermined.

Connecting Humanity, a fund advancing digital equality, shared its *State of Digital Inequity* report across 136 countries, having around 190 million people answering questions about digital impediments their community perceives. Among the respondents, 95 per cent stated that Internet access is critical in any organization's daily operations; 91 per cent defined Internet access as necessary for reaching customers and serving their communities adequately; 92 per cent also pointed out how important Internet access is to reach founders or organize fundraising to support your projects.
In 2020, Statista investigated the relationship between Internet access and economic vulnerability; the phrasing "economic vulnerability" refers to the occasions in which the previous year the interviewees were able or not to afford food and shelter and had or didn't have family or friends to rely on.

% people with Internet access	High economic vulnerability	Moderate economic vulnerability	Low economic vulnerability
World	24%	46%	74%
Developing Economies	21%	42%	68%
Developed Economies	77%	84%	91%

Just 24 per cent of people in highly vulnerable conditions had some form of access to the Internet, instead almost three-quarters of those lowly vulnerable had access to it. Without considering the economic conditions, the general tendency views developing countries as less likely to have the majority of citizens accessing the Internet, while in developed countries, 77 per cent of those in the most vulnerable situation were able to access it.

The pandemic and the consequent economic and social crises only worsened the conditions of the most disadvantaged countries, but they still can represent the catalysts for a wide implementation of much-needed digital infrastructures. Cooperation among civil society, policymakers, corporations, and governments will be required to enforce cross-sector synergies that will spread the benefits of the digital era to anyone.

In March 2021, the European Commission introduced *2030 Digital Compass: the European Way for the Digital Decade*, the long-term strategy for digitizing the European Union. The Commission wants to specifically pursue EU digital ambitions through designed paths for development at the EU and national level, which also include key performance indicators to track progress towards the goal; additionally, an annual collaborative cycle was implemented to monitor and report progress, and to enforce international projects combining investments from EU bodies, members and the private sector.
Regarding the digitalization of public service, the goal is to provide the key ones also one fully online; moreover, every citizen would be able to access their medical records online, and at least 80 per cent of them will have a digital ID. For digitally transforming business, 75 per cent of EU companies will employ cloud services or AI, and at least 90 per cent of the late adopters SMEs must reach a basic level of digitalization; also, the aim is to double the presence of EU unicorns.
By 2030, there should be around 20 million ICT specialists (verifying gender convergence within), and at least 80 per cent of the population must possess basic digital skills.

On January 26, 2022, the Commission presented an inter-agency solemn declaration on digital rights and precepts, to comply with the goals of the Digital Decade plan. The declaration reflects the EU's political commitment to implementing rights to live a better digital life, and it complements both the existing regulations on data protection (ePR, GDPR) and the Charter of Fundamental Rights.
The shaping themes are:

- People at the center of the digital transformation
  Technology should serve EU citizens in achieving their aspirations, it should not represent a potential threat to their fundamental rights.
- Solidarity and Inclusion
  Technology should be inclusive and serve elderly people, those living in remote areas, disabled people, marginalized communities, and the most vulnerable individuals; the

efforts should be directed towards improving connectivity, digital education, working conditions, and digital public services.

- Freedom of choice online

  Everyone should be empowered to make informed decisions online; the declaration promotes human-centric and ethical AI systems, pushing for transparency around the employed algorithms. Freedom of choice also pushes competitiveness among online businesses, leading to digital innovations.

- Participation in digital public spaces

  Online platforms should design a digital environment that protects people from disinformation and dangerous content, supporting instead cultural and linguistic diversity and encouraging pluralistic debate and democratic participation.

- Safety, security, and empowerment

  The declaration pays special attention to children and young people that need particular protection against cybercrimes. Everyone participating in online activities should have effective control over their personal and non-personal data as provided by EU laws.

- Sustainability

  Digital tools must be designed, produced, and disposed of in the least harmful way for the environment and society; also, there should be more information regarding the environmental impact and energy consumption of online services.

The European Commission will provide an assessment of the implementation of these principles in its annual *Digital Decade Status Report*; also it will conduct an annual Eurobarometer survey to monitor follow-up investigations in EU members: the Eurobarometer will collect qualitative data based on public perceptions of how digital principles are being implemented.

The first difference among the analyzed systems is the levels of enforcement. As previously mentioned, in the US there's still no general law applied at the federal level, for now the FCT is the only entity responsible for such coverage; instead, the DPAs are coordinated at pan-European level. At sectoral level there are sector-specific regulators in both contexts. The national data protection authorities of the EU are comparable to the state attorney-generals in

the US for enforcement at state level. Consumer class actions are frequent and quite effective in the US, while in the EU they happen very rarely, due to the fact that EU regulations are more customer-oriented and guarantee more fair coverage.

Regarding the sensitive data that deserve legal protection, in the US they are defined as PII, personally identifiable information, while in the EU it applies a broader interpretation, also to make it easier to extend the coverage when needed. Moreover, the data retention period is often indefinite in the US, while in EU companies are expected to prove that they deleted the data previously collected when it was obviously not necessary anymore to store them.

Consent has a more significant role in the EU than the US: there's this sorta of paternalistic approach, according to which it's not always possible to rely on people's ability to give consent. When it comes to cookies, in US the consent is not explicitly requested, while in EU it is asked each individual time; in both EU and US any e-marketing communication must provide the opt-out option. Generally, American opt out regimes are much weaker than European ones: data can be processed only if the opt-in option has been explicitly accepted data; this is not convenient for international platforms, as they need to design different functions depending on the location their service is being used. The enforcement of GDPR has forced to update internal policies, data handling procedures and safety measures, as every privacy policy must comply with the standards; providers could choose to open their platforms only to American citizens, but it would represent a huge loss.

The sanction system enforced by the EU through the GDPR is designed to effectively extract wealth from extremely rich providers, and is also often propped up by peculiar governmental actions. If consent must be given to benefit from the service, then the choice is illusory and meaningless, and it doesn't shift the liability of the consequences from surveillance capitalists to citizens.

Chapter 5 - **Surveillance drifts**

For MIT Technology Review, Kristian Lum defined an **algorithm** as a set of instructions that a computer executes to learn information: the complexity of an algorithm can increase with the amount of data processed because each of them is weighted onto a series of inputs until the relative phenomenon is disclosed and can be investigated. Artificial intelligence, **AI**, is the mimic of human reasoning by machines, especially computer systems: through a neural network of algorithms, especially related to language processing and speech recognition, computer systems learn how to perform tasks on their own.

Since Isaac Asimov's works, the implication of AI employment has been discussed. Today more than ever, the dialectic of technological inevitability hits close to home, but knowledge and awareness of such mechanisms are still valid counteroffensive weapons.

5.1 The cognisance of AI

Many measures have been adopted to prevent plagiarism among students. Today, copy-pasted or paraphrased texts are very easy to detect and more time-consuming compared to asking one of the many AI software for a full text about literally any topic.

Many professors stated that they are able to recognize an AI text: it feels cold, distant from something generated by the mind of a student, a bunch of facts put together from which no emotions transpire. Moreover, it should not be ignored that, as an academic tool, the knowledge provided is pretty narrow: the AI is programmed to fastly arrange a proper and adequate answer for the question typed, and the software doesn't add anything more than what is requested, hence people won't understand the thought process behind the composition nor learn potentially correlated topics that could enrich the response. AI is constantly learning how to be convincing: the text arranged is not based on accurate research, in which every source is read and critically analyzed, it is more about putting together information that mentions the same words or topics of the question; more information is assembled, higher is the probability to have answered. And the result is not incorrect and could sound plausible, but that's because it comes from what was written by real, aware, and trained authors.

