Surveillance and AI

HS7.301 Science, Technology and Society

Project Report

Srujana Vanka - 2020102005

Shreeya Singh - 2020102011

Sankalp S Bhat - 2020112018

Contents

1 Historical Context

1.1 Evolution of Surveillance Technologies

Surveillance technologies have undergone a dramatic transformation throughout history. From the watchful eyes of guards patrolling castle walls to the presence of CCTV cameras, the methods for monitoring and securing spaces have continuously evolved.

The invention of the printing press in the 15th century facilitated the creation of wanted posters, used to spread information about criminals to a wider population. The telegraph, developed in the 19th century, allowed for faster communication of threats and suspicious activity. The Panopticon was a theoretical prison in the 18th century. It aimed to control inmates through the feeling of being constantly observed, even if the observer was unseen.

The 20th century called for a new era of surveillance with the development of closed-circuit television (CCTV) in the 1940s. These cameras offered a significant leap forward compared to human guards, finding use in a growing range of settings, from traffic monitoring to retail stores. However, as the number of CCTV cameras proliferated, a new challenge emerged: the sheer volume of footage generated by multiple cameras became overwhelming.

1.2 Introduction of AI in Surveillance

Through the introduction of AI algorithms, AI surveillance has shaped its way of data collection. The integration of artificial intelligence (AI) technologies, particularly machine learning and computer vision algorithms, revolutionized surveillance capabilities.

1.3 How has AI reshaped surveillance?

Human limitations in monitoring vast camera networks created a gap. AI's ability to analyze vast amounts of data in real-time ushered in a new era of intelligent security. Machine learning algorithms can now act as tireless and ever-watchful guardians, offering a range of capabilities that empower proactive security measures: like pinpointing objects and people of interest, and analyzing past data to predict crime hotspots. AI has fundamentally reshaped surveillance practices by enhancing data collection, analysis, and decision-making capabilities.

2 Actor-Network Theory

Actor-network theory (ANT) offers a unique lens to analyze AI surveillance. It moves beyond solely examining societal factors, emphasizing the connections among all elements within the network. This includes:

1. **Humans and Objects:** Security personnel interact with AI algorithms, cameras act as data sources for algorithms, and data storage systems become repositories for the network's output.

2. **Objects and Objects:** Cameras communicate with AI systems through networks, algorithms process data from cameras, and data storage systems house information generated by both.

3. **Humans and Objects:** Citizens are monitored by cameras, security personnel utilize AI alerts, and policymakers create regulations that govern the network's operation.

2.1 Enables in the System

2.1.1 Human Actors:

- **Security Personnel:** Monitor alerts generated by AI systems, investigate suspicious activity, and make decisions on interventions.

- **Policymakers:** Develop regulations governing the use of AI surveillance, balancing security needs with privacy concerns.

2.1.2 Non-Human Actors:

- **AI Algorithms:** Analyze video feeds, identify objects and people of interest, and trigger alerts for potential threats.

- **Cameras:** Capture video footage from various locations, providing the raw data for AI analysis.

- **Data Storage Systems:** Store vast amounts of surveillance data for later analysis or retrieval.

- **Communication Networks:** Enable real-time data transmission between cameras, AI systems, and security personnel.

2.2 Actants and Quasi-Objects: The Network's Building Blocks

2.2.1 ANT introduces two key concepts:

Actants: Anything within the network that can be said to "act" or influence its operation. This includes not just humans (corporations, governments, citizens) but also non-human entities like AI algorithms, cameras, data storage systems, and communication networks.

Quasi-Objects: These are entities that can trigger actions within other actants. In AI surveillance, cameras act as quasi-objects, providing the raw data (video footage) that prompts AI algorithms to analyze and potentially trigger alerts for security personnel.

2.3 Power, Interests, and Dynamics

Understanding the network of actants and their relationships helps us analyze the power dynamics at play:

- **Corporations:** As developers of AI systems, they hold power through their control over the technology and their influence on policy decisions. Their primary actant role is to develop and sell these systems, with profit as their driving force.

