SCC.141 Professionalism in Practice

Week 12: Privacy

22nd January 2025

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

Learning Objectives

Lancaster University

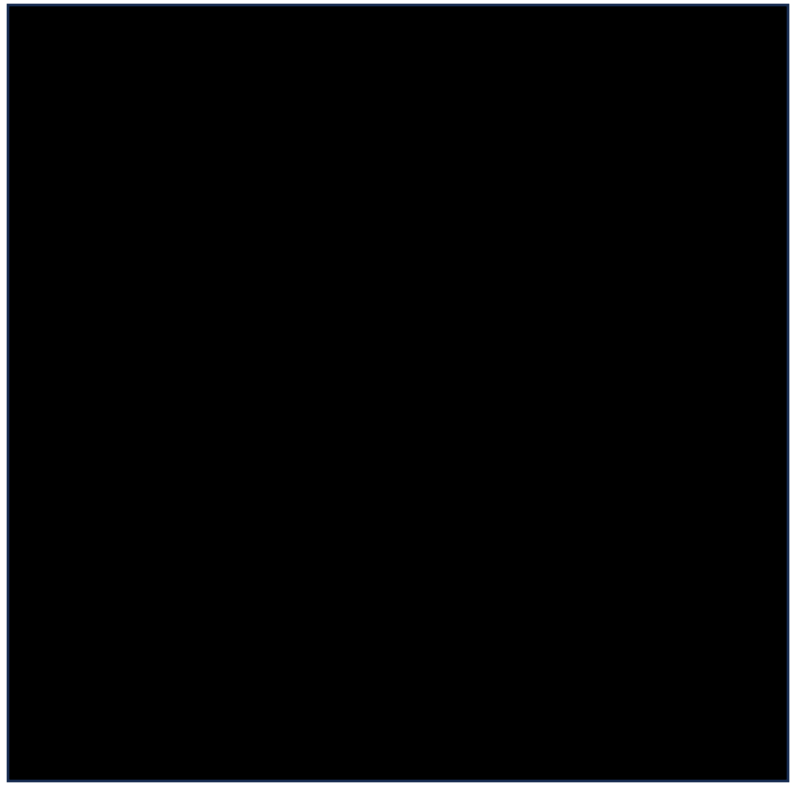
- **Explain** what privacy is, why it matters, and what is “privacy paradox”
- **Evaluate** the effectiveness and limitations of existing regulatory frameworks (e.g., GDPR)
- **Identify** key privacy risks arising from robotics, AI, and other emerging technologies
- **Discuss** common arguments around privacy (e.g., “nothing to hide”)
- **Reflect** on how your own views on privacy might have shifted by the end of the session

Agenda

Lancaster University

- On Defining Privacy
- The Privacy Paradox
- Regulatory Approaches: GDPR & Beyond
- Privacy in AI and Robotics
- New Frontiers of Privacy Concerns
- Key Takeaways & Future Outlook

Quick Menti Activity



What is Privacy?

Lancaster University

"Privacy…is too complex a concept to be reduced to a singular essence. It is a plurality of different things that do not share any one element but nevertheless bear a resemblance to one another. For example, privacy can be invaded by the disclosure of your deepest secrets. It might also be invaded if you're watched by a peeping Tom, even if no secrets are ever revealed. With the disclosure of secrets, the harm is that your concealed information is spread to others. With the peeping Tom, the harm is that you're being watched. You'd probably find that creepy regardless of whether the peeper finds out anything sensitive or discloses any information to others. There are many other forms of invasion of privacy, such as blackmail and the improper use of your personal data. Your privacy can also be invaded if the government compiles an extensive dossier about you."

Solove, D. J. (2011). Why privacy matters even if you have 'nothing to hide'. Chronicle of Higher Education, 15.

What is Privacy?

"**Privacy…is too complex a concept to be reduced to a singular essence. It is a plurality of different things** that do not share any one element but nevertheless bear a resemblance to one another. For example, privacy can be invaded by the disclosure of your deepest secrets. It might also be invaded if you're watched by a peeping Tom, even if no secrets are ever revealed. With the disclosure of secrets, the harm is that your concealed information is spread to others. With the peeping Tom, the harm is that you're being watched. You'd probably find that creepy regardless of whether the peeper finds out anything sensitive or discloses any information to others. There are many other forms of invasion of privacy, such as blackmail and the improper use of your personal data. Your privacy can also be invaded if the government compiles an extensive dossier about you."

