Evaluating the Impact of Mass Surveillance Through Ethical Theories

Master of Science in Technology thesis
University of Turku
Department of Computing, Faculty of Technology
Cyber Security Engineering
January 2025
Camilla Lähteenmäki

Supervisors:
Antti Hakkala
Jani Koskinen

UNIVERSITY OF TURKU
Department of Computing, Faculty of Technology

CAMILLA LÄHTEENMÄKI: Evaluating the Impact of Mass Surveillance Through Ethical Theories

Master of Science in Technology thesis, 57 p., 0 app. p.
Cyber Security Engineering
January 2025

This thesis explores the ethical implications of mass surveillance and the concept of the data double, framed through the lenses of deontology, consequentialism, and virtue ethics. Mass surveillance, encompassing technologies like facial recognition, AI, machine learning, and GPS tracking, presents significant challenges to privacy, autonomy, and societal trust. The thesis examines how these ethical theories assess the practices and consequences of mass surveillance, highlighting the interplay between individual rights, societal benefits, and moral character. To illustrate global implications, special attention is given to contemporary trends, such as the EU-U.S. Data Privacy Framework and China's Social Credit System. The concept of the data double—a digital reflection of individuals—serves as a focal point to understand surveillance's multifaceted impacts. The research underscores the interconnectedness of ethical considerations through critical analysis and offers practical recommendations for more ethically aligned surveillance practices.

Keywords: Mass Surveillance, Data Double, Deontology, Consequentialism, Virtue Ethics, Privacy, AI, Machine Learning, Facial Recognition, EU-U.S. Data Privacy Framework, Social Credit System, Ethics

Contents

Chapter 1

Introduction

The world has become a digital space, and we are being followed. At all times without us even realizing it. We are being surveilled whenever we read the news online, check the timetable for the bus, or even walk to our local store with phones in our pockets. From social media activity to GPS tracking and facial recognition, all these technologies gather data from and about us. Mass surveillance has transformed from a dystopian vision to a commonplace reality. While these technologies offer conveniences and security benefits, they have also raised significant ethical questions about privacy, individual autonomy, and the balance of power between citizens and corporations or governments. [1]

Mass surveillance is an increasingly pervasive aspect of contemporary society, characterized by the systematic collection, analysis, and usage of personal data on a vast scale. Whether through facial recognition systems, GPS tracking, or AI-driven data analysis, the implications of these technologies extend far beyond convenience or security, raising profound ethical questions. At the heart of this thesis lies an exploration of the ethical dimensions of mass surveillance and the data double, a digital representation of individuals crafted through aggregating their data.

Current research [2] highlights several aspects of mass surveillance, including its technological advancements and its societal and individual impacts. Concepts like the panopticon, surveillance capitalism, and the ethical challenges introduced by AI and ma-

chine learning provide a foundation for analysis. Recent trends, such as the rapid adoption of surveillance technologies during the COVID-19 pandemic and high-profile legal cases like Schrems II [3], further illustrate these issues' global and varied nature. While privacy regulations like the GDPR aim to address some concerns, they often fail to resolve deeper ethical conflicts about the very existence and use of data doubles.

The motivation for this thesis stems from the growing tension between technological innovation and individual rights. Mass surveillance technologies promise societal benefits, such as enhanced security and efficient governance, yet they also threaten fundamental values like privacy, autonomy, and trust. The creation of data doubles worsens this tension, as these digital profiles are increasingly used for decisions affecting individuals' lives, often without their knowledge or consent. Understanding these practices is critical for developing ethical frameworks to guide their use.

1.1 Problem statement

The thesis seeks to answer the following central questions:

- RQ1: How do different ethical theories evaluate the moral implications of mass surveillance?
- RQ2: How do these theories assess the existence and use of data doubles?

1.2 Objectives

This thesis aims to define and contextualize mass surveillance by examining its evolution, key terms, and recent trends, including the role of AI, machine learning, and high-profile legal cases. It introduces and applies ethical theories (deontology, consequentialism, and virtue ethics) to evaluate the moral implications of mass surveillance and data doubles

Finally provides a comparative ethical analysis of how these theories align or diverge in their evaluations of surveillance practices and data doubles.

1.3 Methodology

This thesis belongs under the domain of IT ethics, as it delves into the moral implications of technologies and practices related to mass surveillance, such as AI, machine learning, and data collection. These technologies directly shape societal structures and individual freedoms, making ethical scrutiny crucial in understanding their impact. The ethical review through deontology, consequentialism, and virtue ethics is a suitable method for this inquiry because it provides a structured, philosophical approach to analyzing moral dilemmas and their broader societal effects. Unlike a systematic literature review, which focuses on summarizing and synthesizing existing studies, the ethical review directly interrogates the values and principles underpinning surveillance practices. This approach not only uncovers normative tensions but also allows for a more nuanced evaluation of their justifications, consequences, and alignment with societal virtues, making it the optimal method for addressing the complexities of IT ethics in mass surveillance.

1.4 Thesis Structure

This thesis begins by defining key terms and providing an overview of mass surveillance, including its historical evolution and current trends. Chapter 2 introduces concepts like the panopticon, data doubles, global regulatory frameworks such as the GDPR and EU-US Data Privacy Framework, and recent developments in AI and machine learning. Chapter 3 shifts focus to Ethic. I go over what ethics are, what theories it includes and my reasoning for using the main three foundational ethical theories—deontology, consequentialism, and virtue ethics— that provide the tools for analysis.

The core of the thesis lies in Chapter 4, where these theories are applied to critically

assess the ethical implications of mass surveillance and data doubles. It explores questions such as how surveillance practices impact privacy, autonomy, trust, and transparency, as well as how the concept of the data double challenges traditional notions of personhood and moral responsibility. Comparative analysis reveals how the theories align, diverge, and complement one another in addressing these challenges. Finally, Chapter 5 brings this all together in the Conclusion and goes over all the key aspects discussed in this thesis.

Chapter 2

Mass surveillance

Mass surveillance refers to the large-scale, systematic monitoring of a large part of or entire populations, typically carried out by governments, corporations, or other entities with the means to collect and analyze vast amounts of data [4]. This practice has grown in scope and sophistication with the advancement of digital technologies, prompting debates around privacy, security, and ethics. While surveillance has historically been used to maintain public order and security, modern techniques leverage digital data from online activities, mobile devices, and social networks, making it possible to track individuals in unprecedented detail. Especially the rise of Surveillance capitalism [5] has increased the amount private corporations collect and monetize personal data for profit.

The 21st century has witnessed explosive growth in mass surveillance capabilities, fueled by the rise of big data [6] and advanced technologies such as artificial intelligence (AI) and facial recognition [7] [8]. Big data is crucial in mass surveillance as it provides the raw material for analysis and pattern recognition. When data from and about individuals is collected and monitored through their digital interactions and online behaviour, it is also known as **dataveillance** [4]. Unlike traditional surveillance, which relies on physical observation or listening, dataveillance gathers data from digital sources, including online and offline activities, to monitor behaviours and track patterns. These behaviours can include internet browsing, social media usage, and mobile phone metadata.

Dataveillance is often done in the background without the active participation of the monitored individual, gathering data continuously through devices, platforms, and services. For example, different social platforms do dataveillance by tracking users' interactions, likes, and shares to build a detailed profile of them. Companies use browsing history, search queries, and purchase data to target individuals with personalized ads [4]. Furthermore Internet of Things (IoT) [9] devices, like smart home assistants and fitness trackers, collect data about individuals' daily routines, health metrics, and preferences, which can again be used for profiling.

The collected data is analyzed to understand and predict behaviour, often using algorithms and AI to generate insights about individuals or groups, which can be used for targeted advertising, predictive policing [10], or other decision-making processes. The use of algorithms and data analysis can be used to predict where crimes are likely to occur or who is likely to commit them. It is a controversial form of surveillance because it can reinforce biases and lead to over-policing of certain communities. [11]

In this day and age, it is basically impossible to avoid being online. Everything is done via the internet, on the phone and computer, through apps and web pages. For example, in Finland, when you need to identify yourself securely, you must do it online through bank credentials or with mobile ID or identity card. This need for the internet to function in a society creates a problem, where one can not choose to be invisible or forgotten. For ones presence is recorded to the void that is the internet.

Gathering data in the background without the individual's active participation and using it further raises concerns of lack of informed consent, violation of privacy, and transparency. Laypeople are often unaware of how and how much data is gathered from and about us and cannot fully consent to data gathering. For example, many agree to cookies without a second thought just to get to a web page as fast as possible. Making the information about their data and how it is used more of a nuisance and inconvenience than an important conscious decision the individual has given. The collected data can be

private and sensitive and, in the worst case, derive harmful information. But because this is done basically at all times and everywhere, laypeople have become desensitised and almost numb to data gathering. [1]

2.1 Metadata and Data double

Metadata is often described as "data about data." It provides information that describes, identifies, or contextualizes a particular dataset, document, or file. Metadata does not constitute the primary content but rather enriches it by enabling better organization, understanding, and retrieval. Metadata plays a significant role in surveillance systems, for example, with call detail records, web traffic, location data, and social media. Metadata includes details such as timestamps, geolocation, communication patterns, and device identifiers. It excludes direct content, such as the body of an email or a phone conversation, but provides a powerful means to infer behavioural patterns, preferences, and connections. [12] [13]

Now consider if all data from private and public databases, as well as online services, were consolidated into a single profile, it would create a highly detailed and accurate dossier of an individual. Such a profile, if misused with malicious intent, could cause irreversible harm. This highlights the alarming nature of pervasive surveillance and profiling. Even if the probability of this scenario affecting a specific individual is minimal, the sheer potential for abuse and its catastrophic consequences make it a deeply unsettling concept.

These inferences are the building blocks that can be used for a **data double** — a digital replica created by aggregating and analyzing such metadata. Although metadata may not include personal content, patterns and correlations can often re-identify individuals. Individuals often have little control over how their metadata is collected, aggregated, and interpreted, reducing their agency in shaping their digital representations. Metadata,

though seemingly innocuous, can reveal sensitive information when analyzed at scale. This challenges traditional notions of privacy and informed consent and raises ethical concerns. The accuracy and fairness of data doubles depend on the integrity of metadata collection and analysis. Errors or biases in metadata can lead to misrepresentations, perpetuating inequality and injustice. Awareness of constant metadata surveillance can alter behavior, discouraging free expression or experimentation in digital spaces. [6]

Governments argue that these tools are essential for national security, crime prevention, and counterterrorism efforts. For instance, the USA PATRIOT Act of 2001 [14] expanded the powers of U.S. surveillance agencies following the 9/11 attacks, while countries like China have implemented comprehensive surveillance systems, including the controversial social credit system [15].

