Surveillance as Biopower: Analysing and comparing corporate surveillance narratives in the EU and the US

Chris Groot Wassink

S2926669

29/06/2025

Management Society and Technology

University of Twente

First supervisor: Ringo Ossewaarde

Second supervisor: Guus Meershoek

Word count: 11647

In this work generative artificial intelligence has been used. Please see the appendix for the disclosure statement.

ABSTRACT

This paper examines the development of the corporate surveillance discourse in both the EU and the US from 2013 to 2025. It focuses on how biopower is exercised through surveillance narratives. The analysis applies Foucauldian theory and combines this with contemporary theories of surveillance capitalism. By using case studies such as the Snowden revelations, the Cambridge Analytica scandal, and the COVID-19 pandemic, this paper demonstrates that safety and privacy are considered competing interests in both the EU and the U.S. It argues that the expansion of surveillance is legitimized through crises, and the normalization of increasingly intrusive data collection methods. Additionally, the article contrasts the European rights-based approach to privacy with the US's market-based approach to privacy. The paper concludes by discussing the dangers of surveillance and provides policy recommendations for safeguarding privacy norms.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 BACKGROUND

In 2013 Edward Snowden, an employee at the National Security Agency, leaked classified information to the newspaper "The Guardian." (Fuchs & Trottier, 2017). These leaks showed that the NSA had collected large amounts of metadata from various social media platforms such as Facebook and Google. These operations resulted from several laws implemented by the Bush and Obama administrations. These laws provided the NSA with the necessary mandate to spy on both national and foreign citizens to prevent terrorism after the 9/11 attacks in 2000. These laws led to programmes, including PRISM and Keyscore, that were aimed at gathering bulk metadata on citizens. The Snowden leaks led to a political backlash, in particular from European nations, and resulted in the "European Parliament resolution of 12 March 2014 on the US NSA surveillance programme" in which the European Parliament strongly condemned these actions.

The Snowden revelations led to an important change in the surveillance discourse in both the US and the EU. In the past, surveillance discourse was mainly centred on physical surveillance and wiretapping (Fuchs & Trottier, 2017). However, as a result of the Snowden revelations, the debate shifted to the digital domain. Additionally, this discourse changed the perception of the nature of surveillance itself, which became associated with Big Data (Wood & Wright, 2015). This shift in discourse was intensified after the Snowden revelations due to other incidents, including the Cambridge Analytica scandal. The Cambridge Analytica scandal showed that Facebook had sold personal data to third parties that exploited this data to affect the US elections. (MacAskill et al., 2013). This change of discourse will be the core of this paper and will be analysed using a Foucauldian discourse analysis, which provides a comprehensive lens through which the relation between surveillance and power can be analysed.

This paper aims to analyse the surveillance discourse from the viewpoint of biopower. Biopower refers to the coercive mechanisms through which the state regulates the lives of citizens by controlling their physical existence (Arnason, G.,2012). In this view, surveillance becomes a means to exert power by monitoring, controlling, and measuring the biological/physical sphere of human life (Foucault,1977, pp. 195-197). In capitalist liberal democracies, surveillance is exercised through a mechanism referred to by the author

Shoshana Zuboff as “surveillance capitalism” (Zuboff, 2019, p.8). Surveillance capitalism is a concept to describe a new economic model in which large tech corporations extract personal data for profit.

This paper will critically analyse the contemporary surveillance discourse, using both Foucault´s theories of biopower and Shoshanna Zuboff´s concept of surveillance capitalism. Additionally, it will explore how surveillance capitalism functions as an extension of Foucault´s concept of biopower within liberal democracies. To understand the modern version of biopower, it is important to understand the discourse surrounding its regulation. Understanding these mechanisms makes it essential to understand questions such as: who is being monitored? Who profits from this discourse? What are its historical roots? Furthermore, even more importantly, whose opinion is being ignored?

1.2 SCIENTIFIC AND SOCIAL RELEVANCE

This article aims to understand the surveillance discourse. The strength of a Foucauldian discourse analysis is that it takes into account not only the most dominant narratives, but also allows the researchers to see the underlying structure that allows him/her to access the information and to see how discourses are historically shaped (Khan & MacEachen, 2021). This allows for underrepresented voices to be better heard. This is especially important as surveillance becomes increasingly essential as a control method. This research will examine how surveillance narratives are constructed by large actors, and what this means for the subjects. Understanding the power dynamics of both regions adds depth to the analysis, which is an underdeveloped field of research.

This thesis adopts a cosmopolitan perspective, in which surveillance issues are considered global problems rather than national ones. Understanding the underlying discourse on privacy in the EU and the US is important, since European privacy regulations tend to have an international scope. Consequently, third-party entities outside EU territories are still subject to EU law according to the GDPR section 3.2 (European Council, 2016). Discrepancies in regulatory and judicial frameworks could lead to tensions between the EU and the US. As a result, various frameworks, such as the data protection framework (DPF) and the Safe Harbor Protection Shield, have sought to address such tensions. However, with the inauguration of Donald Trump, such negotiations began to falter again (Walle, 2025). This makes it more important than ever to understand the underlying power structures that shape the discourse

behind both jurisdictions, in order to better anticipate the outcomes of future negotiations between the two regions.

Gaps exist within the theoretical frameworks developed in scientific literature. Narrative analyses on how laws, policies, and debates in media legitimize surveillance for biopolitics are underexplored, particularly the role of corporate surveillance (Cheek & Cheek, 2008). Psychological effects, like self-regulation, normalization, and subjectification that lead to what Foucault calls biopower, are rarely mentioned within the literature.

This thesis explores the corporate surveillance narratives in the EU and the US as relatively new and under-researched cases. Additionally, few research has been done to bridge the theoretical gap between writers like Foucault, who explain the rationality behind discourse, and contemporary theories of the neoliberal economic logic behind surveillance, like Zuboff's theory of surveillance capitalism. Current research often focuses either on the technical aspects of surveillance, such as Andrejevic's *infoglut* (2013, pp.47-50), who focusses on the ICT infrastructure of surveillance. Or surveillance literature is aimed at large global political trends, such as Bauman and Lyon, who wrote the article *liquid surveillance* (Lyon, 2010). However, research in which the political, technical and sociological domains are synthesized into a coherent framework, are scarce.

The thesis aims to fill these gaps by analysing how the EU and US discursively frame privacy through the lens of Foucault's theory of biopower. It aims to analyse this by focusing on historical, legal, subjective, and corporate dimensions of privacy regulations. And by analysing the relationship between corporate surveillance, technology and biopower.

1.3 RESEARCH QUESTIONS

To define this problem correctly, the following research question has been developed: *How is biopower exercised through corporate surveillance narratives in EU and US privacy discourses?*

This research question aims to describe the relationship between corporate surveillance and bio-governance clearly. It will look at this from a Foucauldian perspective. Therefore, the analysis tends to focus on surveillance from a highly constructivist perspective. The research paper defines surveillance and privacy as historical, cultural, and social constructs in which power is the most important denominator. To comprehensively and constructively answer this research question, a couple of sub-questions have been developed:

1. How has the corporate surveillance narrative in the EU and the US developed since the Snowden revelations in 2013?

2. What are the key similarities and differences in corporate surveillance narratives between the EU and the US?

3. How do these differences reflect the exercise of biopower in both contexts?

These sub-questions are mainly interpretative and are designed to inform the broader analysis. The first sub-question sets the historical context with a starting point in 2013, during which the Snowden revelations occurred. The reason for choosing this time frame is twofold: Firstly, this period marks key developments that significantly shaped the digital surveillance discourse (Fuchs & Trottier, 2017). Examples include the Cambridge Analytica scandal and the introduction of the GDPR. Secondly, digital platforms only started to rise in the early 2000s, and decisive narratives around corporate surveillance only gained prominence after the pivotal events like the Snowden leaks (Fuchs & Trottier, 2017). The paper will trace the discourse to its starting point of 2013 and follow it until 2025. Therefore, it conducts what Foucault calls a `genealogical tracing´ of discourse. It aims to get to the very origins of the discourse. Finally, the third sub-question combines both aspects and seeks to interpret the information through the lens of biopower.

2. THEORY

2.1 INTRODUCTION

This chapter aims to clarify the relationship between biopower and surveillance capitalism by combining the theoretical underpinnings of both concepts. It provides a foundational framework in which biopower and surveillance capitalism are connected.

