Privacy: A Surmountable Challenge for Computer Vision

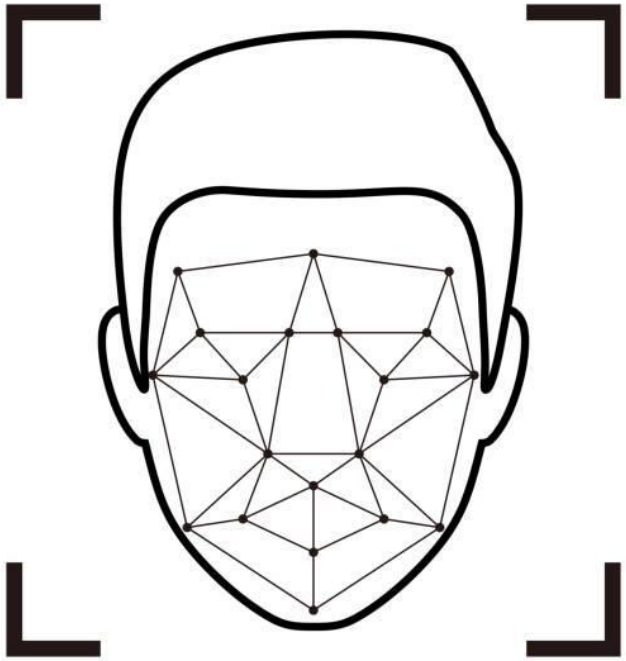
Susan Kennedy, PhD
Assistant Professor of Philosophy
Santa Clara University

POLICY | TECH | PRIVACY

IRS will end use of facial recognition after widespread privacy concerns

The use of ID.me's services had been strongly criticized since the partnership was announced

