Smart Cities and IoT:
Privacy and information security

Dr Monique Mann
Lecturer, School of Justice
Crime and Justice Research Centre
Intellectual Property and Innovation Law

QUT Law

"Technology is neither good nor bad, *nor is it neutral*"

Kranzberg (1986)

Facial recognition software trials in Queensland alarm privacy advocates

The World Today By Annie Guest

Updated 10 Mar 2017, 2:57pm

A facial recognition technology trial is underway in Queensland, alarming privacy advocates who fear such developments could lead to bigger databanks of stored personal information.

The Toowoomba Regional Council has begun trialling the software called iOmniscient on behalf of the Brisbane, Gold Coast and other councils.

iOmniscient works by analysing images recorded by existing CCTV cameras.

A rollout of similar software has been supported by the Federal Government for passport processing in Australia, and the Northern Territory police are already using something similar.

Monique Mann, a law lecturer at the Queensland University of Technology and member of the Australian Privacy Foundation, said the Toowoomba Council's decision was alarming.

PHOTO: The new software analyses CCTV images from existing cameras in the area.
(ABC News: Jordan Hayne, file photo)

MAP: Toowoomba 4350

Key points:

- Similar software in use by NT Police, expected to be rolled out in airports
- Toowoomba Council says it has not talked about using the software on streets

National

Facial recognition cameras on public transport in Gold Coast trial

Charles Miranda, News Corp Australia Network
June 9, 2017 12:30am
Subscriber only

EXCLUSIVE: Facial recognition technology is set to be deployed on the public transport network including trains, trams and buses at the Gold Coast Commonwealth Games next year, to identify potential terror suspects before they can get close to any sporting or public venue.

Privacy protection?

- Exemptions to *Privacy Act 1988* (Cth), no constitutional protection of human rights, no privacy tort, no relevant jurisprudence

- We need to consider and question:
  - Privacy in public spaces
  - Behavioural monitoring in public spaces
  - Data linkage
  - Issues of consent / opt-out
  - Concept of consent in increasingly connected censor society

Security researchers reveal mystery North American casino was hacked through its connected FISH TANK

- A new report from security firm Darktrace reveals even a fish tank can be hacked
- A North American casino installed a high-tech tank that can control temperature
- But, despite efforts to protect it, it turned out to be a weakness in their network
- Before being stopped, hackers transfered 10GB of data to a device in Finland

Controversial security cameras in Moreton Bay have been compromised but Council will not provide details

By Josh Bavas

Updated 23 Jun 2017, 4:14pm

Controversial security cameras in the Moreton Bay region have been compromised, but the council will not provide details.

More than 330 of the 874 council-run cameras were fitted with the ability to record audio earlier this year, with plans to upgrade hundreds more.

But documents obtained by ABC News under Right to Information showed some of the cameras had "compromised IP addresses".

A Moreton Bay Regional Council spokeswoman rejected the cameras were hacked and said "there had been no unauthorised access to council's CCTV network".

PHOTO: A security camera in Strathpine, north of Brisbane. (ABC News: Josh Bavas)

RELATED STORY: Concern about 'big brother' surveillance use in Moreton Bay area

Information security

- IoT devices are notoriously insecure
- Provides a huge attack surface for malicious actors
- Interconnected nature of devices poses risks to infrastructure of smart cities
- Monetised data with commercial value will entice malicious actors
- Information storage and security, by design
  - Siloed information storage and defensive security architecture

m6.mann@qut.edu.au
@DrMoniqueMann