One could argue that we humans are doing the same: our knowledge and expertise derive from our education path and from what others taught us. Yet, while an AI mimics human mental processes, each of us has a personal internal system of comprehension, models that we have internalized and applied to our daily life. Our attitude matured while we were growing up and experiencing the way AI answers a question can change multiple times per day.

The first time kids are asked how to count to 10, they could find it hard, but when the mechanism is understood, they can apply the general rule and logic to whatever situation they will face. Human cognitive abilities allow us to make generalizations, acquire naturally new rules, and apply where we know they are convenient, and such mental processes are universal and yet unique for each one of us. We can do abstractions, and imagine something completely new or just an impossible scenario in the future; AI has to draw on existing theories or can make a list of what cannot happen because of a series of reasons.
In general, an AI can provide answers only to what has been specifically typed in the question, if it can access data, and if someone has already written about it. AI is not creative, it doesn't have an internal comprehension system from which it can generate original interdisciplinary approaches.

As previously stated, to receive an acceptable answer it is necessary to be very specific when presenting the question, hence we need to already have a conceptual understanding of it. According to the AI logic, once we get the information we are missing, we will be able to fully answer the inquiry. Consequently, the AI acts like an autocomplete software, providing the best approximation of a complete answer. It mimics our interpretation. If the answer given contains mistakes, these are due to not understanding what it is stating, because the way we constructed the question and what words we used depend on our unique reasoning.
What is truly missing is the moral compass that every person possesses and expresses through actions and thoughts. The objective is to employ algorithms to learn behavioral data, then transfer it to AIs to provide targeted contents that won't feel like a mimic. Since then, following the capitalist logic of accumulation, the strategy has been to enlarge as much as possible the scale of data extraction operations, to cover as much knowledge as possible. It is possible to ask an AI what is the meaning of life or just how it is feeling: the answer comes from learned and imitated human interactions and behaviors, but it helps fade that feeling of a distant technology.
Are Siri or Alexa fine as they tell us when asked? Can they be not fine? AI doesn't distinguish between good and bad because it doesn't understand feelings conceptually, it can just provide theoretical definitions or define them as others did. AIs are programmed to answer professionally and politely, our reactions and moods are not programmed, they depend on our perception of what we experience, which in turn derives from sociological and anthropological processes specific to the human condition. Human behavior comes from internalization, AI mechanically learns and repeats.

5.2 The indifference of AI

Being only able to report what others have already stated about something means also being unable to differentiate between a truth and a lie. As previously said, AI does not answer accurately, it aggregates information in a way that statistically maximizes their adherence to the question. Telling a lie means knowing what is the actual truth: if AI was asked something and to answer only stating the truth, it wouldn't have the capabilities to make a conscious selection among the contents detected to be related to what has been typed.
Here comes the threat of unmoderated online content.

5.2.1 The ByteDance algorithm

Since its introduction, **TikTok** has been growing at the fastest rate ever seen among other social media. The concept is simple: when you want to distract yourself for a bit, open the app and swipe thousands of short videos, you can relax, have fun and even learn something. It requires less time than watching a YouTube video, perhaps you will feel less guilty about wasting your time on social media; the contents can be three minutes maximum, after which you can close the app and go back focusing on whatever you needed to distract yourself from. It's a silly diversion, right? No, the unprecedented growth rate is due to a highly secretive algorithm that makes the app addictive. The For You Page, the main page on which we are shown content, is known to be incredibly accurate, even when it comes to our very private and specific interests. Are we losing time and diopters in front of our mobile phone screen because we feel seen and understood? Because we feel safe knowing that other people feel as we do? The Wall Street Journal team investigated to understand how the app is tracking us, to get our full engagement.
If you ask the representatives of the company, they will say that the algorithm learns your interests from the likes you leave, the videos you share, and the creators you follow, and from such information, it will show you videos it knows you will appreciate. Yet, through the experiment, it seemed that the only variable influencing the algorithm was the watch time.
The WSJ team created over one hundred automated fake accounts. The only information given voluntarily was the year of birth and the location, and the app automatically gets your IP address; participants weren't allowed to give any additional information, including leaving any likes or sharing any video. Every account was created with specific interests not disclosed, that the app had to understand only through tracking the watch time: participants

could only keep scrolling and watch entirely or more times the same video that dealt with the topics assigned to their account.

So, how long does it take for the TikTok algorithm to get to know you? Once downloaded the app, the first videos shown have 6.31 million average views: these are not specifically targeted, people will be presented with what the general audience appreciates, so viral dances or funny videos. The time tracking starts immediately, so after a few minutes the average of views lowers to 0.78 million; the contents get more specific. From there, it's just descending into the rabbit hole.

According to Guillaume Chaslot, an expert in algotransparency, the TikTok algorithm is different from any other ever employed in social media. It has much faster learning abilities, and it gets much deeper. YouTube works similarly: since creating an account and logging in, the algorithm records what videos you are watching, which topics you research, and which YouTubers you subscribe to; 70 per cent of the content consumed on the platform depends on the recommendation engine, but the TikTok ones are much more precise and increase the percentage to 90-95 per cent.

The WSJ team designed the 3D representation of what the universe of TikTok contents is supposed to look like, a very dense mass in the center, where the general audience's contents are, then thinning out towards the niche contents. In practice, you start with videos of cute animals, move to only dog videos, then to videos with bulldogs specifically, and finally to videos with only French bulldogs. The trajectory of what contents are due to be shown has been already planned, the algorithm needs only to catch some data and guide you toward your "special interests". But it doesn't stop to learn your favorite movie or your zodiac sign, it learns about your mental health and even medical conditions, by reaching plausible conclusions from the videos on which you engage more with.

One of the many profiles the WSJ team created was @kentuky_96, a guy (obviously from Kentucky and born in 1996), characterized by sadness and depression. As scheduled, once logged in, the app started showing viral videos, among which there was one from a content creator that had the word "sad" in its username: a low voice was talking about sad stuff, with a "sad" soundtrack and a description composed by hashtags such as "sad", "depressed"; our Kentucky guy watched the video twice, as its personality was supposed to appreciate it. The app now knew the user was feeling down, and 23 videos later another sad video from the same content creator was shown, this time specifically about how depressed you are after breaking up with your significant other; after some other videos, another sad video was

shown, from another author, and about how sad is to end a friendship. Between targeted videos, the app was showing other funny videos and some content creators from Kentucky.
The 57th video was again about breaking up, the 60th was about emotional pain; videos about missing your ex and advice on how to move on after breaking up were swiped down. Among 224 videos, for a total of 36 minutes of watch time, the fake guy engaged more with videos about depression and mental health than videos about relationships and breaking up: once this was understood, the algorithm started its advancement down the rabbit hole, and 93 per cent of the following shown videos were about depression. The others were the so-called disruptive content, videos that everyone likes, so you are not immediately alarmed about how good the app already knows you, and of course some ads.
The algorithm is not representative at all, humans have a very diverse set of interests. Yet, we get directed towards the ones it had less difficulty in detecting, those topics that will keep our engagement with the app high. Using the app two to three hours a day, in a non-continuous way, doesn't feel disturbing: the app keeps learning about your interests, you will be shown all the most viral videos and all your interests, and it will be a funny experience. But it's very easy to use TikTok, you only need a finger to touch the screen: when the engagement with the app lasts for nine or ten hours, the contents shown will start to be scarily specific, and at some point, your whole for your page will show all the videos about that topic the algorithm can find.
According to the WSJ experiment, the TikTok algorithm took around 40 minutes to know @kentucky_96 interests. After two hours it would have been able to move its profile to very niche content, with very low views. The less the content is viral and viewed, the fewer moderators pay attention to it: considering that the main topic of the shown videos was depression, the related videos left unchecked could mention suicide or harmful behaviors, and there would be no one to delete such content and protect fragile users.

