The Need for Inherently Privacy-Preserving Vision in Trustworthy Autonomous Systems

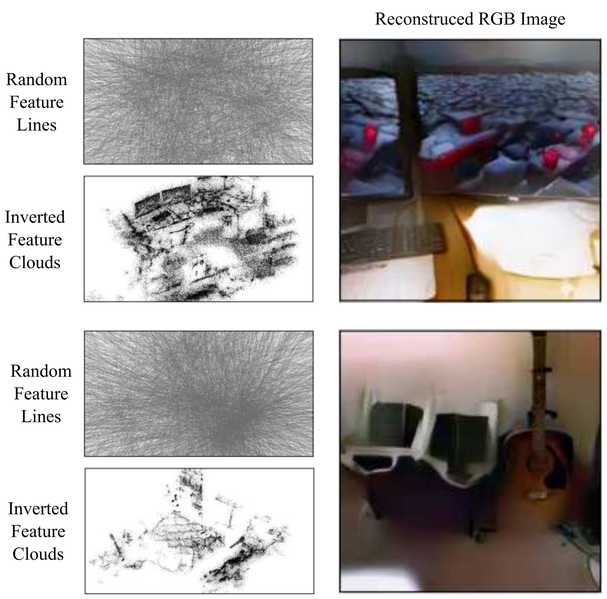
Adam K. Taras†, Niko Suenderhauf, Peter Corke, and Donald G. Dansereau

What is privacy?

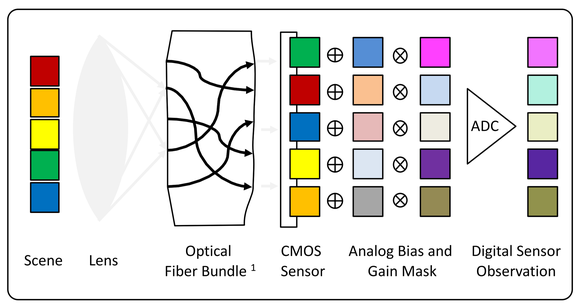
- There are different concepts and standards; we focus on informational privacy
- Cameras motivated the original "right to be left alone" definition
- Only 0.5% of robotics papers from 1982-2019 mention privacy [1]
- Privacy concerns create social boundaries where current technologies cannot operate

Current Gaps

- Most methods are simply not privacy preserving! [2]

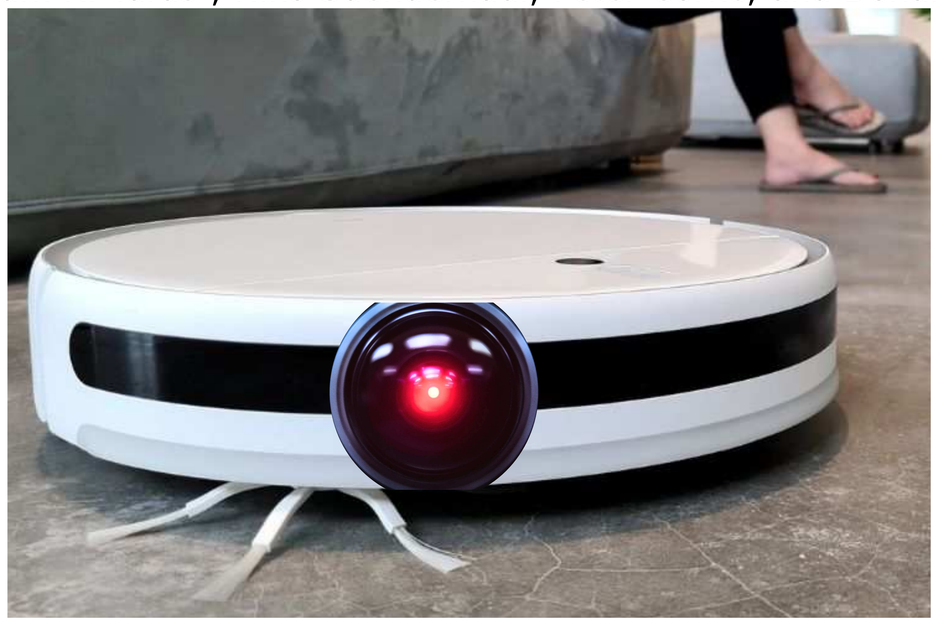


- The rest are infeasible to manufacture at scale [3]