- **Governments:** They exert power by authorizing and regulating AI surveillance, dictating its purpose and limitations. They act as gatekeepers, influencing how the network functions to achieve security objectives.

- **Citizens:** While holding less direct power, they influence the network through public opinion and legal actions advocating for privacy protections. Their role as actants is to resist or negotiate the extent to which they are monitored.

2.4 The Network in Action

These interconnected actants and quasi-objects shape AI surveillance:

- Corporations compete to develop the most advanced AI systems, influencing the network's technological capabilities.

- Governments negotiate the acceptable boundaries of AI use, shaping the network's purpose and scope.

- Citizens push back against potential privacy violations, potentially altering the network's configuration through legal and social means.

By examining AI surveillance through an ANT lens, we gain a deeper understanding of the complex interplay between technology, society, and the ethical implications of this powerful system.

3 Political Implications of AI Surveillance

The integration of artificial intelligence into surveillance practices has had an impact on the power dynamics, social control and personal sovereignty. This deployment of AI surveillance gives authorities unprecedented power and control over the public.

3.1 Case Study: France AI Surveillance Law

- **Pretext:** The French Prime Minister announced a pension reform increasing the retirement age without a parliamentary vote, triggering no-confidence votes and public outrage.

- **Protests:** This led to widespread strikes and protests across France, disrupting various services.

- **State Response:** Authorities responded with increasing violence and police brutality during protests along with attacks on the journalists covering the protest and the AI surveillance law under the 2024 Olympic Games Law (article 7).

- **AI Surveillance Law:** This law allows the use of AI surveillance tools in public spaces to detect suspicious behaviour and prevent terrorist attacks and CCTV cameras, drones, body scanners, and DNA tests for anti-doping controls at sporting events.

- **Concerns:** There are fears that this law could lead to permanent surveillance measures and infringe on privacy and civic freedoms. The law's impact on human rights and the EU AI Act has also been questioned, with concerns about mass surveillance methods and threats to privacy laws. The passage of the AI surveillance law have sparked international scrutiny and criticism.

3.2 Implications for Society

Governments worldwide are increasingly deploying AI surveillance technologies for various purposes, including maintaining control, enhancing security, and managing social order. This can be seen as a form of social control, influencing behavior and perceptions of public spaces. Such Political decisions reflect broader ideologies and priorities within a society. They shape the balance between security measures and individual freedoms.

Mass protests and public backlash against such policies highlight the tension between security concerns and civil liberties, with protesters arguing that their rights are being threatened. Increased surveillance can lead to a culture of suspicion and fear, affecting social cohesion and trust between citizens and authorities.

3.3 Feedback Loop between Politics and AI Surveillance

- Political dynamics and societal pressures influence the development and deployment of AI surveillance.

- Government policies, public opinion, and cultural norms shape the parameters within which surveillance operates.

- At the same time, AI surveillance can impact political decision-making, policies and campaigns by providing data-driven insights into public behaviours, opinions and sentiments.

AI surveillance with politics and society highlights complex ethical, legal, and social considerations. It underscores the importance of responsible governance, informed public discourse

3.4 Quashing Dissent: Impact of AI Surveillance on Protests

Governments around the world are increasingly employing AI surveillance technologies to monitor and control dissent and protests. These technologies encompass facial recognition, geolocation tracking, web traffic analysis, and other automated detection methods.

Previously, mass protests helped the protesters maintain anonymity and security, but now authorities can now identify and target individuals en masse, making protest activities riskier and more susceptible to persecution.

Examples:

- **Anti-CAA Protests in India**
  During the Citizenship Amendment Act (CAA) protests in India, facial recognition was used to identify and target protesters, particularly minorities, including Muslims.

  The disproportionate targeting of minorities through facial recognition raised concerns about discriminatory practices.