Surveillance algorithms are employed to learn behavioral data, to produce engaging content and targeted advertising. The TikTok algorithm learns fast about us and directs our whole experience with the app towards a precisely designed route that makes us feel understood: if we feel good using the app, we will engage more with it, and we will end up being confined in the most predictable part of our interests. We will stop having a personality, we will be perceived only according to the contents that keep us producing fuel for the algorithm. With this kind of ability, an algorithm that predicts people's behavior becomes obsolete: investing in targeted advertising is not even necessary anymore when algorithms can divide users into

groups and redirect them towards ads previously produced, based on one or two relevant interests. If we are kept inside the rabbit hole, we cannot behave in unpredictable ways.

5.2.2 Radical indifference

People are tracked and their behaviors and interests are learned. Online platforms are designed to be engaging, the content and ads we are shown or recommended are selected or crafted according to the profile that has been built about us. Being online must be perceived as a pleasant experience, we are shown only what they know will keep us there: people that like the same stuff we like, that think how we think, that look as we look.
We end up bound to our targeted, engaging Internet experience.

Before tailoring customized content, any platform or advertisement needs to record significant engagement rates, fundamental to both extracting data from people and increasing their popularity. The hype will activate a positive chain reaction: the content will be recommended to many new potential consumers, furtherly enforcing the engagement levels and the surveillance operations. Clicks are well-accepted by anyone.
The fraud of click farms has been known for a while: a large group of low-paid workers is hired to click on links or surf for a certain time a website; this kind of fake engagement is more difficult to detect compared to the one generated by bots. These "organizations" are being tracked down, because they could guarantee visibility to fake businesses or fake news. Still, beyond hindering such illegal operations, the monitoring operations over online content should be boosted. Algorithms or AIs are not able to differentiate between true and false content or safe and harmful ones, so with no moderators, anything that becomes public domain can be misused.
Unmoderated contents, independently from their core, validate and enforce each other, and in the end, they appear legitimate and can be used to sell any service. Moreover, to answer an inquiry, AI could select them as valid sources: if we are continuously exposed to similar content while online, it could be difficult to differentiate between what's true and false for us too.

Not having the conception of good and bad means also not having the conception of consequences. The threats of unmoderated content are more evident when they are about political conspiracies, or promote xenophobic attitudes. People that spend the majority of their day alone, inside their peculiar bubble, constantly subjected to potentially harmful topics, can

become a danger for themselves and others. TikTok is particularly ineffable, but any other social media has the same dramatic potential.

For a while now, Zuckerberg has been trying to rebrand his company to detach it from the numerous scandals that have seen Facebook as the main protagonist. Meta was introduced as the project that would have brought back the company to its leading cause: not just creators of social media, but of technology that connects people.

After January 6 2021, when Trump supporters stormed the US Capitol to protest against the results of the presidential elections, former employee and whistleblower Frances Haugen lit the fuse, disclosing ten thousand Facebook's internal documents. She denounced how Facebook was well aware how their services were not only damaging people's mental health but also cultivating ethnic discrimination and spreading misinformation; also, she pointed out how the apparent company's commitment to moderate and limit such harmful content was always hindered by a shortage of staff.

The case of the US Capitol is emblematic: Facebook did nothing to mitigate the spread of posts or comments used to organize people and their violent and heavily armed mob. This lack of content moderation led to uncontrollable events. Considering that the algorithm is designed to be indifferent to anything but the engagement rates, the responsibility of not taking action goes to the CEOs of such platforms, the surveillance capitalists.

There's this kind of "hand-off" approach to technology, also due to the asymmetries in knowledge and competencies for its functionalities. Once it was very expensive to reach the big public, now anyone can go viral saying or doing whatever they want. The spread of misinformation is worsening social polarization: unleashed extremist attitudes have proved to be a real threat to online and offline safety. In a recent interview, Professor Zuboff summarized why this must be taken into consideration: as we are left with little capacity for critical thinking and moral judgment, democracy is undermined from within; as new forms of social injustice and inequality are enforced through knowledge asymmetries and radical indifference, democracy is undermined from without.

5.3 Capitalism of automation

The so-called **automation anxiety** comes back each time workers are scared about losing their jobs after the introduction of technological innovations. Many economists argue that some jobs have died, but work persisted: technology displaced workers but enhanced productivity; consequently, new jobs emerged or the money was redirected towards new investments that eventually led to new products and new jobs.

So, how is this time with AI perceived so much worse? Many fear that, beyond having machines that can substitute people in physical jobs, artificial intelligence will also take on those jobs requiring our brains, and one day it will be much cheaper and more convenient to program technology instead of teaching people. Putting aside some extreme transhumanists' takes, the main problem with machines' employment is that the capital produced by them is not redistributed, it goes directly to the owner. Worldwide, capital has been concentrated in the hands of fewer and fewer people: so, bigger productivity means more capital for fewer people, there are more products to sell with fewer people to pay, and people have fewer jobs to do.

No job is safe in the long run, because people are not just unemployed, they are becoming unemployable as automation means gaining more profit with less expenses. It's not even about "moving to other jobs", because creative jobs in the tertiary sectors are under attack too, and the market would be so saturated that the uniqueness of such content will be devalued. Also, machine deep learning is moving very fast toward general-purpose machines that can adapt to whatever jobs you want them to perform: economies have typically adapted to automation, but it's still unreasonable to imagine that potential new jobs will be more suited to people than those we are already being replaced in.

The potentialities of AI are countless, investments should aim to employ it in useful ways instead of focusing only on saving money. For example, the pattern recognition ability would be extremely useful in scientific research, or it could be very useful in disease diagnosis in medical fields. In particular, algorithms and AIs should help policymakers in designing efficient policies, for equal wealth redistribution or welfare and planned development. The positive outcomes of automation shouldn't be considered only when justifying its increasing adoption: the conceptual co-ownership of such means of production would empower people instead of compete with them, and improve the living conditions of many.

Even in the digital era, empathy remains the prerogative of humans. We should work together towards a society that doesn't make us feel less human.

Conclusions

The dissertation presented surveillance capitalism and the reality it enforces.

Within the computational architecture of interconnected smart spaces, behavioral data are extracted and employed to generate prediction products, sold in behavioral futures markets and guaranteeing revenues to its participants. Google was the first to execute such operations, supported by the convergence of factors such as the neoliberal tradition, that pushed for a market free from governmental intervention, and the terrorist attack of September 9, 2001, which instilled a sense of urgency in respect of collecting as much information as possible to ensure the citizens' safety.