At the same time, mass surveillance raises serious ethical questions, particularly regarding individual privacy rights. It can be argued that these systems disproportionately infringe upon civil liberties, creating what has been described as a surveillance society where individuals' activities, movements, and communications are constantly monitored. Shoshana Zuboff's concept of surveillance capitalism further critiques the monetization of personal data by corporations, which collect and sell user information without adequate transparency or consent [5].

2.2 Panopticon

The concept of **Panopticon** has become a foundational metaphor for understanding surveillance, control, and power in modern society. Originally proposed in the late 18th century by English philosopher and social theorist Jeremy Bentham, the Panopticon was designed as an institutional structure—specifically for prisons—that would allow a single guard to observe all prisoners without them knowing if they were being watched at any given moment. This design aimed to create a psychological effect in which individuals would

regulate their behaviour under the assumption that they were always being observed, fostering internalized discipline. [16]

Bentham's Panopticon is typically depicted as a circular building with a central watchtower that provides a view of each cell. Prisoners are isolated from each other and unable to see into the watchtower, creating a state of constant gaze that substitutes overt control with psychological influence. Bentham theorized that the uncertainty about when and if they were being observed would lead prisoners to adopt behaviours deemed "acceptable" by authority figures, internalizing the power dynamic and reducing the need for physical punishment or enforcement. [16]

Michel Foucault, a 20th-century philosopher and social critic, expanded on Bentham's Panopticon in his seminal work Discipline and Punish (1975) [17], symbolizing broader societal structures of surveillance and control. In this work, Foucault argued that the Panopticon represented a new form of disciplinary power that operates not through direct violence or coercion but through an internalized sense of surveillance. He suggested that modern institutions—schools, hospitals, factories, and bureaucratic organizations—embody Panopticon-like structures in which individuals self-regulate due to a perceived sense of oversight, even when no direct surveillance occurs.

In the context of digital surveillance, the Panopticon metaphor has become increasingly relevant as governments and corporations collect massive amounts of data on individuals' digital footprints. Today, mass surveillance technologies like CCTV (Closed-Circuit Television), which are often integrated with facial recognition and other advanced technologies [18], internet monitoring systems, and data-collection algorithms serve as modern equivalents to the Panopticon's central watchtower. Unlike Bentham's design, however, digital surveillance is often invisible and ubiquitous, making it difficult for individuals to know when they are being observed or what data is being collected.

Several features characterize modern digital Panopticism. Much like Bentham's Panopticon, where prisoners could be observed at any time, digital surveillance allows for con-

stant data collection on individuals, creating a state of perpetual visibility. Self-regulation through perceived surveillance is one of the effects of the modern Panopticon. Just as the prisoners in Bentham's Panopticon adjust their behaviour due to the possibility of being watched, individuals may alter their online behaviours or limit self-expression due to perceived surveillance by corporations, governments, or other users. This phenomenon, often referred to as the **chilling effect**, [19] can lead to self-censorship and an erosion of personal freedoms. Automated Panopticism results from advancements in artificial intelligence and machine learning because surveillance systems now autonomously track and analyze vast datasets. For instance, algorithms can detect patterns in social media posts or predict individuals' future behaviour based on past data [20]. This automation removes human overseers from the process, extending the Panopticon's reach and reducing accountability, as decisions are made based on opaque algorithms rather than explicit human intentions. Unlike Bentham's centralized Panopticon, modern digital surveillance is often decentralized across multiple entities, from social media companies to government agencies. This distributed form of surveillance broadens the scope of data collection and makes it difficult for individuals to understand or challenge who holds and uses their data.

The implications of this model are particularly relevant to discussions of privacy, democracy, and personal freedom. The inability to control or even understand the extent of data collection can create power imbalances, where individuals feel helpless against the surveillance practices of corporations and governments. Legal frameworks such as the General Data Protection Regulation (GDPR) [21] in the European Union and California Consumer Privacy Act (CCPA) [22] aim to address these concerns by providing individuals with greater control over their personal data. GDPR is a legal framework in the European Union designed to protect individuals' data privacy and regulate how companies collect, store, and use personal data. However, questions remain about whether such regulations are sufficient to protect privacy in the face of ever-evolving surveillance technologies. Moreover, the public's awareness and understanding of the extent

of surveillance is often limited, leaving many individuals powerless to assert control over their own data.

2.3 Surveillance trends

Mass surveillance has a long history, but its scale and reach have grown exponentially in recent decades. The practice has evolved from simple physical observation techniques, like police patrols and CCTV cameras, to more complex systems involving digital surveillance tools such as internet monitoring, mobile phone tracking, and biometric identification. The post-9/11 era marked a significant turning point, especially with the rise of counterterrorism measures that justified greater surveillance powers for national security purposes. The Edward Snowden revelations in 2013 [23] exposed the extent to which the U.S. government, through agencies like the NSA, was collecting data on its own citizens and foreign nationals alike. Since then, AI and data analytics advancements have enhanced the ability to process and interpret the enormous amounts of data individuals generate daily.

2.3.1 COVID-19 and surveillance

The COVID-19 pandemic accelerated the use of surveillance technologies under the pretext of public health. Contact tracing apps [24], health monitoring devices, and the use of drones for crowd control [25] became common, raising concerns about the potential normalization of mass surveillance post-pandemic. Governments introduced contact tracing apps to identify and notify individuals who may have been exposed to COVID-19. These apps varied in design, with some utilizing Bluetooth technology to anonymously track encounters without precise location data, such as Apple and Google's joint framework [26]. Others, particularly in China and South Korea, relied on GPS-based location tracking, offering more precise data on individuals' movements but raising higher privacy

concerns [27].

Health monitoring technologies became common in workplaces, airports, and public spaces, including temperature-checking cameras, biometric sensors, and wearables such as wristbands that track body temperature or location. While these devices offered real-time health monitoring, the data collected posed risks for long-term privacy violations, as health data is sensitive and highly personal.

The rapid rollout of COVID-related surveillance raised several ethical and privacy issues, including, for example, lack of informed consent, data collection without limits, and normalization of surveillance. Many COVID-19 surveillance measures were implemented under emergency policies, often with limited input from the public. Individuals had little choice but to comply with contact tracing and health monitoring to access essential services or workplaces. In some cases, COVID-19 apps and devices lacked clear guidelines on data collection, storage, or deletion. This led to situations where health data could be retained indefinitely, raising concerns about repurposing or reusing data after the pandemic. The pandemic arguably made citizens more accepting of surveillance in everyday life, potentially normalizing practices that would be considered intrusive in a pre-COVID-19 context. [28] This normalization could pave the way for expanded surveillance beyond health emergencies, for instance, in policing or behavioural tracking.

2.3.2 Facial recognition technology

Facial recognition technology has also seen widespread adoption, with its use expanding beyond security into areas such as retail, marketing, and social control. Facial recognition technology has rapidly evolved into one of the most widely used surveillance tools worldwide. It enables authorities, companies, and private entities to identify and verify individuals based on their unique facial features. This technology relies on artificial intelligence and machine learning algorithms that analyze and match facial patterns, raising significant questions about privacy, consent, accuracy, and bias. [29] Countries such

as China and Russia have widely adopted facial recognition technology, integrating it into state surveillance systems to monitor public behaviour and assess citizen compliance [15]. China's "social credit system," for instance, combines facial recognition technology with other data points to evaluate citizen behaviour and access to services [15].

While facial recognition technology has made significant contributions to security and convenience, its adoption raises serious ethical and privacy issues, particularly concerning consent, accuracy, and potential misuse, for example, lack of consent and transparency, potential for misuse, data security risks, and misidentification and bias. [29] One of the central ethical concerns with facial recognition technology is the lack of informed consent. Individuals are often unaware when they are being scanned, and their data is collected without explicit permission. For example, live facial recognition technology deployments in public spaces provide no practical way for individuals to opt-out, raising questions about the right to privacy. As facial recognition technology becomes more advanced, it can track individuals' movements and interactions, even in situations unrelated to their original intent. [18]

In some cases, private companies have partnered with law enforcement to share facial recognition technology data, blurring the lines between public and private surveillance and leading to concerns about function creep—the unintended expansion of a tool's use beyond its intended purpose. Facial recognition technology relies on large databases of biometric data, which are vulnerable to cyberattacks. Breaches of these databases can lead to the theft of sensitive information that cannot be changed, unlike passwords. This creates long-term risks for affected individuals. Studies have consistently shown that facial recognition technology has higher error rates when analysing images of people from minority backgrounds, women, and children. Inaccuracies in identification have led to wrongful arrests and detentions, sparking criticism that facial recognition technology can perpetuate and amplify systemic discrimination in law enforcement. [18] [30]

2.3.3 China's Social Credit System and AI

China's Social Credit System (SCS) is one of the most comprehensive examples of state-led surveillance intertwined with behavioural regulation. Officially introduced as a policy framework in 2014, the SCS aims to monitor, evaluate, and influence the behaviour of individuals, businesses, and government entities by assigning them scores or ratings. These scores reflect their "trustworthiness" based on diverse criteria, ranging from financial creditworthiness to adherence to social norms. [15]

The Social Credit System operates by aggregating and analysing vast amounts of data, including credit card payments, loan histories, and tax compliance. Public behaviour, such as jaywalking or adherence to traffic rules, and online activities, such as posts on social media. Records of legal disputes, penalties, or criminal activities. Positive behaviours like paying bills on time or volunteering may result in rewards like easier access to loans or reduced bureaucracy. Negative behaviours, such as spreading misinformation or failing to pay debts, may lead to penalties like travel restrictions or exclusion from certain services. [15]

Citizens often do not know how scores are calculated, what data is used, or how to appeal decisions. The centralised control of personal data and behaviour monitoring creates risks of misuse for political repression or discrimination. Constant surveillance may discourage legitimate expression or activism, stifling creativity and innovation. Marginalised groups are more likely to face penalties, reinforcing existing social and economic disparities. [15]

China's Social Credit System illustrates the extreme potential of mass surveillance when integrated with behavioural regulation. It serves as a cautionary tale for other nations exploring surveillance technologies, particularly in balancing state interests with individual rights.