- **Anti-Hijab Protests in Iran**
  Iran's government used AI-assisted surveillance, including facial recognition, to enforce strict morality codes, particularly targeting women protesting against compulsory hijab laws.

  The technology facilitated the identification and persecution of individuals based on their appearance and activities.

Governments often justify the use of AI surveillance as a means to ensure security and public order. However, these tactics have broader implications for society, leading to a culture of fear, self-censorship, and reduced participation in democratic processes. This poses significant challenges to democratic norms, individual freedoms, and human rights.

4 Social Constructivism vs Technological Determinism

AI surveillance and society exist in a complex feedback loop. The debate surrounding AI surveillance hinges on two opposing viewpoints: Social Constructivism and Technological Determinism.

4.1 Social Constructivism: Society Shapes Technology

Social Constructivists argue that AI surveillance is not a preordained force shaping society, but rather a technology shaped by society. Here's how society influences AI surveillance:

- **Values and Needs:** Societal values and priorities guide the development and deployment of AI surveillance. For example, a society prioritizing security might invest heavily in facial recognition systems, while one valuing privacy might develop stricter regulations on data collection.

- **Social Norms and Laws:** Existing social norms and legal frameworks influence how AI surveillance is used. Public concerns about privacy can lead to stricter data protection laws, shaping how AI systems collect and analyze information.

- **Power Dynamics:** The distribution of power within a society shapes who controls AI surveillance and for what purposes. For example, governments might use the technology for social control, while corporations might leverage it for targeted advertising.

4.1.1 Social Constructivism in Action: The Singapore Example

Singapore's Smart Nation initiative utilizes AI surveillance through lamppost-mounted cameras. While this technology offers security benefits of crime prevention and faster emergency response times, it has also sparked public concerns about privacy and potential misuse of data. This citizen pushback exemplifies the concept of Social Constructivism in action. Here's how societal anxieties are shaping the implementation of AI surveillance in Singapore:

- **Public anxieties drive scrutiny:** The extensive use of AI cameras raised concerns about constant monitoring, potential privacy violations, and a lack of transparency in data collection and usage.

- **Social Constructivism at play:** In response to public pressure, the government revisited its approach to AI surveillance. This demonstrates social constructivism – societal concerns are influencing the development of this technology.

- **Legislative and Policy Changes:** The government responded with the Public Sector (Governance) Act of 2018. This act strengthens data protection safeguards and increases oversight mechanisms for government use of AI surveillance technology.

- **Government assurances:** Singaporean authorities have also provided assurances about data usage, emphasizing anonymization, secure storage, and restricted access to authorized personnel.

4.2 Technological Determinism: Technology Shapes Society

Technological Determinists believe that AI surveillance, like other technological advancements, has an inherent and inevitable impact on society. They argue that this technology will fundamentally reshape how we live, work, and interact with the world:

- **Social Control and Crime Prevention:** AI surveillance could lead to a more controlled society, with increased crime prevention capabilities.

- **Shifting Power Dynamics:** Control over AI surveillance systems could concentrate power in the hands of governments and corporations, potentially leading to social stratification and a loss of individual autonomy.

- **Reshaping Social Norms:** The constant presence of surveillance could normalize monitoring and erode expectations of privacy, fundamentally altering social interactions and behavior.

4.2.1 Example: The Rise of Automated Facial Recognition (AFR)

Automated Facial Recognition (AFR) technology is a prime example of Technological Determinism at play in the world of AI surveillance. Deep learning advancements have reshaped surveillance in turn impacting freedoms:

- **The Algorithmic Gaze:** The growing network of cameras created a pervasive ”algorithmic gaze,” where individuals were constantly monitored and identified. This has led to:
    - Erosion of Privacy Expectations: Public expectations of privacy in public spaces began to erode. People might have become accustomed to being constantly monitored, even in areas where they previously expected anonymity.
    - Mass Surveillance and Chilling Effect: Ubiquitous AFR surveillance potentially could have affected free speech and assembly. Knowing they might be identified and tracked could have discouraged participation in protests or activities deemed suspicious.
- **The Automation Bias:** Like any AI technology, AFR systems were susceptible to bias based on the data they were trained on. This can lead to:
    - Discriminatory Outcomes: Biased datasets could cause AFR systems to disproportionately misidentify individuals from certain demographics, exacerbating social inequalities.
    - Loss of Trust in Law Enforcement: Inaccurate identifications by AFR systems and repeated instances of bias could have eroded public trust in law enforcement.

