SCC.141 Professionalism in Practice

Week 13: Surveillance and Censorship

29th January 2025

Dr Elmira Yadollahi, e.yadollahi@lancaster.ac.uk
School of Computing and Communications

*Inspired by Lecture by Dr Bran Knowles.

Learning Objectives

Lancaster University

- **Define** key concepts of surveillance (**state**, **corporate**, **personal, self**) and censorship
- **Examine** surveillance tools, the mechanisms of censorship, and ethical implications like algorithmic bias and privacy
- **Explore** explore real-world examples such as **state programs**, **corporate practices**, **self-surveillance tools**, and **censorship tools**
- **Reflect** on **ethical**, **social**, and **legal** implications, and also your own **positionality**

Agenda

Lancaster University

- On Defining Surveillance
- Types of Surveillance and Tools
- On Defining Censorship
- Censorship in the Digital Age
- Revisiting Privacy and Balancing it with Surveillance and Censorship
- Key Takeaways & Future Outlook

PART1: Surveillance

Does Surveillance Concern You?

Lancaster University

- Take **2 minutes** to discuss with someone next to you:
  - How concerned are you about government (state) surveillance? Or corporate surveillance? **(For example, on a scale of 1-5)**
  - Are there other forms (e.g., social media, workplace) that worry you?

Defining Surveillance

- **Macnish, 2015*:** "[T]he monitoring of [people] over a period of time without their consent"
  - **Monitoring** people without their consent over time
- **Thomsen, 2019*:** "Targeted observation of a person over a sufficiently extensive period of time as to obtain information about this person "
  - **Targeted observation** over a sufficiently extensive period to gain information
- **Lyon, 2001**:** "[A]ny collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered"
  - Collection and processing of personal data for **managing or influencing people**

*Thomsen, F. K. (2019). The concepts of surveillance and sousveillance: A critical analysis. Social Science Information, 58(4), 701-713.
** Lyon, D. (2007). Surveillance studies: An overview.

Defining Surveillance

Lancaster University

Bring it all Together:

- The **systematic observation** or **data collection** concerning **people**, often with the **aim of influencing** or **managing** their behaviour

What are the Key Concepts?

- **Consent:** Are we aware and okay with being watched?
- **Power:** Who has the authority to watch, and do we have recourse?
- **Data:** What is being collected, and how is it used?

Different Types of Surveillance

- **State (Government) Surveillance**
- **Corporate Surveillance**
- **Personal Surveillance**
- **Self-Surveillance**

Photo Credit https://www.linkedin.com/pulse/what-we-know-you-welcome-surveillance-state-issue-152-kevin-novak-n3vqe/

Different Types of Surveillance

- **State (Government) Surveillance**
- **Corporate Surveillance**
- **Personal Surveillance**
- **Self-Surveillance**

- **Covert Surveillance**
  - Techniques used discreetly so the subject is unaware of being monitored
  - (e.g., hidden cameras, undercover monitoring)
- **Overt Surveillance**
  - Visible and recognizable monitoring methods
  - (e.g., signposted CCTV cameras, public security patrols)

Different Types of Surveillance

Lancaster University

Surveillance Type	Primary Purposes
State (Government) Surveillance	• National security • Law enforcement and crime prevention • Public safety (e.g., counterterrorism)
Corporate Surveillance	• Profit motive (selling behavioural data, optimizing ads) • Consumer profiling (predict preferences, tailor marketing) • Productivity oversight (monitoring employees for efficiency)
Personal Surveillance	• Safety (child protection, home security) • Personal convenience (home deliveries, letting family know whereabouts) • Peace of mind (tracking personal belongings)
Self-Surveillance	• Self-improvement (health goals, productivity) • Personal insight (tracking habits, measuring performance) • Sharing achievements (gamification, social bragging rights)

Different Types of Surveillance

Lancaster University

Surveillance Type	Potential Issues
State (Government) Surveillance	• **Privacy Violations:** Data collected at scale, often without informed consent • **Power Imbalance:** Government holds vast data; citizens have little oversight • **Overreach & Abuse:** Risk of targeting dissidents, indefinite data retention
Corporate Surveillance	• **Lack of Consent / Transparency:** Users rarely realize how much is tracked • **Data Monetization:** Personal data sold to third parties • **Ethical & Legal Concerns**: Biased analytics, manipulative recommendation systems
Personal Surveillance	• **Consent & Boundaries**: Monitoring someone else (spouse, child) can erode trust • **Misuse or Abuse**: Stalkerware, controlling behaviour in domestic contexts • **Data Security**: Personal devices susceptible to hacking or data leaks
Self-Surveillance	• **Data Privacy**: Personal health metrics stored in corporate servers • **Over-Monitoring**: Obsession with metrics can create anxiety or skew behaviour • **Commercial Exploitation**: Collected data can be resold or used for advertising