As AI and machine learning have advanced, they have transformed the capabilities of surveillance systems, enabling more efficient data analysis, pattern recognition, and

even predictive analytics. [31] By processing vast data sets in real time, AI-powered surveillance systems can detect suspicious behaviours, predict incidents, and even identify individuals, all with minimal human intervention. AI and ML in surveillance raise critical concerns about individual privacy, transparency, fairness, and the risks associated with predictive accuracy. AI-powered surveillance systems often operate in public and semi-public spaces without explicit consent from monitored individuals. [32]

For instance, retail stores or workplaces using AI to track customer behaviour or employee productivity do not always inform individuals that their behaviour or emotions are being analysed, raising ethical privacy concerns. Since AI algorithms learn from historical data, they may inadvertently reinforce biases present in that data. For example, predictive policing models can exacerbate existing biases if they rely on arrest records from neighbourhoods already subject to higher police scrutiny. This can create feedback loops, where biased data leads to biased policing, generating more biased data. Additionally, emotional recognition algorithms have been shown to be less accurate for people of certain ethnicities, raising concerns about fairness and accuracy. [33]

2.3.4 Schrems cases and new Data Privacy Framework

The Schrems I [34] and Schrems II [3] cases, named after Austrian privacy activist Max Schrems, have profoundly impacted data privacy laws and practices, especially around international data transfers between the European Union and the United States. These cases have underscored fundamental conflicts between EU privacy standards and U.S. surveillance practices, resulting in significant rulings by the European Court of Justice (CJEU) that have implications for global data governance and digital privacy.

The first Schrems case (commonly referred to as "Schrems I") challenged the EU-U.S. Safe Harbor Framework, which allowed companies to transfer data between the EU and the U.S. Max Schrems argued that his data, stored by Facebook in the U.S., was vulnerable to U.S. surveillance practices that did not meet the EU's data protection standards. The

European Court of Justice agreed, invalidating the Safe Harbor Framework because U.S. government surveillance did not adequately protect EU citizens' personal data. [35] In the follow-up case, Schrems II, the European Court of Justice examined the EU-U.S. Privacy Shield, a successor to Safe Harbor intended to improve protections for EU citizens' data in the U.S. Schrems again argued that Privacy Shield was insufficient, citing ongoing U.S. government surveillance practices authorised under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and Executive Order 12333. The European Court of Justice ruled that Privacy Shield also failed to provide adequate protection, effectively invalidating it and significantly impacting any business that relied on transatlantic data flows. [36]

The Schrems cases have spurred developments in data privacy regulations around the world. In response to the Schrems II ruling, the EU and the U.S. introduced the EU-U.S. Data Privacy Framework in 2023 as a replacement for the Privacy Shield. This new framework aims to address the concerns raised by the European Court of Justice by incorporating more stringent protections and oversight mechanisms to limit U.S. government access to EU citizens' data. [36]

The introduction of the EU-U.S. Data Privacy Framework (DPF) in 2023 is a significant development in the context of mass surveillance and international data transfers. The DPF introduces stricter oversight mechanisms aimed at limiting U.S. government access to data transferred from the EU. It also establishes a Data Protection Review Court (DPRC) to handle complaints from EU citizens regarding U.S. surveillance. U.S. surveillance practices must meet specific thresholds of necessity and proportionality, addressing arbitrary or bulk data collection concerns. [37]

For businesses, the DPF provides a legal framework for transferring personal data across the Atlantic, reducing uncertainty and risk of non-compliance. However, it also places increased responsibility on organisations to ensure transparency, accountability, and adherence to privacy principles. [37]

The Data Privacy Framework also connects directly to the discussion of data doubles. Transferred data used to build digital profiles under this framework will now operate within revised constraints, offering some degree of protection. However, concerns persist about how much influence individuals have over their data doubles, especially in cases where profiling affects decisions about them without their knowledge. The Data Privacy Framework mechanisms encourage more visibility into how data is used, a positive step for reducing the chilling effects of mass surveillance. [37]

Having explored the scope, mechanisms, and evolving trends in mass surveillance, it becomes evident that the practice profoundly impacts fundamental aspects of society, including privacy, trust, and autonomy. These impacts are not merely technological or legal concerns but are deeply ethical in nature, raising questions about the moral justification and consequences of such surveillance practices.

To address these concerns, it is essential to evaluate mass surveillance within a structured framework. How does one determine whether surveillance practices are morally acceptable, harmful, or beneficial? Ethics provides a systematic approach to answering such questions by examining actions, their outcomes, and the virtues they reflect. To evaluate these complexities, the following chapter introduces three foundational ethical theories—deontology, consequentialism, and virtue ethics—offering distinct perspectives for critically assessing the moral dimensions of mass surveillance and its implications for individuals and society.

Chapter 3

Ethics

Ethics, derived from the Greek word ethos, is the philosophical study of morality—what is right and wrong, good and bad, just and unjust. It seeks to provide a systematic framework for evaluating human actions and guiding behavior based on moral principles. [38]

Ethics is primarily concerned with how things should be rather than merely describing how they are. For instance, instead of observing that people lie, ethics asks whether lying is morally permissible. It establishes standards or norms to guide human behavior. Ethical principles often aim for universality, meaning they apply to everyone in similar situations. For example, the idea that fairness is essential in justice systems transcends cultural boundaries.

Ethics is not just theoretical—it has practical implications. It helps individuals and societies make decisions about contentious issues like environmental protection, medical advancements, or social justice. Ethics involves critically analyzing moral beliefs and practices. It challenges assumptions and encourages reasoned debate about what is right or wrong. [38] Ethical frameworks adapt over time as societies evolve and face new challenges, such as technology's impact on privacy or the ethical considerations of artificial intelligence.

Ethics deals with values like honesty, justice, kindness, and courage. These values act as benchmarks for assessing actions and character. [38] Ethics explores questions of

accountability: Who is responsible for an action? When are individuals or groups morally blameworthy or praiseworthy? It examines what rights individuals have (e.g., the right to free speech) and what duties they owe to others (e.g., the duty to tell the truth or prevent harm). Ethics questions the nature of "the good life" and what constitutes evil or harm, seeking to define and promote human flourishing.

Ethics encompasses several subfields, each addressing different aspects of moral philosophy. **Metaethics** investigates the nature of morality itself. Metaethics asks questions like: What does "good" mean? Are moral truths objective or subjective? For example, debating whether moral truths exist independently of human opinion. **Normative ethics** is concerned with establishing principles or rules for moral behavior. Includes theories like deontology, consequentialism, and virtue ethics. For example, deciding whether lying is always wrong or acceptable in some cases. **Applied ethics** applies ethical principles to specific real-world issues. Topics include IT ethics, medical ethics, environmental ethics, business ethics, and bioethics. [39] For example, is it ethical to use animals in medical testing? Furthermore this thesis is also part of applied ethics.

This thesis employs deontology, consequentialism, and virtue ethics as its primary ethical frameworks because they are the three most prominent and foundational theories in the field of ethics and also in IT ethics. [40] Together, they offer a robust and comprehensive means of analyzing the moral implications of mass surveillance from different perspectives. These three theories were chosen because they are the cornerstones of ethical thought, each representing a unique dimension of moral reasoning—principles (deontology), outcomes (consequentialism), and character (virtue ethics). Their widespread application across disciplines and enduring influence make them the most suitable frameworks for a holistic analysis of mass surveillance.

3.1 Deontology

Deontology is an ethical theory focused on the importance of duty, rules, and obligations, often called "duty ethics." Many theories are considered deontological, but the most known one is from Immanuel Kant's. Deontology maintains that certain actions are inherently right or wrong, regardless of their consequences. This contrasts consequentialist theories like utilitarianism, which assess morality based on outcomes. In deontology, moral duty is the basis for determining ethical action, and this is anchored in universal principles and respect for individuals as autonomous agents. [41]

Kant first argues that morally correct actions can only stem from duty. His second argument is that the motives of the person who carries out the action make them right or wrong, not the consequences of said action. [41] Kant posits that actions have true moral worth only when they are performed out of a sense of duty rather than inclination, personal gain, or emotional impulse. In this context, duty refers to adherence to the categorical imperative—a universal moral law that rational beings must follow irrespective of their desires or specific circumstances. Consider a shopkeeper who does not overcharge customers. If they act honestly to build a good reputation or avoid penalties, their actions lack moral worth in Kant's framework. However, if the shopkeeper acts honestly because they believe it is their duty to treat others fairly, their actions are morally right.

Kant's second argument emphasises the intention or motive behind an action as the key determinant of its moral value. Unlike consequentialist theories (e.g., utilitarianism), Kantian ethics holds that the outcome of an action does not matter; what matters is whether the action was done from a sense of duty. For Kant, the only thing that is inherently "good" is a "good will"—the resolve to act according to moral principles purely because it is the right thing to do. [41] Suppose a person donates to charity. If their motive is to genuinely fulfill their duty to help others, the action is morally commendable, even if the charity ultimately misuses the funds. Conversely, if the person donates solely for public recognition, the act loses its moral worth, regardless of its positive out-

comes. According to Kant, the morality of an action depends on its alignment with duty, not on the pleasure or pain it produces. Deontology often supports moral absolutism, where some actions (like lying, killing, or stealing) are always considered wrong, no matter the circumstances. This makes it unique because it often requires moral actions that might conflict with what would otherwise be rational or beneficial in a consequentialist framework. [41]

The core concepts of deontology include categorical imperative, duty and good will, and moral absolutism. One of Kant's key contributions, the categorical imperative, is a principle meant to guide moral action. The three meaningful formulations are: 1) Act only according to a maxim that you would will to become a universal law. For example, if one believes that lying is wrong, then lying would be wrong universally in all situations. 2) Always treat humanity, whether in yourself or others, as an end and never merely as a means. This emphasises respecting the intrinsic value of individuals, not using them solely as tools for achieving another end. 3) "Every rational being must so act as if he were through his maxim always a legislating member in a universal kingdom of ends." This means that individuals should act by principles they believe could justly apply to everyone, aiming to contribute to a moral community where people treat each other with respect and autonomy. As a "legislator," each person should act in ways that uphold universal ethical standards, creating a world in which everyone's dignity is valued, and everyone acts out of moral duty. This idea is foundational to Kant's categorical imperative, which demands actions that respect the intrinsic worth of all people. [41]

In real-world ethics, deontological principles often form the foundation for human rights and legal systems, such as human rights and professional codes of conduct. Many human rights frameworks are deontological because they establish rights as inherent and non-negotiable, such as the right to life or freedom from torture. Many professions, such as medicine and law, have ethical codes that reflect deontological principles, such as a doctor's duty to maintain confidentiality and prioritise patient welfare regardless of the

consequences.

The strengths of deontology are its emphasis on justice, which means deontology's commitment to universal rules can provide a strong basis for justice and equality, and predictability and consistency, which means the reliance on duty and rules allows for predictable outcomes and clear guidance, beneficial for social and legal structures. By establishing clear rules for what is right or wrong regardless of outcomes, deontology ensures that actions are morally justifiable.

