* 2019 – Facial Recognition to Replace Opal Cards
  + Argument for convenience of travel – to just turn up and go
    - Customers already embraced credit cards/electronic device to tap on/off
    - Vision similar to Amazon’s “Just Walk Out” – supermarket where shoppers are facially scanned, pick items from shelves, leave 🡪 auto account charge
    - Facial recognition for ‘opted in’ customers, linked to Opal account 🡪 no more gate barriers
    - Digital identity verification – allows contactless payments, entry to buildings, on to planes, at banks and hotels
  + Argument against – disregard for community opinion
    - Data collected would be enormous commercial value to whomever owns it
      * Claims NSW taxpayers used by government to make money
    - People have right to expect certain level of privacy when navigating public spaces
    - Citizens must be able to trust governments are taking appropriate action to protect privacy
      * Opt-out systems difficult to implement 🡪 everyone using transport systems is being scanned
      * Europe’s strict privacy laws 🡪 affects European citizens using Australian transport
* 2019 – AFR discusses Facial Recognition
  + Argument for facial recognition – convenience + used for the greater good
    - Hotel check-in a lot easier, and operates without staff
    - Facial recognition to detect stalkers at Taylor Swift concert
    - 3000 missing children found in a four-day period
    - Facial recognition – access services, pay things, secure precious possessions
    - Smart cities – detection for criminal behaviour, spot accidents
    - Community safety – Australian mass surveillance program through Identity-Matching Services Bill 2018 (IMSB) (pooling of passports + drivers’ licences)
      * System accessed at different levels for security, enforcement and identification issues
      * Guidelines appear to grant significant operational latitude – law enforcement due to suspicions, monitoring major events
      * Low-tier systems available to body corporates to verify identities
    - iOmniscent
      * Software compliant with EU’s privacy regulations
      * Face redaction feature – only reversible for certain cases by authorized individuals
      * Company maintains control over post-sale technology – features can’t be tweaked by user
      * Autonomous response system enabled police to shorten response time to potential terrorist event
        + Balance between security and privacy specific for each society – being alive (terrorism) vs privacy
    - LoopLearn – automated attendance-marking system
      * Records presence of students every 5-10 mins
      * Data anonmysied, under school’s control, students aware
  + Argument for – giving the people what they want
    - Advertisers can have ads specific to people
      * Men’s facial hair commercial – responding to appearance + complementing beard/moustache
  + Argument against – scope for abuse
    - Industry behind technology is cautious – technology outpacing regulation
    - Could unleash mass surveillance on unprecedented scale
    - Google also avoiding implementation until it can address how to avoid “abuse and harmful outcomes”
    - Potential dystopia – China’s implementation of Skynet is shaming jaywalkers publicly on a giant screen
    - Normalized the pervasive nature of facial recognition due to biometrics + Face ID on mobile devices
      * “We are getting used to convenience and forgetting that it comes at the cost of loss of privacy”
  + Argument against – government and corporate surveillance
    - Stifling intellectual privacy – place where we can be alone to think
      * Concept of privacy + freedom of association disappears fairly rapidly
        + Cairns facial recognition in school’s toilet to tackle bullying
    - Affecting power balance between individuals and observers – increases risk of blackmail, discrimination + persuasion
      * Knowledge is power – Washington DV police blackmailing married patrons of gay club by looking up licence plates of cars outside
    - Lack of transparency or full disclosure of government of how they will use the power 🡪 overall feelings of distrust of government
      * QLD government won’t say how they matched security footage and driver’s licence photos in last year’s Commonwealth Games
      * The laws will have an unprecedented impact on Australians’ privacy
        + Anticipates processing thousands of identity-matching requests per day
      * Capability’s NSW enabling legislation stripped 2 privacy protections from state law
        + Nature of surveillance is poorly described
    - May enable police to directly target people on Suspect Target Management Program (STMP) list
  + Argument against – accuracy of technology is less than humans
    - Effectiveness of technology shows it is still less accurate than humans
    - Accuracy rates significantly lower for people with darker skin and minorities
      * Used by US police force despite inaccuracies
      * Britain – almost entirely inaccurate with false alarms, deployment in Notting Hill Carnival was 98% incorrect
      * Coded gaze – software reflecting the biases of its engineers
      * IBM + Face++ software declared female actors from Black Panther to be male
    - Difficulty with dark faces – not enough detail, in reduced lighting don’t see all lines
    - Affect recognition – facial analysis for detecting if someone’s a terrorist, trustworthy or job ready
  + Argument against – need for enforceable human rights framework for privacy
    - Worries about accuracy + bias need impartial testing groups + meaningful human review
    - Consumers should be told when technology used against them + consent
    - Ongoing government surveillance of specified individuals limited in public either by court order/imminent emergency
* 2019 – Australian Views on Surveillance
  + Police can request access to telephone + internet records 🡪 location, conversations
  + Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 – allows government agencies greater access to encrypted messages
  + Australian views – mild acceptance (52%) of government surveillance
    - Is surveillance needed?
      * Recent terrorists attacks as trigger for regular pushes for anti-terror statutes e.g. Melbourne terrorist attack for new encryption laws
    - Do I trust the government?
      * Trust in Australian government is generally relatively low – people more influenced by general view vs views of specific policies/practices
      * Most didn’t trust government to manage data
        + Large number of people opt out of My Health Record
      * No link between people’s trust in government management of data + acceptance of surveillance
  + Concern for repurposing of surveyed data
    - E.g. insurance companies using info from My Health Record 🡪 legislation to prevent
    - Surveillance data collection is indiscriminate + has no ‘opt out’
* 2018 – Facial Recognition Used by Aus Authorities
  + NSW police preparing to use facial recognition to match CCTV with driver’s licence – detection of criminals + identity theft
  + The Capability
    - Face Verification Service (FVS) – one-to-one image-based match of person’s photo against government record like passport
    - Face Identification Service (FIS) – one-to-many image match of unknown person against multiple government records, to help establish identity
  + Technology breaches privacy rights by allowing collection, storage + sharing of personal details from innocent people who are not suspected of offence
  + NSW Minister for Counter-Terrorism claims there will be threshold limiting system’s use as part of legislation
    - Other Sydney MP argues no proper definitions of how data will be used under current bill
  + Capability only allowed for still images from CCTV, nor real-time/automated surveillance of public spaces
    - NSW – searches to identify person for law enforcement can only happen if offence punishable by 3 years imprisonment or more