To answer the question of how biopower is exercised through corporate surveillance discourse, this chapter develops a framework consisting of three elements. First, the economic logic behind surveillance. Next, the political normalization of surveillance. And finally, the legitimization of surveillance through crises. These elements interact with each other, creating a positive feedback loop where surveillance capitalism forms the economic incentive structure for surveillance, which is then embedded in discourse through biopolitics and is expanded through crises. Together, these theories will establish an interpretative lens for further inquiry into the subject of biopower is exercised through corporate surveillance narratives.

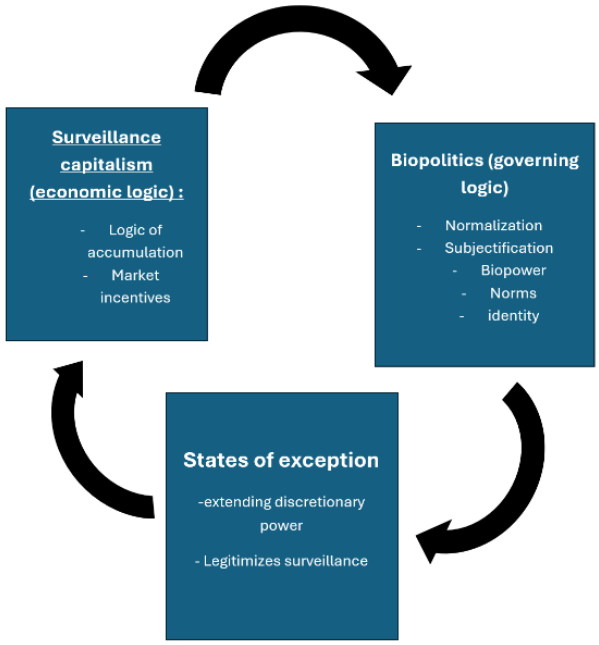

Figure 1: The positive feedback loop of surveillance capitalism

2.2 THE CONCEPT OF SURVEILLANCE CAPITALISM

This section argues that surveillance is no longer primarily exercised through nation states and explores how surveillance capitalism extends the neoliberal paradigm. This section describes how capitalism places knowledge production at the centre of the economic system and rebrands personal data as a commodified resource for economic growth. This shift provides a new way of data collection. Additionally, this section will discuss the underlying mechanisms

of surveillance as a new means of knowledge production, and how it relates to modern interpretations of Foucault's panopticon.

Knowledge and surveillance play crucial roles in exercising biopower. To implement this knowledge and data-gathering process, a new type of economic logic has emerged within liberal democracies. This can best be described using Shoshanna Zuboff's concept of surveillance capitalism. Surveillance capitalism refers to a new neoliberal system in which Big Tech corporations have reshaped the economic order and have made surveillance their primary focus (Zuboff, 2019).

Contrasting industrial capitalism, where economic value is primarily created through labour and production, surveillance capitalism relies primarily on what Zuboff calls the "behavioural surplus" (Zuboff, 2019, pp. 319). This surplus consists of streams of personal data collected beyond what is necessary to keep the digital platform functioning. While a search engine may gather only the data necessary to give relevant recommendations, new tech companies collect extensive personal data, including social connections and scrolling speed on websites. (Leclercq-Vandelannoitte & Bertin, 2024). This data is sold on "behavioural futures markets", where predictive models of customer behaviour are traded. These models can accurately predict future consumer behaviour and can manipulate consumer actions. This leads to the core principle of surveillance capitalism referred to as "the logic of accumulation" (Zuboff, 2019 , pp.63-68). Data collection creates an incentive for more data collection, leading to a positive feedback loop. Richer datasets result in better products sold on a `behavioural future market´ for greater profit. This cycle generates more capital for the investment in increasingly more data collection. It is important to mention that the gathering of data does not happen through coercive means, but rather is subliminally embedded in the digital architecture of social media platforms (Zuboff, 2019). By interacting with the platform, the subject (unknowingly) decides to provide the corporation with their data.

To understand surveillance capitalism from a historical perspective, a literary device can be used by Foucault, known as the "panopticon" (Leclercq-Vandelannoitte & Bertin, 2024). The original author of this idea is Bentham, who describes a circular prison with transparent cells that allow for constant observation of the prisoners. However, the prisoners could not see when the security guards were watching them. This creates uncertainty regarding the frequency of surveillance. As a result, prisoners learn to self-regulate their behaviour as they must always behave as if they were being watched (Foucault,1977, pp. 195-197).

Surveillance within Western societies mirrors this panoptic model, as individuals are often unaware of when intelligence agencies are monitoring them. While the form of surveillance remains the same, the methods are highly influenced by technological developments (Leclercq-Vandelannoitte & Bertin, 2024). Therefore, panoptic surveillance can still be divided into three distinct historical stages based on the technologies that facilitate it.

The first stage is physical panoptic surveillance. This refers to physical surveillance focused on the body, through disciplinary mechanisms mainly enforced in physical spaces such as hospitals, schools, and prisons. The second stage is the post-panoptic stage, where surveillance's digital and physical spaces overlap. The final stage is contemporary surveillance, which is entirely digital and cannot be shut off by the consumer. It aims to build a complete and comprehensive "avatar" of one's identity in which absence can be considered a part of the profile. (Leclercq-Vandelannoitte & Bertin, 2024)

In the final stage, identity becomes entirely digitalized and measurable. Shoshana Zuboff's description of surveillance capitalism matches this last stage of the panopticon. It is characterised by the consumer's inability to shut down surveillance. The surveillance network is therefore always present and always manipulates the behaviour of consumers. Zuboff describes this level of surveillance as the "Big Other"(Zuboff, 2019, pp. 376–382).

In conclusion, surveillance capitalism presents the latest stage in the development of panoptic surveillance. Transitioning from physical to inescapable digital surveillance creates a society where individuals can be controlled through biopower. By embedding surveillance in the economic system, market incentives have been created to intrude on individual privacy.

2.3 THE CONCEPT OF BIOPOWER

Surveillance capitalism explains how surveillance is driven by neoliberal market rationality. However, it does not explain how such practices become integrated into the lives of individuals and in public discourse. Michel Foucault's concept of biopower offers a comprehensive framework for understanding how modern power works through repressing individuals and constructing identities and norms. Unlike traditional power, biopower is deeply connected to knowledge production. This knowledge production is embedded in surveillance discourse and is critical in constructing truth. This section explores biopower and its primary mechanisms, such as norm-setting and knowledge production.

Biopower refers to the exercise of power over human life and populations. According to Foucault, biopower started in the early modern states of the 17th and 18th centuries, when early states started to gather medical information from hospitals (Foucault, 2003, p. 243). Unlike the hierarchical top-down power relations in early sovereign statehood, biopower is distinguished by its creative and productive dimension (Foucault, 1990, p. 136). An important aspect of this creativity is the close relationship between knowledge and power. Knowledge shapes and is shaped by power, though the two remain distinct (Arnason, 2012).

As conceptualized by Foucault, biopower has two distinct dimensions: antonomo-politics, which exerts disciplinary power over the individual, and biopolitics, which regulates entire populations. Biopolitics involves controlling statistics such as birth rates, reproduction, and mortality (Foucault, 1976, pp.139-140). Therefore, biopolitics requires a vast surveillance apparatus to collect sufficient data for effective policy making. By embedding this knowledge into discourse, power legitimizes itself by making certain social realities visible, controllable, and manipulable (Foucault, 1995, pp. 220–228).

Governments make social realities visible and measurable through a process called *normalization.* Normalization starts with positioning a model of how a citizen *ought to be,* determined by statistical averages within the population (Foucault, 1990, pp. 144-145). This model sets a specific *norm* or standard to measure an individual. Those who deviate from the norm are subjected to disciplinary correction to bring them in line. In this definition, we can find that normalization not only restricts behaviour but also constructs correct behaviour. It not only represses abnormalities but actively constructs *norms* and enforces such norms (Foucault, 2003, pp. 38-39). Contrasting sovereign statehood, normalizing strategies are especially effective in managing people and allow new exploitation methods. Normalizing techniques are strongly tied to surveillance, for if they are not monitored, norms cannot be maintained, and abnormalities cannot be successfully detected (Lawlor, L., & Nale,2014).

In conclusion, biopower, as conceptualized by Foucault, provides a valuable lens through which to understand how power operates in society. Foucault explores how power moves from the individual level to the collective, influencing individuals through embedding knowledge in discourse.

