Project Outline

Surveillance using AI

Srujana Vanka
Shreeya Singh
Sankalp S. Bhat

Contents

Historical Context - (thoda kam hee cuz intro types & unrelated to course content)

- Evolution of surveillance technologies.
- How does AI surveillance differ from previous forms (e.g., panopticon)?

Actor-Network Theory

- Analyze the actors involved (e.g., corporations, governments) and their interests.
- Enables in the system - human and non-human actors (e.g., algorithms, cameras).
- Power relations within the network.

Politics in Technology

- Political implications of AI surveillance - control, repression etc
- Issues of power, control, privacy, and social control.
- Eg. recent AI surveillance policy by France - Civic Space Watch | FRANCE: Plagued by mass protests and new AI surveillance law
    - Intention? To prevent real-time terrorist attacks
    - Anti-doping tests on sports persons (full body scans)
    - Protest rights threatened

Quashing Dissent

- How protests have been impacted by AI eg. Anti-CAA, Anti Ukraine War, Anti Hijab Protest - How governments use facial recognition for protest surveillance - Rest of World
- Targeting minorities - (Muslims, blacks, women) facial recognition - The AI Assault on Women: What Iran's Tech Enabled Morality Laws Indicate for Women's Rights Movements | Council on Foreign Relations

Social Constructivism vs Technological Determinism

- How AI surveillance shapes society vs. how society shapes AI surveillance

Reverse Adaptation

- How AI surveillance might be subtly shaping social norms, expectations of privacy, and even self-censorship.
- The potential for a power shift where AI exerts a form of control on society through constant monitoring and adaptation.

Technical Arrangements as Forms of Order

- Analyze how AI categorizes and classifies individuals.
- Does AI surveillance restrict movement and activity in certain areas or for specific groups (e.g., racial profiling)
- Social biases can be incorporated into Technology -> more suppression & discrimination against weaker social sections
- Impact of AI surveillance on social trust and cohesion

Megamachine

- Autonomous technical system

Question of Autonomy

- Analyze the impact of AI surveillance on individual and collective autonomy.
- Discuss concerns about freedom of movement, expression, and assembly
- algorithmic accountability - fairness & transparency?
- Scientific Controversies

Paradigm Shift

- Consider how AI surveillance might lead to a fundamental shift in social norms and expectations of privacy

Examples

- Singapore - Smart Nation Initiative
- CCTV Monitoring

Srujana

Historical Context

- Evolution of surveillance technologies.
- How does AI surveillance differ from previous forms (e.g., panopticon)?

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, a primitive form of public surveillance that was 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, enabling a more coordinated response to potential dangers. The Panopticon, was a theoretical prison designed by philosopher Jeremy Bentham in the 18th century. It aimed to control inmates through the feeling of being constantly observed, even if the observer was unseen. However, the Panopticon's effectiveness relied on a centralized structure and the invisibility of the observer, which wasn't always achievable.

The 20th century called for a new era of surveillance with the development of closed-circuit television (CCTV) in the 1940s. CCTV cameras offered a significant leap forward compared to human guards. Unlike guards who required breaks and could be susceptible to fatigue or distraction, CCTV cameras provided a wider field of view and continuous monitoring capabilities. The adoption of CCTV cameras boomed in the latter half of the 20th century, 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. Manually reviewing hours of footage to identify suspicious activity proved to be a laborious and time-consuming task, often exceeding human capabilities. This is where Artificial Intelligence (AI) entered the scene, revolutionizing the way we approach surveillance.

How AI is reshaping 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:

- Identify & Filter: AI sifts through video feeds, pinpointing objects and people of interest, filtering out irrelevant information and focusing on potential threats.
- Accuracy & Efficiency: AI reduces false alarms triggered by non-threatening movements, allowing security personnel to concentrate on genuine concerns.

- Predict & Prevent: AI analyzes past data to predict crime hotspots, enabling preventative measures like increased patrols or targeted security briefings.