"The Right to be left alone" (**Louis Brandeis, 1890: Harvard Law Review**)

"The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude, and their behaviour to others" (**Alan Westin, 1967: *Privacy and Freedom***)

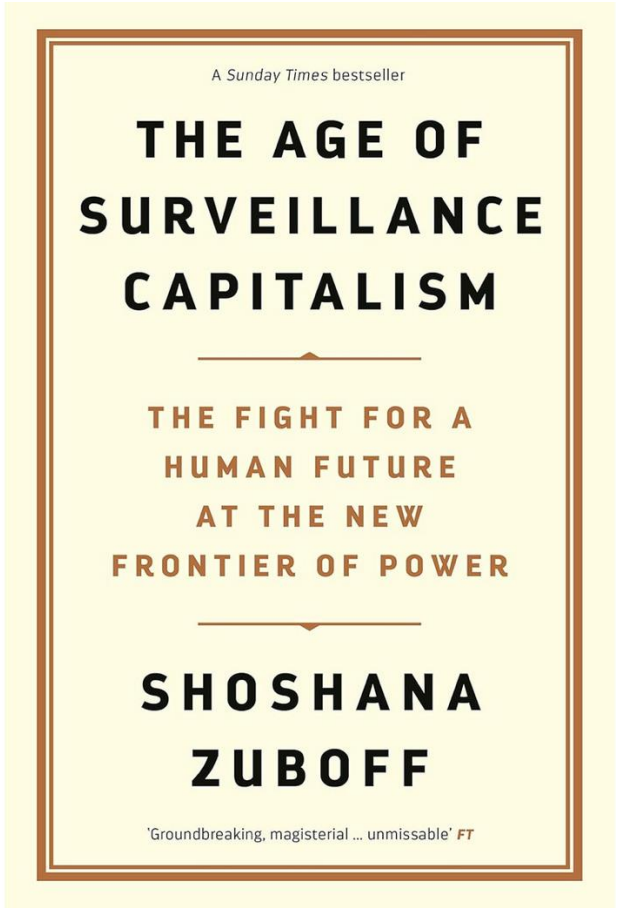
"The degree to which human information is neither known nor used" (**Neil Richards, 2021: *Why Privacy Matters***)

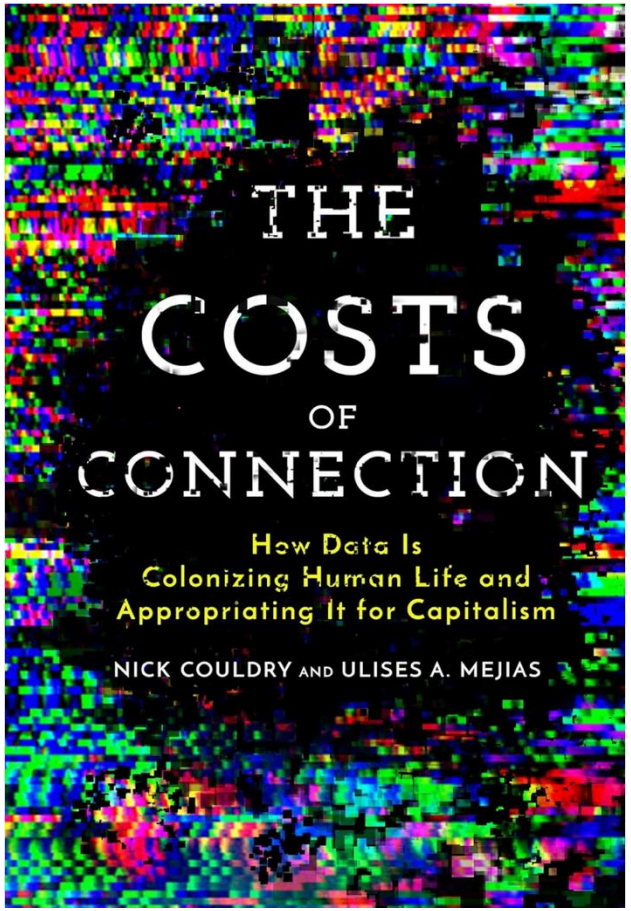
Ethical & Philosophical Dimensions of Privacy