2.4 THE BIOPOLITICS OF SURVEILLANCE CAPITALISM

Building upon the early discussion of biopower and its role in regulating the population, this section explores the role of knowledge in this process, particularly through discourse.

Governments use discourse as a tool to shape categories by which individuals are understood and understand themselves. This process, known as subjectification, is important in how power operates in society. Additionally, this section will discuss how governments use crisis narratives to expand their surveillance capabilities.

Surveillance is a key instrument of biopower due to its intrinsic link to the construction of truth through discourse. Foucault argues that truth is not a self-evident concept, but is constructed within the context in which knowledge is applied (Powell, 2024). Consequently, knowledge is not the result of individual enquiry, but rather a social practice that actively constructs the world. Therefore, knowledge becomes strongly related to the exercise of power in discourse and influences how individuals are categorized and how they see themselves. (Powell, 2024, pp.30).

To maintain safety and social order, states use a set of practices that Foucault refers to as *governmentality.* This set of practices creates frameworks for understanding and categorizing individuals to develop fitting policies. Central to this process is *subjectification* (Anarson, 2012). Subjectification takes place on two levels. First, individuals identify themselves with a certain category constructed within discourse. Foucault refers to this mechanism as *self-subjectification* (Powell, 2024, pp. 29). Citizens conform to social roles by recognizing themselves in them. Secondly, subjectification is driven by the dominant discourse's epistemological assumptions referred to by Foucault as “epistemes”. These assumptions, or epistemes, determine the categories and limitations in which individuals can be understood by others and understand themselves (Powell, 2024).

When it comes to the processes of subjectification and knowledge gathering, liberal democracies have two conflicting goals. This tension is best described using Agamben’s theory of crises. Agamben, similarly to Foucault, argues that surveillance results from governments wanting to protect their citizens against harms such as pandemics, wars, and terrorist attacks (McLoughlin, 2012). Therefore, governments are incentivised to gather as much knowledge as possible from their population through the market-driven mechanisms of surveillance capitalism, as described previously. On the other hand, liberal democracies also want to grant their citizens human rights such as privacy and freedom. To alleviate these tensions, policy documents often include passages for specific crises in which an intrusion on human rights can be made only temporarily. The philosopher Giorgio Agamben defines crises in which executive discretionary powers are extended as `states of exception´ (McLoughlin, 2012). During these exceptional states, laws and clauses allow governments to gather data

beyond the scope possible under normal circumstances. Consequently, administrations are incentivized to call out a crisis when this is unnecessary (Peters, 2014). However, the primary goal of such a crisis is not only to solve an immediate crisis, as governments tend to gather information about citizens beyond what is necessary to solve the problem. However, this data is often used to improve the effectiveness of bio governance.

This normalization of exception creates a paradox; what was once seen as a state of exception becomes part of everyday life, eroding the line between surveillance and normal government operations. As the state continually justifies expanded surveillance measures, the balance between security and privacy will shift towards favouring security (McLoughlin, 2012) . The long-term consequences are the erosion of citizens' fundamental right to privacy.

Conclusively, the interaction between biopower and Agamben's concept of 'states of exception" reveals tensions within governments where safety and surveillance are conflicting interests. By leveraging these crises, governments tend to normalize surveillance that was not previously considered acceptable. Additionally, surveillance functions as a critical tool in shaping discourse. It shapes both individual and collective truths by imposing individuals to normative standards. Surveillance helps reinforcing normative standards that reinforce power structures that govern personal identities and maintain social order.

2.5 CONCLUSION

In contemporary societies, power operates through complex control mechanisms rather than top-down hierarchical systems. Power that controls and regulates the population and the individual through knowledge and discourse is conceptualized by Foucault as biopower. Central to this concept is the relationship between knowledge and power, particularly through surveillance (Arnason, 2012). Surveillance becomes a tool for regulating behaviour. This regulatory function of knowledge is embedded in the neoliberal paradigm of the 21st century and led to what Shoshanna Zuboff calls surveillance capitalism. This concept highlights how Big Tech corporations have reshaped the economic order and have put knowledge gathering at the core of the economic logic of accumulation. This logic is aimed at collecting behavioural surpluses, a type of personal data gathered beyond what is necessary to keep the platform running (Zuboff, 2019).

However, the implementation of biopower causes a significant problem in modern liberal democracies. On the one hand, liberal democracies seek to protect their citizens against harm, aligning with Foucault's biopower concept. On the other hand, these same democracies are

committed to protecting individual freedoms such as privacy. Governments expand their discretionary powers to omit this tension during what Agamben calls “states of exception.” (McLoughlin, 2012). Where governments extend their discretionary powers during crises to ensure national security, the issue arises when these discretionary powers are unnecessary but become normalised. This blurs the line between exceptional situations and normal governmental operations. This could lead to increasingly more intrusive surveillance measures.

Conclusively, the interaction between biopower, surveillance capitalism, and states of exception causes a fundamental conflict between the state’s need for control and its incentive to protect citizens from surveillance and intrusion.

3. METHODOLOGY

3.1 INTRODUCTION

This chapter outlines the methodological approach to analyse the research question: *How is biopower exercised through corporate surveillance narratives in EU and US privacy discourses?*

The first section focuses on case selection, including the Snowden revelations, the Cambridge Analytica scandal, the COVID-19 pandemic, and contemporary policy documents on privacy and surveillance, including the GDPR and the California Consumer Privacy Act. The second section discusses the data collection method, including the criteria for selecting policy documents, media reports, and legislation. Finally, the method of analysis is examined, emphasizing using a Foucauldian discourse analysis to develop a coherent coding scheme based on the theoretical framework. This section aims to deliver a comprehensive understanding of the relationship between corporate surveillance and biopower. Additionally, it will describe tools such as ATLAS.TIs that are being used for conducting analysis.

3.2 CASE DESCRIPTION

To conduct a clear discursive analysis of the issue of surveillance a number of cases have been selected to provide insight into how the surveillance narratives have developed over the

last 10 years. This chapter aims to provide a clear overview of the discourse and capture its contemporary context.

The discourse discovers how surveillance is constructed by both the European Union and the U.S. government, with a strong emphasis on corporate surveillance. It examines how this discourse frames subjects and how governments legitimize surveillance. The evolving framings of this discourse revolve around a long-standing debate about privacy versus security, which is hundreds of years old. However, what distinguishes the contemporary surveillance discourse is the nature of the surveillance methods employed. What differentiates surveillance in the age of "surveillance capitalism" is its scope and strong emphasis on digital data.

The data-oriented surveillance discourse began in 2013, after the Snowden revelations were released. This research will trace the discourse until 2020, when the COVID-19 pandemic resulted in a wide range of surveillance measures (Fuchs & Trottier, 2017). In this context, *discourse* refers to a set of meanings, representations, and frames through which the debate on corporate surveillance is constructed (Khan, T. H., & MacEachen 2021). Key elements of framing discourse include threats, security measures, and the framing of victims and risk carriers. This discourse is manifested through various materials, including news articles, policy documents, laws, interview transcripts, and official statements from important leaders. Furthermore, this research will focus on defining the roles of corporate actors, corporate-public relations, and the impact of technology, including how these relations have evolved.

The three cases will be analysed to trace how this discourse materializes. The first case involving Snowden gives a clear overview of how the surveillance discourse developed into a data-oriented surveillance discourse aimed at threat mitigation. The Snowden revelations are particularly insightful, as many original reports are easily accessible from security agencies, such as the NSA, which are publicly available, including interviews with key NSA leaders.

The second case is the Cambridge Analytica scandal, which complements the Snowden Revelations. This case displays how corporate actors use personal data, not only for financial gain but also for political influence, therefore extending their reach into the democratic sphere of society. The case demonstrates how Big Tech corporations like Google abuse personal data to shape public discourse and opinion. An additional analytical advantage of both cases is that the documents were leaked rather than officially released, meaning they were not subjected to institutional framing or modification.

Finally, the COVID-19 case reveals how the nature of collected data and the level of government intervention significantly changed due to a global pandemic. This case illustrates how a universal threat is constructed, namely the possibility of that person being infected, instead of the surveillance efforts directed at particular target groups or individuals. Finally, several policy documents and responses will be analysed. Such as the GDPR and the CCPA, to understand how government officials frame corporate surveillance and security to exert biopower.

Together, this examination of multiple cases allows for a genealogical tracing of the surveillance discourse and considers numerous actors. It illustrates how discourse has evolved from a post-9/11 security-based discourse into a broader strategy for governing through data.