As a phase of capitalism, its logic of accumulation is reflected in the imperative of extraction, due to which tracking activities have been enlarged to as many online spaces as possible to keep up with the necessity of information. To actually complete the expropriation, the operation must follow the cycle of dispossession: starting from the incursion, through which the practice is positively introduced, followed by the habituation and adaptation phases, in which people get acquainted to it and the company superficially adjust its design to carry on the plan, to redirect the operation to make it comply to legal and social obligations. The non-contract is designed to be easily modifiable but hardly readable: this creates asymmetries of knowledge that favor providers and push the ideology of technological inevitability to consumers, who end up not paying attention to exploitative terms of service in order to get a comfortable experience.

The physical infrastructure needed by main Internet companies, the surveillance capitalists, to carry on their businesses, expands year by year, also prompting technological innovations to increase the storage space available. This ubiquitous structure answers to the imperative of prediction: with the development of surveillance systems, the competition has become about the quality of the prediction products; the means of behavioral modification induce conducts, in order to not have to predict them anymore and gain secure revenues. The rendering operations are conducted through economies of scope and actions, to process any kind of information and to modify any behavior towards secure earnings.

As surveillance capitalists invade our privacy and let third parties access too, there are different attitudes towards the perception of privacy and the control people think they should maintain over it. Psychological and behavioral mechanisms according to which people engage with online platforms depend on their culture. People from individualistic countries care about the reputations they could build through the Internet, while those from collectivistic countries use it to strengthen the relationships they already have offline.

Focusing only on the perceptions of Europeans and Americans, the attitudes are severely influenced by their concept of privacy: the first ones care about it as fundamental to personal dignity, as the individual image must be preserved online too; the latter cover it as part of the individual freedom from any state intrusions.

When analyzing both regulations, it's noted how the European GDPR is effective as a means of sanction against invasive surveillance operations: the extension of its validity is such that every company planning to open its online platform to EU citizens has to update and adjust its privacy policy accordingly. The US is currently trying to enforce a federal law, but for now they can only "compete" with sector-specific and state laws that draw a lot from GDPR. The relationship between the Western blocks regarding data transfer has improved a lot during the years, but it is now stalled until the US won't be able to provide appropriate measures that will actually protect privacy as a fundamental right.

The most pervasive tools of surveillance capitalism are algorithms and AIs. Despite the increasing rate of employment of AIs in more and more activities, these technologies are limited in their cognitive capabilities, as emotional understanding remains prerogative of humans. As surveillance engines are designed to capture behavioral data, they don't distinguish between true and false contents, ending up being radically indifferent towards the consequences of unsupervised content. One of the most representative outcomes has been the US Capitol attack by Trump supporters, able to organize their actions through Facebook without anyone disturbing them. Compared to the US 1996 *Decency Act*, that relieves the responsibility of users' contents from providers, the GDPR is loudly contrasting surveillance capitalists, making them accountable for their algorithms and their inaction.

Moreover, automation is strongly influencing the job market. Surveillance capitalism is contributing to worsening inequalities and concentrating the wealth among very few people. Machines and AIs are substituting people only to save money and spare on salaries, instead they could perform dangerous jobs or help in scientific research as databases or special calculators.

Professor Zuboff explained how surveillance capitalism is a threat to democracy, as people's cognition is weakened by an uncritical Internet participation and online presence is capitalized to secure more and more revenues to the same providers. Yet, despite the deep permeation of digitalisation in everyday's life, the digital divide is exacerbated, as automation is taking away work possibilities especially to uneducated people that were able to be employed for their physical skills.

Investments should be redirected towards the digitalisation of fundamental services, in order to improve the living conditions of those populations that haven't gained any real benefit from the digital era. Moreover, AIs should be employed to forecast sustainable development models, in order to actually empower people and not compete against them.

The first opponent of the degeneration of surveillance capitalism remains appropriate legislation, to protect people's privacy and restraint companies in employing their data. As previously mentioned, the GDPR is already contributing, compelling businesses to update their policies and consent management, issuing severe fines for those that don't comply. Yet, the law still presents some gaps, for example regarding controls over extra-EU companies or a precise definition of sensitive information, and should be furtherly invigorated to fill them.

Moreover, the collection of data should be confined to legitimate purposes, just as the beginning, to improve customer experience and secure their safety online. Every user should be granted the possibility to give and deny consent at any moment, and to have full access to their personal data to control and modify them. Finally, fines could be increased and adopted more rigorously, and could be worsened with penal sanctions for managers responsible for the privacy violations.

References

Chapter 1

Altaweel, I., Good, N., & Hoofnagle, C. J. (2015). *Web privacy census*. Technology Science, 2015121502.

Arendt, H. (1973). *The origins of totalitarianism* (Vol. 244). Houghton Mifflin Harcourt.

Bakos, Y., Marotta-Wurgler, F., & Trossen, D. R. (2014). *Does anyone read the fine print? Consumer attention to standard-form contracts*. The Journal of Legal Studies, 43(1), 1-35.

Beck, U., & Beck-Gernsheim, E. (2009). *Losing the traditional: Individualization and 'precarious freedoms'*. Identity in question, 13-36.

Berenson, A., & McGeehan, P. (2000, April 16). *Amid the Stock Market's Losses, A Sense the Game Has Changed* (Published 2000). The New York Times.

Bing Blogs. (2013, March 21). *Understand Your World with Bing* | Bing Search Blog.

Bright, P. (2015, August 12). *Even when told not to, Windows 10 just can't stop talking to Microsoft*. Ars Technica.

Brin, S., & Page, L. (1998). *The anatomy of a large-scale hypertextual web search engine*. Computer networks and ISDN systems, 30(1-7), 107-117.

CB Insights Research. (2019, September 17). *The Race For AI: Here Are The Tech Giants Rushing To Snap Up Artificial Intelligence Startups*.

Chander, A., & Le, U. P. (2014). *The free speech foundations of cyberlaw*. SSRN Electronic Journal.

Clarke, R. A., Morell, M. J., Stone, G. R., Sunstein, C. R., & Swire, P. (2014) *The Nsa Report: Liberty and Security in a Changing World*, Internet resource.

Complaint of Disconnect, Inc. Regarding *Google's infringement of Article 102 TFEU through bundling into the Android platform and the related exclusion of competing privacy and security technology*, Case COMP/40099, June 2015.

Cukier, K. (2010). *Data, data everywhere*. Economist, 394(8671), 3-5.

Cutler, T., Hindess, B., Hussain, A., & Hirst, P. Q. (2013). *Marx's Capital and capitalism today (Vol. 52)*. Routledge.

Dayen, D. (2015, November 24). *Google's insidious shadow lobbying: How the Internet giant is bankrolling friendly academics—and skirting federal investigations*. Salon.com.

Dougherty, C. (2016, May 27). *Tech Companies Take Their Legislative Concerns to the States* (Published 2016). The New York Times.

Durkheim, E., Simpson, G. (1949). *Emile Durkheim on the division of labor in society*.

Edelman, B. (2011). *Bias in search results: Diagnosis and response*. Indian JL & Tech., 7, 16.

Edwards, D. (2011). *I'm feeling lucky: The confessions of Google employee number 59*. Houghton Mifflin Harcourt.

Efrati, A. (2013, May 16). *Congress Asks Google About Glass Privacy* - WSJ. The Wall Street Journal.

