IS1103 IS Innovations in Organisations and Society [revamped]

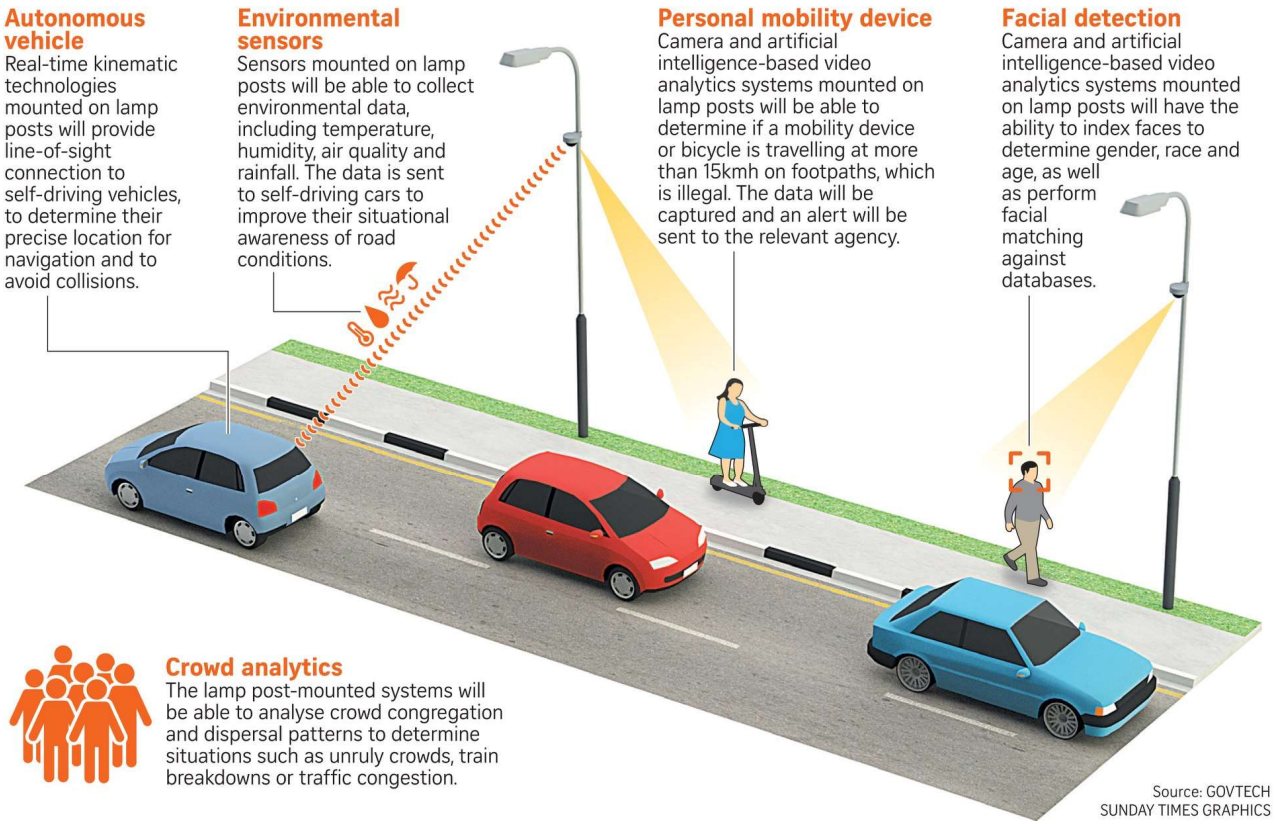
Lecture 5 – Surveillance and Pervasive Technology II

A/P Tan Chuan Hoo
chtan@comp.nus.edu.sg

Public place surveillance

What 'smart' lamp posts can do

Lamp posts in one-north and Geylang will be turned into "smart" fixtures to collect and communicate environmental, crowd and vehicular data to government agencies, for better urban planning and management. The project could be expanded nationwide involving more than 100,000 lamp posts.