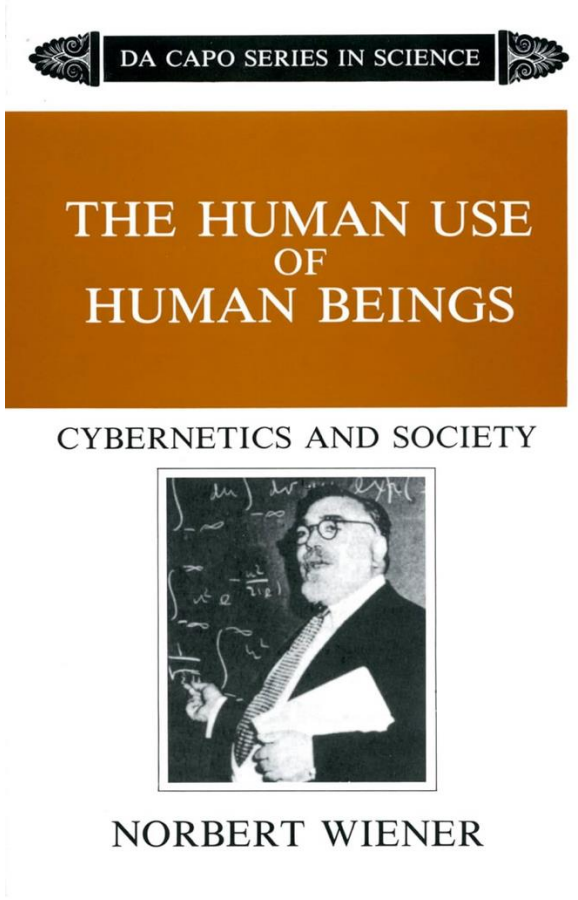
Lancaster University

- **Deontological Perspective:**
  - Privacy as a fundamental right
  - Not to be infringed upon, regardless of potential outcomes
- **Utilitarian Perspective:**
  - Balancing individual privacy vs. societal benefits
  - Example: Public health initiatives using aggregated data to prevent disease outbreaks
- **Virtue Ethics:**
  - Privacy as part of human flourishing and dignity
  - Protecting privacy shows respect for individual dignity
- **Feminist Perspectives:**
  - Power imbalances in data collection and usage
  - privacy as a tool to protect vulnerable communities

Book Recommendations







Privacy Paradox

Lancaster University

Definition:

- "When people disclose personal info in ways that are inconsistent with the high value they claim to place on privacy"

Potential explanations **TL;DR**

- *Rational ignorance*: "Too long; didn't read" approach to privacy policies
- *Transparency paradox*: Overload of complicated details → People tune out
- *Control paradox*: We like having control, but we rarely exercise it
- *Disincentivized to protect privacy*: "Trade convenience for data"

Question: "Are we *actually* making a choice, or is it an illusion of choice?"

What do you know about Cambridge Analytica Scandal?

Who Was Involved?

Lancaster University

Key Players:

- **Cambridge Analytica (CA):** A political consulting firm specializing in data analytics to influence elections
- **Facebook:** The social media platform from which vast amounts of user data were improperly harvested
- **Aleksandr Kogan:** A researcher who developed an app called "This Is Your Digital Life," used as a tool for data collection

How Did the Data Misuse Occur?

