Trusting the Computer in Computer Vision: A Privacy-Affirming Framework

Andrew Tzer-Yeu Chen, Morteza Biglari-Abhari, Kevin I-Kai Wang
Embedded Systems Research Group
The University of Auckland, New Zealand

21 July 2017

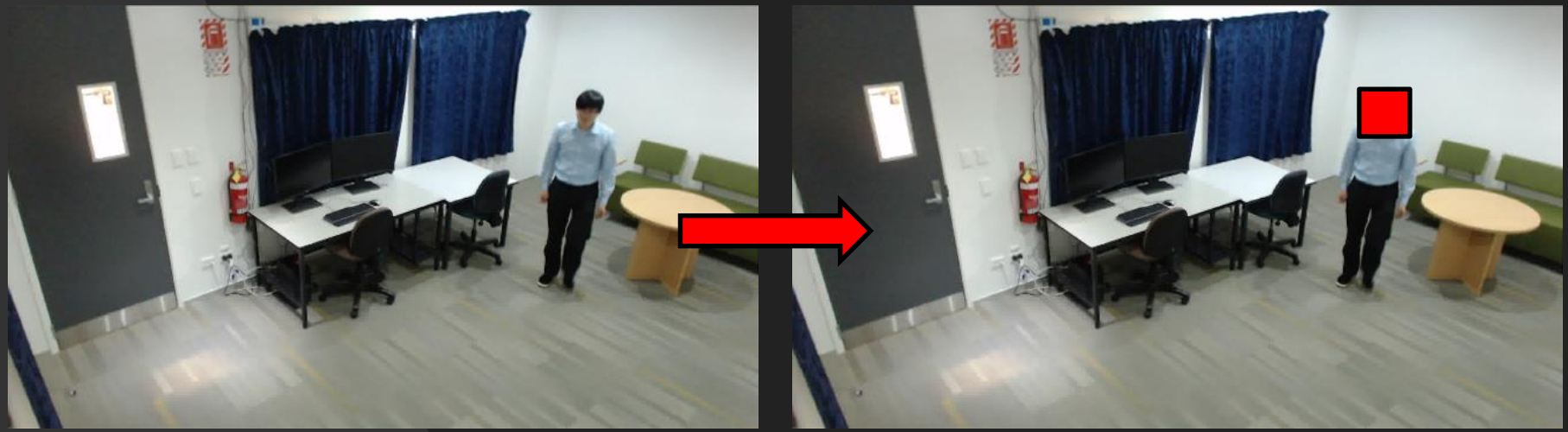
Privacy:

"The condition of not having undocumented information known or possessed by others"
– William Parent (US Philosopher)

Information often becomes documented when it is *recorded* and *reproducible*

Privacy is not binary – specificity and scale can be important

Privacy-Aware:



What information are we receiving in the image?

What information do we genuinely need to collect?

What other undocumented information are we unintentionally collecting?

How can we best minimise unintentional breaches of privacy?

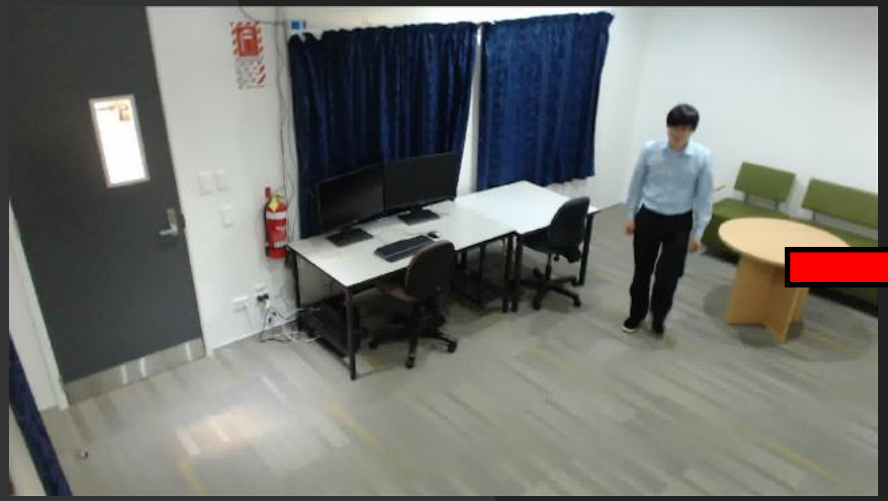
The act of documenting information may not be of significant concern in itself

- Who has *access* to the information?

Human operators can be a weakness in the system; maliciously or accidentally

- Do we really need a *human-in-the-loop*?