Source: GOVTECH
SUNDAY TIMES GRAPHICS

Public place surveillance

"SINGAPORE (Reuters) - In the not too distant future, surveillance cameras sitting atop over 100,000 lampposts in Singapore could help authorities pick out and recognize faces in crowds across the island-state… The plan to install the cameras, which will be linked to facial recognition software, is raising privacy fears among security experts and rights groups. The government said the system would allow it to "perform crowd analytics" and support anti-terror operations… Prime Minister Lee Hsien Loong said last week that the Smart Nation project was aimed at improving people's lives and that he did not want it done in a way "which is overbearing, which is intrusive, which is unethical"…

Adam Schwartz, senior staff attorney at the U.S.-based rights group Electronic Frontier Foundation, urged Singapore and other governments not to adopt facial recognition surveillance technology, in a response to a request for comment from Reuters. He said he was concerned such technology could be turned on political opponents or used to curb free speech by deterring peaceful protest. Facial recognition technology typically allows authorities to match people picked up on cameras with those in databases."

2MP Fixed Dome Network Camera

- 2MP 1/2.8'' Progressive scan CMOS
- Support dual streams
- Up to 30 meters IR range
- -S: Two-way audio
- -S: Audio/Alarm I/O
- -W: Support Wi-Fi
- IR cut filter with auto switch
- DC12V & PoE
- Built-in Micro SD/SDHC/SDXC card slot, up to 128 GB

Source: https://www.reuters.com/article/us-singapore-surveillance/singapore-to-test-facial-recognition-on-lampposts-stoking-privacy-fears-idUSKBN1HK0RV

Public place surveillance --- CCTV

- A public (private) space is one in which any person may (not) come without permission AND the space is available to all other people

- Ethical issues with public place surveillance
  1. Discrimination
  2. Proportionality
  3. Consent
  4. Authority

2MP Fixed Dome Network Camera

- 2MP 1/2.8'' Progressive scan CMOS
- Support dual streams
- Up to 30 meters IR range
- -S: Two-way audio
- -S: Audio/Alarm I/O
- -W: Support Wi-Fi
- IR cut filter with auto switch
- DC12V & PoE
- Built-in Micro SD/SDHC/SDXC card slot, up to 128 GB

Discrimination

- Discriminating surveillance – example, traditional police surveillance, such as tailing people on foot or by car, carrying out phone taps and potentially bugging properties in which suspects are known to operate

- Non-discriminating surveillance – CCTV in public area: anyone could be a criminal (or indeed a victim), and so everyone should be monitored for purposes of detection and deterrence

- Is discriminating or non-discriminating surveillance more ethically questionable?

Conceptualizing surveillance

- Surveillance technologies afford particular epistemic actions – they enable information to be linked to people in two ways: (1) where a person is the source of the information, and (2) where a person is the target of information.

- With the addition of a semantic element provided by people such as CCTV operators, surveillance technologies produce meaningful information about people.

- Surveillance technologies allow identity relations to be created and recognised between people in the world and an informational representation of a person, the Virtual Identity. These identity relations are constructed through aggregation of information.

- Information is aggregated to make that information practically useful. This aggregation not only changes the usefulness of that information; it also changes the moral importance of that information.

Source: Adam Henschke, ethics in an age of surveillance, 2017

The root of surveillance is concern over…

- Data collected and utilized.

- Personal data - any information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. (Article 2(a) European Data Protection Supervisor, 2001)

- Four key moral justifications for protecting data

1. Information-based harms
   - arise when someone is harmed by the use of Personal Information, like identity theft resulting in financial and physical damages
2. Informational inequality
   - Occurs when a person has unequal access to a service or product as the result of handing over or giving access to their Personal Information
2. Informational injustice
   - occurs when information intended for use in a particular context is used in another context. Example, using surveillance information gathered in a national security context for economic gain: the original context of the information was national security and it is an injustice if this information is then used for economic benefit
2. Encroachment on moral autonomy
   - Lack of privacy may expose individuals to outside forces that influence their choices

Source: Adam Henschke, ethics in an age of surveillance, 2017

Identity

[T]here is no you prior to your choices and actions because your identity is in a quite literal way constituted by your choices and actions ...When you deliberately decide what sorts of effects you will bring into the world, you are also deliberately deciding what sort of cause you will be. And that means you are deciding who you are.