Lancaster University

Data Collection:

- Kogan's app, presented as a personality quiz, collected **detailed personal information**
- The app accessed data from **users' Facebook friends** without their explicit consent
- Around **270,000** users downloaded the app, but data from **up to 87 million** people were harvested due to the **friends-of-users loophole**

Unauthorized Use:

- The data was shared with **Cambridge Analytica**, violating Facebook's platform policies
- Cambridge Analytica used the data to build **psychological profiles of users**

Election Influence:

- During major campaigns (e.g. **2016 U.S. Presidential Election** and the **Brexit referendum**), profiles were used to create highly targeted political advertisements
- Users were unknowingly manipulated through **tailored messages** designed to exploit their psychological vulnerabilities

The Case for Privacy Regulations

Lancaster University

Problems Without Regulations:

- Data **misuse** (e.g., Cambridge Analytica scandal)
- **Lack of transparency** and **accountability** in AI
- Erosion of privacy and **trust** in technology

Why Regulations Are Necessary:

- Protect **fundamental rights** to privacy
- Provide **guidelines** for ethical data usage
- Foster innovation by **establishing trust**

The Case for Privacy Regulations

Lancaster University

Problems Without Regulations:

- Data **misuse** (e.g., Cambridge Analytica scandal)
- **Lack of transparency** and **accountability** in AI
- Erosion of privacy and **trust** in technology

Why Regulations Are Necessary:

- Protect **fundamental rights** to privacy
- Provide **guidelines** for ethical data usage
- Foster innovation by **establishing trust**

General Data Protection Regulation (GDPR)

Lancaster University

Why?

- Address inconsistencies in data protection laws across the EU
- Strengthen individuals' control over their personal data
- Respond to high-profile data breaches and growing public concern

What it Does?

- Establishes principles like data minimization and purpose limitation
- Grants rights: access, erasure, portability
- Requires consent and transparency

KEY FACTS:

- Introduced in 2016
- Enforced in 2018
- Applies to organizations handling data of EU citizens, regardless of location

PERFORMANCE:

- Over €1.5 billion in fines since inception.
- Criticisms: High compliance costs, unclear guidelines for SMEs.

General Data Protection Regulation (GDPR)

Lancaster University

Was GDPR success or failure?

GDPR – A “Successful Failure”?

Lancaster University

Arguments for Failure	Arguments for Success
Privacy paradox persists	Forces explicit consent, raising awareness
High burden on the user to manage privacy (reading endless policies)	Documents the “illusion” of choice
Do people truly feel empowered?	Strengthens the argument that people *don’t* really care about privacy, ironically proving the point

GDPR’s effectiveness is subjective, depending on whether we focus on awareness or outcomes
It’s a 'successful failure'—**effective in raising awareness** but **challenging in execution**

Gordon Hull. 2015. Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data. Ethics and Information Technology 17, 2 (2015), 89–101.

GDPR Enforcement: Real Cases

Lancaster University

- Major fines on Big Tech (e.g., Google, Meta) for privacy breaches
  - Meta fined €265m by Irish Data Protection Commission*
- Non-compliance: failure to obtain proper user consent or meet GDPR obligations
  - Google hit with £44m GDPR fine over ads**
- SMEs (small & medium enterprises) also face challenges (unclear guidelines)
  - Austrian website's use of Google Analytics found to breach GDPR†
- Growing cross-border investigations by EU regulators
  - British Airways fined £20m over data breach††

* https://www.bbc.co.uk/news/world-europe-63786893
** https://www.bbc.co.uk/news/technology-46944696
† https://techcrunch.com/2022/01/12/austrian-dpa-schrems-ii/
†† https://www.bbc.co.uk/news/technology-54568784

The EU Artificial Intelligence Act (EU AI Act)

Why?

- Address risks of unregulated AI applications.
- Promote trustworthy AI aligned with ethical principles.

What it Does?

- Classifies AI systems by risk (unacceptable, high, limited, minimal)
- High-risk AI: strict compliance (e.g., medical devices, biometric ID)
- Encourages transparency and accountability