Different Types of Surveillance

Lancaster University

Surveillance Type	Examples / Tools
State (Government) Surveillance	• **Legislation:** USA Patriot Act, Investigatory Powers Act (UK) • **Intelligence programs:** NSA (PRISM), GCHQ (Karma Police) • **Infrastructure:** CCTV networks, border drones, biometric scanners
Corporate Surveillance	• **Data mining** from social media platforms, search engines • **Targeted advertising** (tracking user behaviour across websites) • **Workplace monitoring systems** (time-off-task tracking, keystroke logging)
Personal Surveillance	• **Home cameras** (baby monitors, doorbell cams) • **Smartphone location sharing** (families, friend circles) • **Tracking apps** (monitor a family member's phone or children's devices)
Self-Surveillance	• **Wearable tech** (fitness trackers, smartwatches) • **Health apps** (calorie counters, sleep trackers) • **Social media** "check-ins" or constant self-logging

USA Patriot Act (2001)

- Signed into law following 9/11 terrorist attacks
  - Under the veil of “national security”
- Allowed searching of emails and telephone records **without a warrant**
- Openly conducting surveillance on US and foreign citizens

- **Criticisms:**
  - Not made aware when they were being surveilled
  - Did away with “innocent until proven guilty”
    - *Indefinite detention without due process*

USA Patriot Act (2001)

- Signed into law following 9/11 terrorist attacks
  - Under the veil of “national security”
- Allowed searching of emails and telephone records **without a warrant**
- Openly conducting surveillance on US and foreign citizens

- **Criticisms:**
  - Not made aware when they were being surveilled
  - Did away with “innocent until proven guilty”
    - *Indefinite detention without due process*

Exemplifies tension between
positive freedom (e.g. freedom of speech)
and
negative freedom (e.g. freedom from harm)

Mass Surveillance

Lancaster University

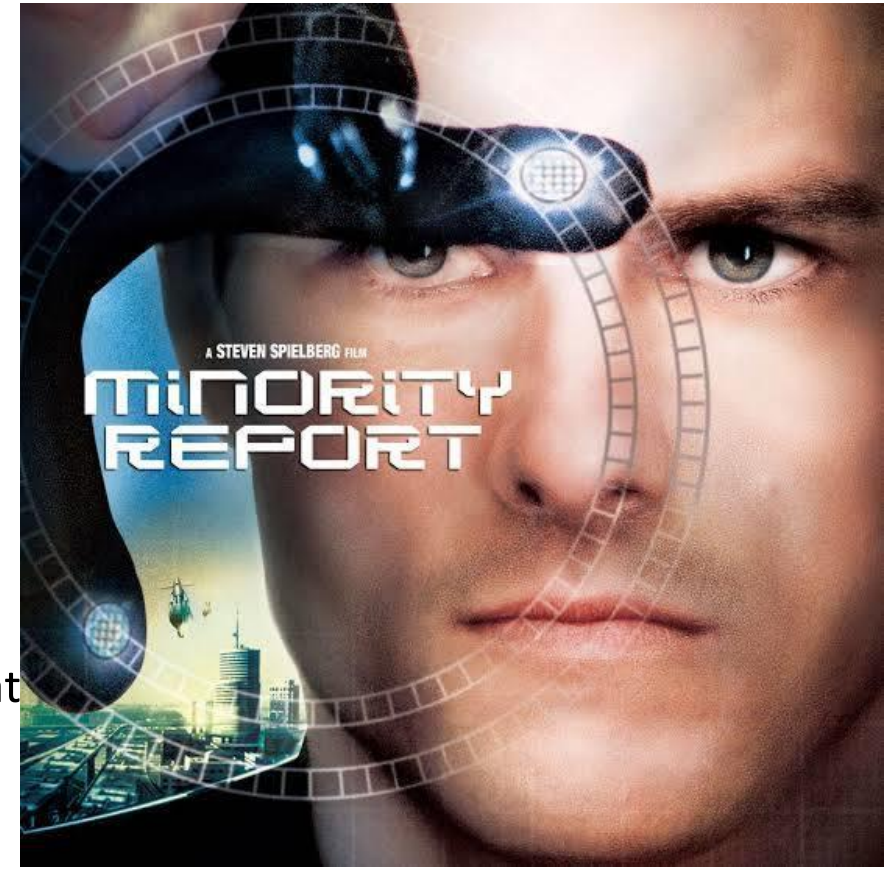
- **Definition:** The practice of spying on a significant part of a population
  - US National Security Agency (NSA), PRISM:
    - *requested data from major tech companies on users' communications*
    - *search expanded several degrees beyond person of interest*
  - UK Government Communications Headquarters (GCHQ):
    - **Karma Police:** monitored website browsing history and transaction metadata
    - **Black Hole:** data repository feeding multiple surveillance systems
    - **Mutant Broth**: enabled searching of Black Hole
  - *Violations of legal principle of **probable cause***
    - *Would not meet the legal threshold for search and seizure*