(Emphases Original, Korsgaard, 2009, p.19)

Source: Adam Henschke, ethics in an age of surveillance, 2017

What is identity?

- Numeric Identity - concerned with a person's persistence through time
  - criteria for Numeric Identity: (1) a person's psychological states connect through time, (2) persistence of the physical body - as long as Sally's body persists through time she remains the same person
- Character Identity - the qualitative personality of an individual
  - mental states and attitudes – example: "I am the sum of my plans and policies; I work towards a goal and I understand myself in terms of my background – where I'm coming from, as we say, is where I come from . . . Memory links my past to my future self, and makes me the person I am"
- Group Identity - socio-political communities, i.e., ethnic groups, cultural groups, nations, particular personal relationships, even sporting teams are legitimate elements of a person's identity
- Essentialised Identity - reduction of a person to a specific identifier
  - de-personalise an individual, or group of people, in a number of significant ways: (1) biometric identifier like a fingerprint or retinal scan

Source: Adam Henschke, ethics in an age of surveillance, 2017

What is identity?

- Numeric Identity that ‘I perceive myself to be the same person I was yesterday’,
- Character Identity that ‘I perceive myself to be a funny guy’,
- Group Identity that ‘I perceive myself to be an anarchist’, and
- Essentialised Identity that ‘I perceive myself to be employee #5425777’

Source: Adam Henschke, ethics in an age of surveillance, 2017

Virtual Identity

- A particular type of information, which encourages the observer to experience the information as Personal Information

- To illustrate: Sally as a policewoman monitoring the CCTV screens with a person walking on the street. The visual data is ordered in such a way that Sally will experience the image of the person. While the photo itself is just a set of coloured dots arranged in a particular way, because Sally is a human and a policewoman with a given set of experiences and knowledge about the world, her capacity to experience the "person" as anything but a walking object is heavily constrained. In this sense, the image is a Virtual Identity of that person.

- A Virtual Identity can refer to anything from a single name, a fingerprint, a genetic profile, to a photo, to a very rich and detailed one, a biography like The Identity of Elvis Presley. Or an online profile like Sally's Facebook page

- digital dossiers - collection of detailed data about an individual in order to reach a judgment' about the subject of the dossier. These dossiers produce a virtual identity

Source: Adam Henschke, ethics in an age of surveillance, 2017

Target Pregnancy Score

- Target assigns every customer a Guest ID number, tied to their credit card, name, or email address that becomes a bucket that stores a history of everything they've bought and any demographic information Target has collected from them or bought from other sources.
- Using that, Pole looked at historical buying data for all the ladies who had signed up for Target baby registries in the past.
- Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August.

Source: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#651eff166686

Ease of creating virtual identity

Bring your mobile or Garmin device whenever you run, walk, bike or do any other outdoor sport across a distance. While you are out there, your route is automatically tracked together with your distance, end time, average speed, split time, calories burned, and more. If you use a GPS phone, you will be informed about your speed for each kilometer or mile and your effort is tracked in real time sparing you for synchronizing with your computer manually . . . Users can choose to create a profile on Endomondo.com, which will then host their personal training diary and enable them to challenge their friends . . . Live tracking also enables your personal fans to follow you live and to send you pep talk messages that will be read out loud to you while you exercise. Users can integrate their Endomondo profile with Twitter and Facebook to auto-post their activities.

(Endomondo.com 2012)

Source: Adam Henschke, ethics in an age of surveillance, 2017

Virtual identity and vulnerability

Endomondo Terms And Conditions state:

You allow Endomondo to anonymise your personal data and then copy, process, use, public display and distribute such anonymised data. Such anonymised data is, when anonymised, no longer considered "personal data".

You give your explicit consent that Endomondo may transfer and make public the content, including personal data, you automatically upload to the Site by using the Endomondo services, unless you restrict such data processing by changing your privacy settings on the Site. Hence, your data will by default be published and made publicly available on the internet from any country in the world upon upload.