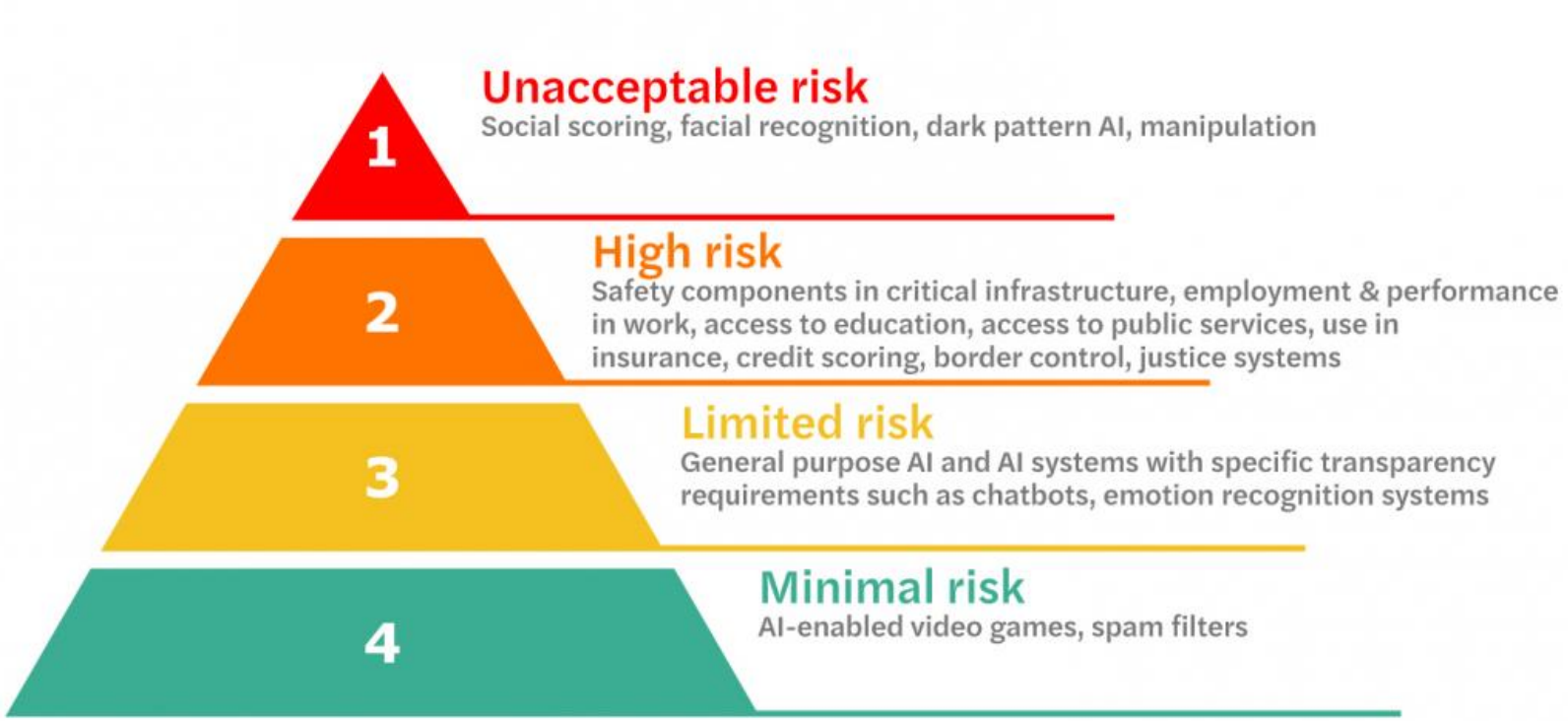
KEY FACTS:

- Proposed in April 2021
- Expected enforcement by 2025
- World's first comprehensive AI regulation

PERFORMANCE:

- Still under refinement, expected to set global standards
- Criticisms: Potential to stifle innovation, unclear scope for SMEs

The EU Artificial Intelligence Act (EU AI Act)



KEY FACTS:

- Similar technologies might fall into different categories, depending on their use
- Some feel it's still too broad or vague, especially as AI evolves rapidly

https://www.forvismazars.com/ie/en/insights/news-opinions/eu-ai-act-different-risk-levels-of-ai-systems

Regulations in Other Countries

Lancaster University

- **US:** No unified federal privacy law
  - Sectoral approach: HIPAA (healthcare), COPPA (children), etc
  - State-level regulations:
    - **California Consumer Privacy Act (CCPA)**: Closest to GDPR
    - Virginia Consumer Data Protection Act (VCDPA)
- **UK:**
  - GDPR adopted as UK GDPR post-Brexit
  - Data Protection Act 2018 complements GDPR principles
  - Focus on balancing data-driven innovation with privacy
- **China:**
  - Personal Information Protection Law (PIPL): Comparable to GDPR
  - Cybersecurity Law and Data Security Law

Lancaster University

Privacy in AI and Robotics

Do We Need a Separate Regulation for Robots?