UK Surveillance Legislation

- Anti-Terrorism, Crime and Security Act, 2001
  - *enabled retention of communication data voluntarily*
  - *does not include content of communications*
  - *provisions override Data Protection Act, 1998*
- Communications Data Bill, 2012 (Snooper's Charter)
  - *`To catch criminals and protect children'*
  - *Requires all ISPs to store user data for 12 months*
- Investigatory Powers Bill, 2016 (Snooper's Charter 2.0)
  - *Enables bulk collection of data*
  - *Companies assist in bypassing encryption*
- **Landmark judgment against Snooper's Charter, 2022**
  - *cites insufficient safeguards*
  - *requires independent approval that the data collection is necessary and proportionate*

Have You Watched Minority Report?

- **Predictive Surveillance**:
  - The film's "Precrime" system **predicts crimes** before they happen, using precogs (psychics) and data-driven insights
  - Raises questions about the ethical and practical limits of predictive surveillance systems, **similar to today's AI-driven predictive policing tools**
- **Loss of Privacy:**
  - **Ubiquitous surveillance** is depicted, including retinal scans that identify individuals and personalize advertisements
  - This reflects concerns about **biometric surveillance**, corporate data collection, and personalized tracking



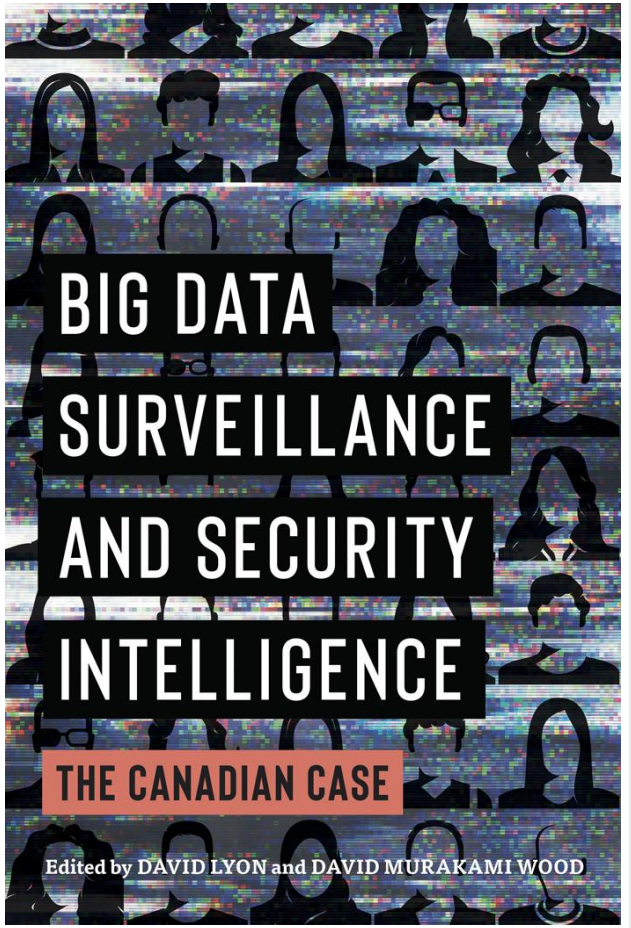
Big Data Surveillance

Lancaster University

- **Definition:** Big data surveillance refers to the **systematic collection**, **analysis**, and **use of massive datasets** for monitoring and control