3.3 METHOD OF DATA COLLECTION

The data was collected using a targeted document selection process, based on keyword searches across public online websites and platforms. This method was selected as it allowed for a broad range of texts while maintaining thematic coherence. Given the nature of the research question, this method was best suited. The keywords as displayed in Appendix A were used to answer the following questions: Who are the important actors? (see keywords: “Snowden”, “Cambridge Analytica”). What practices do they legitimize? (see keywords: “mass surveillance”, “metadata collection”). And finally, how do they impose such actions through official discourse? (see keywords: “GDPR”, “CCPA”). Additionally, the sources were selected based on specific inclusion criteria, including: language (English), publication date (2013-2024), and accessibility (open-access). This process is displayed in figure 2 below.

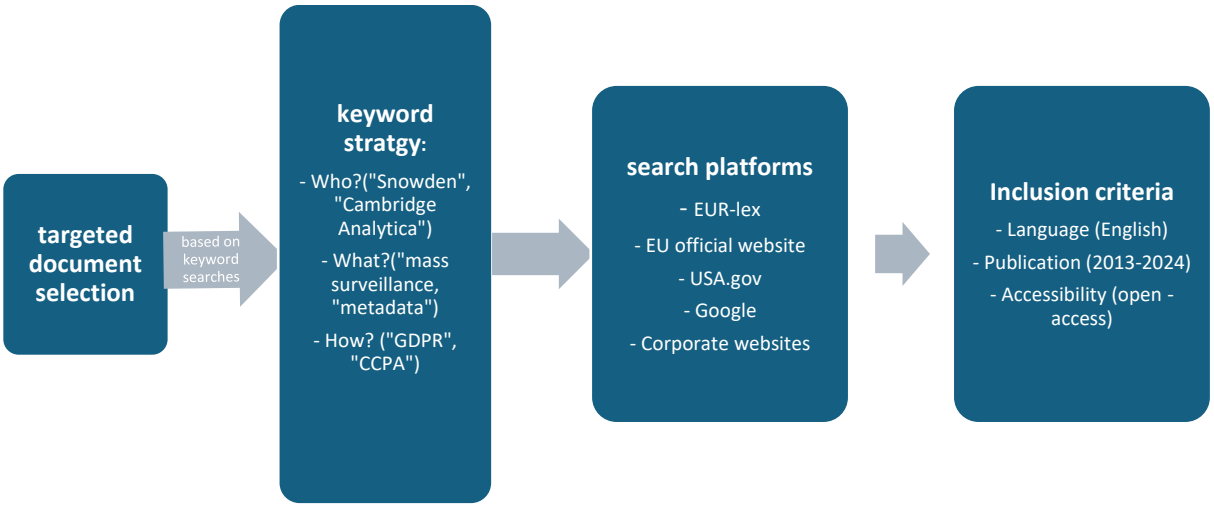

Figure 2: Overview of the data gathering process

The data collection method involves analysing both primary and secondary sources. The secondary sources will primarily include news coverage related to the Cambridge Analytica scandal and the Snowden revelations. The data was gathered using search terms on various websites, including EUR-lex, the official European Union website, Google, the website of the Federal Trade Commission, and the USA.gov website for finding relevant sources of information. The news sources were selected, including European and U.S. news outlets with an equal distribution of right and left-winged news. This was done to avoid bias as much as possible.

The research on the Snowden revelations gathered a total of fifteen sources. These sources can be categorized into three categories. Firstly, ten news articles on the Snowden leaks and their relation to the NSA were selected. Secondly, the transcripts of interviews from important actors during the scandal, including Richard Ledgett, Edward Snowden, and Barack Obama were chosen. These have been included to get a good overview of the framing of the NSA and the president within the public debate. Additionally, responses from the European Union have been analysed, including one document concerning the EU's response to the Snowden revelations.

Concerning the Cambridge Analytica scandal, nine sources were collected, including pivotal news articles from both the Guardian and the BBC. Additionally, interviews with Mark Zuckerberg (head of Facebook) and the whistleblower, as well as the formal response of the European parliament, were collected. These documents are used to disclose how large corporations justify their surveillance efforts to the public and give an overview of the various activities that were undertaken to undermine the U.S. elections.

Eleven news articles from a plurality of news sources were analysed for the analysis of the COVID-19 pandemic. Furthermore, the official website of Palantir has been analysed as it played a prominent role in the data gathering process during the pandemic.

Several documents have been selected for the analysis of official policy documents. Using the official platforms of both jurisdictions. These documents are the key legal documents responsible for building a normative framework for privacy and surveillance in both legal contexts. These include documents such as the GDPR, the European Convention on Human Rights, the EDPB guidelines, and the CCPA. These documents have been selected as they are key documents responsible for shaping the legal categories and the legislative framework through which subjects within the surveillance discourse have been framed.

The selected documents aim to show both the progression of the privacy debate and uncover the legal framework responsible for creating effective norms for regulation. They also provide a framework under which privacy rights have been ignored by authorities under certain circumstances.

3.4 METHOD OF DATA ANALYSIS

This paper will conduct a Foucauldian discourse analysis. This qualitative method will analyse various texts, such as transcripts, newspapers, leaked documents from security agencies, and legal documents. This type of analysis will be primarily qualitative and focused on uncovering relevant dimensions of surveillance within Western discourse.

FDA's fundamental assumptions are rooted in social constructivism. This argues against objective truth outside of the realm of subjective experience . This feature of the analysis method makes it highly suitable for conducting a discourse analysis on surveillance and biopower, as it considers power a primary source of knowledge creation (Khan, T. H., & MacEachen 2021) . Therefore, important questions within Foucauldian discourse analysis concern the construction of subjects. This will be a core element of the analysis. It seeks to answer questions such as: how are subjects categorized within discourse, and what can or cannot be said within surveillance discourse? Who benefits from this discourse?

Discourse, according to Foucauldian thought, is not merely a reflection of a static social reality but actively shapes and produces it. Discourse produces knowledge, and through knowledge it exerts power. By tracing how surveillance is framed over time, the analysis explores how these discourses enable or constrain citizens and consumers regarding their subjectivity. It also shows how governments are restricted or allowed to intrude on individual rights.

Due to the contemporary nature of discourse and its non-structural assumptions, Foucauldian discourse analysis does not aim to be generalizable, but rather precise and context-dependent. The analysis will focus on framings of both corporate and governmental actors. It does this by tracing the discourse back to several key events and documents such as the Snowden revelations, the Cambridge Analytica scandal, and some key legislation, effectively leading to the construction of a genealogy of the discourse from 2013 until 2025. This analysis aims to uncover patterns, structures, and frames relevant to the EU and US surveillance discourse.

The discourse analysis will be essentially deductive, starting with a coding scheme based on the theory described in the previous chapter. Table 1 aims to define the coding categories as clearly as possible by applying Foucault's theory of biopower, Zuboff's theory of surveillance capitalism, and Agamben's theory of states of exception; this will provide a coherent conceptualization of the codes. This coding scheme will be operationalized using Atlas. Ti. This tool allows for a practical analysis of large bodies of data.

The codes are derived from the theory and reflect the distinct elements of the theoretical framework. For instance, some of the codes are based on Foucault´s concept of subjectification. The section *normalization* is integrated to expand on Foucault's mechanisms of biopower. Similarly, categories such as *innovation discourse* draw on the same neoliberal logic described by Zuboff.

For an exact overview of the theories in relation to their corresponding code, see figure 3.

Theory	Corresponding category	codes
Subjectification (Foucault's theory of biopolitics)	Subject	Risk carrier, vulnerable
Surveillance capitalism	subject	Consumer, data subject
Agamben's theory of crises & Foucault's theory of biopower	Governance rationality	Health treat, psychological threat, social order
Surveillance capitalism	Governance rationality	Consent and compliance, innovation discourse
Governance privacy rationality	Governance privacy rationality	Democratic deliberation, autonomy, privacy as fundamental human right, transparency and harmonization.
Foucault's theory of knowledge production	Type of data gathering	Behavioural data, biometric data, non digital data, social media, geolocation, health data, geographic data
Surveillance capitalism/Agamben's theory of crisis situations	Corporate-state entanglement	Public/private collaboration, crisis collaboration
Foucault's theory of biopower	normalization	Moral normalization, productivity, behaviour optimization, health

Figure 3: codes and their corresponding theories

3.5 CONCLUSION

In conclusion, the methodology employed in this research is based on a combined theoretical framework in which the theories of Foucault, Agamben, and Zuboff are integrated. By applying a Foucauldian discourse analysis, this study ensures that discourse is analysed not only for its meaning but also for its underlying power structure. By using deductive coding grounded in the theoretical framework, the research aims to ensure that it captures all the important theoretical elements of the framework.