AI goes beyond enhancing existing methods. It offers an automated, data-driven, and proactive approach to security, fundamentally reshaping how we safeguard people and places.

Actor-Network Theory

- Analyze the actors involved (e.g., corporations, governments) and their interests.
- Enables in the system - human and non-human actors (e.g., algorithms, cameras).
- Power relations within the network.

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:

- **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.
- **Objects and Objects:** Cameras communicate with AI systems through networks, algorithms process data from cameras, and data storage systems house information generated by both.
- **Humans and Objects:** Citizens are monitored by cameras, security personnel utilize AI alerts, and policymakers create regulations that govern the network's operation.

Enables in the System

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.

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.

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

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.

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.

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.

Social Constructivism vs Technological Determinism

- How AI surveillance shapes society vs. how society shapes AI surveillance

AI surveillance systems undoubtedly impact how we live, but society also plays a crucial role in shaping how this technology is developed and used. The debate surrounding AI surveillance hinges on two opposing viewpoints: Social Constructivism and Technological Determinism. Social Constructivism emphasizes how societal values and needs influence the development and use of this technology. Technological Determinism, on the other hand, argues that AI surveillance inherently shapes society, impacting everything from crime prevention to social norms.

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.

Social Constructivism in Action: The Singapore Example

Consider Singapore's Smart Nation initiative, which utilizes AI surveillance through lamppost-mounted cameras. While this technology offers security benefits, it has also sparked public concerns about privacy and potential misuse of data. This citizen pushback exemplifies Social Constructivism – societal anxieties are shaping the implementation of AI surveillance. The government's response with the Public Sector (Governance) Act and assurances about data usage reflects how social values and legal frameworks can influence the development and deployment of such technology.

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. However, this could also lead to a chilling effect on free speech and movement.
- **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.

Example: The Rise of Automated Facial Recognition (AFR)

Automated Facial Recognition (AFR) technology is a prime example of Technological Determinism at play in the realm of AI surveillance. Advancements in deep learning algorithms have enabled AFR systems to achieve remarkable accuracy in identifying individuals from cameras and video footage. This technological leap has significant social implications, shaping how surveillance is conducted and potentially impacting individual freedoms:

- **The Algorithmic Gaze:** The increasing accuracy and affordability of AFR have led to its widespread deployment in public spaces, security systems, and even personal devices. This growing network of cameras creates a pervasive "algorithmic gaze," where individuals are constantly monitored and identified. This can lead to:
    - **Erosion of Privacy Expectations:** The normalization of AFR technology could erode public expectations of privacy in public spaces. People might become accustomed to being constantly monitored, even in areas where they previously expected anonymity.
    - **Mass Surveillance and Chilling Effect:** The potential for ubiquitous surveillance through AFR could lead to a chilling effect on free speech and assembly. Knowing they might be identified and tracked could discourage people from participating in protests or engaging in activities deemed suspicious by the authorities.
- **The Automation Bias:** AFR systems, like any AI technology, are susceptible to bias based on the data they are trained on. This can lead to:
    - **Discriminatory Outcomes:** If trained on biased datasets, AFR systems might disproportionately misidentify individuals from certain ethnicities or demographics. This could lead to wrongful detentions and exacerbate existing social inequalities.
    - **Loss of Trust in Law Enforcement:** Inaccurate identifications by AFR systems can erode public trust in law enforcement. Repeated instances of bias could lead to a perception that the technology is unfair and unreliable.

In this case study, the technological advancements in facial recognition algorithms inherent to AFR are driving societal changes. 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.

Reverse Adaptation

- How AI surveillance might be subtly shaping social norms, expectations of privacy, and even self-censorship.
- The potential for a power shift where AI exerts a form of control on society through constant monitoring and adaptation.

- Add examples here

AI surveillance isn't merely a watchful eye; it might be subtly reshaping our social reflection. This concept, reverse adaptation, proposes that as AI surveillance systems become more intricate, they may inadvertently influence our behavior and expectations of privacy.