Deontology places a high value on individual rights and personal autonomy, protecting individuals from being treated as mere means to an end. This principle ensures that individuals are valued and respected in themselves, which is central to concepts like human rights and justice. For instance, deontological ethics supports the idea that each person has inherent dignity and should not be sacrificed for the greater good, as in the context of privacy rights or medical ethics. Deontology also provides clear moral rules that can simplify complex ethical decisions, especially in situations where consequences are hard to predict or quantify. This rule-based clarity is beneficial in fields like law, where objective standards are essential for maintaining fairness and accountability. For instance, the rule "do not lie" provides a straightforward guideline that individuals can apply without needing to calculate potential outcomes. [42]

Many professional fields, such as medicine, law, and business, rely on deontological principles to establish codes of conduct. These codes outline duties (e.g., confidentiality, honesty) that professionals must uphold regardless of outcomes. For example, medical ethics emphasise the principle of "do no harm," which is rooted in deontological thinking. These professional standards help create a trustworthy environment for practitioners and clients alike.

On the other hand, criticisms regarding this theory come from inflexibility and neglect of consequences. Its rule-based approach can lead to situations where moral obligations conflict without a clear way to resolve the tension. For instance, if lying to save a life

is against a deontological rule, then one must tell the truth, even if it results in harm. This rigidity can seem overly restrictive, leading to morally uncomfortable conclusions. Deontology sometimes faces issues when duties conflict, as it does not provide a clear way to resolve situations where two moral obligations contradict each other. For example, if one has a duty to be honest and a duty to protect others, these two duties can conflict in a scenario where telling the truth would cause harm. Deontological frameworks often lack mechanisms for prioritising one duty over another, leaving adherents with difficult, sometimes irresolvable dilemmas. Critics also argue that ignoring outcomes entirely can lead to harm or injustice when rigidly applying rules without considering the context. [42]

It can be argued that deontology's disregard for consequences is problematic, as it can lead to morally questionable outcomes. By focusing exclusively on the morality of actions based on their adherence to rules, deontology may justify actions that unintentionally result in significant harm. For instance, adhering to a duty to follow the law might prevent a person from disobeying unjust laws that perpetuate harm or injustice. This exclusion of outcomes from moral consideration can seem detached from the real-world implications of ethical decisions. [42]

Defining universal moral duties or rules can be challenging and leads to ambiguity within deontological ethics. For example, Kant's "categorical imperative" suggests that actions should be universally applicable, but it does not always clarify how these universal duties are to be formulated or determined. [41] This leaves room for interpretation, and different people might come to different conclusions about what specific rules are required. This vagueness contrasts with the clarity that consequentialism provides by focusing on outcomes.

Kantian deontology emphasises rationality as the foundation of moral duty, which has been criticised as limiting, as it does not account for emotions or personal relationships in moral decision-making. [42] Deontologists generally believe that moral duties are deter-

mined through reason alone, which can ignore human emotional experiences, empathy, and other relational factors that people often consider integral to morality. This emphasis on cold rationality can feel unrealistic and fails to accommodate moral intuitions rooted in human emotions.

Modern ethical issues, like those in technology, bioethics, or environmental ethics, often involve complex, large-scale consequences that deontology may struggle to address adequately. For instance, dilemmas around AI ethics, climate change, or genetic engineering require consideration of broad societal impacts. A rigid rule-based system might be insufficient to address these challenges, as these problems often require nuanced responses that take the greater good into account, which a strict deontological approach may overlook.

3.2 Consequentialism

Consequentialism is an ethical theory that judges the rightness or wrongness of an action based solely on its outcomes or consequences. In other words, the morality of an action is determined by the effects it produces. The best-known form of consequentialism is utilitarianism, but there are other consequentialist theories with different criteria for evaluating outcomes.

Consequentialism is a moral philosophy that evaluates the ethical value of actions based on their outcomes or consequences. Consequentialism asserts that the ethical value of an action is directly tied to the good or harm it produces. Actions that result in positive consequences are considered morally good, while those that result in harm or negative consequences are deemed morally wrong. [43] This approach centers on the idea that the rightness or wrongness of an action depends not on the action itself, nor the actor's intentions, but on the results it produces. In healthcare, administering a risky treatment to save a patient's life might be considered ethically sound under consequentialism because

the positive outcome (saving a life) outweighs the potential harm (risk of side effects). Many forms of consequentialism, such as utilitarianism [43], aim to maximise overall well-being or happiness. The morally right action is the one that produces the greatest net benefit for the largest number of people. For example, a government imposing strict lockdowns during a pandemic may justify the action as ethical because it prevents widespread harm, even if it restricts individual freedoms temporarily.

There are multiple types of consequentialism, for example, utilitarianism [43], rule consequentialism [44], state consequentialism [45], ethical egoism [46], two-level consequentialism [47], motive consequentialism [48], and negative consequentialism [49]. Utilitarianism was developed by philosophers Jeremy Bentham and John Stuart Mill; utilitarianism is the most popular consequentialist approach. It holds that actions are right if they promote the greatest happiness for the greatest number, often referred to as maximising utility. [43]

Egoistic consequentialism argues that individuals should act in ways that maximise their own long-term happiness or well-being. In altruistic consequentialism actions are judged solely by how much they benefit others, sometimes even at the expense of one's own welfare. In rule consequentialism, rather than judging individual actions, rule consequentialism evaluates the morality of following rules that generally lead to the best consequences. This approach allows for some stability and predictability, as rules are designed to yield positive outcomes if followed consistently. [47]

Qonsequentialism's strengths lie in pragmatism and flexibility and focus on welfare and outcomes. Consequentialism adapts well to complex and varied situations because it assesses the specific results of an action, allowing for more context-based decision-making. By focusing on the outcomes of actions, consequentialism provides a straightforward approach to evaluate moral decisions: the right action is the one that produces the best overall results. This outcome-focused framework is often useful in real-world applications, such as policy-making, public health, and business ethics, where achieving

beneficial outcomes is crucial. Consequentialism supports humanitarian and progressive causes, including public health, environmental conservation, and human rights, by emphasising positive outcomes and minimising harm.

Consequentialism is well-suited for tackling modern ethical challenges, including those related to technology, global health, and environmental sustainability. For instance, in climate ethics, a consequentialist approach can weigh the far-reaching impacts of carbon emissions and climate policies, encouraging actions that would lead to the greatest benefit for the environment and future generations. This adaptability to large-scale, complex problems makes consequentialism a valuable tool in areas requiring an assessment of widespread impact. The outcome-based nature of consequentialism provides clarity, as it allows for a more quantitative approach to ethical decisions. [43]

Consequentialism requires individuals to consider the effects of their actions on others, promoting a sense of responsibility for the broader consequences of their decisions. [43] This sense of accountability is integral in both personal and public ethical decisions, encouraging people and institutions to consider how their actions will impact the well-being of others. Consequentialism's focus on maximising outcomes also enables it to balance competing values and interests by weighing the pros and cons of different courses of action.

Then again, it can be difficult to accurately predict any action's full range of consequences, especially in complex scenarios. Consequentialism can also justify morally questionable actions if they lead to a greater good, potentially violating individual rights. For instance, sacrificing one person's welfare to benefit many others could be justified within a strict consequentialist framework.

Consequentialism relies heavily on assessing future consequences, but these can be uncertain, especially in complex situations with far-reaching impacts. For example, in policy-making, actions intended to create positive social change (like economic reforms) can sometimes produce unintended side effects that are hard to foresee. This unpre-

dictability makes it difficult to consistently apply consequentialist principles, as even well-intentioned actions may inadvertently cause harm.

Consequentialism, particularly utilitarianism, is sometimes criticised for its potential to justify actions that violate individual rights or justice if they lead to a greater overall benefit. This is often illustrated in trolley problem-like scenarios where sacrificing one individual might save multiple others. [43] It can be argued that this approach can lead to morally problematic situations where the rights of minorities or individuals are disregarded, treating people as mere means to achieve the greatest good for the majority. For example, consequentialism could, in theory, justify punitive policies like scapegoating or even sacrificing innocent people if it were to maximise social welfare—a view that many find morally unacceptable. Consequentialism often demands a high level of sacrifice from individuals, which some argue is unreasonable. The theory implies that people should continuously act to maximise positive outcomes, which could mean forgoing personal happiness, resources, or well-being to benefit others. Critics highlight that this high standard may be unsustainable or impractical, especially if it requires individuals to act against their own interests or the interests of loved ones. This demandingness can create moral burnout or, alternatively, encourage people to disengage from moral considerations altogether. [44]

One of the critical blind spots of utilitarianism lies in its rigid focus on maximizing overall happiness or utility, which can lead to morally questionable conclusions when analyzing individual cases. The theory's framework suggests that if all other conditions remain unchanged, and an action improves the well-being of even one individual without negatively impacting others, the action is morally justified. While this may seem straightforward, it raises significant ethical concerns. Utilitarianism focuses on the total sum of happiness or utility, often sidelining the distribution of that happiness. The happiness of one individual can outweigh concerns about fairness or moral intuitions if it increases the total utility. The principle can lead to morally perplexing scenarios where individual

rights and dignity are disregarded in favor of the aggregate good. For example, a minor increase in one person's happiness might justify intrusive or unfair actions if they leave the happiness of others unaffected.

The focus on outcomes is often criticised for ignoring the moral significance of intentions and character. For example, a well-meaning act that results in harm would be judged as morally wrong in consequentialist terms, even if the intent was to do good. This can lead to moral evaluations that many find counterintuitive, as it dismisses the importance of an agent's motives or ethical character. Utilitarian versions of consequentialism aim to maximise "utility" or "happiness," but measuring and comparing happiness across different people is inherently challenging. For instance, how does one accurately quantify the happiness that one action brings versus another? Moreover, how can happiness be weighed against other values, like autonomy or dignity, that people may find equally important? Consequentialist theories often struggle with this quantification, as they oversimplify complex human experiences into measurable units of "good" or "happiness." [44]

Consequentialism may require us to treat everyone's interests equally, which can conflict with personal relationships or duties. For instance, a parent might feel an obligation to prioritise their child's well-being over that of strangers, but strict consequentialism could demand impartiality. This requirement to ignore "special obligations" or personal ties can feel unrealistic and ethically undesirable, as it overlooks the moral significance of personal relationships and commitments that are central to many people's lives. Consequentialist outcomes can depend on factors outside an individual's control, a concept known as "moral luck." For instance, two people might perform identical actions with the same intent, but one could result in positive consequences while the other results in harm due to unforeseeable circumstances. Critics argue that moral evaluations based on luck undermine fairness, as individuals should not be held responsible for outcomes beyond their control.

Consequentialism has wide-ranging applications, especially in areas where decisions have complex outcomes that impact many people. Consequentialism is often applied in public policy because policymakers must weigh the potential benefits and harms of regulations on society. Policies designed to maximise public welfare, reduce harm, and promote equality often rely on consequentialist principles. For instance, during public health crises (like pandemics), consequentialist reasoning supports measures like lockdowns, surveillance through GPS or vaccination mandates if they are expected to save lives and prevent widespread illness despite potential individual inconveniences or freedoms being restricted.