Focusing on key cases such as the Snowden Revelations, the Cambridge Analytica scandal, and the COVID-19 pandemic, this research aims to facilitate a genealogical tracing of the surveillance discourse from 2013 until 2020. It clearly explains how state and corporate actors influence this debate to exercise biopower.

Coding scheme 1

category	subcategory	description	Key words
Subject	consumer	Individual positioned as data source and buyer	User, customer, account holder
	Data subject	Legal holder of individual identity under privacy law	Data subject
	Risk carrier	An individual who poses a risk to society and needs monitoring and/or prediction	Disinformation, terrorist, contagious, spy, foreign soldier, criminal
	Vulnerable	Framed as needing protection or correction	Minor, addict, radicalized, unhealthy, isolated, elderly, low-literacy, poor
Governance rationality surveillance	Health threat	Framed as justifying data collection in case of a crisis (e.g., pandemic)	Virus, immunity, exposure, contagious
	Psychological threat	Framed as causing harm to mental health or mental well-being	Graphic content, addiction, radicalization, isolation,
	Social order	Framed as required for maintaining social order	Terrorism, war, disinformation, spying, spy
	Innovation discourse	Surveillance legitimized by reference to progress	Innovation, UX, frictionless, economic growth, mass personalization
	Consent and compliance	Surveillance justified through procedural consent	Consent, privacy policy, opt-in, privacy agreement
Governance privacy rationality	Democratic deliberation	Privacy as a means for democratic deliberation	Polarization, echo chamber, targeting,
	autonomy	Subject requires meaningful control over data and/or choices	Nudging, addiction, manipulated, filtered, dark patterns, consent, autonomy
	Privacy is a fundamental human right.	Privacy is framed as a fundamental human right	Rights, privacy rights, human rights, UCHR
	Surveillance as a threat to mental health	The subject gets severe harm as a result of surveillance	Chilling effects, addiction, dark patterns, algorithms, panopticism

	Transparency and harmonization	Privacy is described as necessary for the harmonization of bureaucratic processes.	Transparency, cross-border harmonization,
Type of data gathering	Behavioural data	Monitoring clicks, app usage, language,	User behaviour, activity, footprint,
	Biometric data collection	Gathering data from the body	Face scan, biometric, fingerprint, iris scanner
	Data from non-digital communication platforms	Gathering data from communication technologies that are not digitized yet.	Telephone, fax, post, camera, handwriting,
	Social media	Gathering data from open-source platforms	Social media, posts, comments, and account
	Geolocation tracking	Use of GPS, Bluetooth, or Wifi to trace physical movement	GPS, location history, proximity data,
	Health data	Gathering data about the subject's health	Fitness tracking, heartbeat, symptom tracking, wearable data
	Geographic data		
Corporate-state entanglement	Public/private collaboration	State turns to a private entity for data intervention	Collaboration, data sharing, partnership
	Crisis collaboration	State turns to a private entity for crisis intervention	Data sharing, crisis collaboration, and temporary partnership,
Normalization	Moral normalization	Influencing citizens' moral stances, setting moral norms	Responsibility, trustworthiness, good citizenship, healthy behaviour, and family relationships
	productivity	Construction of an ideal work/life balance	Productivity, balance, efficiency, health
	Behaviour optimization	Nudging citizens towards desired behaviour	Engagement, recommendation, optimization, and collaboration
	health	Nudging citizens towards the ideal health standard	Health, BMI, cleanliness, balanced,

4. ANALYSIS

4.1 INTRODUCTION

This chapter analyses how surveillance practices in the transatlantic region were discursively legitimized and constructed between 2013 and 2025. It argues that what began as a response to terrorist threats has turned into a normalized means of state control. It argues that the EU and the US are stuck between two conflicting interests; they must protect their citizens against harms such as terrorist attacks, pandemics, and wars, which require surveillance, while simultaneously both nations should ensure freedom and privacy. The acceptability and expansion of the surveillance apparatus in both areas have been made possible through several legitimizing frames favouring safety over privacy.

To understand how surveillance measures have been extended and normalized, the empirical findings from discourse analysis have been organized into three chapters describing how discourse shifted across three dimensions. Firstly, this chapter will discuss how the normalization of increasingly more intrusive surveillance measures was legitimized in discourse. Secondly, this discourse increasingly led to indiscriminate means of data collection. Finally, corporate actors have become increasingly more important in the surveillance debate; these changes are not only empirical developments but also embedded in discourse by powerful actors. Additionally, this chapter will demonstrate that frames of safety, autonomy, and human rights have been used as instrumental to legitimizing corporate surveillance.

4.2 JUSTIFYING SURVEILLANCE

Building from the introductory chapter, this section delves deeper into the initial phase of normalization after the Snowden revelations in 2013 and the state-legitimization of increasingly non-discriminatory measures. Starting from the NSA's targeting of terrorism, to the COVID-19 gathering surveillance of the entire population. This section argues that the frames of governmental agencies are increasingly less targeted, and allow for a larger part of the population to be subjected to surveillance.

The Snowden revelations were a pivotal event in shaping the surveillance discourse as it disclosed the methods intelligence agencies used to gather large amounts of data from the population. In response to terrorist threats, the U.S. established several surveillance programmes such as PRISM and Keyscore (MacAskill et al., 2014). The Snowden revelations led to public outrage towards the United States government, which led to the U.S. government developing a framing method to legitimize its operations. The National Security Agency

(NSA) framed its operations as necessary for public safety and adopted a metaphor of "finding a needle in a haystack" (Ledgett, n.d.). Surprisingly, despite the intense public outrage about these programmes, government officials reframed surveillance as necessary for national security. Illustrative of this is Obama's remark on the surveillance programme during a press conference. He remarked:

> Well, the fact that I said that the programs are operating in a way that prevents abuse, that continues to be true, without the reforms. The question is, how do I make the American people more comfortable? If I tell Michelle that I did the dishes — now, granted, in the White House I don't do the dishes that much — (laughter) — but back in the day — and she's a little sceptical, well, I'd like her to trust me, but maybe I need to bring her back and show her the dishes and not just have her take my word for it. (*Remarks by the President Obama in a Press Conference*, 2013)

This response from the president was not an appeal to legality, but rather a paternalistic response to surveillance concerns. The president further framed surveillance not as a matter of human rights, but rather as a matter of institutional trust. It reveals surveillance as a power that operates in a Foucauldian way. It becomes a form of biopolitics in which the individual has to be protected from an external threat. Therefore, the subject is no longer primarily perceived as a rights-bearing citizen, but rather as a statistical datapoint who has to be managed by a dependable, rational government. The war on terror, from which the surveillance programmes developed through legislation such as the Patriot Act and the Terrorism Act, was a means for expanding surveillance without facing strong resistance from privacy advocates. Here, Agamben's concept of the state of exception becomes important. The U.S. justification of mass surveillance reflects the suspension of standard legal protections. The war on terror and its surveillance programmes extended surveillance capacities, which were not retracted for a decade after the 9/11 crisis in 2002.

The European Union's response offered a contrasting paradigm in which privacy as a human right was central. In its 2014 resolution, the European Parliament adopted a critical stance on the NSA programmes that initiated the mass-surveillance of European citizens. The resolution provided "compelling evidence of the existence of far-reaching, highly technologically advanced systems" that were misused for blanket mass surveillance (Official Journal of the European Union, 2014). This was articulated in the following statement:

> Members considered that recent revelations in the press by whistleblowers and journalists, together with the expert evidence given during this inquiry, admissions by authorities, and the insufficient response to these allegations, have resulted in compelling evidence of the designed by US and some Member States' intelligence existence of far-reaching, complex and highly technologically advanced systems services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner
>
> (Official Journal of the European Union, 2014)

Nonetheless, even the EU´s rights-based approach to privacy proved to be vulnerable to crises. In the EU, the privacy discourse normalized and increased the acceptability of surveillance during the COVID-19 pandemic. This reflected a paradigm shift in Europe in which subjects were not only traced if considered a specific threat, but rather, all citizens became possible threats. Risk was not restricted to merely being a terrorist or criminal. The citizen became a risk carrier by default. The EU's human rights discourse can, like the U.S. discourse, prioritise safety over privacy. Governments justified intensive tracking, which was framed as solidarity in relation to public health. In official discourse, the EU prioritized Article 2 of the ECHR over Article 8 of the ECHR. (ECHR, 1950, Art. 8)

In conclusion, the U.S. showed during the Snowden revelations that it adopted a paternalistic, trust-based legitimization of its surveillance programmes. Despite backlash from the public, the U.S. refused to withdraw its surveillance efforts. The EU responded strongly to U.S. surveillance, but it has itself been vulnerable to crises as a means of extending surveillance. However, it differs from the U.S. as the EU tends to adopt a human-rights approach.