A Society Reshaped by Surveillance:

Imagine a society where cameras are ubiquitous, and AI algorithms meticulously analyze our every move. This constant monitoring could lead to:

- **Privacy:** A Fading Norm? The ever-present gaze of AI might gradually erode our sense of privacy. Public spaces, once considered havens for anonymity, could become zones of perpetual observation. This societal shift could normalize a level of monitoring that was previously unthinkable.
- **Self-Censorship and the Chilling Effect:** Knowing we're constantly under observation could lead to a chilling effect on free speech and expression. People might self-censor their behavior and conversations for fear of triggering an alert or attracting unwanted scrutiny. This could stifle dissent and creativity.
- **A Power Shift: From Monitoring to Control?** As AI surveillance evolves, it might become adept at not just observing but also predicting behavior. This raises concerns about a potential power shift, where AI systems could exert a subtle form

of control by influencing how people act and behave. Imagine a society where algorithms, not laws, dictate acceptable behavior.

The Algorithmic Gaze: A Society Under Scrutiny

Imagine a society where AI constantly monitors and analyzes our actions, adjusting its algorithms in response to shifts in behavior. This "algorithmic gaze" could have unintended consequences:

- **Reinforcing Societal Biases:** AI trained on historical data might perpetuate societal biases, potentially normalizing certain behaviors and marginalizing others. This could exacerbate existing inequalities.

- **Pre-Crime and the Erosion of Freedom:** AI could become so adept at predicting potential crimes that it preemptively restricts freedoms, blurring the lines between prevention and pre-emptive punishment. This raises questions about due process and individual rights.

- **Social Interactions Under Scrutiny:** Constant monitoring could lead to a decline in spontaneous and genuine social interactions. People, aware of being observed and judged by algorithms, might become more guarded and less likely to engage authentically with others.

—---

The concept of reverse adaptation underscores the importance of proactive measures to address the potential downsides of AI surveillance:

- Transparency is Key: Clear guidelines and regulations are crucial to ensure transparency in how AI surveillance systems collect and use data. Citizens have the right to understand how they are being monitored and what data is being collected about them.

- Human Oversight, Not Algorithmic Rule: AI systems should remain tools under human control, with limitations on their autonomy and decision-making capabilities. Algorithmic oversight should complement, not replace, human judgment. Humans should maintain ultimate control over how AI surveillance is

used and ensure it aligns with societal values.

- A Public Conversation About the Future: Open discussions about the societal impact of AI surveillance are essential. By fostering public discourse, we can ensure that the development and utilization of this technology aligns with societal values and ethical principles. It's crucial to have a public conversation about the acceptable boundaries of AI surveillance and how to mitigate the potential for reverse adaptation.

  —---

Question of Autonomy

- Analyze the impact of AI surveillance on individual and collective autonomy.
- Discuss concerns about freedom of movement, expression, and assembly
- algorithmic accountability - fairness & transparency?
- Scientific Controversies

The rise of AI surveillance raises significant concerns about its impact on individual and collective autonomy, which refers to the freedom and independence to make choices without undue external influence. These powerful systems hold the potential to monitor our movements, analyze our activities, and even predict our behavior. While advancements in AI surveillance offer possibilities for security and crime prevention, their unchecked use can lead to a dystopian future where our freedoms are constantly under threat. Here's how these systems can potentially limit our freedoms:

1. **Restricted Movement and Assembly:** The constant awareness of being monitored by AI surveillance systems can have a detrimental impact on individual liberties. It discourages people from exercising their right to freedom of assembly and movement. The fear of being watched can lead to self-censorship, hindering free expression and open discourse.

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 envisioned as a comprehensive system that gathers data on citizens from various sources, including:

- Financial records: Timely payments of bills, loans, and taxes contribute to a positive score.
- Online activity: Likes, shares, and posts on social media can be monitored for signs of "disloyalty" or "dishonesty."
- Government interactions: Traffic violations, jaywalking, or even negative interactions with public services can lower a score.
- Private behavior: Reports from neighbors or landlords regarding "uncivil" behavior could be factored in.