3.3 Virtue ethics

Virtue ethics began with Socrates and was later developed further by Plato, Aristotle and Stoics [50]. Virtue ethics focuses on cultivating moral character rather than simply following rules (as in deontology) or maximising outcomes (as in utilitarianism). Virtue ethics asks not "What should I do?" but rather "What kind of person should I be?" Its central idea is that by developing good habits or virtues (qualities like courage, kindness, honesty, and wisdom), a person can lead a morally fulfilling life and make ethical decisions more naturally. [51]

Virtues are positive character traits that allow individuals to flourish and fulfil their potential. Aristotle identified various virtues, such as courage, temperance, justice, and wisdom, which he believed were essential for achieving eudaimonia, often translated as "flourishing" or "well-being." [52] Virtue ethics posits that by cultivating these traits, individuals will tend to make good moral choices in diverse situations. [53]

Aristotle argued that virtue is often found between two extremes, known as vices. For example, courage lies between recklessness (an excess) and cowardice (a deficiency). Generosity lies between wastefulness (an excess) and stinginess (a deficiency). By aim-

ing for this "mean" or balance, virtue ethics seeks a harmonious development of character traits. [52] Virtue ethics emphasises the importance of practising virtues until they become habitual. It's not enough to simply know what the right action is; one must practice it consistently. Through habit and education, individuals can cultivate virtues that align with their reason and emotions, ultimately shaping their moral character. Virtue ethics also recognises the importance of role models—figures we admire and aspire to emulate. Aristotle believed that observing and learning from virtuous individuals in one's community fosters moral growth and development. This social aspect of virtue ethics highlights the role of relationships and social environments in shaping our character. [52]

By prioritising personal development, virtue ethics offers a more holistic view of ethics, where moral decisions are a natural result of a well-cultivated character. Unlike rigid rule-based systems, virtue ethics considers individual circumstances and moral complexities, encouraging a more adaptable approach. However, virtue ethics can be vague in specific situations since it doesn't prescribe clear rules for action. For example, while courage is a virtue, virtue ethics may not precisely indicate when and how to act courageously in a complex moral dilemma. Also, the interpretation of virtues can vary across cultures and individuals, leading to disagreements about what traits are most important or how they should be practiced. [52]

Virtue ethics prioritises the development of good character traits, such as honesty, kindness, and courage, which guide people to act ethically across various situations. Rather than focusing on isolated actions, virtue ethics emphasises becoming a morally good person. This holistic approach encourages continuous self-improvement and self-reflection, aiming to cultivate a well-rounded moral character over time. Unlike deontological or consequentialist ethics, which often rely on rigid rules or outcome-focused calculations, virtue ethics is adaptable and context-sensitive. It recognises that ethical decisions are nuanced and situational. This flexibility allows individuals to apply virtues differently depending on the circumstances, accommodating real-life complexity where

straightforward rules might be inadequate. For instance, virtues like courage, humility, or patience may need to be applied differently in personal relationships, workplaces, or public life. [51]

Virtue ethics acknowledges the role of emotions and relationships in moral life, which some other ethical theories may overlook. By integrating emotional intelligence and empathy into the cultivation of virtues, it presents a more comprehensive and realistic view of moral motivation. This approach emphasises that emotions are not just obstacles to rational decision-making but can guide individuals toward moral insights and help build caring relationships. Rather than simply following rules or calculating outcomes, individuals are encouraged to live meaningfully by developing virtues that lead to personal fulfilment and community well-being. This focus on living a fulfilling and purposeful life offers a motivating and aspirational vision of ethics that appeals to those who view moral behaviour as integral to human happiness. [51]

Virtue ethics is particularly effective in addressing moral issues within interpersonal relationships, where virtues like compassion, loyalty, and kindness guide actions. It encourages people to consider how their actions affect others on a deeper, relational level, promoting trust and mutual respect. In this sense, virtue ethics is well-suited to family, friendship, and community dynamics, where impersonal rule-following or outcome-focused thinking may feel inadequate.

One of the main criticisms is that virtue ethics does not provide clear guidelines for action. Unlike consequentialism or deontology, which offer more direct rules (like maximising happiness or following moral laws), virtue ethics focuses on character development without offering specific instructions for how to act in particular situations. This can be problematic, as people might find it challenging to know the "right" thing to do in complex or unfamiliar moral dilemmas. [51] It can be argued that virtue ethics, by emphasising character over action, lacks practical applicability in urgent or high-stakes decisions.

Virtue ethics depends heavily on the interpretation of virtues, which can vary widely across cultures. For example, virtues like honesty, humility, or courage might have different expressions or even levels of importance in different societies. This cultural relativity makes it challenging to define a universal set of virtues. Critics, therefore, argue that virtue ethics risks endorsing practices simply because they align with cultural norms rather than because they are inherently moral.

Defining what constitutes a "virtue" is another point of contention. For example, virtues like "courage" or "generosity" can be interpreted differently depending on the context, and it is not always clear what the "mean" between two extremes (Aristotle's "Doctrine of the Mean") would look like in practice [54]. This can lead to vagueness and inconsistencies, as individuals may understand virtues in different ways, which can lead to conflicting actions even among virtuous people.

Virtue ethics is susceptible to the problem of "moral luck," which suggests that factors beyond a person's control can influence their ability to be virtuous [55]. For instance, individuals raised in challenging or unethical environments might struggle to develop virtues through no fault of their own. This can make virtue ethics seem unfairly demanding since not everyone has the same opportunities to cultivate a virtuous character. A fair ethical theory should account for circumstances and offer moral worth that isn't tied to one's upbringing or luck in moral education. It is also often critiqued for emphasising character and motivation over the consequences of actions or adherence to moral rules. Focusing solely on the agent's virtue in high-stakes scenarios might lead to morally questionable outcomes. [55] [51] For instance, a "courageous" act could unintentionally lead to harm, and virtue ethics would focus more on the virtue of courage rather than the harm caused. This focus on character can sometimes disregard practical outcomes or rights, potentially overlooking the well-being of those affected by an action.

Virtue ethics is less equipped to address modern ethical challenges, such as technology, environmental crises, or global injustice. Many of these issues involve complex sys-

tems and far-reaching consequences that are difficult to address through personal virtues alone. For example, addressing mass surveillance requires systemic changes and policies rather than simply encouraging individuals to act virtuously.

Having established the theoretical foundation through deontology, consequentialism, and virtue ethics, the next logical step is to apply these frameworks to evaluate the ethical implications of mass surveillance practices. This transition moves from understanding the core principles of each theory to actively engaging with real-world issues, analyzing how these ethical perspectives inform judgments on specific practices and their broader societal impacts.

Chapter 4

Evaluating the impact of mass surveillance

Ethical evaluation of different aspects that mass surveillance affects, such as privacy, autonomy, and security, faces a fundamental challenge: these elements are deeply interconnected. Attempting to discuss any one in isolation risks oversimplifying the issue, as their ethical significance often depends on their relationships with the others. For instance, enhancing security usually impacts privacy and freedom, while increasing transparency may bolster trust but also reduce autonomy. However, insufficient security can leave individuals vulnerable, undermining their privacy in other ways.

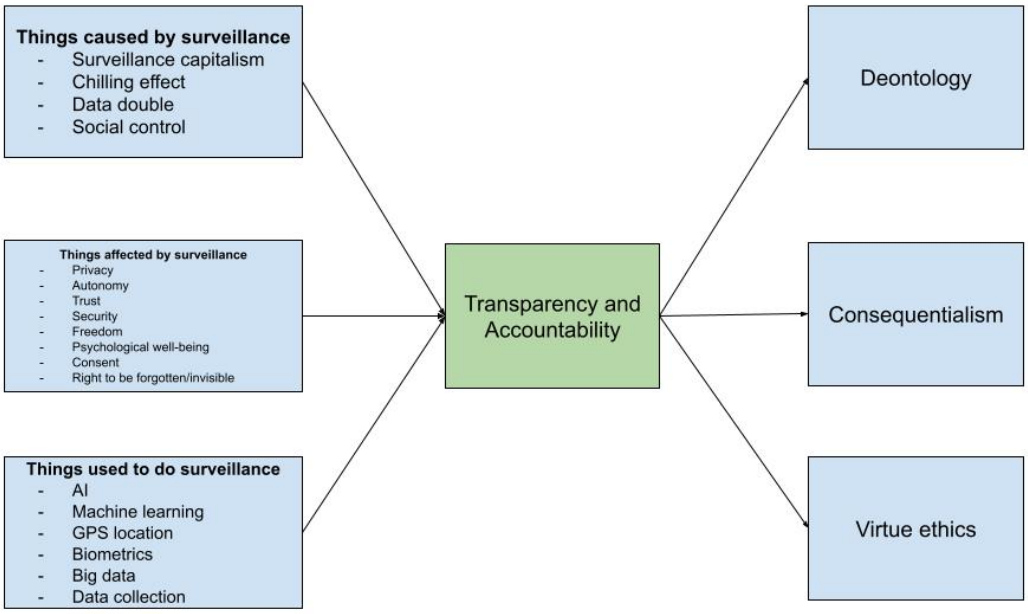
The impact of mass surveillance on different aspects can be categorised into three larger groups: Things **caused** by surveillance, Things **affected** by surveillance, and Things used to **do** surveillance. The first category includes aspects like surveillance capitalism and the chilling effect. Surveillance capitalism occurs when corporations monetise personal data and transform users into products. Platforms use surveillance data to manipulate consumer behavior, fostering dependency and reducing autonomy. The chilling effect is included in the list because individuals alter their behaviour due to the fear of surveillance, inhibiting freedom of expression and creativity.

The second category includes, e.g. privacy, autonomy, and trust. Privacy safeguards autonomy by allowing individuals control over their personal information. Trust in institutions and relationships can erode under pervasive surveillance, as individuals fear misuse of their data.

The third category includes AI and machine learning, biometrics, and big data. AI and ML analyse vast datasets to predict behavior or flag anomalies, often raising concerns about bias and transparency. Biometrics are used for identification and raise concerns about consent, misuse, and invasiveness.

Transparency and accountability do not belong in any category because they act as evaluative tools that determine the moral justification of all other categories. Transparency helps clarify the purpose and scope of surveillance, ensuring that stakeholders understand its implications. Accountability ensures that those responsible for surveillance uphold ethical practices, address abuses, and implement safeguards. With those, we can look more closely at the individual aspects and evaluate them through the lens of ethical theories. Both transparency and accountability are crucial for building and maintaining trust between individuals, organizations, and society. Trust is an ethical cornerstone because it allows for cooperation and the smooth functioning of social structures.