4.3 FROM METADATA TO BIOMETRIC DATA

The justification for targeted data collection against specific threats has progressively developed into a pervasive and indiscriminate surveillance discourse. This development shows the legitimization of a quantitative increase in surveillance data and describes a change in the data type permissible for collection. Additionally, it exposes that the scope of the number of permissible subjects under surveillance has been widened. This paragraph discusses two changes in the surveillance discourse due to the previously mentioned

surveillance rationality. Firstly, the broadened scope of which subjects should be monitored. Secondly, the enhanced intrusiveness of surveillance is normalized in discourse.

In the aftermath of Snowden, the public discourse centred on “metadata”, information about communications. It, for instance, follows who has called whom, and how long the call took. This means the data did not disclose highly personal data about the subjects. The justification for this data gathering was framed through the “needle in a haystack” metaphor, which means that the NSA would only follow citizens who would make suspicious communications. Additionally, the “if you have nothing to hide, you have nothing to fear” frame was adopted . The NSA director pointed out that the data protected U.S. citizens while “simultaneously protecting their right to privacy” Ledgett, R. (2014.). The expansion of surveillance for purposes originally framed as necessary for protecting citizens, particularly after 9/11 raises high concerns among critics about civil liberties. Surveillance powers designed to prevent terrorists have been extended over time in the pursuit of unrelated crimes. Critics refer to this development as a “surveillance creep” and that the pandemic is a “catalysation moment” for increasingly more surveillance (Giglio, 2020). They argue that crises could be an excuse to expand already highly intrusive surveillance measures, mirroring the theory of Agamben.

However, the Cambridge Analytica scandal fundamentally changed this narrative. The case showed an increasing intrusiveness by collecting and exploiting what is called psychometric and behavioural data. Data was not about identifying potential threats but aimed at predicting their political opinions. In this discourse, the ´needle` in the haystack was no longer a terrorist but an individual who could be exploited for political power.

Subjects in discourse became significantly less specific, and corporations like Cambridge Analytica and Palantir started advertising with influence on specific `target groups´. This intrusion's peak occurred during COVID-19, when the entire population became subject to highly intrusive surveillance measures. The discourse shifted from targeting specific threats to framing every individual as a potential risk. This resembles Foucault's concept of population management through surveillance as knowledge production (Powell, 2024). Additionally, the data became increasingly more intrusive, ranging from metadata to behavioural and biometric data. The data seems to increasingly overstep the physical boundaries of the mind and body and try to regulate, as Foucault puts it, `bare life´ of the individual.

In conclusion, the evolution of surveillance after Snowden demonstrates a shift from targeted monitoring, to broad indiscriminate surveillance of entire populations. Initially this was

justified by collecting metadata to trace terrorist. Later, surveillance practices expanded to include psychometric and behavioural data, as can be seen in the Cambridge Analytica scandal. This shift exemplifies Foucault's concept of population management through surveillance as a form of knowledge production. The goal of the government switched to regulation of the entire population rather than specific threats.

4.4 NEOLIBERAL RATIONALITY IN THE SURVEILLANCE DISCOURSE

Building on the surveillance increasing intrusiveness and its state legitimizations, this chapter shifts focus to a parallel development. This development is the increasing importance of corporate actors in normalizing surveillance. From 2013 to 2025, a reframing of corporate entities took place within the surveillance discourse. Corporate actors were first perceived as passive victims but became active participants in state surveillance over time. This evolution is central for understanding surveillance as an embedded feature of digital life and can best be described by what Shoshanna Zuboff terms `surveillance capitalism` (Zuboff, 2019).

Shortly after the Snowden Revelations, the framing of social media corporations that provided metadata to the NSA was relatively positive. Rather than blaming these social media platforms, news outlets framed them as victims. These platforms were often depicted as being in a `tough position´ due to government intrusion. Moreover, critics of the PRISM programme mentioned that the government intentionally misled these corporations. However, the Snowden revelations exposed the link between markets and surveillance for the first time. This is marked by a statement by the NSA director who argued that the Snowden revelations led to an unfair marketing advantage. In this interview, he argued that other nations unfairly used the Snowden revelations to promote their social-media platforms over American-owned ones (Ledgett, R. 2014.).

The Cambridge Analytica scandal changed the victimhood perspective on social media companies. This was a strange abnormality, as the U.S. government and media outlets did not target the Trump administration as the main perpetrator. A particularly uncomfortable fragment shows that the responsibility for protecting privacy is now placed on the social media platform Facebook instead of governments themselves, as can be read from the following interaction displayed in the Guardian between senator Dick Durbin and Facebook CEO Mark Zuckerberg;

- Dick Durbin: "Would you be comfortable sharing with us the name of the hotel you stayed in last night?"

- “Um,” Zuckerberg said
- "If you have messaged anybody this week, would you share with us the names of the people you have messaged?"
- "Senator, no, I would probably not choose to do that publicly here," Zuckerberg said.
- Dick Durbin: I think that might be what this is all about - your right to privacy, the limits of your right to privacy, and how much you'd give away in modern America,"

(Watson, 2018)

Both the US and the EU governments responded harshly to Meta. Ironically, as opposed to corporations being victimized, governments are now victimizing themselves. In a resolution, the EU stated that the Cambridge Analytica scandal was a “huge risk to democracy” and a threat to “fundamental rights to information as well as media freedom and pluralism” (Official Journal of the European Union, 2019)

This shift towards blaming corporations like Cambridge Analytica and Palantir is highly unusual both corporations market themselves to governments. Cambridge Analytica explicitly advertised its ability to “mobilize voters “ and “understand every individual in your target group” through targeted data. Similarly, Palantir claims to deliver “mission-critical outcomes for the West’s most important institutions.” (*Palantir*, n.d.) This frame strongly matches Zuboff's framework of surveillance capitalism and Zuboff's idea of behavioural future markets, in which governments and other institutions incentivise corporations to generate large amounts of data to create highly accurate platforms for data analysis. As Zuboff describes, this market-driven rationality functions according to the logic of accumulation, pushing corporations to gather more consumer data (Zuboff, 2019, p. 8).

Conclusively, it can be said that the evolution of this market-based approach overlaps with Shoshanna Zuboff’s concept of surveillance capitalism. Corporations appear to be incentivized to collect more data. This corporate rationality normalizes data collection and turns it into a regular feature of the digital domain, creating what Foucault refers to as a panopticon, a space where the user is completely visible and where state surveillance is both untransparent and arbitrary.

4.5 LEGISLATIVE RESPONSES

The evolving corporate surveillance rationality has been met with diverging responses from the EU and the U.S., each representing a different construction of subjects. The GDPR in

Europe has a firm rights-based orientation, which starkly contrasts the U.S. market-based orientation towards privacy. This section will compare the GDPR to the American equivalent, the CCPA.

The core of the EU's privacy philosophy is embedded in Article 8 of the Charter of Fundamental Rights of the European Union. The EU adopts the subject position as constructed by the European Convention on Human Rights and frames individuals as "identifiable natural persons" regardless of nationality or residence . This is rooted in values such as the right to be forgotten, necessity, effectiveness, and proportionality. Even data that has undergone pseudonymisation is protected by the GDPR with relatively strict standards. Children are particularly well protected under this law (European Union, 2016, Articles 4, 8, 17).

An important aspect of the GDPR is that it focuses its efforts on the processes of the processor itself. The GDPR requires corporations to implement "privacy officers" to oversee the data-gathering process within the organization . This law seems to reduce the exercise of biopower in favour of privacy significantly and seems to be a mechanism to prevent the abuse of the state of exception, described by Agamben. It limits the data processor by regulating the data collection mechanisms themselves (European Union, 2016, Articles 37-39)..