A Score for Every Citizen: This collected data is then used to calculate a social credit score for each citizen. A high score translates to benefits such as easier access to loans, travel permits, and preferential treatment in job applications. Conversely, a low score can lead to significant disadvantages, including:

- Difficulty obtaining loans or mortgages.
- Restrictions on travel and movement within China.
- Exclusion from desirable jobs or educational opportunities.
- Public shaming and social stigma.

The Chilling Effect: 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 in activities deemed undesirable by the government, for fear of jeopardizing their score. This can stifle creativity, critical thinking, and dissent, impacting the social and political fabric of the country.

Beyond Individuals: The SCS is not limited to individuals. Businesses and organizations can also be assigned social credit scores based on factors like environmental compliance and adherence to government regulations. This can create a system where companies prioritize self-preservation and toe the government line to maintain a good score, potentially hindering innovation and entrepreneurial spirit.

Concerns and Uncertainties: The SCS remains under development, and the exact scope and implementation details are still unclear. However, several concerns have been raised

about privacy violations, lack of transparency and even potential biases within the data collection process could lead to unfair discrimination against certain segments of the population.

The Future of the SCS: The long-term impact of the Social Credit System remains to be seen. However, the potential for this system to erode individual autonomy, stifle dissent, and create a climate of fear warrants close scrutiny and international discussion.

2. **Opaque Algorithms and Accountability**

   The lack of transparency in AI algorithms that power surveillance raises serious concerns. Bias in these algorithms can lead to unfair profiling and discrimination. Furthermore, with limited accountability for these systems, it becomes difficult to challenge their decisions or hold anyone responsible for potential misuse.

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

Incarceration rates in the United States are some of the highest in the world, with a disproportionate impact on minority communities. This trend extends to pre-trial detention, where individuals are held while awaiting trial. One attempt to address this issue involved using 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: Prior to 2016, bail decisions at Rikers Island were often subjective and lacked consistency. In an effort to create a fairer and more objective system, New York City implemented an AI algorithm to assess a defendant's risk of flight (not appearing for trial) and recidivism. The algorithm considered various factors including criminal history, social media activity, and employment status.

Unintended Consequences: While the goal was to create a neutral system, the algorithm ended up perpetuating racial bias. The data used to train the algorithm likely reflected existing societal inequalities. For instance, people of color are more likely to be arrested for minor offenses, leading to a skewed criminal history record. Similarly, social media activity patterns might differ based on race and socioeconomic background. These biases

within the training data ultimately led the algorithm to unfairly assess the risk of recidivism for people of color, resulting in their pre-trial detention at a higher rate.

The Human Cost: The consequences of this algorithmic bias were significant. People of color were denied bail simply because of the algorithm's skewed assessment, leading to lost jobs, strained family relationships, and potential job discrimination upon release. This pre-trial detention could have a long-term impact on their lives and hinder their chances of successful reintegration into society.

Fighting for Reform: Public outcry and lawsuits challenged the use of this biased algorithm in bail decisions. New York City eventually began reforming its pretrial detention system, placing less reliance on algorithms and increasing human oversight in bail decisions.

The Rikers Island case study serves as a reminder of the potential pitfalls of AI in critical decision-making processes. It highlights the importance of using fair and representative data to train AI systems, maintaining human oversight, and ensuring transparency and accountability in their development and deployment.

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 or dissent. This undermines the collective ability to challenge power structures and advocate for change.

   Case Study: Black Lives Matter Protests (2020)

   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. These demonstrations drew millions of people demanding racial justice and police reform. However, the movement also faced challenges due to the pervasive use of social media surveillance by law enforcement.

The Power of Social Media for Activism: Social media platforms have become a powerful tool for social movements like Black Lives Matter. Activists use these platforms to share information, document police brutality, and call for action.

The Surveillance State and Social Media: However, law enforcement agencies have also become adept at using social media for surveillance purposes. They utilize various

tools to track and identify activists, including **Automated monitoring, Geofencing, and** Advanced facial recognition software to identify individuals from protest footage and social media profiles.