By Corin Faife | @corintxt | Feb 7, 2022, 2:50pm EST

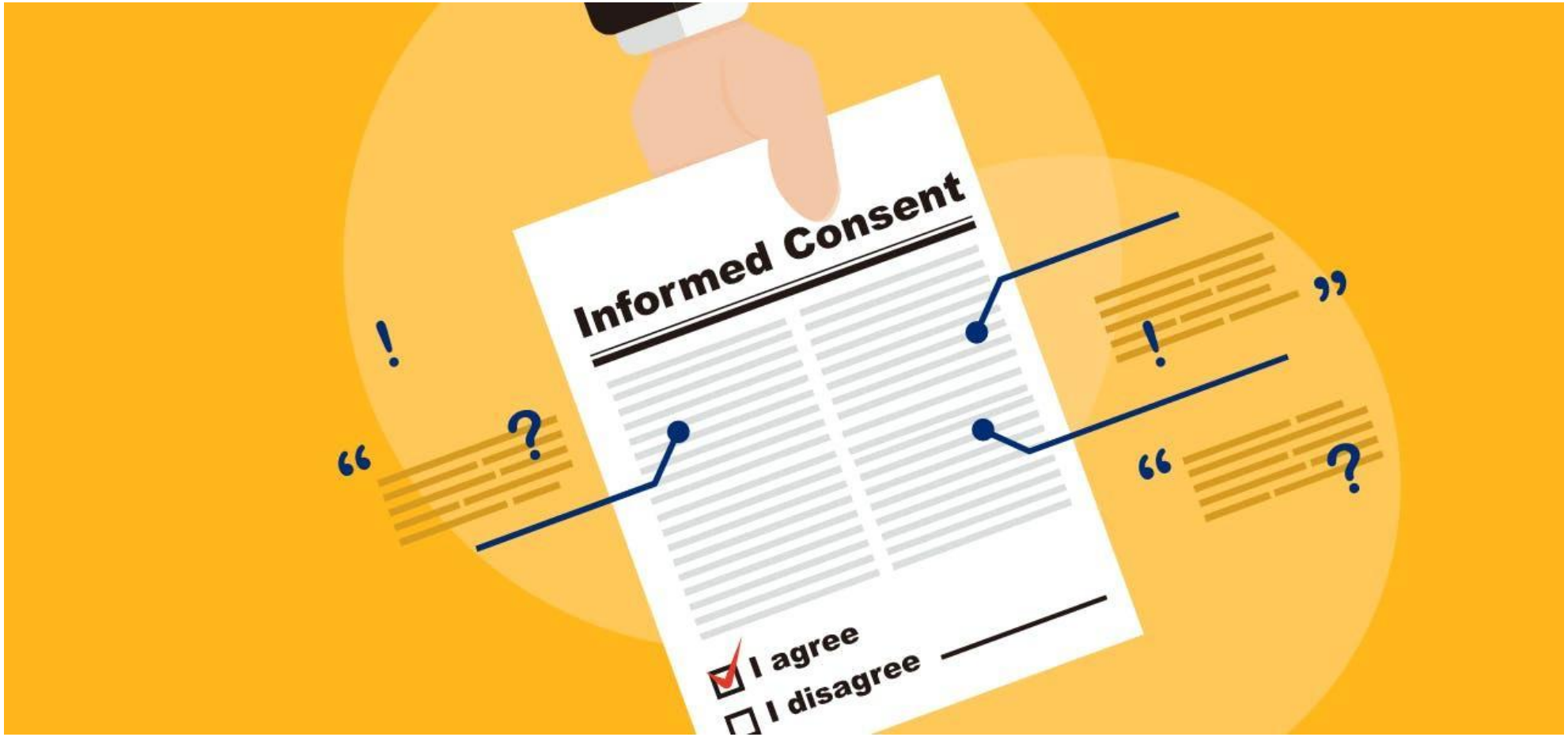


Privacy: A Roadblock for Innovation?

Agenda

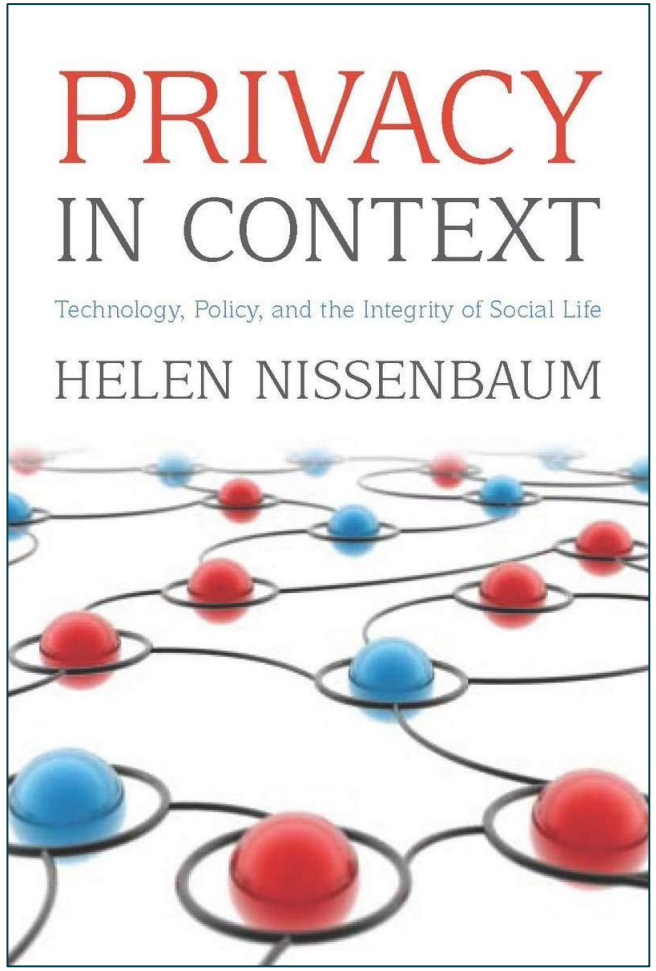
- Limitations of Current Privacy Procedures
- Contextual Integrity Framework
- Case studies: Privacy in Practice
- Key Takeaways

Looking Beyond Informed Consent



Contextual Integrity

- Context shapes users' expectations of privacy
- Privacy is a **right to the appropriate flow of information**



Context-Relative Informational Norms

Context: What is the prevailing context?