This approach starkly contrasts U.S. legislation such as the CCPA, which appears to frame privacy differently. The CCPA is more aligned with a market-based rationality. Although the incentives to produce this legislation rose from similar concerns as the GDPR, it differs from it as it tends to construct its subjects as "customers" rather than citizens or natural persons (California Legislature, 2018). Additionally, the CCPA is not as concerned with the internal organizational structure and methods of data gathering, but rather aims to enhance the autonomy of its consumers. The CCPA tends to value consumer consent and regulates outcomes rather than processes. This leads to a different type of logic in which the consumer is made responsible for managing his/her privacy through legal action (California Legislature, 2018).

The US also shows a greater tolerance for invasive surveillance powers in crises. Laws like the Patriot Act and section 702 of the FISA Amendment Act have led to mass metadata collection, such as phone records. Critics argue that these laws have justified the persecution of other crimes, demonstrating that they have been used beyond their original scope. They

argue that the Patriot Act led to “secret judges in a secret court based on secret interpretations of law,” which would lead to reduced accountability (Snowden, 2014) .

In conclusion, the EU’s GDPR and other European privacy frameworks diverge from the US’s approach to privacy. While the EU’s approach is highly human-rights oriented, the US’s approach is based on autonomy instead. Furthermore, the EU’s approach is consciously aimed at reducing the ability of governments to abuse pseudonymized data, whereas this is not specified in the US. Additionally, the US allows for greater extension of surveillance capacities by the Federal Government through special clauses such as the FISA Amendment Act and the Patriot Act. What differentiates the US even more is its framing of subjects as consumers rather than citizens which displays the US’s market-based approach to privacy.

4.5 CONCLUSION OF THE ANALYSIS

The theory and analysis together lead to the formulation of the sub-questions, in this section the answers to the sub-questions will be discussed.

First, How has the corporate surveillance narrative in the EU and the US developed since the Snowden revelations in 2013? Since 2013, the corporate surveillance narrative has changed as it has normalized increasingly more intrusive surveillance, and the nature of surveillance has become increasingly more indiscriminate. Additionally, corporate actors have become increasingly more important actors whose image has changed from positive to highly negative.

Second, what are the key similarities and differences in corporate surveillance narratives between the EU and the US? From the case studies discussed, the EU tends to have a more human rights-oriented approach to surveillance, and the U.S. a more market-oriented approach. Both narratives are similar in using safety as a central argument to legitimise surveillance.

Finally, how do these differences reflect the exercise of biopower in both contexts? In the U.S., biopower is exercised through a market-based and individualized approach and tends to focus on risk prevention only. This individualised character reflects a strategy of governing through personal responsibility. In contrast, the EU uses its human rights-based approach in a way that seems to shift towards population-level monitoring. The EU has a strategy of governing through protection.

5. CONCLUSION

5.1 KEY INSIGHTS

This thesis aimed to explore the development of and structure of corporate surveillance narratives through a Foucauldian lens. The main research question was: "How is biopower exercised through corporate surveillance narratives in EU and US privacy discourses?"

The analysis showed that biopower is exercised by normalizing increasingly intrusive means of surveillance. First, the type of data gathered by governmental institutions has become more intrusive. Second, the framing of subjects that require monitoring or are considered a threat has become increasingly more indiscriminate. Finally, the EU uses the human rights discourse to extend its surveillance capabilities by framing safety and surveillance as an extension of the right to life as formulated in the ECHR article 2. The U.S., on the other hand, tends to frame surveillance through a more market-based rationality in which personal autonomy is central. Governments tend to use crises to legitimize extending their surveillance capacities, and there are concerns about whether this power will be retrieved after such crises.

Due to this market rationality in surveillance, there has been a clear shift from framing social media companies as victims to them being perpetrators. These social media companies are incentivized to collect personal data to build better predictive products. The impact of this development is that citizens are framed as consumers, and personal data has become highly commodified.

In short, these findings show that corporate surveillance narratives increasingly legitimize more intrusive and indiscriminate means of surveillance and that this is legitimized in what Agamben calls *states of exception (*McLoughlin,2012*).* Additionally, the discourse evolved to emphasise the influence of corporate actors more concretely in the government's efforts to exercise biopower.

5.2 THE DIRECTION OF FUTURE RESEARCH

This research focused on the relationship between biopower and corporate surveillance narratives. Foucauldian perspectives on corporate surveillance have remained relatively unexplored, especially in a transatlantic context. This research, therefore, provided a power-knowledge-centred lens to understand contemporary corporate surveillance. Additionally, the

research traced the discourse to find patterns of surveillance discourse and find similarities and differences between both the EU and the US. The research found clear patterns but has not fully addressed some important issues which shows the importance of further research in this topic.

For this research, scholars such as Zuboff and Foucault are still important for understanding corporate surveillance. Agamben is still relevant in understanding the nature of state surveillance. However, the framework's limitations exist as there appears to be no theory of the interaction between government and corporate entities in surveillance. Traditional perceptions of surveillance from Foucault and Agamben still strongly rely on the continuation of the sovereign nation state, whereas Zuboff tends to focus solely on companies and international markets.

This paper has filled a research gap by extending Foucault's theory of biopower to contemporary theories of surveillance capitalism in a transatlantic context. Where Foucault focused mainly on the governance rationality of surveillance, and Zuboff emphasised the economic logic of surveillance, this thesis has integrated both theories. This was done to get a better understanding of the interaction between corporate and state actors within the public debate. Few studies have applied Foucauldian discourse analysis to research transatlantic surveillance discourses. Scholars such as David Lyon (2007) have written about the sociological dynamics behind surveillance. But have not connected this to the transatlantic discourse, nor have they connected it to Foucauldian theory. This paper filled this gap by connecting the theories and by applying them to a concrete case.

What is missing is that theories within surveillance, such as Deleuze's theory of control and Foucault's theory of biopower, are mainly grand theories (Galič et al., 2016). In the field of surveillance discourse, there appears to be a lack of mid-range theories that fill the gap between micro-level theories and grand theories. Furthermore, future research could explore several important factors: the effect of technological developments on corporate surveillance, the interaction between states and corporate actors, and the effects of citizen participation on creating privacy legislation. Moreover, the codes that were used in this thesis only reflect a component of Foucault's biopower. Additionally, many more discursive elements in discourse could be researched, such as dataveillance, or from a perspective of networks. That could improve the understanding of surveillance discourse.

5.3 PREVENTING THE SURVEILLANCE CREEP

The analysis reveals that data collection by states and corporations has become more intrusive and often indiscriminate. To prevent state surveillance from extending beyond what is reasonably necessary policy adjustments are required. This paragraph will discuss the policy recommendations that logically follow from the research.

Firstly, policymakers should develop a predefined framework of acceptable crisis situations in which additional surveillance is allowed to be initiated. This should be done in consultation with data protection authorities such as the European general data protection board (EDPB). Additionally, standardized expiration dates should be formulated ranging from 30 days to 90. The expiration date only be renewed after a parliamentary vote in which more than 50% of the votes are in favour of renewal.

Secondly, governmental institutions require new policies concerning the gathering of citizen data from corporate actors. Intelligence agencies, or other governmental institutions, should not buy data from data analytics corporations as well as from social media platforms without the owner of this data being notified. If the notifying the citizen could compromise safety, citizens should be notified after the data is not considered necessary anymore for mitigating the perceived risk.

Finally, to reduce the increasing intrusiveness of surveillance. A guideline should be created which clearly describes which measures should be used in which crisis situation. This should include strict criteria for each situation. To link the crisis category to the correct surveillance tool the scope, duration, target population, data type has to be defined. A recommendation of the most likable types of crises are displayed below, displaying the format of a guideline.

- Public health crisis: location data permitted, contract tracing apps permitted, only anonymized data allowed. Duration: 3 months before renewal process.
- National security crisis: subject to judicial review, individual targeting permitted, metadata collection permitted. Duration: 6 months before renewal process.

If democratic societies have no clear oversight over surveillance measures, surveillance could sneak into our lives without us noticing it. It is unreasonable to believe surveillance is a phenomenon of authoritarian states. It could just as well absorb liberal democracies such as

the EU and the US as an extension of neoliberal market capitalism. Therefore, careful action is required.