While the application of transparency and accountability might vary depending on the context (e.g., limited transparency during emergencies), their ethical foundation is universally seen as "good" because they prevent deception and exploitation, promote fairness and justice, enhance trust and cooperation, and align with moral virtues and societal expectations. In essence, transparency and accountability are universally valued because they are integral to ethical governance, equitable social interactions, and the preservation of individual rights.



From a deontological perspective, mass surveillance poses significant ethical challenges due to its impact on individual rights, especially the right to privacy. Deontologists, especially followers of Kantian ethics, emphasise the importance of respecting individuals as ends in themselves rather than merely as means to an end. Privacy is considered an intrinsic right that safeguards personal autonomy, dignity, and individuality. Consequently, deontology argues that violating an individual's privacy is morally unacceptable, even if such a violation is intended to achieve greater security or social benefit. [41]

One of the critical issues in analysing mass surveillance from a deontological lens is the potential conflict between the duty to protect society and the duty to respect individual privacy. Governments and institutions may argue that they have a moral duty to protect their citizens from harm, including threats such as terrorism, cybercrime, and other security risks. However, a deontologist would argue that the duty to respect individual rights—such as privacy—should not be compromised for the sake of another duty, as it

sets a precedent for justifying rights violations under certain conditions, which contradicts the rule-based nature of deontology. [41]

Consequentialism, and specifically utilitarianism, assesses the morality of actions by focusing on the outcomes they produce. When applied to mass surveillance, a consequentialist perspective examines whether the benefits of surveillance (such as increased security, crime prevention, and the protection of public welfare) outweigh the negative consequences (such as privacy invasion, potential misuse of data, and psychological impacts). According to this viewpoint, mass surveillance can be considered morally justifiable if it leads to a net positive impact on society. [43]

This approach prompts a detailed cost-benefit analysis of surveillance systems. For instance, the argument that mass surveillance is essential for national security could be examined against the extent of privacy invasion and potential societal harm caused by continuous data monitoring. In this analysis, a consequentialist would support mass surveillance if the data collected and monitored genuinely reduces crime rates and terrorism, as well as improves public safety, creating a greater good that justifies individual privacy sacrifices. [43]

Virtue ethics approaches mass surveillance by examining the character and motivations of those who implement and enforce surveillance systems. Unlike deontology and consequentialism, which focus on rules and outcomes, respectively, virtue ethics is concerned with the moral character and virtues of individuals and institutions involved in surveillance. This perspective asks whether mass surveillance practices foster virtues such as integrity, honesty, respect, and responsibility. The focus here is not solely on whether surveillance is legally permissible or has beneficial outcomes but on whether it aligns with moral character and virtuous intentions. [51]

In the context of surveillance, virtue ethics encourages us to question the motivations behind surveillance initiatives. For instance, if surveillance is conducted transparently and with the aim of genuinely protecting citizens, it may reflect virtues of care, respon-

sibility, and prudence. However, if surveillance is driven by control, profit, or political gain, it risks embodying vices such as manipulation, dishonesty, or even exploitation. Virtue ethics thus promotes a self-reflective approach to surveillance, where authorities' motivations play a crucial role in determining its ethical validity. [51]

Below is a breakdown of how deontology, consequentialism, and virtue ethics evaluate the morality of mass surveillance as it impacts the listed aspects. If mass surveillance affects it positively, it is ethical; if mass surveillance has a negative effect, it is unethical. If something has "depends" on it, the effects can be good or bad depending on how it is used, or in virtue ethics, what virtues are fostered while using it. For example, consequentialism evaluates biometrics based on their outcomes. If biometric systems improve security, reduce crime, and prevent harm, their use might be justified. However, if the societal harms—such as discrimination, chilling effects, and misuse—outweigh the benefits, they are deemed unethical. Furthermore for example, In virtue ethics, the ethicality of AI depends on how it aligns with virtuous practices such as fairness, accountability, and respect. If AI systems are designed to foster trust and transparency, they may be viewed as ethical; otherwise, they promote vices like exploitation.

Aspects	Deontology	Consequentliasm	Virtue Ethics
Transparency	Ethical	Ethical	Ethical
Accountability	Ethical	Ethical	Ethical
Privacy	Unethical	Depends	Unethical
Autonomy	Unethical	Depends	Unethical
Trust	Unethical	Depends	Unethical
Security vs freedom	Unethical	Depends	Depends
Data collection	Depends	Depends	Depends
Psychological well-being	Unethical	Depends	Unethical
Consent	Ethical	Depends	Ethical
Social control	Unethical	Depends	Unethical
Big data usage	Depends	Depends	Depends
Surveillance capitalism	Unethical	Unethical	Unethical
Chilling effect	Unethical	Unethical	Unethical
Biometrics	Unethical	Depends	Depends
Right to be forgotten and invisible	Ethical	Depends	Ethical
AI usage	Unethical	Depends	Depends
Machine learning usage	Unethical	Depends	Depends
GPS location usage	Unethical	Depends	Unethical
Data double	Unethical	Depends	Depends

Table 4.1: Evaluating the impact of mass surveillance on different aspects

From the table can be seen how rigid deontology is. Deontology is rooted in strict adherence to moral duties and rules, emphasizing principles over outcomes. This rigidity is evident in its consistent classification of many aspects as either "Ethical" or "Unethical," with little room for contextual nuance. Consequentialism evaluates actions based on their outcomes, making ethical judgments highly dependent on context. Virtue ethics

evaluates actions based on whether they align with virtuous behaviour and societal values. This leads to varied and context-dependent moral justifications: privacy, autonomy, and trust are "Unethical" if they undermine virtuous character traits such as respect and dignity. However, many aspects (e.g., data collection, big data usage, AI usage) are classified as "Depends," as their ethical evaluation hinges on whether they align with virtuous intentions and promote societal flourishing.

Deontology provides clear-cut answers based on universal principles but lacks adaptability. Consequentialism focuses on outcomes, offering flexibility but risking moral compromises. Virtue ethics centres on character and societal values, making it highly contextual and nuanced. This table illustrates how these theories can lead to vastly different conclusions when evaluating the same aspects, highlighting the need for comprehensive ethical analysis.

But it would not be feasible to go over every aspect and how mass surveillance affects them in depth through the lens of the three ethical theories, which is why next, I focus solely on data double. The concept of the data double refers to the digital profile created through the aggregation of an individual's data across multiple sources, as described in Chapter Two. It serves as a virtual representation of a person, often used by organisations, governments, and corporations for purposes such as targeted advertising, decision-making, and surveillance. While its practical applications can be beneficial, the ethical implications of creating and utilising data doubles raise significant questions.

4.1 Deontology

A fundamental tenet of deontology is the duty to respect the autonomy of individuals. This requires that individuals be fully informed about and provide explicit consent for how their data is collected, processed, and used. In the context of data doubles, this principle is frequently violated. Data is often collected without clear, informed consent,

and individuals are rarely aware of the full extent to which their data is used to create profiles that influence their lives. Kantian ethics would argue that this lack of transparency and consent violates the moral duty to treat individuals as autonomous agents capable of making informed decisions about their data.

Kant's categorical imperative asserts that one should act only according to maxims that can be universally applied. In the case of data doubles, the question arises: Can the practice of aggregating and using personal data without explicit consent be universalised without contradiction? If every organisation engaged in such practices, it would lead to a surveillance culture where personal autonomy and privacy are systematically undermined. According to deontology, such a practice would fail the universality test because it would erode the foundational principles of trust and respect necessary for ethical social interactions.

Deontology demands that individuals be treated as ends in themselves, not merely as means to an end. The creation and use of data doubles often reduce individuals to data points, using their profiles for purposes such as profit maximisation, predictive analytics, or surveillance. This commodification of personal data clearly violates the Kantian duty to respect human dignity. By treating individuals as tools for achieving organisational goals, data double practices fail to honour the intrinsic worth of each person.

Governments and organisations may argue that the creation of data doubles serves a greater good, such as public safety or economic efficiency. However, from a deontological perspective, utilitarian calculations of benefit cannot override the duty to respect individual rights and dignity. For instance, while data doubles might help identify security threats, the indiscriminate use of surveillance data risks violating the privacy and autonomy of countless individuals who are not threats. Data double practices often involve multiple stakeholders, including corporations, governments, and third-party data brokers. A deontological critique must consider the responsibilities of all parties involved and ensure that each entity adheres to moral principles.

To align data double practices with deontological ethics, the following measures should be adopted: Organisations must implement transparent data collection policies and provide clear, accessible information about how data will be used. Individuals should be able to give or withdraw consent at any point, ensuring respect for their autonomy. Governments and international bodies should establish strict regulations to prevent the misuse of data doubles and hold organisations accountable for ethical lapses. Regular audits and assessments can ensure compliance with moral duties. Developers and data scientists should adopt ethical design principles that prioritise the dignity and autonomy of individuals, minimising risks such as bias and misuse.

4.2 Consequentialism

Consequentialism, which evaluates the morality of actions based on their outcomes, provides a robust framework for analysing the benefits and harms of data double practices. By focusing on the consequences for individuals and society, consequentialialism highlights the potential for both profound advantages and significant risks.

Data doubles allow for tailored services and personalised experiences. For example, in healthcare, digital profiles enable predictive analytics that can foresee medical conditions and optimise treatment. In commerce, personalised advertising ensures that consumers receive relevant information, improving their decision-making experience. From a consequentialist standpoint, these outcomes maximise overall utility, contributing to societal well-being and individual satisfaction.

Data doubles can aid in crime prevention and national security efforts through predictive policing and threat detection. For example, tracking suspicious activities based on aggregated data can prevent terrorism or fraud. These outcomes promote the greater good by enhancing collective safety, aligning with consequentialist principles.

Aggregated data doubles fuel research in fields such as artificial intelligence, epidemi-

ology, and social sciences, leading to innovations that improve lives. For instance, during the COVID-19 pandemic, data doubles played a crucial role in tracking infection rates and developing targeted interventions, demonstrating their potential to generate positive outcomes on a global scale.

The creation and use of data doubles often occur without informed consent, leading to significant privacy concerns. Individuals may lose control over their information, resulting in a sense of disempowerment. The harm caused by such invasions of privacy can outweigh the benefits, especially when sensitive data is exposed or misused, undermining trust and security.

Data doubles often reflect and reinforce existing biases within datasets, leading to discriminatory practices. For example, biased algorithms may disproportionately target minority groups for policing or deny them access to loans. These outcomes result in harm to vulnerable populations, reducing societal utility and contradicting the consequentialist aim of maximising collective well-being.

When data doubles are used for mass surveillance, they contribute to an environment of constant monitoring, stifling free expression and eroding trust in institutions. Examples include China's social credit system, where data doubles are used to control and punish behaviour, raising concerns about authoritarianism and societal harm.