Chilling Effect on Activism: The knowledge that their online activity is being monitored by law enforcement can have a chilling effect on activists. People are less likely to share information, express strong opinions, or participate in protests for fear of retribution or legal repercussions. This hinders the movement's ability to organize effectively and send its message to a wider audience.

Legal Concerns and Transparency: The use of social media surveillance by law enforcement raises significant legal concerns. First Amendment guarantees of freedom of speech and assembly could be compromised if individuals feel pressured to self-censor due to surveillance. Additionally, there are transparency issues, as the extent and legal basis for social media surveillance by law enforcement agencies often remain shrouded in secrecy.

The Need for Reform: The Black Lives Matter protests highlighted the tension between public safety and individual liberties in the digital age. There is a need for reforms that ensure transparency in social media surveillance practices, while also protecting the fundamental rights of free speech and assembly. This could involve requiring law enforcement to obtain warrants for social media data, increasing public oversight and independent audits of these surveillance programs, and exploring ways to anonymize or minimize the data collected from peaceful protests.

Scientific Controversies

The Challenge to Scientific Autonomy: Policing, Punishment, and External Influence

The development and deployment of AI surveillance technology raise concerns that challenge the very autonomy of scientific research:

- **Policing and Punishment:** Researchers advocating for stricter regulations on AI surveillance or highlighting potential biases in the technology might face pressure from funding agencies or government bodies with vested interests in seeing the technology deployed. This can stifle critical discussion and scientific inquiry.

- **Case Study: Early Facial Recognition Research (1960s-1990s)** (https://en.wikipedia.org/wiki/Facial_recognition_system)

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. Additionally, early facial recognition algorithms primarily focused on identifying Caucasian male faces, leading to biased systems with lower accuracy for other demographics. This case study highlights the tension between scientific progress driven by external funding and the ethical considerations raised by AI surveillance technology.

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

Case Study: Rekognition and Racial Bias (Amazon)

Background: Amazon Rekognition is a cloud-based facial recognition service offered by Amazon Web Services (AWS). Launched in 2016, Rekognition was touted for its ability to identify objects, people, and even emotions in images and videos. However, the technology quickly came under fire for exhibiting racial bias.

Evidence of Bias: In 2018, a study by the ACLU (American Civil Liberties Union) found that Rekognition falsely matched photos of 28 members of Congress (all people of color) to a mugshot database. This alarming error rate highlighted the potential for Rekognition to disproportionately misidentify individuals from certain demographics, raising concerns about bias within the algorithm. (https://www.aclu.org/press-releases/aclu-statement-amazon-face-recognition-moratorium)

Pressure and Consequences: Following the ACLU's report, Amazon faced pressure from civil rights groups and lawmakers to address the racial bias in Rekognition. However, the company initially downplayed the issue, suggesting the study's methodology was flawed. This response raised questions about Amazon's transparency and accountability regarding its AI technology.

Long-Term Impact: The Rekognition case exemplifies the real-world consequences of biased AI surveillance systems. Potential repercussions include:

- Unjustified Scrutiny: Individuals from certain demographics might be wrongly flagged as suspicious by biased algorithms, leading to increased surveillance and potential harassment by law enforcement.
- Erosion of Trust: Public trust in law enforcement and government agencies can erode if AI surveillance is perceived as discriminatory and unfair.
- Legal Challenges: Lawsuits challenging the use of biased AI by law enforcement agencies could arise, impacting the technology's future deployment.

These examples highlight how external forces can exert undue influence on scientific research related to AI surveillance. The pressure to publish positive results, secure funding, or maintain good relations with commercial partners can stifle critical inquiry and prioritize profit or political agendas over the objective pursuit of knowledge.