The capabilities of the technology itself, rather than necessarily societal values or needs, are shaping how surveillance is conducted and potentially impacting individual freedoms. This exemplifies Technological Determinism – technology acting as a force for social change.

5 Reverse Adaptation

AI surveillance isn’t merely a watchful eye; it might be subtly reshaping our social reflection. This phenomenon, termed ”reverse adaptation,” describes how society adjusts its behavior and expectations in response to pervasive monitoring.

5.1 How are we adapting?

People are adapting to this evolving landscape in several ways:

1. **Privacy calibration:** The blurring of public and private spheres prompts a more cautious approach to sharing information, both physically and online. This has led to the adoption of coping mechanisms, such as encrypted messaging apps and more discerning public behavior.

2. **Self-Censorship and silencing:** The constant awareness of being monitored across platforms has led to a chilling effect on free speech. Discussions become more guarded, with individuals strategically avoiding controversial topics or activities for fear of triggering an alert or attracting unwanted scrutiny.

3. **Technological counters and opt-out mechanisms:** The rise of AI surveillance has led to the development of counter-technologies and a growing awareness of privacy settings. Privacy-centric browsers and exploring opt-out mechanisms on social media platforms have become routine.

5.2 Societal Implications

These adaptations have significant societal consequences:

- **Normalization of Surveillance:** As coping mechanisms become commonplace, constant monitoring becomes normalized. This normalization may diminish concerns about privacy intrusion, potentially facilitating further surveillance measures.

- **Loss of Trust:** Effect on free speech and the potential for social media platforms to curate content based on algorithms limit exposure to diverse viewpoints. This erodes trust within society and hinders social cohesion.

- **Loss of Individual Autonomy:** The shift towards AI systems predicting and potentially influencing behavior raises concerns about individual autonomy. If algorithms shape acceptable behavior based on extensive data, individuals may conform to avoid negative repercussions, compromising personal values.

This ”reverse adaptation” phenomenon normalizes constant monitoring, potentially undermining privacy expectations and free expression. Moreover, as AI becomes proficient at predicting behavior, a concerning power shift emerges, with algorithms dictating acceptable behaviour and subtly influencing actions.

6 Incorporation of Social Biases

AI surveillance categorizes and classifies individuals, often based on social groups rather than individual characteristics. This can unfairly target and harm certain groups like people of color, migrants, religious minorities, LGBTQ+ individuals, and those facing economic hardships such as single parents or people with chronic illnesses.

The burden of monitoring and tracking is higher for these targeted groups, creating a vicious cycle of suspicion, scrutiny, and marginalization. Technologies like facial recognition or automated systems can make discrimination worse and even unfairly treat people who are struggling financially.

6.1 Digital Technologies in Practice

The categorization of individuals as ”undeserving” and ”deserving” can lead to reduced aid. This is often based on predetermined criteria set within the AI algorithms, which may not consider the nuanced realities of individual circumstances.

As seen in the instances presented in the course, the Child Welfare program in Pittsburg was wrong 70% of the time and predicted referrals to child abuse rather than abuse itself.

6.2 Poorhouse

As seen in the course, the poorhouse was a physical place where society segregated and mistreated the poor for meagre aid to their families. Similarly, in modern times, AI surveillance technologies can perpetuate biases and discrimination, particularly against marginalized groups such as people living in poverty, migrants, and minorities.