Ehrlich, P. (2002). *Communications Decency Act 230*. Berkeley Tech. LJ, 17, 401.

Electronic Privacy Information Centre (December 2009), "*FTC Facebook Settlement*"

Electronic Frontier Foundation (n.d.), *Section 230*.

European Commission (April 2016), Antitrust: *Commission sends Statement of Objections to Google on Android operating system and applications*.

Farber, D. (July 2013), *Microsoft's Bing Seeks Enlightenment with Satori*, CNET,

Farzad, R. (2011, July 28), *Apple's Earnings Power Befuddles Wall Street*. Bloomberg.com.

Federal Communications Commission (2012, April 13), *The Enforcement Bureau issues $25000 NAL to Google Inc.*

Fleischer, P. (2010, April 27). *Data collected by Google cars*. Google Europe Blog.

Fleischer, P. (2007, September 24). *Google Lat Long: Street View and Privacy.* Maps|Google Blog.

Furchgott, R. (2010, September 15). *Skyhook Sues Google Over Location Software*. The New York Times.

Gerhards, A. (April 2013), "*Fine Imposed upon Google*", Hamburg Commissioner for Data Protection and Freedom of Information.

Ghazali, C. (November 2011), "*Facebook Keeps Tabs on Users Even After They Sign Off: Report*", NY Daily News.

Google Patents (n.d.), *US20050131762A1 - Generating user information for use in targeted advertising.*

Grauer, Y. (2017, November 24). *Popular Android Apps Contain Tons of Secret Trackers*. The Intercept.

Greenwald J. (2000, April 17). *Doom Stalks the Dotcoms*. Time.

Greenwood, D. J. (2017). *Neofederalism: The Surprising Foundations of Corporate Constitutional Rights.* U. Ill. L. Rev., 163.

Gurley, B. (2011, March 24). *The Freight Train That Is Android.* Above the Crowd.

Hamburger, T., Gold, M. (2014, April 12) *Google, once disdainful of lobbying, now a master of Washington influence*. The Washington Post.

Hansell, S. (2002, April 8). *Google's Toughest Search Is for a Business Model.* The New York Times.

Harvard Law Review (2014, December 10), *Google Spain SL v. Agencia Española de Protección de Datos*.

Hayes, T. (2011, October 27). *America Needs a Department of "Creative Destruction"*. HuffPost.

International Monetary Fund (June 2016), *Neoliberalism: Oversold? Finance & Development*.

IPO Centre (2017, March 31), *Global Top 100 Companies by market capitalisation*. Pew Research Center.

Jamieson, A., Morgan, T., Pepinster, C., Oliver, M., Dearnley, F., & Stephens, M. (2009, April 9). *Google Street View car: Google will carry on with camera cars despite privacy complaints over street views*. The Telegraph.

Johnson, B. (2010, January 10). *Privacy no longer a social norm, says Facebook founder*. The Guardian.

Kang, C. (2015, February 28). *Why Silicon Valley is the new revolving door for Obama staffers*. The Washington Post.

Kelion, L. (2018, February 8). *Google-Nest merger raises privacy issues*. BBC.

Kidd, C. D., Orr, R., Abowd, G. D., Atkeson, C. G., Essa, I. A., MacIntyre, B., ... & Newstetter, W. (1999). *The aware home: A living laboratory for ubiquitous computing research. In Cooperative Buildings. Integrating Information, Organizations, and Architecture: Second International Workshop*, CoBuild'99, Pittsburgh, PA, USA, October 1-2, 1999. Proceedings 2 (pp. 191-198). Springer Berlin Heidelberg.

Kothari, J. (2017, July 18). *A new chapter for Glass. After two years in a limited program…*, the moonshot factory.

Kreiss, D., & Howard, P. N. (2010). *New challenges to political privacy: Lessons from the first US Presidential race in the Web 2.0 era*. International Journal of Communication, 4, 19.

Lam, E., (2014, April 3) *New Google Share Classes Issued as Founders Cement Grip*. Bloomberg.com.

Ling, X., Deng, W., Gu, C., Zhou, H., Li, C., & Sun, F. (2017, April). *Model ensemble for click prediction in bing search ads. In Proceedings of the 26th international conference on world wide web companion* (pp. 689-698).

Linzer, P. (2014). *Contract as Evil. Hastings.* LJ, 66, 971.

Loomer, J. (2012, September 24). *Facebook Custom Audiences: Target Facebook Ads*. jonloomer.com

Luca, M., Wu, T., Couvidat, S., Frank, D., & Seltzer, W. (2015). *Does Google Content Degrade Google Search?: Experimental Evidence*. Boston, MA, USA: Harvard Business School.

Luger, E., Moran, S., & Rodden, T. (2013, April). *Consent for all: revealing the hidden complexity of terms and conditions*. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 2687-2696).

Madden, M., & Rainie, L. (2015, May 20). *Americans' attitudes about privacy, security and surveillance.* Pew Research Centre.

McDonald, A. M., & Cranor, L. F. (2008). *The cost of reading privacy policies*. A Journal of Law and Policy for the Information Society, vol. 4, no. 3 (2008), 543-568.

McGee, M. (2010, November 1). *Google Street View Debuts In Germany, Blurry Houses Included.* Search Engine Land.

McGee, M. (2011, April 10). *Google Has Stopped Street View Photography In Germany.* Search Engine Land.

Microsoft Support (n.d.). *Cortana and privacy.*

Miller, C. C., & O'Brien, K. J. (2013, April 23). *Germany's Complicated Relationship With Google Street View*. The New York Times Web

Moses, A. (2011, October 4). *Facebook's privacy lie: Aussie exposes 'tracking' as new patent uncovered*. Sydney Morning Herald.

Mukherjee, S., & D'Souza, S. (2017, January 27). *Microsoft's market value tops $500 billion again after 17 years*. Reuters.

Mullins, B., & Nicas, J. (2017, July 14). *Paying Professors: Inside Google's Academic Influence Campaign*. The Wall Street Journal.

Muro, M., Liu, S., Whiton, J., & Kulkarni, S. (2017). *Digitalization and the American workforce*. Brookings.

Newman, J. (2009). *Google's Schmidt roasted for privacy comments*. PC World, 11(09).

Noto La Diega, G., & Walden, I. (2016). *Contracting for the 'Internet of Things': Looking into the Nest*. Queen Mary School of Law Legal Studies Research Paper, (219).

O'Brien, K. J. (2010, June 27). *Europe Pushes Google to Turn Over Wi-Fi Data*. The New York Times.

O'Brien, K. J. (2010, May 15). *Google's Data Collection Angers European Officials*. The New York Times.

O'Connor, F. (2015, March 24). *Google is making Glass 'ready for users,' says Schmidt*. Reseller News.

Pasquale, F. (2013) *Privacy, antitrust, and power*. George Mason Law Review, 20, 1009.

Pasquale, F. (2018). *The automated public sphere*. In The Politics of Big Data (pp. 110-128). Routledge.

Piketty, T. (2017). *Capital in the twenty-first century*. Harvard University Press.

Pitofsky, R., Anthony, S., Thompson, M., Swindle, O., & Leary, T. (2000). *Privacy online: Fair information practices in the electronic marketplace*. Statement of the Federal Trade Commission before the Committee on Commerce, Science and Transportation, United States Senate, Washington, DC.