The knowledge of being constantly monitored can lead to anxiety, stress, and a sense of helplessness, diminishing individuals' quality of life. Such psychological impacts create negative consequences that are difficult to justify under consequentialist principles.

A consequentialist analysis requires weighing the potential benefits of data doubles against their harms. When benefits dominate, for example, in cases where data doubles demonstrably enhances public welfare, such as improving healthcare outcomes or advancing research, they can be ethically justified. For example, using data doubles to combat pandemics saves lives, significantly increasing utility. However, when harms dominate, the risks of privacy violations, bias, and surveillance outweigh the benefits, and data dou-

bles may fail to meet the consequentialist criteria for ethical acceptability. For instance, systems that prioritise profit over individual rights or use data for manipulative purposes create more harm than good.

Consequentialism supports adopting robust safeguards to minimise harms, such as stronger data protection laws, transparency requirements, and ethical design principles. Ensuring that data doubles are created and used with informed consent and fairness can amplify their benefits while reducing negative consequences. Addressing algorithmic bias and ensuring equitable treatment of all individuals can help mitigate the harms of discrimination and inequality. Consequentialism would endorse systems that actively reduce disparities and contribute to a more just society. Striking a balance between leveraging data doubles for innovation and protecting individual privacy aligns with the consequentialist goal of maximising overall utility. Tools such as differential privacy and secure data-sharing protocols can help achieve this balance.

4.3 Virtue ethics

Unlike deontology and consequentialism, which focus on rules and outcomes, virtue ethics emphasises the character and intentions of those creating, managing, and using data doubles. This perspective evaluates whether actions related to data doubles cultivate virtuous qualities like justice, honesty, and respect or promote vices like greed and exploitation.

Virtue ethics, rooted in the philosophy of Aristotle, is concerned with the cultivation of virtues—traits of character that enable individuals and societies to flourish (eudaimonia). In analysing data doubles, the focus shifts from the mere act of collecting data or its consequences to the moral character and virtues of those involved in these practices. A virtuous actor prioritises the well-being of individuals and society. For instance, a health organisation using data doubles to develop personalised treatments demonstrates

benevolence and compassion. In contrast, corporations that exploit data doubles for manipulative advertising or invasive surveillance reflect greed and dishonesty, undermining societal trust and well-being.

Respecting the privacy of individuals and ensuring their dignity in the creation and use of data doubles aligns with virtues like justice and respect. Ethical practices might include obtaining informed consent, ensuring data security, avoiding intrusive surveillance, and reflecting virtuous care for others. Virtue ethics emphasises the importance of trust and solidarity in fostering a thriving society. Data doubles can strengthen community trust and collaboration when used transparently and ethically. Conversely, opaque practices that misuse data doubles for hidden agendas erode trust, reflecting vices like deceit and negligence.

Possible positive applications of data doubles include instances, when designed and used virtuously data doubles can enhance individual and collective well-being. For example, tailored medical interventions based on data doubles can alleviate suffering and improve health outcomes in healthcare. Personalised learning experiences foster intellectual growth in education, reflecting the virtues of care and prudence. Ethical use of data doubles can address systemic inequities. For example, analysing data to identify underserved communities aligns with justice, ensuring fair access to resources and opportunities. Research and innovation driven by data doubles should be guided by integrity and curiosity, aiming to solve societal challenges while respecting ethical boundaries.

Whereas the use of data doubles also has challenges, data doubles are often used to maximise profits at the expense of privacy, reflecting a disregard for virtuous conduct. Hidden data collection practices undermine transparency, violating trust and respect. Algorithms built on biased data doubles perpetuate inequality, contradicting the virtue of justice. For instance, predictive policing based on biased data reinforces systemic discrimination. Reducing individuals to data profiles risks neglecting their humanity. This depersonalisation reflects a lack of empathy and respect, as it treats people as mere tools

for analysis.

Virtue ethics does not prescribe strict rules but encourages continuous reflection on the cultivation of good character. For data double practices, this involves prioritising transparency and honesty, designing systems for human flourishing, and minimising harm and exploitation. Open communication about how data doubles are created and used fosters trust and respect. Ensuring that the primary goal of data doubles is to promote well-being and equitable outcomes aligns with virtues like compassion and justice. Ethical practitioners must actively counteract biases and misuse of data, reflecting virtues of responsibility and integrity.

From the perspective of virtue ethics, the data double is not inherently good or bad but is ethically judged by the character and intentions of those involved in its lifecycle. Practices that align with virtues such as honesty, justice, and respect can transform data doubles into tools for societal and individual flourishing. However, when driven by vices like greed and deceit, data doubles risk becoming instruments of harm. Virtue ethics calls for an ongoing commitment to moral excellence in the design and use of data doubles, ensuring they contribute positively to human flourishing and a just society.

Chapter 5

Conclusion

This thesis has explored the ethical implications of mass surveillance through the lenses of the three main theories: deontology, consequentialism, and virtue ethics. It has analysed how these theories provide perspectives on critical aspects such as privacy, autonomy, trust, and security, focusing on data double. As mass surveillance technologies become increasingly pervasive, the ethical evaluation of their deployment remains complex and multifaceted, influenced by technological advancements, societal values, and regulatory landscapes.

The second chapter introduced the foundational aspects of mass surveillance, detailing its scope, mechanisms, and terminology. The chapter defined critical terms such as dataveillance, metadata, and the data double, establishing a framework to understand the pervasive nature of data collection in contemporary society. The Panopticon was explored as a metaphor for surveillance systems, highlighting how visibility fosters control and behavioural conformity. I also went over trends that came up when researching the subject, like COVID-19, facial recognition, AI, and machine learning. The pandemic accelerated surveillance efforts, including contact tracing and public health monitoring, raising concerns about proportionality and scope creep. AI and machine learning technologies emerged as dominant tools in surveillance, enabling automation and scalability but also introducing issues like bias and lack of oversight. And finally, Schrems Cases: These

landmark legal battles emphasised cross-border data flow concerns, challenging global companies on compliance with data privacy laws and highlighting the ongoing battle between governance and companies doings.

Chapter three laid the theoretical foundation by introducing what ethics is, different brances of ethics and the three major ethical frameworks to evaluate mass surveillance: deontology, consequentialism, and virtue ethics. Deontology centers on duty and principles, emphasising the moral imperative to respect individual rights, autonomy, and privacy. It framed mass surveillance as problematic when it violates these intrinsic rights. Consequentialism evaluates actions based on their outcomes, providing a flexible approach to analyse the benefits and harms of surveillance, such as enhanced security versus the chilling effect on personal freedoms. Virtue ethics focuses on character and societal values, considering whether surveillance practices cultivate virtues like trust, accountability, and fairness or foster vices like manipulation and exploitation.

This thesis aimed to find answers to two research questions: RQ1: How do different ethical theories evaluate the moral implications of mass surveillance? And RQ2: How do these theories assess the existence and use of data doubles?

Chapter Four applied the three ethical theories to critically evaluate mass surveillance and concept of a data double. The analysis revealed that mass surveillance is a complex and multifaceted issue, where moral evaluations depend heavily on the framework applied.

Deontology offered a rigid perspective, emphasizing the inherent rights of individuals. It classified practices such as data collection, privacy violations, and lack of consent as unethical due to their intrinsic violation of autonomy and moral duty. This approach underscores the principle that actions cannot be justified solely by their outcomes, regardless of their benefits. Consequentialism, in contrast, evaluated surveillance practices based on their outcomes. While it justified surveillance in cases where security or public safety was significantly enhanced, it also flagged the risks of harm, such as psychological

distress or societal manipulation, as critical factors in ethical evaluation. This flexible but outcome-dependent approach highlighted the nuanced trade-offs involved. Virtue Ethics emphasized the character and virtues that surveillance practices reflect in society. It advocated for practices aligned with virtues such as trust, transparency, and fairness. It also underscored the importance of societal values, recognizing that the moral implications of surveillance depend on whether it fosters or undermines virtuous behavior.

To better understand the ethical implications of mass surveillance, this thesis introduced a categorization of relevant aspects into three broad groups: Things caused by surveillance: This includes phenomena such as surveillance capitalism, the chilling effect, social control, and the creation of data doubles. These outcomes reflect the systemic consequences of surveillance and their potential to influence societal norms. Things affected by surveillance: This category encompasses privacy, autonomy, trust, psychological well-being, freedom, and consent. These aspects represent fundamental human rights and values that surveillance practices can either uphold or compromise. Things used to do surveillance: This includes technologies and methods such as AI, machine learning, GPS location tracking, biometrics, big data usage, and data collection. These tools enable surveillance but also introduce ethical challenges related to their use and oversight.

Transparency and Accountability: These were treated as overarching principles that must guide the evaluation of all categories. Without transparency and accountability, it becomes impossible to assess whether surveillance practices align with ethical standards.

The analysis revealed how the theories align and diverge in their evaluations. Deontological analysis often deems both mass surveillance and the creation of data doubles as unethical due to violations of autonomy, privacy, and informed consent. For instance, the data double reduces individuals to mere data representations, undermining their intrinsic dignity and the principle of treating people as ends rather than means. Consequentialists may justify both practices if the benefits outweigh the harms. Data doubles can support personalised services, enhanced public safety, or societal efficiency, but their ethical

acceptability hinges on minimising negative outcomes such as profiling, discrimination, and misuse of data. From a virtue ethics perspective, the morality of surveillance and data doubles depends on the societal virtues or vices they promote. Practices fostering trust, fairness, and accountability are viewed as virtuous, whereas those enabling manipulation or eroding public confidence are seen as unethical.

By addressing these research questions, the thesis illuminated the ethical complexities of mass surveillance and data doubles. Mass surveillance raises profound ethical challenges that resist simple solutions. By exploring it through deontology, consequentialism, and virtue ethics, this thesis underscored the importance of pluralistic and context-sensitive evaluations. Each ethical theory offers unique insights, revealing tensions between rights, outcomes, and character. Ultimately, the ethical acceptability of surveillance practices depends on striking a balance between societal benefits and individual rights, guided by a commitment to transparency and accountability. This nuanced understanding underscores the importance of ethical scrutiny and context-aware practices in the deployment of surveillance technologies.

References

[1] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and W. R.B.J., "After snowden: Rethinking the impact of surveillance," *International Political Sociology*, vol. 8, no. 2, pp. 121–144, 2014.