Actors: Who are the subjects, senders and recipients of information?

Attributes: What is the type or nature of information?

Transmission Principle: What are the constraints on the flow of information?

Santa Clara University

Context-Relative Informational Norms

If the new practice results in any changes to these features, the practice is **flagged** as violating privacy

- Context: What is the prevailing context?
- Actors: Who are the subjects, senders and recipients of information?
- Attributes: What is the type or nature of information?
- Transmission Principle: What are the constraints on the flow of information?

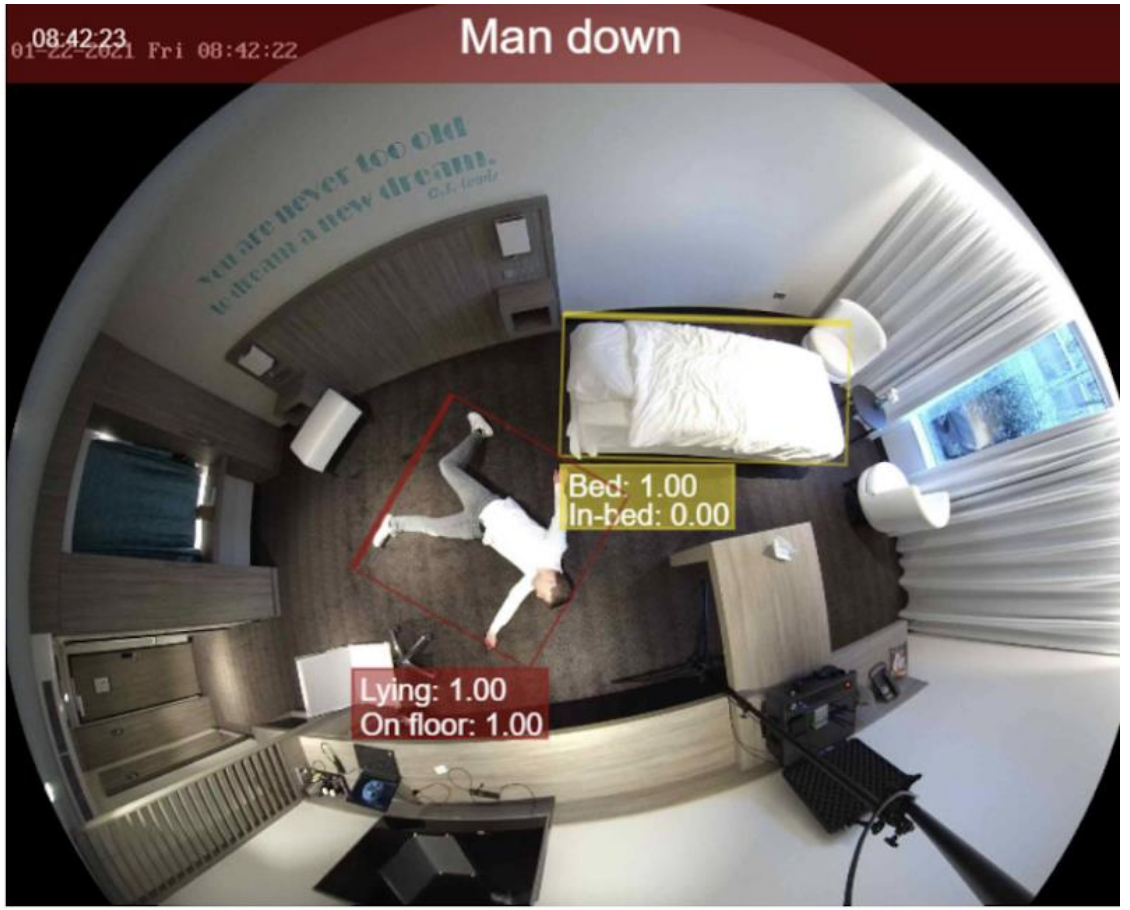
Santa Clara University

Second Chances

- The contextual integrity framework can pinpoint privacy concerns and help guide design solutions
- Practices that are flagged as violating privacy may still be permissible, all things considered