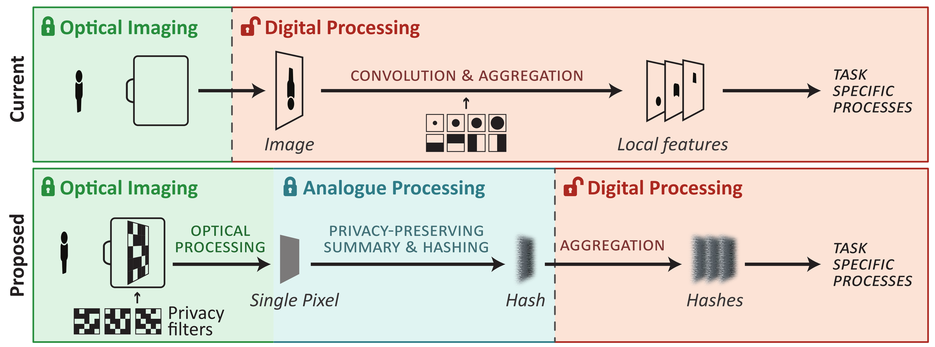
References

[1] S. Eick and A. I. Antón. "Enhancing privacy in robotics via judicious sensor selections" ICRA 2020
[2] K. Chelani *et al.* "How privacy-preserving are line clouds? recovering scene details from 3d lines." CVPR 2021
[3] J. Byrne *et al.* "Key-Nets: Optical Transformation Convolutional Networks for Privacy Preserving Vision Sensors." arxiv 2020



Inherently privacy-preserving vision

Specialise Cameras : Optical/Analogue Processing



Information Destruction

Operations before digitsation **remove information**

Obfuscation

Such that the inverse problem is **intractable**, with brute force as the only valid method

Ambiguity

Even if a solution is found, an attacker **cannot be sure** it is the right one

Use Context

Solutions should be **specialised** to the context through narrow priors

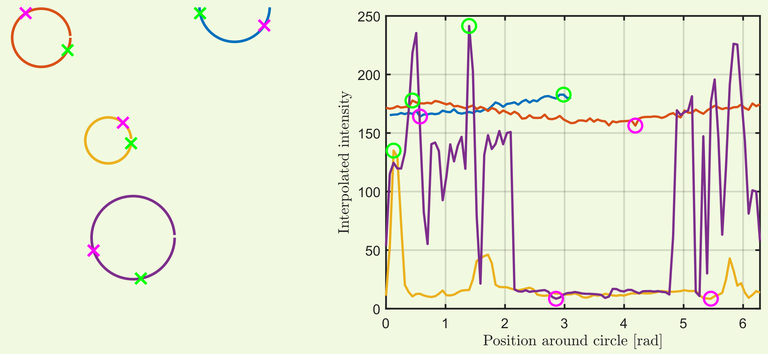
Call to Action

- Privacy concerns prevent deployment of robotic systems in critical contexts including healthcare, manufacturing and defence
- Nuanced understanding the different forms of privacy and their technical implementations is an exciting new space
- Implmenting inherently privacy-preserving vision would permit systems that are currently behind social barriers to become feasible, helping individuals, businesses and governments to leverage automation

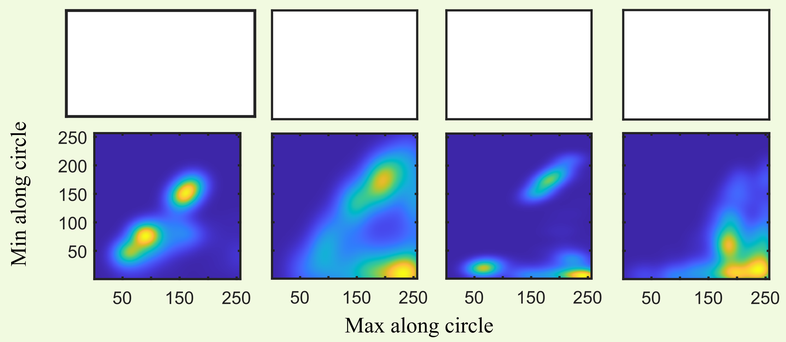
† adam.taras@sydney.edu.au

Proof-of-Concept: Localisation

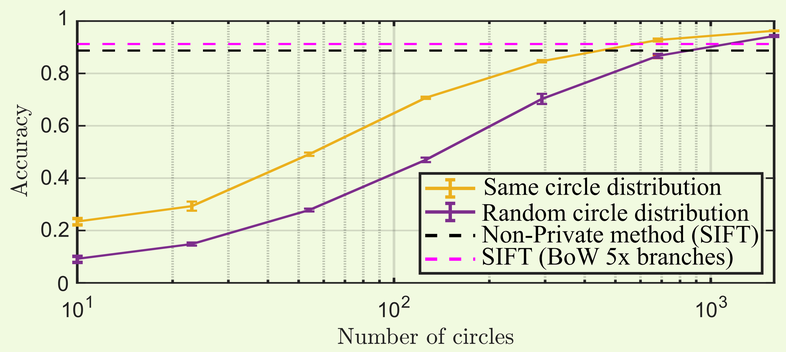
- Imaging-free localisation
- Optical-analogue global appearance fingerprint
- Digital micromirror device (DMD) + single-pixel sensor + max hold circuit
- Proof-of-concept in simulation



- DMD + analogue electronics: find extrema along curves



- Accumulating extrema yields a "fingerprint" of the scene



- Localising using the fingerprints and bag of words
- Performance competitive with conventional SIFT features
- Image reconstruction is intractable