- **Application Areas:**
  - **National security:** Predictive models for identifying potential threats
  - **Law enforcement:** Real-time data from IoT, CCTVs, and AI-driven analytics
  - **Corporate security:** Protecting assets and monitoring employees

- **Key Insight:** Big data enables **predictive policing**, **counterterrorism** strategies, and broader control of populations through **pattern recognition**



Tools and Technologies for Big Data

Lancaster University

- **Data Sources:**
  - Social media platforms, GPS data, IoT sensors, credit card transactions
- **Processing Techniques:**
  - **Machine learning (ML)** algorithms for behavioral analysis
  - **Natural Language Processing (NLP)** for monitoring communications
  - **Graph theory** to map social networks (e.g., identifying key influencers in a network)
- **Examples:**
  - AI-driven surveillance in smart cities (e.g., PRISM, GCHQ's programs)
  - Facial recognition systems in law enforcement and airport security

Predictive Analytics in Security Intelligence

Lancaster University

- **Predictive Intelligence:**
  - Big data analytics can anticipate events, such as potential crimes or terrorist attacks, using historical data
  - **Example:** Predictive Policing tools like **PredPol** that analyze crime patterns and deploy resources proactively
    - **PredPol*** uses predictive analytics and mathematics to identify potential criminal activity
    - The **company's patented algorithm** is based on a model used to predict earthquake aftershocks

- **Cybersecurity Applications:**
  - Network anomaly detection
  - Fraud detection in financial systems
  - Insider threat detection within organizations

* https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes

Sousveillance: Watching the Watchers

Lancaster University

- **Definition:** Sousveillance refers to the practice of individuals monitoring those in power, such as governments, corporations, or other authorities

- **Key Examples:**
  - Recording police actions during protests or public events
  - Whistleblowing to expose misuse of power (e.g., Edward Snowden)
  - Using wearable tech (e.g., body cameras) to document experiences
  - Encryption tools (e.g., Signal, ProtonMail) as a means of reclaiming privacy

- **Purpose:** Empowers individuals to hold authorities accountable and challenge abuses of surveillance systems

Back to Nothing-to-hide Argument

Lancaster University

"If you've got nothing to hide, you've got nothing to fear."

Easy to find someone guilty of something even when they aren't, right?

- **Example:**
  - **Distortion:** Surveillance can create the appearance of guilt by misinterpreting data or framing innocent behaviors as suspicious
    - Creating criminals* (Pascoe County, Florida, US)
  - **Exclusion:** Surveillance systems often prevent people from knowing how their data is being used or correcting inaccuracies
    - Errors in data can misrepresent individuals as criminals

* https://www.nbcnews.com/tech/tech-news/predictive-policing-strategies-children-face-pushback-n1269674

Back to Nothing-to-hide Argument

Lancaster University

"If you've got nothing to hide, you've got nothing to fear."

Easy to find someone guilty of something even when they aren't, right?

- **Example:**
  - **Distortion:** Surveillance can create the appearance of guilt by misinterpreting data or framing innocent behaviors as suspicious
    - Creating criminals* (Pascoe County, Florida, US)
  - **Exclusion:** Surveillance systems often prevent people from knowing how their data is being used or correcting inaccuracies
    - Errors in data can misrepresent individuals as criminals

Privacy isn't just about hiding—it's about fairness, transparency, and preventing harm

* https://www.nbcnews.com/tech/tech-news/predictive-policing-strategies-children-face-pushback-n1269674

PART2: Censorship

Defining Censorship in the Digital Age

Lancaster University

- **Traditional Censorship:** Blocking books, banning movies, or controlling broadcast media
- **Digital Censorship:** Automated systems filter content, block websites, or suppress dissenting opinions online

- **Actors:**
  - **State Actors:** Governments imposing restrictions to control public discourse (e.g., China's Great Firewall)
  - **Corporate Actors:** Platforms like Facebook, YouTube, and Twitter censor misinformation, hate speech, or politically sensitive topics
  - **Algorithmic Moderators:** AI systems tasked with removing harmful content, often resulting in unintended censorship due to biases