Privacy in AI and Robotics: Why It Matters

Lancaster University

- **Unique challenges posed by autonomous systems:**
  - Continuous data collection via sensors
  - Need for real-time decision-making
- **Examples of data types collected:**
  - Visual (cameras in robots)
  - Behavioural (interaction data)
  - Biometric (facial recognition, voice)
- **Purpose of Data Collection:**
  - Navigation and environment mapping (e.g., autonomous vehicles)
  - Human-robot interaction (e.g., social robots understanding emotions)
  - Customization of user experience

How Robots Collect and Use Data

Lancaster University

- **Sensors and Data Sources:**
  - Cameras, LiDAR, microphones, wearables, etc
- **Primary Risks:**
  - Unauthorized access or data breaches
  - Lack of transparency in AI algorithms (black-box problem)
  - Bias in AI leading to unfair outcomes
  - Ethical concerns in surveillance applications
- **Privacy-Preserving Technologies**
  - **Federated Learning:** Training AI models locally to avoid raw data transfer
  - **Differential Privacy:** Adding noise to datasets to anonymize individual data
  - **Encryption:** Ensuring secure data transmission and storage

Federated Learning

Lancaster University

- **What is it:**
  - A decentralized machine learning training models directly on users' devices without transferring raw data to a central server
- **How it works:**
  - Devices process data locally to improve the model
  - Only aggregated updates (e.g., parameter changes) are sent to a central server for model improvement, ensuring raw data stays on the device
- **Why it’s important:**
  - Protects sensitive data by eliminating the need for centralized data storage.
  - Reduces the risk of data breaches.
- **Example:**
  - Google’s Federated Learning on Android Devices
  - Used to improve predictive text suggestions without uploading user-specific typing data

Differential Privacy

Lancaster University

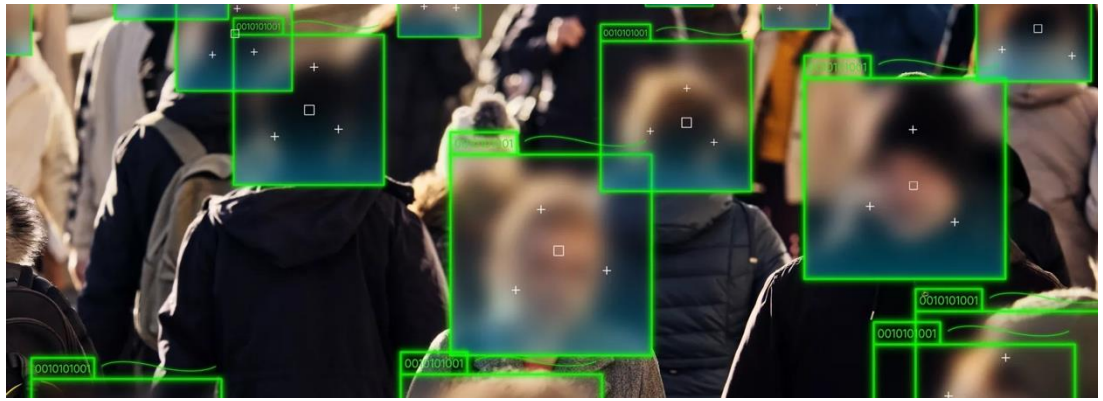
- **What is it:**
  - Protecting individual data points by introducing statistical noise, making it impossible to trace data back to a specific individual
- **How it works:**
  - Adds randomness to queries or computations on the dataset while preserving aggregate trends
  - Ensures that outputs provide useful insights without compromising individual privacy
- **Why its Important:**
  - Balances the need for data utility (e.g., for AI training) with robust privacy safeguards
  - Makes data breaches less damaging, as individual identities remain hidden
- **Example:**
  - Apple's Use of Differential Privacy
  - Apple employs this method to collect usage statistics (e.g., emoji usage, search patterns) without compromising user privacy