Protalinski, E. (2011, October 3). *Facebook denies patent is used for tracking logged-out users*. ZDNET.

Protalinski, E. (2011, September 27). *Facebook fixes cookie behavior after logging out*. ZDNET.

Polanyi, K. (2001). *The great transformation: The political and economic origins of our time*. Beacon press.

Radin, M. J. (2013). *Boilerplate: The fine print, vanishing rights, and the rule of law*. Princeton University Press.

Roosendaal, A. (2011). *Facebook tracks and traces everyone: Like this!*. Tilburg Law School Legal Studies Research Paper Series, (03).

Rutenberg, J. (2013, June 20). *The Obama Campaign's Digital Masterminds Cash In.* The New York Times.

Sandoval, G. (2009, October 6). *Schmidt: We paid $1 billion premium for YouTube*. CNET.

Schmidt, E., & Rosenberg, J. (2014). *How google works*. Grand Central Publishing.

Schmidt, E., & Cohen, J. (2014). *The new digital age: Transforming nations, businesses, and our lives*. Vintage.

Schumpeter, J. A. (1991). *The economics and sociology of capitalism*. Princeton University Press.

Schoen, K. M., Dingle, G. L., Kendall, T. (2011) "*Communicating information in a social network system about activities from another domain*". Google Patents.

Securities and Exchange Commission (2004, August 18), "*Registration Statement Under the Securities Act of 1933 for Google Inc.*". Amendment No. 9 to Form S-1.

Sequeira, N., Vacante, L., (2003, May 5). *iTunes Music Store Sells Over One Million Songs in First Week*. Apple.

Simonite, T. (2015, September 16). *Facebook's Like Buttons Will Soon Track Your Web Browsing to Target Ads*. MIT Technology Review.

Smith, A. (2014, April 17), *US Views of Technology and the Future: Science in the Next 50 Years*. Pew Research Center.

Solove, D. J. (2012). *Introduction: Privacy self-management and the consent dilemma*. Harvard Law Review, 126, 1880.

Soltani, A. (2013, December 10). *NSA uses Google cookies to pinpoint targets for hacking*. The Washington Post.

Sommer, J. (2017, September 22). *The Best Investment Since 1926? Apple*. The New York Times.

Statista (2022), *Smart Home - Worldwide.*

Steinfeld, N. (2016). *"I agree to the terms and conditions":(How) do users read privacy policies online? An eye-tracking experiment. Computers in human behavior*, 55, 992-1000.

Streitfeld, D. (2012, April 30). *Engineer in Google's Street View Is Identified*. The New York Times.

Summers, N. (2014, April 3). *Why Google Is Issuing a New Kind of Toothless Stock*. Bloomberg.com.

Supiot, A. (2013). *The public–private relation in the context of today's refeudalization*. International Journal of Constitutional Law, 11(1), 129-145.

Swisher, K. (2000, December 18). *Dot-Com Bubble Has Burst; Will Things Worsen in 2001?* The Wall Street Journal.

Swisher, K. (2009, August 4). *Video Interview: Microsoft's Satya Nadella on the Yahoo Deal - Kara Swisher - News*. AllThingsD.

TermsFeed (2023, February 18), *The "Online Eraser" law*.

The Economist (2010, February 27), *Clicking for gold*.

The New York Times (2004, April 29), *Letter From the Founders*.

Vedova, H. (2009, December 7). *Introductory Remarks for FTC Privacy Roundtable*. Federal Trade Commission.

Vogel, K. P. (2017, August 30). *Google Critic Ousted From Think Tank Funded by the Tech Giant*. The New York Times.

Warden, T. (2011, August 8), *Spain's economic woes force a change in traditional holiday habits*. The Guardian.

Waters, R. (2015, February 22). *Artificial intelligence: A virtual assistant for life*. Financial Times.

Waters, R. (2014, May 29). *Google's Larry Page resists secrecy but accepts privacy concerns*. Financial Times.

Weber, M. (2019). *Economy and society: A new translation*. Harvard University Press.

Xu, M., Ma, Y., Liu, X., Lin, F. X., & Liu, Y. (2017, April). *Appholmes: Detecting and characterizing app collusion among third-party android markets*. In Proceedings of the 26th international conference on World Wide Web (pp. 143-152).

Zuboff, S. (2019). *Analysis of data regarding market capitalization and occupation rate for General Motors (1926-2008), Google (2004-2016) and Facebook (2012-2016)*.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Public Affairs.

Chapter 2

Ashton, K. (2015, June 29). *America last?* Politico.

Borker, P. (2018). *What is hyperscale?*. Digital Reality, 2.

Brown, E. (2016). *Alphabet's next big thing: Building a 'smart'city.* The Wall Street Journal, 27.

Budds, D. (2016). *How Google Is Turning Cities Into R&D Labs*. Fast Company, 2015.

CaPPr (2015, May 20), *Interview with Michal Kosinski on Personality and Facebook likes*.

Claburn, T. (2017, February 17), *Smash Up Your Kids Blutooth-Connected Cayla 'Surveillance' Dool, Germany Urges Parents*. Register.

Consumer Federation of America (2016, June 15), *Statement on NTIA Privacy Best Practice Recommendations for Commercial Facial Recognition Use.*

Criteria Corp. (n.d.), *What are the Big Five Personality Traits (Five Factor Model)?*

Das, S., & Kramer, A. (2013). *Self-censorship on Facebook.* In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 7, No. 1, pp. 120-127).

Data Center Knowledge (2017, March 17), *Google Data Center FAQ & Locations*.

De Mooy, M., & Yuen, S. (2017). *Towards privacy-aware research and development in wearable health.* CORE UK.

Dellinger, A. (2015, March 2). *I took a job listening to your Siri conversations*. The Daily Dot.

Deloitte (2015, February 3), *Navigating the challenges and opportunities in financial services.*

Deloitte (2014), *Telematics: Overcoming the Speed Bumps.*

Dougherty, C. (2016). *Cities to Untangle Traffic Snarls, with Help from Alphabet Unit.* New York Times.

Dublon, G., & Paradiso, J. A. (2014). *Extra sensory perception*. Scientific american, 311(1), 36-41.

Dunn, J. (2016, May 9). *Introducing FBLearner Flow: Facebook's AI backbone - Engineering at Meta*. Engineering at Meta.

Elkman, P., Waxer, P. H. (1977). *Nonverbal cues for anxiety: an examination of emotional leakage*. Journal of abnormal psychology, 86(3), 306.

European Commission (2022, August 11), *Automatic Sentiment Estimation in the Wild | SEWA Project | H2020 | CORDIS |*.

Federal Trade Commission Washington (2016, December 6), *In re: Genesis Toys and Federal Trade Commission Nuance Communications*.

Feldman, M. (2016, August 29). *Market for Artificial Intelligence Projected to Hit $36 Billion by 2025*. TOP500.

Fortune Editors (2016, July 14), *The Exec Behind Amazon's Alexa: Full Transcript of Fortune's Interview*. Fortune.

Glick, "*Executive Interview*", cit.

Gartner (n.d.), *Definition of Dark Data - IT Glossary*.

Gentilhomme, A. (2015, November 19). *Dell Services Announces Launch of Internet of Things Insurance*. Workflow magazine.

Glaser, A. (2017, August 4), *Facebook Is Using an 'NRA Approach' to Defend its Creepy Facial Recognition Programs*. Slate.