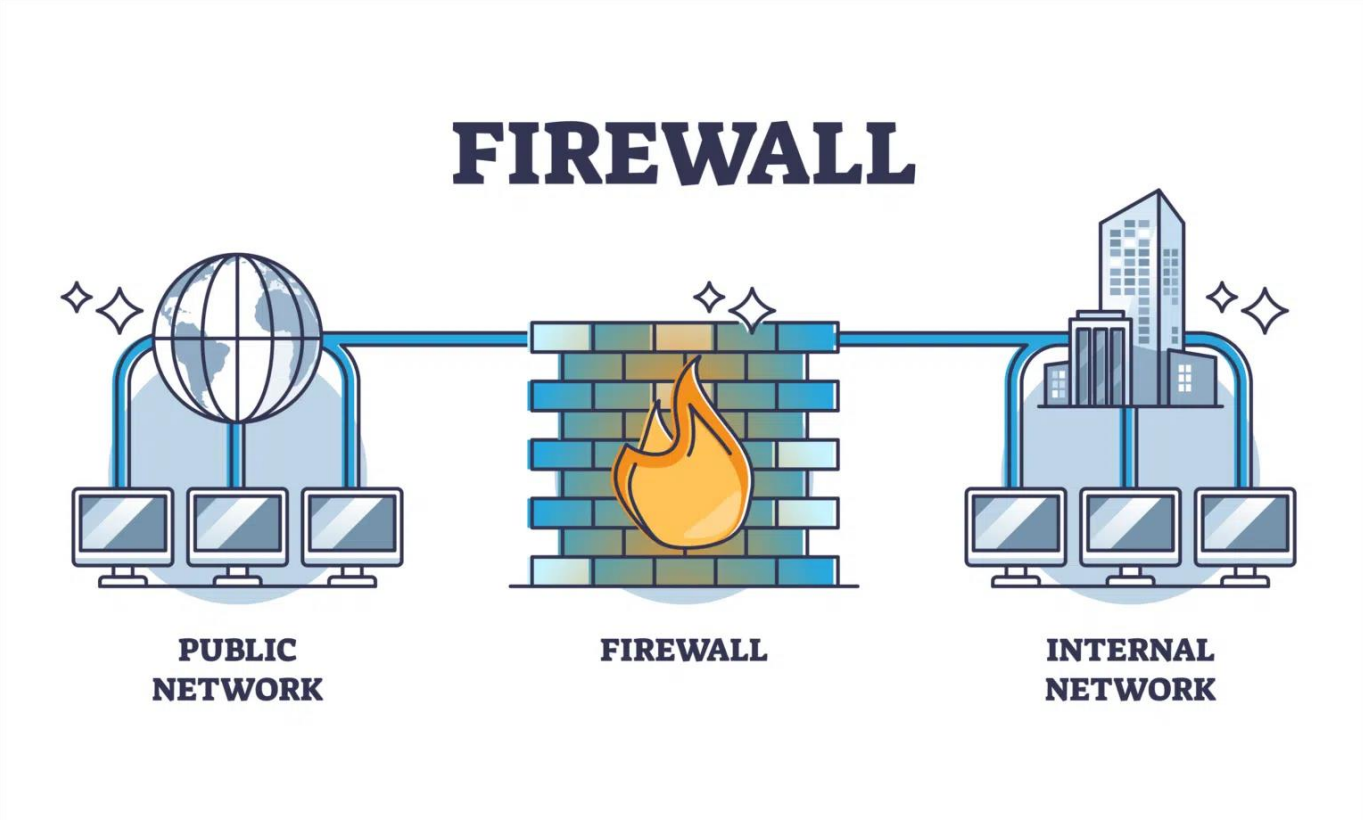
Types of Censorship

Lancaster University

- **Network-Level Censorship:**
  - Blocking websites or services (e.g., Great Firewall of China, Russia's internet restrictions)
  - Techniques: DNS tampering, IP blocking, or deep packet inspection (DPI)
- **Platform-Level Censorship:**
  - Content moderation on platforms like Twitter, Facebook, or YouTube
  - Algorithms detect and remove flagged content (e.g., hate speech, copyrighted material)
- **Self-Censorship:**
  - Individuals modify behavior knowing they are being monitored or flagged (linked to surveillance)
- **Algorithmic Censorship:**
  - AI filters unintentionally remove content due to training bias or lack of contextual understanding.