Encryption

- **What is it:**
  - A process of converting data into an unreadable format (ciphertext) that can only be accessed with a decryption key
- **How it works:**
  - **During transmission**: Data is encrypted before being sent and decrypted upon arrival
  - **During storage:** Data is kept encrypted to prevent unauthorized access
- **Why it's important:**
  - Prevents eavesdropping, tampering, and unauthorized access during data transfer and at rest
  - Essential for protecting sensitive information in robotics and AI systems, such as personal data collected by robots
- **Example:**
  - End-to-end encrypted messaging apps (e.g., Signal, WhatsApp)

Learning from Real-World Examples

- **Case 1: Autonomous Vehicles**
  - Privacy concerns: Cameras and sensors capturing pedestrians and license plates
  - Current solutions: Edge computing for real-time decision-making without cloud storage



https://wowowow.com/challenges-of-implementing-ai-in-self-driving-cars

- **Case 2: Social Robots in Public Spaces**
  - Privacy concerns: Recording interactions or behaviours
  - Proposed solutions: Clear policies on data retention and anonymization

https://www.brookings.edu/articles/when-robots-are-everywhere-what-happens-to-the-data-they-collect/

New Frontiers of Privacy Concerns

Lancaster University

- **Generative AI & Deepfakes:** Identity theft and spread of misinformation
- **Biometric Data:** Privacy challenges from face, voice, and gait recognition technologies
- **Neurotechnology:** Brain-computer interfaces (BCI) raise questions about mental privacy
- **Consent Fatigue:** Endless pop-ups result in users ignoring privacy agreements
- **Rapid Tech Evolution:** Laws struggle to keep up with advancements

“Nothing to Hide” Argument

Lancaster University

Common Claim: “If you've got nothing to hide, you've got nothing to fear”

Counterpoints (Solove’s Approach):

- **Aggregation:** Harmless data points + harmless data points = revealing conclusion
- **Distortion:** Data taken out of context may mislead or cause harm
- **Exploitation:** Collected data can be weaponized for manipulation

Solove, D. J. (2011). Why privacy matters even if you have ‘nothing to hide’. Chronicle of Higher Education, 15.

Is Privacy Dead?

Is Privacy Dead?

Lancaster University

Solove on the complexity of privacy: Not a single essence but many overlapping concerns, It's about more than secrecy

- *Privacy as control:* Over personal data
- *Privacy as autonomy:* Freedom from constant scrutiny
- *Privacy as dignity:* The ability to choose how you present yourself to the world

Hopeful Trust

Lancaster University

Key Idea: People trust systems even when privacy is violated

- **Information disclosure** can be a pragmatic response to limited privacy protections
- **Justifications:**
  - “Surely if it were really bad, someone would step in!”
  - “The company has so many users—it must be safe”

- **Insight:** This “**hopeful trust**” reveals people want a world where these services are worthy of trust—hence privacy isn’t “**dead in our hearts**”

User-Centric Privacy Tips

Lancaster University

- Use strong, unique passwords; enable multi-factor authentication
- Regularly review app permissions and privacy settings
- **Limit oversharing**: think before posting personal details online
- Be cautious with public Wi-Fi or unencrypted websites (HTTP) --> use **HTTPS**
- Consider **privacy-focused tools** (VPNs, secure messaging apps)

Key Takeaways

Lancaster University

- Privacy is **multifaceted** and **context-dependent**
- New tech (IoT, robotics, AI) **magnifies old privacy dilemmas** while creating **new ones**
- Existing regulations (like GDPR) are **necessary** but **not always sufficient**
- **Everyone**—users, policymakers, developers—**plays a role** in shaping the future of privacy

Future Outlook

- **Questions?**

- **Looking Ahead:** Next week—Surveillance & Censorship (a.k.a. Privacy Part 2). We'll explore government surveillance, censorship, and why it matters for privacy rights

Lancaster University

Thank you for listening, any questions?