This comparison to the poorhouse highlights the danger of using AI as it can lead to exclusion, increased surveillance, and the erosion of social support systems. Just like the poorhouse was a flawed way to manage poverty, using AI with social biases can worsen inequalities and keep harmful biases alive, creating a digital version of the old poorhouse.

7 Megamachines

In the modern world, the concept of mass surveillance has become increasingly prevalent, raising concerns about privacy, individual freedom, and the power dynamics within society.

7.1 Megamachines in Action

At its core, mass surveillance embodies the convergence of science, technology, economy, and political power, characteristic of Megamachines. It represents a concerted effort to control and monitor the activities of individuals on a vast scale, often justified under the guise of national security or public safety.

One key aspect of mass surveillance is its reliance on advanced technologies, such as CCTVs, facial recognition software, and data mining algorithms. These technologies enable the collection, analysis, and storage of massive amounts of information about individuals' behaviors, movements, and communications.

The proliferation of mass surveillance reflects a culture that prioritizes the conquest of privacy and the control of information over the enhancement of individual freedoms. In this culture, values such as privacy and autonomy are often seen as obstacles to the efficiency and effectiveness of surveillance systems.

Moreover, mass surveillance is often justified by its proponents as necessary for maintaining order, preventing crime, and combating terrorism. However, these justifications overlook the depersonalized and dehumanizing nature of surveillance systems, which treat individuals as mere data points to be monitored and analyzed.

7.1.1 Case Study - PRISM

William Binney, a former intelligence official at the National Security Agency (NSA), exposed the PRISM program in 2002. PRISM involved the collection of massive amounts of data from internet companies such as Google, Facebook, and Microsoft, under the guise of counterterrorism efforts. This program allowed the NSA to access emails, chat logs, and other online communications of millions of individuals, both within the United States and abroad, without proper oversight or legal authorization.

Binney's disclosure shed light on the secretive nature of government surveillance programs and raised concerns about the erosion of privacy rights in the digital age. It sparked public outcry and renewed debates over the balance between national security and civil liberties.

7.2 Power Structure and Dynamics

The implementation of mass surveillance requires a centralized power structure capable of coordinating the collection and analysis of vast amounts of data. This structure mirrors the hierarchical organization of Megamachines, with leaders wielding unparalleled authority and legitimacy.

Furthermore, the bureaucratic apparatus of mass surveillance operates without ethical concerns, prioritizing the goals of those in power over the rights and freedoms of individuals. This echoes the role of bureaucracy as ”servo-units” within Megamachines, working to serve the interests of rulers without question.

The rise of mass surveillance has also led to the emergence of what can be described as a ”surveillance-industrial complex,” akin to the military-industrial complex. This complex encompasses the intertwined interests of government agencies, technology companies, and private contractors involved in the development and implementation of surveillance systems.

7.2.1 Case Study - Clearview AI

Clearview AI, a facial recognition company, gained notoriety for its practice of scraping billions of images from social media platforms and other online sources to create a vast database for law enforcement purposes. This database allowed authorities to identify individuals in real-time based on a single photograph, raising serious concerns about the potential for abuse and misuse of personal data.

7.3 The all-seeing Panopticon

In the face of mass surveillance, individuals are increasingly subjected to constant scrutiny and control, reminiscent of the ”beleaguered” and ”obsolete” individuals described within Megamachines. The erosion of privacy and autonomy reduces individuals to passive subjects within the surveillance apparatus, deprived of agency and autonomy. Furthermore, the technical surveillance and data collection mechanisms employed in mass surveillance create a pervasive sense of being watched, akin to the ”all-seeing eye” of the Panopticon. This constant surveillance fosters a climate of self-censorship and conformity, stifling dissent and individual expression.

Ultimately, mass surveillance represents a manifestation of the totalitarian technocracy envisioned within Megamachines, where centralized power and control are prioritized over the real needs and values of human life. In this world, individuals are reduced to mere cogs in the machinery of surveillance, existing in a world ”fit only for machines to live in.”