Technical Mechanisms of Censorship

- **Network-Level Controls:**
  - Deep Packet Inspection (DPI)
  - Firewalls
- **Automated Content Moderation:**
  - AI Moderators
- **Data Manipulation:**
  - Search Engine Filtering
  - Social Media Echo Chambers
- **IoT and Censorship:**
  - Smart Devices



Technical Mechanisms of Censorship

Lancaster University

- **Network-Level Controls:**
  - **Deep Packet Inspection (DPI):** Scans packet data in real time to block or restrict specific types of content (e.g., keywords, URLs)
  - **Firewalls:** Centralized systems for blocking access to domains or IP addresses (e.g., China's great wall)
- **Automated Content Moderation:**
  - **AI Moderators:** Use natural language processing (NLP) to detect inappropriate or harmful content
- **Data Manipulation:**
  - **Search Engine Filtering:** Algorithms prioritize or suppress search results based on political or corporate interests
  - **Social Media Echo Chambers:** Algorithms amplify specific content while suppressing opposing views, limiting information diversity
- **IoT and Censorship:**
  - **Smart Devices:** IoT sensors can restrict or block access to specific functionalities (e.g., disabling internet access in certain areas during protests)

Ethical Considerations in Censorship

Lancaster University

- **Algorithmic Transparency:**
  - How do content moderation algorithms make decisions?
  - Are these decisions explainable and justifiable?
- **Bias in AI:**
  - Training data often reflects societal biases, leading to over-censorship of marginalized voices
  - How can developers ensure training data represents diverse and equitable perspectives?
- **Balancing Free Speech and Harm Reduction:**
  - Striking the right balance between allowing free expression and preventing harm (e.g., hate speech, misinformation)
- **Government vs. Corporate Power:**
  - Who decides what content is censored—state regulators, private companies, or the public?

PART 3: Revisiting Privacy

Tying it all together

Privacy in the Age of Surveillance

Lancaster University

*Privacy as a **human right**: Enables autonomy and protects freedom*

- **Challenges** in the digital age:
  - State and corporate surveillance
  - Big data and AI-driven profiling
  - IoT's pervasive data collection

- **Intersection with surveillance:**
  - How surveillance erodes privacy
  - Ethical questions: At what cost?

Balancing Privacy and Surveillance

Lancaster University

Ethical frameworks for Privacy in surveillance systems

- **Privacy-by-Design:** Embed privacy features into technology at the design stage
- **Transparency:** Clear data usage policies for users
- **Anonymization Techniques:**
  - Use differential privacy in datasets
  - Limit identifiability in data collected for analytics
- **Challenges in AI Systems:**
  - Bias in training data compromising anonymity
  - Balancing utility with minimization of data collection

Back to the Privacy Paradox

Lancaster University

- **Three Core Barriers to Protecting Privacy:**
  - **Ignorance:** Can we realistically be expected to understand every app, device, or platform we use?
  - **Futility:** Many of us feel there's no point in resisting
  - **Foreclosure of Alternatives:** Let's face it, Big Tech has a near-monopoly

- **Action Points:**
  - Demand transparency in data practices
  - Support ethical design in technology (e.g., privacy-first solutions)
  - Advocate for robust legal frameworks to protect privacy as a right, not a responsibility

Back to the Privacy Paradox

Lancaster University

- **Three Core Barriers to Protecting Privacy:**
  - **Ignorance:** Can we realistically be expected to understand every app, device, or platform we use?
  - **Futility:** Many of us feel there's no point in resisting
  - **Foreclosure of Alternatives:** Let's face it, Big Tech has a near-monopoly

- **Action Points:**
  - Demand transparency in data practices
  - Support ethical design in technology (e.g., privacy-first solutions)
  - Advocate for robust legal frameworks to protect privacy as a right, not a responsibility

*Recognizing our **right not to hide** is the first step in fighting for a future where privacy and freedom coexist with technology*

Key Takeaways

- **Privacy**, **Surveillance**, and **Censorship** are interconnected
- Surveillance has **Dual Impacts:** Enhances security but risks overreach, bias, and misuse
- **Surveillance Capitalism:** Companies commodify data, eroding privacy and trust while amplifying power imbalances
- **Balancing** privacy and security is essential
- The **Privacy Paradox** shows there is a tension between valuing privacy and compromising it for convenience

Future Outlook

Lancaster University

- **Questions?**

- **Looking Ahead:** Next week— Malware

Lancaster University

Thank you for attending, any questions?