[2] S. Ribeiro-Navarrete, J. R. Saura, and D. Palacios-Marqués, "Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy," *Technological Forecasting and Social Change*, vol. 167, pp. 636–656, 2021. [Online]. Available: https://doi.org/10.1016/j.techfore.2021.120681

[3] "Judgment of the court (grand chamber) of 16 july 2020. data protection commissioner v facebook ireland limited and maximillian schrems." 2020. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62018CJ0311

[4] R. Clarke, "Information technology and dataveillance," *Communications of the ACM*, vol. 31, no. 5, pp. 498–512, 1988. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/42411.42413

[5] S. Zuboff, "Big other: Surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology*, no. 30, pp. 75–89, 2015. [Online]. Available: https://papers.ssrn.com/abstract=2594754

[6] M. Andrejevic and K. Gates, "Big data surveillance: Introduction," *Surveillance & Society*, vol. 12, no. 2, pp. 185–196, 2014. [Online]. Available: https://research.monash.edu/en/publications/big-data-surveillance-introduction

[7] D. E. O'Leary, "Artificial intelligence and big data," *IEEE Intelligent Systems*, vol. 28, no. 2, pp. 96–99, 2013. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6547979

[8] O. Kaynak and S. Yin, "Big data for modern industry: Challenges and trends [point of view]," *Proceedings of the IEEE*, vol. 103, pp. 143–146, 2015.

[9] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," 2015. [Online]. Available: https://www.google.com/url?client=internal-element-cse&cx=015267653312545538371:nexkswtg5_g&q=https://www.internetsociety.org/wp-content/uploads/2021/01/ISOC-IoT-Overview-20151014_0.pdf&sa=U&ved=2ahUKEwiRsKPVt_aKAxUIGBAIHZrDDecQFnoECBUQAg&usg=AOvVaw2KVDACIvbjwWB2r_J5UGxC&fexp=72821495,72821494

[10] A. Meijer and M. Wessels, "Predictive policing: Review of benefits and drawbacks," *International Journal of Public Administration*, vol. 42, no. 12, pp. 1031–1039, 2019. [Online]. Available: https://www.tandfonline.com/doi/epdf/10.1080/01900692.2019.1575664?needAccess=true

[11] M. Kevin, "Total surveillance, big data, and predictive crime technology: Privacy's perfect storm," *Journal of Technology Law & Policy*, vol. 19, no. 1, 2014.

[12] J. Riley, *Understanding metadata: what is metadata, and what is it for*, ser. NISO Primer series. National Information Standards Organization, 2017.

[13] E. Duval, W. Hodgins, S. Sutton, and S. L. Weibel, "Metadata principles and practicalities," *D-Lib Magazine*, vol. 8, no. 4, 2002. [Online]. Available: http://www.dlib.org/dlib/april02/weibel/04weibel.html

[14] "The USA PATRIOT act: Preserving life and liberty." [Online]. Available: https://www.justice.gov/archive/ll/subs/h_patact.htm

[15] R. Creemers, "China's social credit system: An evolving practice of control," 2018. [Online]. Available: https://papers.ssrn.com/abstract=3175792

[16] J. Bentham and M. B, *The Panopticon and Other Prison Writings (Wo Es War)*. Verso Books, 1995.

[17] F. Michel, *Discipline and Punish The Birth of the Prison*. A Division of random house, INC., 1995.

[18] M. Smith and S. Miller, "The ethical application of biometric facial recognition technology," *AI & SOCIETY*, vol. 37, pp. 167–175, 2022. [Online]. Available: https://doi.org/10.1007/s00146-021-01199-9

[19] F. Schauer, "Fear, risk and the first amendment: Unraveling the chilling effect," *Boston University law review*, vol. 58, no. 5, p. 685, 1978.

[20] M. A. Al-garadi, K. D. Varathan, and S. D. Ravana, "Cybercrime detection in online communications: The experimental case of cyberbullying detection in the twitter network," *Computers in Human Behavior*, vol. 63, pp. 433–443, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563216303788

[21] R. EU, "2016/679 of the european parliament and of the council of 27 april 2016 on the protection of naturalpersons with regard to the processing of personal data and on the free movement of such data, and repealing directive95/46," 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[22] J. S. Baik, "Data privacy against innovation or against discrimination?: The case of the california consumer privacy act (CCPA)," *Telematics and Informatics*, vol. 52, 2020.

[23] J. Ball, J. Borger, and G. Greenwald, "Revealed: how US and UK spy agencies defeat internet privacy and security," *The Guardian*, 2013. [Online]. Available: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[24] R. A. Kleinman and C. Merkel, "Digital contact tracing for COVID-19," *CMAJ*, vol. 192, no. 24, pp. E653–E656, 2020. [Online]. Available: https://www.cmaj.ca/content/192/24/E653

[25] S. A. H. Mohsan, Q. u. A. Zahra, M. A. Khan, M. H. Alsharif, I. A. Elhaty, and A. Jahid, "Role of drone technology helping in alleviating the COVID-19 pandemic," *Micromachines*, vol. 13, p. 1593, 2022. [Online]. Available: https://www.mdpi.com/2072-666X/13/10/1593

[26] "Apple and google partner on COVID-19 contact tracing technology." [Online]. Available: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[27] Y. Yang and J. Zhu, "Coronavirus brings china's surveillance state out of the shadows," 2020. [Online]. Available: https://www.reuters.com/article/technology/coronavirus-brings-chinas-surveillance-state-out-of-the-shadows-idUSKBN2011HO/

[28] M. M. Mello and C. J. Wang, "Ethics and governance for digital disease surveillance," *Science*, vol. 368, no. 6494, pp. 951–954, 2020. [Online]. Available: https://www.science.org/doi/full/10.1126/science.abb9045

[29] L. Introna and D. Wood, "Picturing algorithmic surveillance: The politics of facial recognition systems," *Surveillance & Society*, vol. 2, 2002. [Online]. Available: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3373

[30] J. Lynch, “Face off: Law enforcement use of face recognition technology,” *EFF*, 2019. [Online]. Available: https://www.eff.org/wp/face-off

[31] E. Brynjolfsson and T. Mitchell, “What can machine learning do? workforce implications: Profound change is coming, but roles for humans remain,” *Science*, vol. 358, pp. 1530–1534, 2017.

[32] J. R. Saura, D. Ribeiro-Soriano, and D. Palacios-Marqués, “Assessing behavioral data science privacy issues in government artificial intelligence deployment,” *Government Information Quarterly*, vol. 39, no. 4, p. 101679, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0740624X22000120

[33] L. Bennett Moses and J. Chan, “Algorithmic prediction in policing: assumptions, evaluation, and accountability,” *Policing and Society*, vol. 28, no. 7, pp. 806–822, 2018. [Online]. Available: https://doi.org/10.1080/10439463.2016.1253695

[34] “Judgment of the court (grand chamber) of 6 october 2015. maximillian schrems v data protection commissioner.” 2015. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0362

[35] C. Kuner, “Reality and illusion in EU data transfer regulation post schrems,” *German Law Journal*, vol. 18, no. 4, pp. 881–918, 2017. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179440670&doi=10.1017\%2fS2071832200022197&partnerID=40&md5=0509951c696ff358fe497500c336b76f

[36] A. Chander, “Is data localization a solution for schrems II?” *Journal of International Economic Law*, vol. 23, no. 3, pp. 771–784, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85096992721&doi=10.1093\%2fjiel\%2fjgaa024&partnerID=40&md5=a937bfcf5ebc6e07a7ec67d7c266695a

[37] S. Batlle and A. v. Waeyenberge, "EU–US data privacy framework: A first legal assessment," *European Journal of Risk Regulation*, vol. 15, no. 1, pp. 191–200, 2024. [Online]. Available: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/euus-data-privacy-framework-a-first-legal-assessment/6CC12E43F649CD011677E16D9658B73E

[38] J. Dewey and J. H. Tufts, *Ethics*. DigiCat, 2022.

[39] D. Pritchard, *What is this thing called Philosophy?* Routledge, 2015.

[40] B. C. Stahl, "Morality, ethics, and reflection: A categorization of normative is research," *Journal of the Association for Information Systems*, vol. 13, no. 8, pp. 636–656, 2012.

[41] I. Kant, "Foundations of the metaphysics of morals," in *Seven Masterpieces of Philosophy*. Routledge, 2008.

[42] P. Conway and B. Gawronski, "Deontological and utilitarian inclinations in moral decision making: A process dissociation approach," *Journal of Personality and Social Psychology*, vol. 104, no. 2, pp. 216–235, 2013.

[43] J. Bentham and J. S. Mill, *Utilitarianism and Other Essays*. Penguin UK, 2004.

[44] S. Scheffler, *Consequentialism and Its Critics*. Oxford University Press, 1988.

[45] B. W. V. Norden and P. J. Ivanhoe, *Readings in Classical Chinese Philosophy*. Hackett Publishing, 2023.

[46] R. Crisp, *The Cosmos of Duty: Henry Sidgwick's Methods of Ethics*. OUP Oxford, 2015.

[47] W. Sinnott-Armstrong, "Consequentialism," *Stanford Encyclopedia of Philosophy*, 2003. [Online]. Available: https://plato.stanford.edu/entries/consequentialism/?trk=article-ssr-frontend-pulse_x-social-details_comments-action_comment-text

[48] R. M. Adams, "Motive utilitarianism," *The Journal of Philosophy*, vol. 73, no. 14, pp. 467–481, 1976. [Online]. Available: https://www.jstor.org/stable/2025783

[49] M. Haigh, J. S. Wood, and A. J. Stewart, "Slippery slope arguments imply opposition to change," *Memory & Cognition*, vol. 44, no. 5, pp. 819–836, 2016. [Online]. Available: https://doi.org/10.3758/s13421-016-0596-9

[50] P. Gardiner, "A virtue ethics approach to moral dilemmas in medicine," *Journal of Medical Ethics*, vol. 29, no. 5, pp. 297–302, 2003. [Online]. Available: https://jme.bmj.com/content/29/5/297

[51] R. Crisp, M. Slote, and M. A. Slote, *Virtue Ethics*. Oxford University Press, 1997.

[52] Aristotle, *Nicomachean Ethics*. Hackett Publishing, 2019.

[53] R. Hursthouse and G. Pettigrove, "Virtue ethics," in *The Stanford Encyclopedia of Philosophy*, fall 2023 ed., E. N. Zalta and U. Nodelman, Eds. Metaphysics Research Lab, Stanford University, 2023. [Online]. Available: https://plato.stanford.edu/archives/fall2023/entries/ethics-virtue/

[54] P. Losin, "Aristotle's doctrine of the mean," *History of Philosophy Quarterly*, vol. 4, no. 3, pp. 329–341, 1987. [Online]. Available: https://www.jstor.org/stable/27743819

[55] D. K. Nelkin, "Moral luck," *Stanford Encyclopedia of Philosophy*, 2004. [Online]. Available: https://seop.illc.uva.nl/entries/moral-luck/