Notwithstanding the above your e-mail, password to the Site and phone number will not be made public unless you decide to do so.

(Emphases Mine, Endomondo, 2011)

Source: Adam Henschke, ethics in an age of surveillance, 2017

“Power” of information aggregation

- The production, aggregation and communication of data about someone’s running practices seems totally innocuous
  - someone intentionally uploading jogging information seems to be of little moral concern as it presents little in the way of either problems for rights, harms or discrimination. Just sharing of jogging information seems ‘morally insignificant’

- However, such data is not morally inert for 3 reasons:

1. When integrated with other information, it can be highly revealing of a given individual or group.
2. when integrated with other information, it can cause suffering in individuals or groups.
3. it can lead to unequal treatment of people.

Source: Adam Henschke, ethics in an age of surveillance, 2017

Google – share of information

"We use different technologies to process your information for these purposes. We use automated systems that analyze your content to provide you with things like customized search results, personalized ads, or other features tailored to how you use our services. And we analyze your content to help us detect abuse such as spam, malware, and illegal content. We also use algorithms to recognize patterns in data. For example, Google Translate helps people communicate across languages by detecting common language patterns in phrases you ask it to translate.

We may combine the information we collect among our services and across your devices for the purposes described above. For example, if you watch videos of guitar players on YouTube, you might see an ad for guitar lessons on a site that uses our ad products. Depending on your account settings, your activity on other sites and apps may be associated with your personal information in order to improve Google's services and the ads delivered by Google.

We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies."

Source: https://policies.google.com/privacy?gl=sg#infosharing

Institution and Information

- 5th of June, 2013, The Guardian newspaper published an article titled 'NSA Collecting Phone Records of Millions of Verizon Customers Daily'.
- 9th of June 2013, The Guardian newspaper published the story 'Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations', revealing that the source of the information was Edward Snowden, a contractor to the US National Security Agency (NSA).
- Starting with the NSA, documents that Snowden had given to the international press rapidly encompassed the US intelligence community, the United Kingdom, other 'Five Eyes' countries and the world's largest technical companies.
- Sparked international diplomatic incidents such as the revelation that the United States was conducting surveillance on allies like the Vice Chancellor of Germany and companies like Brazil's Petrobras
- Snowden's revelations confirmed that surveillance had truly come of age: the idea that governments around the world had us under surveillance was no longer the province of conspiracy theory.
- Also, given the involvement of companies like Google, Facebook and Apple in these surveillance programmes, our willing embrace of information technologies makes us all targets of surveillance.

Source: Adam Henschke, ethics in an age of surveillance, 2017

Big brother and us

- Governments have a monopoly of force and they have moral responsibilities to their citizens --- commands the police and military and it formally decides upon and enforces the laws of the land

- Citizens give up certain rights and responsibilities to the state, however this is construed --- citizens are within the state's jurisdiction, then they are vulnerable to particular decisions that the state makes.

- In response to citizens forgoing certain rights, the state bears particular responsibilities to protect its citizens. There is a 'relationship between sovereign and subject in terms of a "mutual bond and obligation," under which the subject owed allegiance or obedience, while the sovereign was bound "to govern and protect his subjects ..."'

- Essential point: citizens are simultaneously vulnerable to and protected by, the big brother.

Source: Adam Henschke, ethics in an age of surveillance, 2017

Big brother and us

- 'If every problem looks like a security issue then ministers will be conditioned to see the response in terms of seeking more security ... threatening further restrictions domestically on individual liberty and privacy. Care is thus needed that a subliminal message does not become reinforced that Good Government is just about security' (Omand, 2010, p.20).