Privacy-Affirming:



30 Mar 17 11:47AM
Person 3 in Zone B
(Workspace Area)

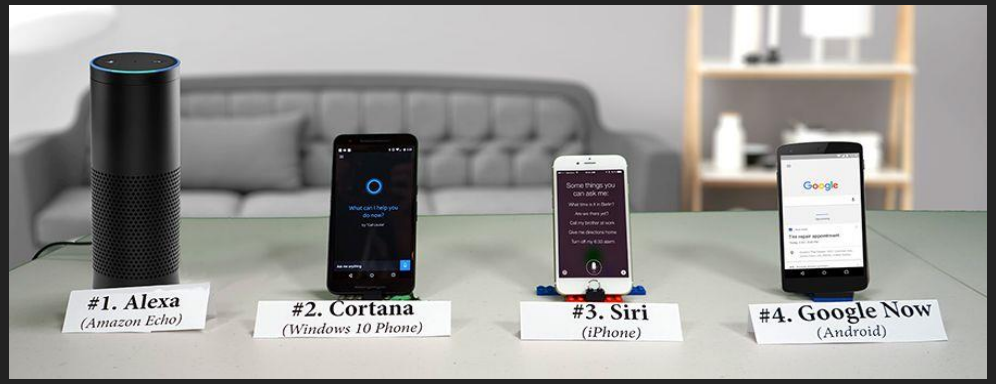
Privacy-Aware vs. Privacy-Affirming
Blacklisting vs. Whitelisting

Privacy-Affirming:

Panasonic

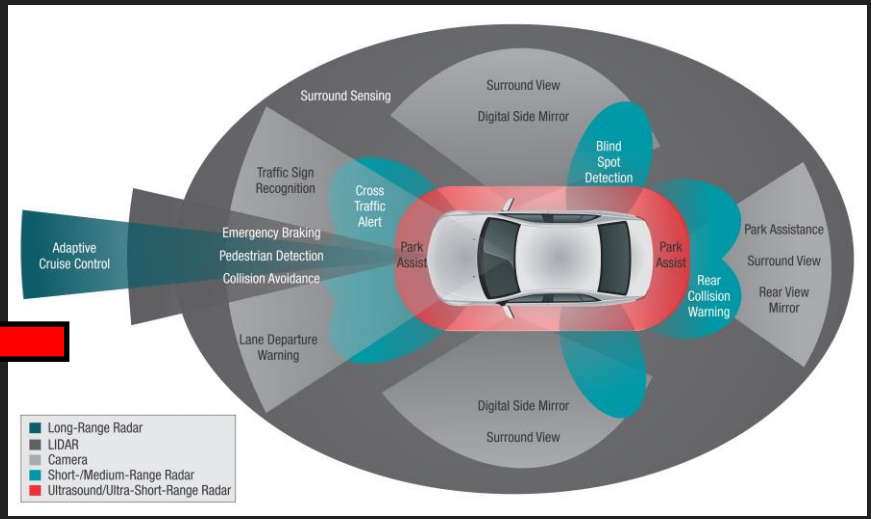
30 Mar 17
11:47AM: ID 3 in Zone B
11:47AM: ID 4 in Zone D
11:48AM: ID 7 in Zone A
11:48AM: ID 6 in Zone G
11:48AM: ID 3 in Zone C
11:49AM: ID 9 in Zone B