Bibliography

1. History https://www.3sixtyintegrated.com/blog/2023/07/26/history-video-surveillance/
2. AI surveillance https://www.forbes.com/sites/forbestechcouncil/2024/02/02/artificial-intelligence-the-new-eyes-of-surveillance/?sh=3659886314f2
3. Wikipedia https://en.wikipedia.org/wiki/Artificial_intelligence_for_video_surveillance
4. ANT for AI https://theacademic.com/actor-network-theory-explains-chatgpt-and-ai/
5. Social constructivism to determinism

https://medium.com/@biswaskaveri66/artificial-intelligence-deterministic-to-social-constructivism-cb0a43c4e9ab

6. Singapore Smart Nation initiative example https://en.wikipedia.org/wiki/Smart_Nation
7. Hong Kong protests https://en.wikipedia.org/wiki/2019%E2%80%932020_Hong_Kong_protests
8. https://en.wikipedia.org/wiki/Facial_recognition_system
9. https://researchoutreach.org/articles/rethinking-reverse-side-artificial-intelligence/
10. https://www.techcube.co.uk/blog/ai-cctv-artificial-intelligence-surveillance/

Surveillance Capitalism

When, where and in what circumstances does this new regime of surveillance capitalism begin?

Launch of Apple's iTunes platform in 2011.

The individual becomes the central actor in the market. The individual's desire to be uniquely catered to as a customer, to exercise control over one's life, is a pivotal moment.

What makes this possible? New digital, networked spaces. Individual mentalities and demands now had to be identified and addressed in this new modernity summoned by the internet and powered by the new information infrastructure and technologies.

Silicon Valley's notion of "permissionless innovation": Unilateral seizure of rights over data without consent in order to cater to these new needs. Apple, Google, Amazon, FB….

Google: True pioneer of surveillance capitalism. Google sets in place an elaborate model of computer-mediated transactions, where the aim is continuous data extraction, behavior prediction, personalization and customization. Personal experience and data is now fully converted into a rich node to be mined by corporations.

Surveillance Capitalism

Surveillance capitalism poses a specific challenge because of its tumultuous impact on the very concepts of consent and privacy.

What is surveillance capitalism? While surveillance capitalism is not technology, new computing tools such as machine learning

are necessary for surveillance capitalism to exist.
It is a new economic order that uses all human experience as raw material. This raw material is extracted in multiple ways and forms through technological means; it is used to predict human intensions, to produce and sell goods and services.
Capacity and potential to modify human behavior in many subtle ways. With this capacity for behavioral modification, it is a threat to human nature itself, just as industrial capitalism was (and is) a threat to the natural world.
“Capitalism’s quest for a new collective order based on absolute certainty has led to a rogue mutation of capitalism”.
This mutation challenges even market democracy and spells a death knell for personal sovereignty.
Behavioral Surplus
“Behavioral surplus”: Surplus value generated by mining enormous amounts of personal data and converting this behavioral data into a marketable product. The surplus represents that behavioral data available for uses beyond service improvement, and whose only purpose is to ensure exponential profits.
Requires “digital dispossession” on a widespread scale. Discovery of behavioral surplus led to the development of surveillance capitalism from earlier models of capitalism. Moving from inferring personal behavior -> predicting behavior with increasing accuracy.
Online -> Offline. Use of smart-home devices, wearables, applications such as Google Maps and Google Earth and self-driving cars. Process of slow habituation.
Physical movements -> Emotional mapping. Human emotions of sadness, anger, disappointment etc. are harnessed by affective computing, emotion analytics and sentiment analysis. If a particular incursion generates too much of an uproar, companies adapt by promising reforms, or by occasionally paying fines.
Inexorable expansion. Ambient computing, ubiquitous computing and the Internet of Things (IoT).
Behavioral Surplus
These computational methods attempt to identify human emotions and sentiments from a variety of sources, including textual and visual sources.

Ambient computing: just about any type of object imaginable is outfitted with computing ability and connectivity. It allows the use of a computer or internet-enabled device, without human beings consciously using it.
Ubiquitous computing: Can occur using any device, in any location, and in any format.
After moving from online to offline monitoring, surveillance capitalism has now entered into a new domain: behavioral control. Not only is data being constantly collected, it is being processed and fed back to trigger certain desired outcomes such as purchase of goods or timely payments of loan installments. Humans as Pavlov's dogs? Punished by the regime of surveillance capitalism for 'undesirable' behaviors and rewarded for 'desirable' ones.