8 Question of Autonomy

While advancements in AI surveillance offer possibilities for security and crime prevention, their unchecked use leads to a future where our freedoms are constantly under threat. Here’s how these systems can potentially limit our freedoms:

8.1 Restricted Movement and Assembly

The constant awareness of being monitored by AI surveillance systems has a detrimental impact on individual liberties. The fear of being watched leads to self-censorship, hindering free expression and open discourse.

8.1.1 Case Study: China's Social Credit System

China's Social Credit System (SCS) is a proposed system that aims to monitor and evaluate the behavior of its citizens. While still under development, it has already raised significant concerns about its potential impact on individual autonomy and freedom of expression.

The Mechanics of the system: The SCS is a comprehensive system that aggregates data from various sources, including financial records, online activities, and government interactions. High scores offer benefits like easier loans and travel permits, while low scores bring disadvantages such as restricted loans, travel limits, and job discrimination.

Self-censorship pressure: The potential consequences of a negative social credit score create a climate of fear and self-censorship. Citizens may be less likely to express dissenting opinions online or participate for fear of jeopardizing their score in turn impacting society dynamics.

Beyond individuals: The SCS extends to businesses, scoring them on factors like environmental compliance. Consequently, companies may prioritize conformity and compliance over innovation and entrepreneurial spirit.

Concerns and Uncertainties: Privacy issues and lack of transparency raise concerns about unfair discrimination in scoring, with uncertainties about its full implementation.

8.2 Opaque Algorithms and Accountability

Bias in AI surveillance algorithms can lead to unfair profiling and discrimination. Furthermore, the limited accountability for these systems makes it difficult to challenge their decisions or hold anyone responsible for potential misuse.

8.2.1 The Rikers Island Bail System: A Case Study in Algorithmic Bias

The United States faces high incarceration rates, particularly affecting minority communities. This disparity extends to pretrial detention. An attempt to address this involved utilizing artificial intelligence (AI) to assess the risk of recidivism (re-offending) in bail decisions. However, the implementation of this system at Rikers Island jail in New York City (2016-2018) became a cautionary tale of how AI, if not carefully designed and monitored, can exacerbate existing societal inequalities.

The algorithmic solution: Before 2016, bail decisions lacked consistency. NYC implemented an AI algorithm considering factors like criminal history and social media to create fairness.

Unintended consequences: Despite intentions, the algorithm showed racial bias due to skewed training data. People of color were unfairly assessed, leading to higher pre-trial detention rates.

Racial discrimination: People of color were denied bail simply because of the algorithm's skewed assessment, leading to lost jobs, strained family relations, and potential job discrimination upon release.

Fighting for reform: Public outcry and lawsuits challenged the use of this biased algorithm in bail decisions. New York City began reforming, relying less on algorithms and increasing human oversight in bail decisions.

8.3 Collective Autonomy Under Threat

This extent of AI surveillance can also weaken collective action and social movements. By tracking individuals and predicting behavior, authorities can anticipate and potentially disrupt protests, undermining the collective ability to challenge power structures and advocate for change.

8.3.1 Case Study: Black Lives Matter Protests

The Black Lives Matter protests of 2020 erupted across the United States in response to the killings of George Floyd, Breonna Taylor, and countless others. While demanding racial justice and police reform, the movement encountered challenges due to extensive social media surveillance by law enforcement.

The surveillance state and social media: Law enforcement agencies utilize various tools like automated monitoring systems and facial recognition software to track activists on social media and at protests.

Effect on activism: Monitoring of online activity by law enforcement can affect activists. It hinders the movement's ability to organize effectively and send its message to a wider audience.

Legal concerns and transparency: Social media surveillance raises legal questions, violating First Amendment rights to freedom of speech and assembly if individuals feel compelled to self-censor due to surveillance.