Fall Detection Devices

Kepler Night Nurse™



Application of Contextual Integrity Framework

Fall Detection Device

Context: Caregiving in health care facilities

Actors: Patients, Caregivers, **Annotators at Kepler**

Attributes: Videos and Images of Patients

Transmission Principle: Caregiver's mandate, confidential

Fall Detection Device - Analysis

- **Design Solutions**
  - Security measures for the annotation process
- **Moral Considerations**
  - Users directly benefit from improved model accuracy
  - Invasions of user privacy are minimized compared to the alternative best practices for caregivers

Application of Contextual Integrity Framework

ID.me Facial Recognition

Context: Identity verification and fraud detection for the IRS

Actors: IRS, **ID.me**, **third parties**

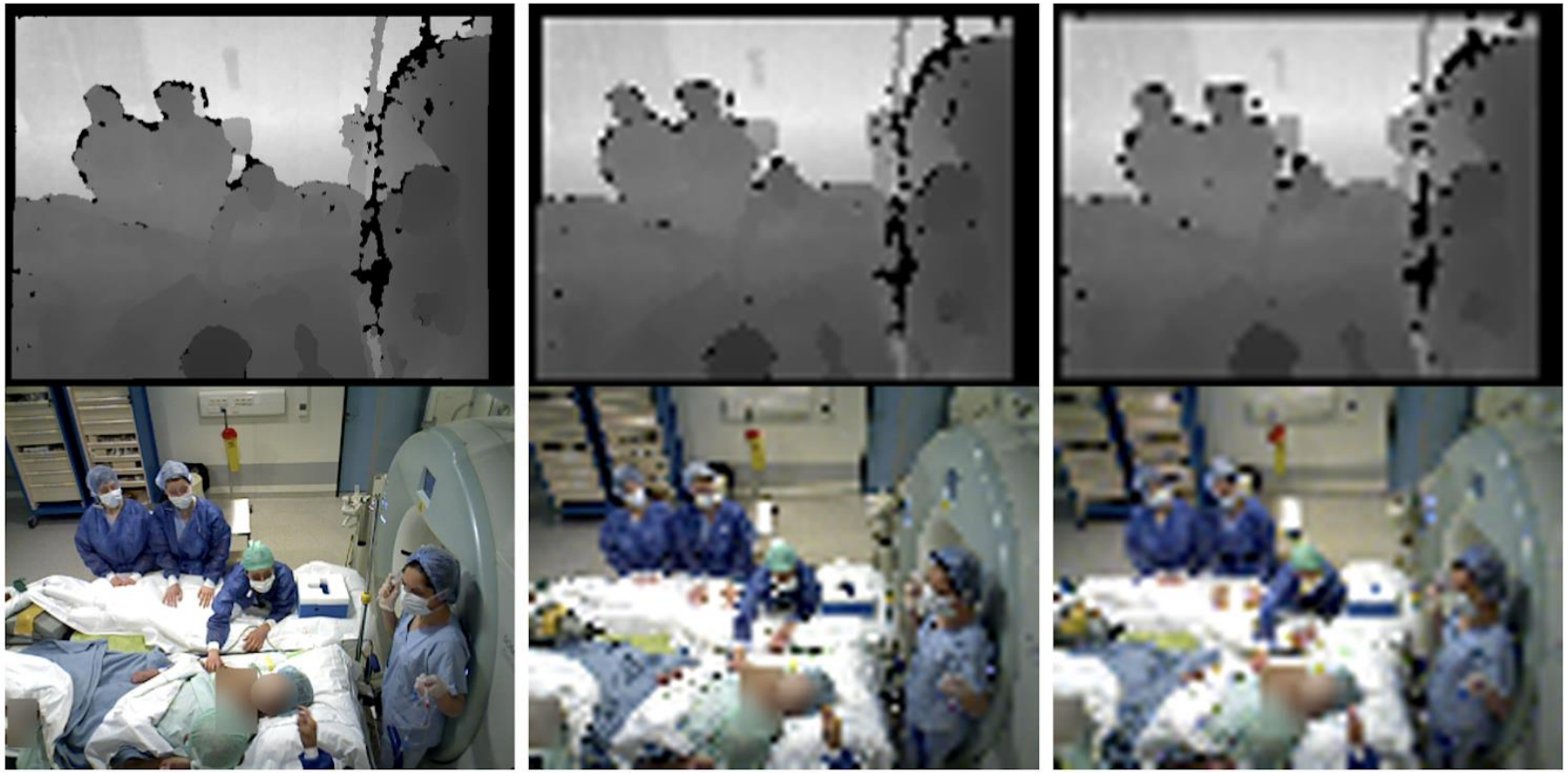
Attributes: **Images of users**

Transmission Principle: **Mandatory**

ID.me Facial Recognition - Analysis

- **Design Solutions**
  - Alternative verification option for users that does not involve facial recognition
  - Create an avenue for users to provide consent for data sharing
- **Moral Considerations**
  - Users directly benefit from improved fraud detection
  - Improves equity by enabling online access to government services for users who are overseas