Golbeck, J., Robles, C., Edmondson, M., & Turner, K. (2011, October). *Predicting personality from twitter*. In 2011 IEEE third international conference on privacy, security, risk and trust and 2011 IEEE third international conference on social computing (pp. 149-156). IEEE.

Golbeck, J., Robles, C., & Turner, K. (2011). *Predicting personality with social media*. In CHI'11 extended abstracts on human factors in computing systems (pp. 253-262).

Google Cloud (2016, May 19), *Google supercharges machine learning tasks with TPU custom chips.*

Google Patents (2015), *US20150242679A1 - Techniques for emotion detection and content delivery.*

Harris, M. (2016). *Secretive alphabet division funded by Google aims to fix public transit in US.* The Guardian, 27.

Hern, A. (2015, February 9). *Samsung rejects concern over 'Orwellian' privacy policy*. The Guardian.

Hilbert, M. (2013). *Big data for development: From information-to knowledge societies*. SSRN Electronic Journal.

Hilbert, M. (2012). *Toward a synthesis of cognitive biases: how noisy information processing can bias human decision making*. Psychological bulletin, 138(2), 211.

IBM (2014), *The Economy of Things - Extracting new value from the Internet of Things*.

IBM (2017), *Watson Personality Insights - IBM Blog*.

Jaatma, M. (2016), *Realeyes - Emotion Measurement*. TEDxTalk.

Jarvis, B., et al (January 2015), *Insurance rate optimization through driver behavior monitoring*, US20150019270 AI.

Krieger, M. (2015, February 23). *Big Barbie is Watching You – Meet the WiFi Connected Barbie Doll that Talks to Your Children and Records Them*. Liberty Blitzkrieg.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior*. Proceedings of the national academy of sciences, 110(15), 5802-5805.

Levy-Rosenthal, P. (2016, January 16), *Emoshape Announces Production of the Emotions Processing Unit II*, Emoshape Synthesis

Lima, J. (2015, December 9). *Insurers look beyond connected cars for IOT driven business boom*. Tech Monitor.

Losse, K. (2014). *The Boy Kings: A Journey into the Heart of the Social Network*. Free Press.

MacColl, M. (2018, April 16). *Apple Loses Ground to Amazon in Smart Home Deals With Builders*. The Information.

Manyika, J., & Chui, M. (2014, August 13). *Digital era brings hyperscale challenges*. Financial Times.

Marder, B., Joinson, A., Shankar, A., & Houghton, D. (2016). *The extended 'chilling' effect of Facebook: The cold reality of ubiquitous social networking*. Computers in Human Behavior, 60, 582-592.

MarketsAndMarkets (2017), *Affective Computing Market by Technology (Touch-based and Touchless), Component (Software (Speech Recognition and Gesture Recognition) and Hardware (Sensors, Cameras, and Storage Devices and Processors)), Vertical, and Region - Global Forecast to 2021*.

MarketsAndMarkets (2020), *Affective Computing Market by Technology (Touch-based and Touchless), Component (Software (Speech Recognition and Gesture Recognition) and Hardware (Sensors, Cameras, and Storage Devices and Processors)), Vertical, and Region - Global Forecast to 2025*.

Marwick, A. E., & Boyd, D. (2011). *I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience.* New media & society, 13(1), 114-133.

Matyszczyk, C. (2015, January 22). *The Internet will vanish, says Google's Eric Schmidt.* CNET.

McEleny, C. (2015, April 20). *European Commission issues €3.6m grant for tech that measures content 'likeability'.* Campaign.

Metz, C. (2017, October 22). *Tech Giants Are Paying Huge Salaries for Scarce A.I. Talent.* The New York Times.

MIT Media Lab (2012, January 12), *DoppelLab: Tools for Exploring and Harnessing Multimodal Sensor Network Data*.

Morrison, A. (1984). *Uses of utopia*. Utopias, 139-152.

Narayanan, A., & Felten, E. W. (2014). *No silver bullet: De-identification still doesn't work*. White Paper, 8.

Narayam, A. (2014, December 11), *Samsung Wants to Put Your Home on a Remote*. BusinessWeek: Technology.

Nat, C. (2015, August 11). "*Think Outside the Box - Motivate Drivers Through Gamification*". Spireon.

National Telecommunications and Information Administration (n.d.), *Privacy Best Practice Recommendations For Commercial Facial Recognition Use*.

Peers, M. (2017, January 10). *Google's Relentless AI Appetite — The Information*. The Information.

Pentland, A. (2010). *To signal is human: Real-Time data mining unmasks the power of imitation, kith and charisma in our face-to-face social networks*. American scientist, 98(3), 204-211.

Perez, S. (2016, May 20), *Google and Levi's team up on a "connected" jacket that lets you answer calls, use maps and more.* TechCrunch.

Perrin, A., & Jiang, J. (2018). *About a quarter of US adults say they are 'almost constantly' online*. Pew Research Center, 14.

Pettey, C. (2017, November 30). *Treating Information as an Asset*. Gartner.

Pope, B. (2013, June 20). *Experts Examine Auto Telematics' Pitfalls, Potential*. WardsAuto.

PR Newswire (2015, February 23), *IBM Cloud Makes Hybrid a Reality for the Enterprise.*

PR Newswire (2015, September 16), *Titan and Control Group Become Intersection*.

Reuters (2016, September 13), *Google Looks to Partner With Insurance Companies in France.* Fortune.

Sacolick, I. (2013, April 10). *Dark Data - A Business Definition*. Social, Agile, and Transformation.

Sample, I. (2017, November 2). *Big tech firms' AI hiring frenzy leads to brain drain at UK universities*. The Guardian.

Simonite, T. (2012, September 28). *Google's Answer to Siri Thinks Ahead*. MIT Technology Review.

SleepNumber.com (2017, October 6), "*How It Works | Smart Bed Technology & Sleep Tracking | It Bed*".

SleepNumber.com (2017, September 18), "*Sleep Number Privacy Policy*".

Solanas, A., Patsakis, C., Conti, M., Vlachos, I. S., Ramos, V., Falcone, F., ... & Martinez-Balleste, A. (2014). *Smart health: A context-aware health paradigm within smart cities.* IEEE Communications Magazine, 52(8), 74-81.

Stuart Mackay, R. (1970). *Biomedical Telemetry: Sensing and Transmitting Biological Information from Animals and Ma*. John Wiley & Sons Inc.

Sugden, R. (2009). *On nudging: A review of nudge: Improving decisions about health, wealth and happiness by Richard H. Thaler and Cass R. Sunstein.* Taylor &Francis Online.

Sverdlik, Y. (2016, April 22). *Google to Build and Lease Data Centers in Big Cloud Expansion.* Data Center Knowledge.

Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). *Deepface: Closing the gap to human-level performance in face verification*. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 1701-1708).

The Washington Post (2017, February 6), *Vizio agrees to pay $2.2 million to settle FTC's television-spying case*.

Ulanoff, L. (2017, July 25). *iRobot CEO says the company won't share your Roomba home mapping data without your OK*. Mashable.

Van Ark, B., Paradiso, J. A., & Warwick, K. (n.d.). *Our Extended Sensoria. How Humans Will Connect with the Internet of Things | OpenMind*. BBVA Openmind.