In conclusion, the rise of AI surveillance poses significant threats to individual and collective autonomy. Case studies such as China's Social Credit System and the use of AI algorithms in the Rikers Island bail system demonstrate the real-world implications of AI surveillance on individual rights and societal justice. These examples highlight the importance of transparency, accountability, and ethical considerations in AI surveillance technologies. The case study of Black Lives Matter protests highlights the effect of social media surveillance on activism and the need for robust legal protections to safeguard collective autonomy and freedom of expression.

9 Scientific Controversies

The development of AI surveillance technology raises concerns that challenge the autonomy of scientific research:

9.1 Policing and Punishment

Researchers advocating for stricter regulations on AI surveillance or highlighting potential biases and issues in the technology face pressure from funding agencies or government bodies with vested interests in seeing the technology deployed. This disrupts the legitimacy and objective nature or scientific research.

9.1.1 Case Study: Early Facial Recognition Research (1960s-1990s)

Early research on facial recognition was funded by government agencies with interests in security applications. Some researchers expressed concerns about the potential for misuse by these very agencies, fearing the technology could be used for mass surveillance. This case study highlights the tension between scientific progress driven by external funding and the ethical considerations raised by AI surveillance technology.

9.2 Interference from external entities

Companies developing AI surveillance systems might pressure researchers to downplay potential risks or manipulate data to present a more favorable outcome of the technology's effectiveness. This undermines the objective pursuit of knowledge and prioritizes commercial interests over scientific integrity.

9.2.1 Case Study: Rekognition and Racial Bias (Amazon)

Background: Amazon Rekognition, a facial recognition service from Amazon Web Services (AWS), launched in 2016 with features like object and emotion identification. However, the technology quickly faced criticism for racial bias.

Evidence of Bias A study by the ACLU found Rekognition falsely matched photos of 28 members of Congress (all people of color) to a mugshot database, highlighting the very potential bias.

Pressure and consequences: Following the ACLU's report, Amazon faced pressure from civil rights groups and lawmakers to address the racial bias in Rekognition. Initially downplaying the issue, Amazon faced questions about transparency and accountability.

Long-term impact: The Rekognition case exemplifies the real-world consequences of biased AI surveillance systems. Potential repercussions include unjustified scrutiny, erosion of trust, and legal challenges.

10 Paradigm Shift

Through the lens of Thomas Kuhn's paradigm shift theory, the evolution of surveillance practices can be understood as a transition from one conceptual framework to another, characterized by changes in meanings, methodologies, and societal implications.

10.1 Established Paradigm

Kuhnian paradigm shifts begin with a period of normalcy, where a prevailing set of ideas, tools, and assumptions form the basis of scientific inquiry. Similarly, in the realm of surveillance, the pre-digital era operated within a paradigm where surveillance was predominantly associated with targeted monitoring by law enforcement or intelligence agencies. Surveillance was conducted through traditional methods such as wiretapping, physical observation, and informant networks, guided by established legal frameworks and ethical considerations.

10.1.1 Case Study - The Watergate Scandal

In 1972, the Watergate scandal captured perfectly the traditional paradigm of surveillance, revealing the extent of targeted monitoring by the Nixon administration. Through wiretapping and physical surveillance, President Nixon's operatives sought to gain an advantage over political opponents, violating ethical and legal boundaries. The scandal exposed the abuse of surveillance powers for political gain, prompting public outcry and legal repercussions.

10.2 Anomalies in the paradigm

With the proliferation of digital technologies and the internet, anomalies began to emerge within this paradigm. These anomalies took the form of technological advancements that enabled unprecedented levels of data collection, storage, and analysis. Initially dismissed as minor deviations, or tools for enhancing traditional surveillance methods, these technological innovations eventually led to a crisis within the existing paradigm. The sheer volume and scope of data generated by digital interactions overwhelmed traditional surveillance practices, necessitating a reevaluation of existing methodologies.