Operating Room Monitoring

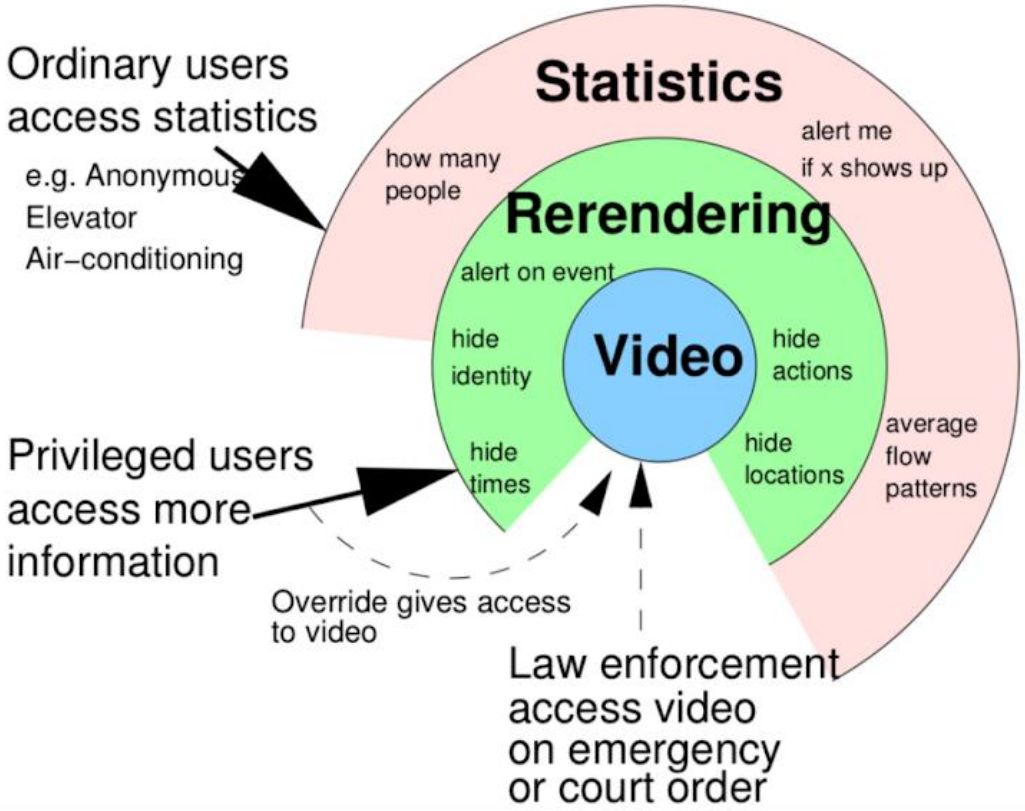


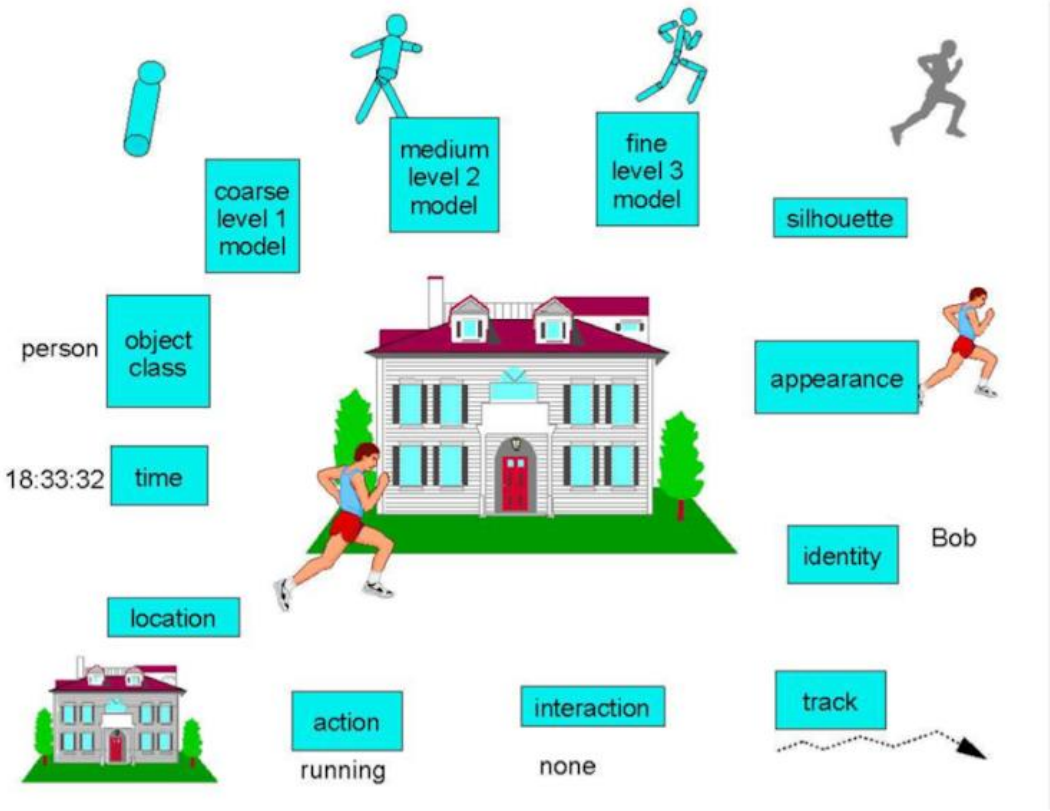
(a) 640x480 (1x) (b) 80x60 (8x) (c) 64x48 (10x)

"Human Pose Estimation on Privacy-Preserving Low-Resolution Depth Images," Srivastav, Gangi, Padoy 2019

Santa Clara University

Design Choices: Levels of Access





"Blinkering Surveillance: Enabling Video Privacy through Computer Vision," Senior, Pankanti, Hampapur, Brown, Tian, Ekin 2004.

Key Takeaways

- The Contextual Integrity framework can be used to:
  - Pinpoint privacy concerns
  - Guide design solutions
  - Frame moral considerations
- Design choices: Hardware selection, de-identification, data minimization, different levels of information access, etc.

Resources

1 – Helen Nissenbaum's book *Privacy in Context*
https://dl.acm.org/doi/10.5555/1822585

2 – Privacy by Design: The 7 Foundational Principles
https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

3 – Privacy by Design – Practical Guidance
https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

2022 Embedded Vision Summit

"Ask the Ethicist: Your Questions about AI Privacy, Bias, and Ethics Answered"

Tuesday, May 17th

2:40 – 3:10 pm PT

Business Insights 1 – Theater (upstairs)