- '[w]hile the government, via surveillance, knows more and more about what its citizens are doing, its citizens know less and less about what their government is doing ... Democracy requires accountability and consent of the governed, which is only possible if citizens know what is done in their name' (Greenwald, 2014, pp. 208–209)

Source: Adam Henschke, ethics in an age of surveillance, 2017

Vulnerability and personal information

- Personal Information makes people, particularly target people, vulnerable to the actions of others, particularly institutions

- "vulnerability" is a matter of being under threat of harm; therefore, protecting the vulnerable is primarily a matter of forestalling harms'

- 5 types of information harms

1. Deliberate Information Harms - use Personal Information to harm others (e.g., using Personal Information access to another's bank details in order to steal money from them)
2. Negligent Information Harms - arise when a Virtual Identity is constructed that targets an individual or group, but the data is not accurate (e.g., combination ofracial profiling and police activities, where police selectively 'target sections of the population, especially ethnic minorities')
3. Incomplete Information Harms - arise when the Virtual Identities are decontextualised and lose their intended meaning (e.g., increased discrimination faced by certain populations following the increased security measures adopted in response to terrorist activity in Western countries)
4. Limited Opportunity Harms - arise when a certain Virtual Identity is used to limit the range of opportunity that an individual might have (e.g., denying people equality of access to particular social institutional roles based on the given gender, ethnicity, religious persuasion and so on)
5. Closed Identity Harms - treating people as less valued than others

Key points

- 2 typical claims from big brothers:

1. an institution needs Personal Information in order to achieve its institutional ends;
2. certain things, such as government surveillance programmes, must remain secret in order to operate effectively.

- Claim (2) about secrecy is derived from the first claim – it is only if that programme is morally justified in the first place that the claims to secrecy stand up.
- social institution derives its moral legitimacy from the collective good that it produces, where the collective good is 'a jointly produced good that is and ought to be, produced and made available to the whole community because it is a desirable good and one to which the members of the community have a joint moral right' (Miller, 2010b, p. 7).
- BUT 'there ought to be moral constraints on institutional activities, for example, human rights constraints' (Miller, 2010b, p. 64)

Key points

- So what of large-scale surveillance programmes?

- Australia Parliamentary Joint Committee on Intelligence and Surveillance (PJCIS) review of the laws around metadata retention recommended 'the authorised officer making the authorisation must be satisfied on reasonable grounds that any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable and proportionate ...[regarding] the gravity of the conduct being investigated' (Parliamentary Joint Committee on Intelligence and Surveillance, 2015).
  - with Personal Information like metadata, proportionality is absolutely core to any justified use of that information.
- Summary: an appeal to justify the collective good of surveillance must also include the emergent information harms from surveillance. For the surveillance programmes revealed by Snowden, those aggregated rights violations and potential information harms are immense: for example, one unit of the NSA, in a thirty-day period, collected data on '97 billion emails and 124 billion phone calls from around the world'

From dispensing toilet paper to shaming jaywalkers, China powers up on facial recognition

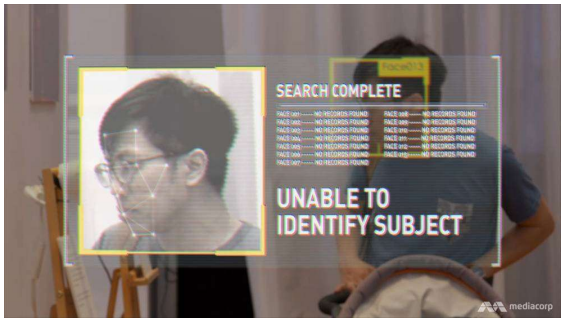
"Jaywalkers would receive a text message from the traffic police about paying a fine. What's more, they would be publicly shamed.

"It doesn't matter if you're walking or riding a bicycle. (Your picture) will be captured, and your face will show up on a screen nearby so everyone can see your face," said Ms Janine Wong, a news researcher in Shanghai.

"Once they identify your face, all your information (like mobile phone number) is linked." .....

To improve the standards of public restrooms, about 70,000 of them were built or renovated at tourist sites across China between 2015 and 2017. And some were fitted with facial recognition technology: Toilet paper dispensers that remember the user's face.

Their job is to set a limit on the amount of toilet paper one can take. "When you stare at it (the machine) for three seconds, you'll get toilet paper," explained Ms Wong"



Source: https://www.channelnewsasia.com/news/cnainsider/shaming-jaywalkers-china-facial-recognition-technology-privacy-11196684