Network Society
A society whose social structure is made of networks powered by microelectronics-based information and communication technologies.
Social structure: Organizational arrangements of humans in relations of production, consumption, reproduction, experience, and power expressed in meaningful communication coded by culture.
Network Society
Transformation in communication leads to a new kind of globalization and a new kind of society.
There have ALWAYS been social networks. What distinguishes network society is the use of ICTs to create and sustain far-flung networks in which new social relationships are created.
Networks are self-reconfigurable, complex structures of communication that ensure unity of purpose and flexibility of its execution by the capacity to adapt to the operating environment.
Networks are not new. Old, flexible networks were replaced by vertical, hierarchical, bureaucratic networks of the industrial age (both statist and capitalist versions).
Beyond a certain threshold of size, complexity, and volume of exchange, they become less efficient than vertically organized

command and control structures, under the conditions of pre-electronic communication technology. The ability of networks to introduce new actors and new contents in the process of social organization, with relative independence of the power centers, increased over time with the evolution of communication technologies.

Network Society

Three processes led to the Network Society (in the late 20th century):

The restructuring of industrial economies to accommodate an open market approach.

The freedom-oriented cultural movements of the late 1960s and the early 1970s, including the civil rights movement, the feminist movement and the environmental movement.

The revolution in information and communication technologies.

Network Society

A network is a set of interconnected nodes. A network has no center, just nodes. Varying relevance of nodes. Absorbing more relevant information + processing info more efficiently -> more relevance. When nodes become redundant or useless, networks tend to reconfigure themselves, deleting some nodes, and adding new ones. Nodes only exist and function as components of networks. The network is the unit, not the node.

Networks involve multiple links between different nodes.

Nodes are centres within communication networks that can both send and receive messages.

Individuals can be seen as nodes. But nodes can take non-human forms as well. For example, communication centres, businesses, government departments.

Network Society

Nature of Networks?

Networks can stretch across natural and cultural boundaries.

They are interconnected with numerous other networks.

Location of power can be harder to pin down in networks.

Horizontal connections between networks can make exercise of hierarchical authority more difficult.

Social change also occurs easily in networks.

Digital Technologies in Practice

Redflagging: Targetting for digital scrutiny is largely as members of social groups, NOT as individuals.

Higher burden of monitoring and tracking borne by people of colour, migrants, unpopular religious groups, sexual minorities, the poor etc.

Targetted groups include those who face long-term challenges to steady employment: racial discrimination (the 10% rule, pg 26), single parenthood, disability, chronic illness.

More suspicion -> more targeting, scrutiny -> more marginalization. Vicious cycle.

Technologies of poverty management are not neutral. They are shaped by fear of economic insecurity and hatred of the poor. Example: TANF (Temporary Assistance to Needy Families). Read pg 7.

“Automated decision-making shatters the social safety net, criminalisesthe poor, intensifies discrimination…”

The Poorhouse Designed to deter the poor from accessing public resources. It polices their labour, spending, sexuality, and parenting. Tries to predict future behavior, and punishes and criminalises those who do not comply.

“Welfare required that poor people trade their rights – to bodily integrity, safe work environments, mobility, political participation, privacy, and selfdetermination – for meagre aid for their families”

Digital Technologies in Practice

From the poorhouse to the digital database: Roots lie in ”scientific charity”; the need to separate the “good”, deserving poor from the “bad”, undeserving poor.

“The conflict between expanding legal rights of welfare recipients and weakened support for public assistance was resolved by a wave of hightech tools”.

EXAMPLES:

1973: nearly half of people living under the poverty line in the US

received AFDC [welfare support]. A decade after the use of high-tech tools, this has fallen to 30%. Today, it is 10%.
Essentially, we are seeing an EXPANSION of the poorhouse, powered by digital technologies.