10.2.1 Case Study - The Snowden Leaks

The revelation of Edward Snowden's leaks in 2013 exemplified the crisis brought about by digital advancements in surveillance. Snowden exposed the vast scope of government surveillance programs, such as PRISM, which collected massive amounts of data from internet communications worldwide. These programs, initially perceived as minor deviations for enhancing security, raised significant ethical and legal concerns as they indiscriminately gathered personal information on a global scale. Snowden's disclosures succeeded in sparking a widespread debate and calls for reform.

10.3 Appearances of a paradigm shift

Mass surveillance introduced a paradigm where surveillance was no longer confined to targeted individuals or specific locations but permeated all aspects of society. Terms such as privacy, anonymity, and consent underwent redefinition in the context of ubiquitous surveillance technologies, challenging established notions of individual rights about privacy and data protection.

10.4 Incommensurability

One of the key implications of this paradigm shift is incommensurability, which comes across as the difficulty of communication or translation between the old and new paradigms. In the case of mass surveillance, the transition from targeted to indiscriminate surveillance posed challenges in adapting to the ethical and legal frameworks of the past, with the capabilities of emerging technologies.

10.4.1 Case Study - The Cambridge Analytica Scandal

The Cambridge Analytica scandal in 2018 epitomized the incommensurability resulting from the shift to mass surveillance. The incident revealed how the company harvested personal data from millions of Facebook users without their consent, exploiting loopholes in existing regulations. This indiscriminate data collection challenged traditional ethical and legal frameworks, exposing the inadequacy of outdated privacy laws in addressing modern surveillance practices.

10.5 Theory-dependence of observations

The theory-dependence of observations became obvious as mass surveillance practices evolved. Rather than data driving the development of surveillance technologies, it was the underlying conceptual frameworks and ideological motives that shaped the trajectory of surveillance practices. The pursuit of national security, crime prevention, and social control became driving forces behind the adoption and expansion of mass surveillance initiatives, overshadowing concerns regarding privacy infringement and civil liberties.

10.5.1 Case Study - The Patriot Act

The Patriot Act, enacted in the aftermath of the 9/11 attacks in New York City, exemplifies how ideological motives shaped the trajectory of surveillance practices. The Act expanded the government's surveillance powers in the name of national security. It allowed authorities to conduct warrantless wiretaps, monitor internet communications, and access personal records, all in the pursuit of preventing terrorism. Despite concerns about privacy infringement and civil liberties, the urgency to combat terrorism overshadowed these worries.

11 Conclusion

This project has covered a wide range of topics related to surveillance, AI, and their impact on society. We have extensively tried to link the concepts taught in class like, ANT, Social Constructivism and Technological Determinism, Megamachines etc. and Surveillance and AI. We also looked at several real-world examples and did an elaborate analysis on them to study the impacts of surveillance and AI on politics, society, institutions etc. Overall, this project has provided a comprehensive understanding of the complexities and implications of AI surveillance in our modern world.

12 Acknowledgment

We would like to express our heartfelt thanks to Radhika Krishnan ma'am for her guidance, support, and valuable insights throughout this project. Her input and suggestions greatly contributed to the development and clarity of this project. We would also like to extend our gratitude to the TA, Anvitha, for her assistance, feedback, and dedication. Overall, this project has been an enlightening journey into the complex world of AI surveillance, and We are grateful for the opportunity to learn and grow through this experience.

13 References

1. Artificial Intelligence on Surveillance
2. History and Evolution of Video Surveillance Technology
3. Artificial Intelligence: Discussions on how artificial intelligence is transforming surveillance capabilities
4. AI CCTV – Artificial Intelligence surveillance
5. How Actor-Network Theory explains the new power relationships in the age of AI
6. Artificial Intelligence: Deterministic to Social Constructivism. The shift from deterministic AI approaches to social constructivism
7. Facial Recognition System Controversies
8. Eyeing the Evolving Landscape of AI Surveillance
9. FRANCE: Plagued by mass protests and new AI surveillance law
10. How governments use facial recognition for protest surveillance - Rest of World
11. The AI Assault on Women: What Iran's Tech Enabled Morality Laws Indicate for Women's Rights Movements