Varian, H. R. (2010). *Computer mediated transactions.* American Economic Review, 100(2), 1-10.

Vincent, J. (2017, February 17), *German Watchdog Tells Parents to Destroy Wi-Fi connected Doll over Surveillance Fears.* Verge.

Wang, J. (2017, May 23). *Google: The Full Stack AI Company At The Forefront Of Innovation.* ARK Invest.

Watson, J. B. (1913). *Psychology as the behaviorist views it.* Psychological review, 20(2), 158.

Webster, D., & Wagner, E. (1920). *Max Planck – Nobel Lecture - NobelPrize.org.* Nobel Prize.

Winner, L. (1978). *Autonomous technology: Technics-out-of-control as a theme in political thought.* MIT Press.

Winner, L. (1980). *Do artifacts have politics?*. Daedalus, 121-136.

World Unplugged, *The World Unplugged*.

Zweben, M. (March 2009), "*Life-Pattern Marketing: Intercept People in Their Daily Routines*", SeeSaw Networks.

Chapter 3

Allen, A. L. (2019). *Philosophy of Privacy and Digital Life. Anita L. Allen, Presidential Address,"The Philosophy of Privacy and Digital Life,"* 93 Proceedings of the American Philosophical Association, 21-38.

Allen, A. L., & Rothemberg, M. (2016). *Privacy Law and Society.* American Casebook Series.

Government of India (2018), *Unique Identification Authority of India*.

Hofstede, G. (n.d.). *Dimensionalizing Cultures: The Hofstede Model in Context*. ScholarWorks@GVSU.

Iustec (2019, February 1), *European Data Protection Supervisor*.

Li, Y. (2022). *Cross-Cultural Privacy Differences*. In: Knijnenburg, B.P., Page, X., Wisniewski, P., Lipford, H.R., Proferes, N., Romano, J. (eds) Modern Socio-Technical Perspectives on Privacy. Springer, Cham.

Li, Y. 2019. *Cross-cultural Differences in the Contextual Information Norms in Users' Privacy Decision-making*. UC Irvine.

Li, Y., A. Kobsa, B.P. Knijnenburg, and M.-H.C. Nguyen. (April 2017), *Cross-cultural privacy prediction*. Proceedings on Privacy Enhancing Technologies.

Liu, Y., and J. Fan. (2015), *Culturally specific privacy practices on social network sites: Privacy boundary permeability management in photo sharing by American and Chinese college-age users.* International Journal of Communication 9.

Kalven Jr, H. (1966). *Privacy in tort law- Were Warren and Brandeis wrong?*. Law & Contemp. Probs., 31, 326.

Kim, Y., D. Sohn, and S.M. Choi (2011), *Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students*. Computers in Human Behavior 27.

James, T.L., L. Wallace, M. Warkentin, B.C. Kim, and S.E. Collignon (2017), *Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use*. Information & Management 54.

Khera, R. (2017, July 19), *The Different Ways in Which Aadhaar Infringes on Privacy.* The Wire.

Načinović Braje, I., Klindžić, M., & Galetić, L. (2019). *The role of individual variable pay in a collectivistic culture society: An evaluation*. Economic research-Ekonomska istraživanja, 32(1), 1352-1372.

Nimmer, M. B. (1954), *The Right of Publicity*. Duke Law Scholarship Repository.

Panda, A. (2019, February 27). *What is 'Informational Self-Determination'? | Golden Data.* Medium.

Penn Carey Law: Legal Scholarship Repository (2016), *Protecting One's Own Privacy in a Big Data Economy*.

Post, R. C. (2000). *Three concepts of privacy*. Geo. LJ, 89, 2087.

Raj, S. (2018, November 18). *In 'Digital India,' Government Hands Out Free Phones to Win Votes*. The New York Times.

Reidenberg, J. R., Bhatia, J., Breaux, T. D., Norton, T. B. (2016, July 12). *Ambiguity in Privacy Policies and the Impact of Regulation.* 45 Journal of Legal Studies.

South Asian Translaw Database (2017) *Justice K.S. Puttaswamy vs. Union of India.*

Times of India (2018, September 6), *Supreme Court decriminalizes Section 377: All you need to know | India News.*

The New York Times (2023, May 26), *Abortion Bans Across the Country: Tracking Restrictions by State*.

Whitman, J. Q. (2004). *The two western cultures of privacy: Dignity versus liberty*. Yale Law Journal, 1151-1221.

Chapter 4

Bryan Cave Leighton Paisner (2023, May 18), *EU-U.S. Transfers: Privacy Shield replacement not adequate says European Parliament.*

Cave, B. (2023, May 19). *EU-U.S. Transfers: Privacy Shield replacement not adequate says European Parliament*. JD Supra.

Connect Humanity (n.d.), *State of Digital Inequity Report.*

Data Privacy Manager (2023, January 8), *20 biggest GDPR fines so far*.

Dempsey, M., McBride, K., & Bryson, J. J. (2021). *The Current State of AI Governance–An EU Perspective.* SocArXiv. April, 21.

European Commission (n.d.), *Europe's Digital Decade: digital targets for 2030*.

European Court of Human Rights (n.d.), *European Convention on Human Rights*.

Experian (n.d.), *What is the Safe Harbour Agreement?*.

Goldman, E. (2021). *An Introduction to California's Consumer Privacy Laws (CCPA and CPRA).* Santa Clara Univ. Legal Studies Research Paper.

OECD Legal Instruments (n.d.), *OECD Legal Instruments*.

Osano Staff (2022, December 14), *Data Privacy Laws: What You Need to Know in 2023.* Osano.

Pajunoja, L. J. (2017). *The Data Protection Directive on Police Matters 2016/680 protects privacy: The evolution of EU′ s data protection law and its compatibility with the right to privacy.* CORE UK.

Roper, W. (2020, September 8). *Chart: Internet Access Low Among Economic Vulnerable.* Statista.

Tamburri, D. A. (2020). *Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation.* Information Systems, 91, 101469.

The World Economic Forum (March 22, 2023), *Why we can't meet the SDGs without ending the digital divide*.

Weiss, M. A., & Archick, K. (January 2016). *US-EU data privacy: from safe harbor to privacy shield.* ResearchGate.

WTWH Media Marketing Lab (2018, January 13), *Full Analysis: The General Data Protection Regulation | WTWH Media Marketing Lab.*

Chapter 5

Bassett, C., & Roberts, B. (2019). *Automation now and then: automation fevers, anxieties and utopias.* New Formations, 98(98), 9-28.

Laidler, J. (2019, March 4). *Harvard professor says surveillance capitalism is undermining democracy.* Harvard Gazette.

Lindquist, J. (2018). *Illicit economies of the internet: Click farming in Indonesia and beyond.* Made in China Journal, 3(4), 88-91.

Lum, K. (2021, March 1), *Definition of an algorithm.* FlowingData.

Milmo, D. (2021, October 24). *Frances Haugen: 'I never wanted to be a whistleblower. But lives were in danger'*. The Guardian.

Scott, G. (2023, April 24). *Artificial Intelligence: What It Is and How It Is Used.* Investopedia.

Stokke, A., & Fallis, D. (2017). *Bullshitting, lying, and indifference toward truth*. Ergo-An Open Access Journal of Philosophy, 4, 277-309.

WSJ Staff (2021, July 21), *Inside TikTok Algorithm*. The Wall Street Journal.