6. REFERENCES

Andrejevic, M. (2013). Infoglut. In *Routledge eBooks*. https://doi.org/10.4324/9780203075319, pp. 47-50

Arnason, G. (2012). Biopower (Foucault). In *Encyclopedia of Applied Ethics* (pp. 295–299). Elsevier. https://doi.org/10.1016/B978-0-12-373932-2.00236-2

California Legislature. (2018). *California Consumer Privacy Act of 2018, California Civil Code, Title 1.81.5 (AB-375)*. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

European Convention on Human Rights - ECHR Official Texts. (n.d.). *ECHR*. https://www.echr.coe.int/european-convention-on-human-rights

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Foucault, M. (1970). *The order of things: An archaeology of the human sciences* (Original work published 1966). Vintage Books.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books. (Original work published 1975), pp. 195–197.

Foucault, M. (1990). *The history of sexuality: An introduction, Volume I* (R. Hurley, Trans.). Vintage Books. (Original work published 1976), p. 136.

Foucault, M. (1990). *The history of sexuality: An introduction, Volume I* (R. Hurley, Trans.). Vintage Books. (Original work published 1976), pp. 139–145.

Foucault, M. (1995). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage Books. (Original work published 1975), pp. 220–228.

Foucault, M. (2003). *Society must be defended: Lectures at the Collège de France, 1975–1976* (D. Macey, Trans.; M. Bertani & A. Fontana, Eds.). Picador, pp. 38–39.

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society*, *15*(4), 412–444. https://doi.org/10.1108/JICES-01-2016-0004

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Giglio, M. (2020, April 24). How much privacy would you give up to stay healthy? *The Atlantic*. https://www.theatlantic.com/politics/archive/2020/04/coronavirus-pandemic-privacy-civil-liberties-911/609172/

Khan, T. H., & MacEachen, E. (2021). Foucauldian Discourse Analysis: Moving beyond a social Constructionist analytic. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211018009

Leclercq-Vandelannoitte, A., & Bertin, E. (2024). How to deal with Big Tech power? The "Big Tech Raj", a new form of biopower in the digital age. *Technological Forecasting and Social Change*, *208*, 123732. https://doi.org/10.1016/j.techfore.2024.123732

Ledgett, R. (2014). The NSA responds to Edward Snowden's TED Talk [Video]. TED Talks. https://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk/transcript

Lyon, D. (2007). Surveillance, security and social sorting. International Criminal Justice Review, 17(3), 161–170. https://doi.org/10.1177/1057567707306643

Lyon, D. (2010). Liquid Surveillance: The contribution of Zygmunt Bauman to surveillance studies1. *International Political Sociology*, *4*(4), 325–338. https://doi.org/10.1111/j.1749-5687.2010.00109.

MacAskill, E., Dance, G., Cage, F., Chen, G., & Popovich, N. (2014, March 23). NSA files decoded: Edward Snowden's surveillance revelations explained. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

McLoughlin, D. (2012). Giorgio Agamben on security, government and the crisis of law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3965656

Peters, M. A. (2014). Giorgio Agamben's Homo Sacer project. *Educational Philosophy and Theory, 46*(4), 327–333. https://doi.org/10.1080/00131857.2014.900313

Palantir. (n.d.). *Palantir*. https://www.palantir.com/

Snowden, E. (2014). Here's how we take back the Internet [Video]. TED Talks. https://www.ted.com/talks/edward_snowden_here_s_how_we_take_back_the_internet/transcript

Walle, R. G. H. D. (n.d.). *Parliamentary question | Consequences of the Trump administration for data protection and privacy | E-000540/2025 | European Parliament*. © European Union, 2025 - Source: European Parliament. https://www.europarl.europa.eu/doceo/document/E-10-2025-000540_EN.html

Watson, C. (2018, May 25). The key moments from Mark Zuckerberg's testimony to Congress. *The Guardian*. https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-testimony-to-congress-the-key-moments

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

7. Appendix

7.1 Cambridge Analytica

Institution	Source type	Keywords used	link
The guardian	News article	Cambridge analytica	Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach | Cambridge Analytica | The Guardian
The Guardian	News article	Cambridge analytica	Facebook's week of shame: the Cambridge Analytica fallout | Facebook | The Guardian
The Atlantic	News article	Cambridge analytica	Facebook and the Cambridge Analytica Scandal, in 3 Paragraphs - The Atlantic
spiegel	News article	Cabridge analytica	Cambridge Analytica: What's behind the data analysis company - DER SPIEGEL X
Euronews	News article	Cambridge analytica + mass surveillance	Cambridge Analytica and the shortcomings of 'psychographic' data | Euronews
Euronews	News article	Cambridge analytica +mass surveillance	A year on, Cambridge Analytica still remains topical – even from beyond the grave | View | Euronews X
Youtube (CNN)	Interview	Mark Zuckerberg +interview	CNN interview: Read Mark Zuckerberg's remarks
Youtube (Pbs)	hearing	Mark Zuckenberg + interview	The key moments from Mark Zuckerberg's testimony to Congress | Mark Zuckerberg | The Guardian
Youtube (BBC)	Interview	Alexander nix + interview	Cambridge Analytica CEO Alexander Nix - BBC Newsnight X

7.2 COVID 19

Institution	Source type	Keywords used	link
The Guardian	News article	Covid + surveillance	Scrapping Covid surveillance study

			would put public health at risk | Letters | The Guardian
The guardian	News article	Covid + surveillance	Coronavirus mass surveillance could be here to stay, experts say | Surveillance | The Guardian
politico	News article	Covid + surveillance	In fight against coronavirus, governments embrace surveillance – POLITICO
politico	News article	Covid + mass surveillance	De opkomst van AI-surveillance - POLITICO
Euro news	News article	Covid + surveillance	Could the coronavirus pandemic lead to mass surveillance in Europe? | Euronews
Euronews	News article	Covid + mass surveillance	We shouldn't accept intrusive surveillance for the sake of our health without safeguards | View | Euronews
The atlantic	News article	Covid + mass surveillance	How Much Privacy Would You Give Up to Stay Healthy? - The Atlantic
Eur-lex	beleidsdocument	Covid + privacy	Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak | European Data Protection Board **X**
Time	article	Covid + privacy	Margrethe Vestager Invites Big Tech to Help Fight COVID-19 | TIME
Gao	Issue	Covid + privacy	Protecting Personal Privacy | U.S. GAO **X**
The guardian	News article	Covid + big tech	Seeing stones: pandemic reveals Palantir's troubling reach in Europe | Technology | The Guardian
Palantir	article	Palantir + data	Search | Palantir

7.3 Snowden revelations

Institution	Source type	Keywords used	link
The Irish times	News article	Snowden + NSA leak	NSA breaches privacy of thousands of US citizens – The Irish Times

The Guardian	News article	NSA + mass surveillance	ACLU lawsuit against NSA mass surveillance dropped by federal court | NSA | The Guardian
The Guardian	News article	NSA + mass surveillance	NSA reform is unavoidable. But it can be undermined if we aren't careful | Trevor Timm | The Guardian
The Guardian	News article	Snowden leaks	NSA files decoded: Edward Snowden's surveillance revelations explained | US news | theguardian.com X
politico	News article	Snowden + NSA leak	Edward Snowden: Mass surveillance making us less safe - POLITICO
politico	News article	NSA + mass surveillance	Obama's NSA plans bring skepticism - POLITICO
Politico	News article	NSA + mass surveillance	The price of surveillance: Government pays to snoop - POLITICO
Euronews	News article	Mass surveillance	Here's what a US surveillance law means for European data privacy | Euronews
Euronews	News article	Mass surveillance	The Brief: data privacy vs surveillance transatlantic clash | Euronews
The atlantic	News article	Snowden revelations	NSA Leak Catch-Up: The Latest on the Edward Snowden Fallout - The Atlantic
Die Spiegel	Interview	Snowden	Interview with Edward Snowden about His Story - DER SPIEGEL
Ted ex	Ted talk	Snowden (search engine Google)	Edward Snowden: Here's how we take back the Internet | TED Talk
TEDex	Ted talk	NSA + surveillance (search engine Google)	Richard Ledgett: The NSA responds to Edward Snowden's TED Talk | TED Talk
Youtube (Associated press)	Speech	NSA + surveillance	Obama: Snowden Not a Patriot

Youtube (oxford university)	Interview	NSA + surveillance	(74) General Michael Hayden | Beyond Snowden: An NSA Reality Check | Oxford Union - YouTube
Obamawhithouse.archives.gov	transcript	Obama + NSA surveillance	Remarks by the President in a Press Conference | whitehouse.gov

AI statement

During the preparation of this work, the author(s) used Grammarly.ai as well as ChatGPT to correct spelling and grammar. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the work. List all the generative AI tools that were used during the work.

- Grammaly.ai
- ChatGPT (OpenAI)