Abstraction



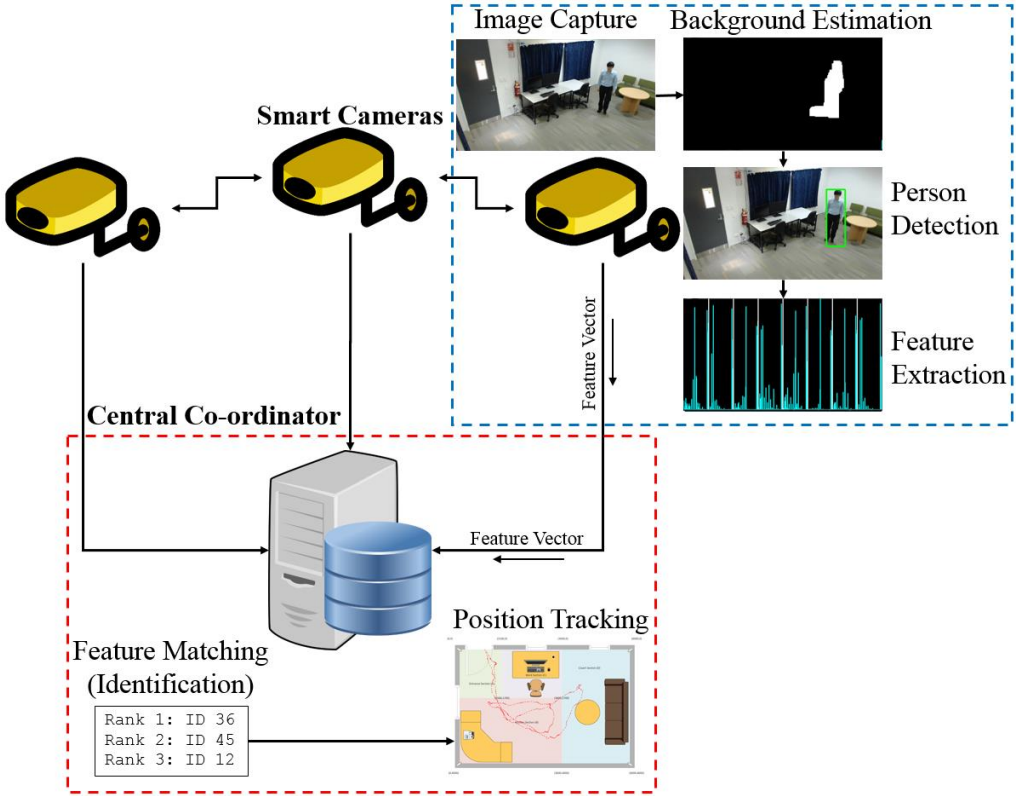
David Pogue, Yahoo! Tech

Ford Motor Company



Texas Instruments

A Distributed Privacy-Affirming Architecture



Darkly (Jana et al., 2013)

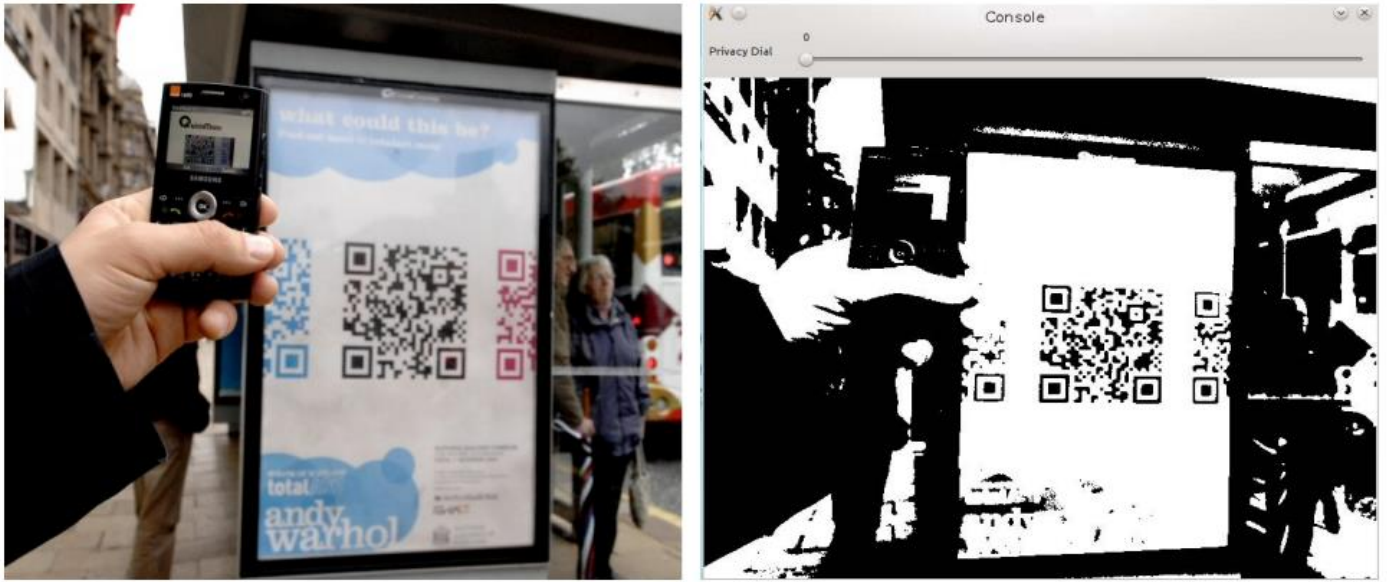


Figure 7. Output of the thresholding binary transform on an image of a street scene with a QR code. QR decoding application works correctly with the transformed image.

A Test for Privacy-Oriented Systems

	Archive-Critical	Archive-Free
Human Processing	Access Control or Permissions	Privacy-Aware
Machine Processing	Privacy-Aware and Permissions	Privacy-Affirming

Towards a Privacy-Affirming Society

- Repeated demonstrations of validity and accuracy
- Certification and auditing regime
- Accepting new ways of making decisions
- Public education and marketing
- Transparency from surveillance network owners
- Strong security and data storage

Privacy in Camera Surveillance Networks

1. Hope that human authorities are benign
2. Democratise access to surveillance
3. Trust the computer in computer vision

Any questions?

andrew.chen@auckland.ac.nz