

---

# Society & Surveillance



Human Rights, surveillance, social issues

Dr Peggy Gregory

# Universal Declaration of Human Rights

- United Nations – created in 1945 by representatives of 50 countries – a response to the end of WW2
- The Commission on Human Rights set up by the UN to draft the UDHR. It was made up of 18 members from various political, cultural and religious backgrounds. Eleanor Roosevelt, widow of American President Franklin D. Roosevelt, chaired the committee
- A roadmap to guarantee the rights of every individual everywhere
- UDHR adopted by UN General Assembly, consisting of over 50 member states, on 10 December 1948, with 8 nations abstaining but none dissenting.
- It marked a historical turning point, as a text promoting peace and diplomacy

# 30 basic human rights

1. Free and equal in dignity & rights
2. Life
3. Freedom from torture
4. Freedom from slavery
5. Liberty and security
6. Seen as a person in law
7. Equality
8. Remedy in law
9. Freedom from arbitrary arrest
10. Fair trial
11. Innocent until proved guilty
12. Privacy & family life
13. Freedom of movement
14. Freedom from persecution
15. A nationality
16. To marry
17. Own property
18. Freedom of thought, conscience, religion
19. Freedom of opinion & expression
20. Freedom of association
21. Take part in govt. and vote
22. Human dignity
23. To work & receive fair pay
24. To rest & leisure
25. Adequate standard of living
26. Education
27. Participate in cultural activities
28. To have rights realised internationally
29. Duty to community
30. Not to have any rights removed

# European Convention on Human Right: ECHR

- Protects the human rights of people in countries that belong to the Council of Europe, including the UK
- The Council of Europe was founded after World War II to protect human rights and the rule of law, and to promote democracy
- The Convention was based on the Universal Declaration of Human Rights. It was signed in Rome in 1950 and came into force in 1953.
- Established the European Court of Human Rights
- Judgments finding violations are binding on the States concerned and they are obliged to carry them out
- Post-Brexit, some UK politicians want to leave the ECHR

# Human Rights Act 1998

- The Human Rights Act is a UK law that received royal assent in 1998 and came into force on 2 October 2000.
- It aims to "give further effect" in UK law to the rights contained in the European Convention on Human Rights
- The Act gives UK courts a **remedy for breach of a Convention right**, without the need to go to the European Court of Human Rights in Strasbourg
- Some additions to UDHR are added (also in ECHR)
- Protocol 1, Article 1: Right to peaceful enjoyment of your property
- Protocol 1, Article 3: Right to participate in free elections
- Protocol 13, Article 1: Abolition of the death penalty

# Example ECHR vs UK cases

- Rights of journalists not to reveal their sources, *Goodwin v UK*, 1996
- Police can't keep innocent people's DNA forever, *S and Marper v UK*, 2008 (right to a private life)
- Phone hacking is a crime, *Halford v The United Kingdom*, 1997 resulting in the Regulation of Investigatory Powers Act 2000 (right to effective remedy)
- Human trafficking and domestic slavery are illegal, *C.N. v UK*, 2012 leading to the Modern Slavery Act 2015 (freedom from slavery)

# Surveillance technologies

- Closed Circuit Television Systems (CCTV)
- Automatic Number Plate Recognition (ANPR);
- Body Worn Video (BWV);
- Unmanned Aerial Vehicles (UAVs, also known as drones);
- Facial Recognition Technology (FRT) and surveillance;
- Commercial products such as smart doorbells and surveillance in vehicles;
- Workplace monitoring, live streaming; and
- Other commercially available surveillance systems that have the potential to process personal data.

# GDPR & DPA for surveillance systems

- DCs must use appropriate technical and org. measures & identify lawful basis
- If a surveillance system processes PD must notify & pay a fee to ICO unless exempt
- Must have measures and records in place to demonstrate compliance
- Have a record of processing: purposes, data sharing agreements, retention
- Take a data protection by design and default approach and perform a Data Protection Impact Assessment (DPIA) if high risk to individuals. This includes:
  - processing special category data;
  - monitoring publicly accessible places on a large scale; or
  - monitoring individuals at work
- Assess whether surveillance is appropriate & impact on rights and freedoms.
- Record in a DPIA before deployment, and if high risks, consult with ICO

# Facial recognition technology (FRT)

- FRT identifies a person from a digital facial image and analyses facial features to produce a biometric template.
- Depending on use, FRT involves processing PD, biometric data and special personal data
- Under the UK GDPR, processing biometric data to uniquely identify an individual is prohibited unless a lawful basis under Article 6
  - consent, contract, legal obligation, vital interests, public interest, legitimate reason
- AND a condition in Article 9 can be satisfied

# Article 9 conditions for special personal data

- a) Explicit consent
- b) Employment, social security and social protection law
- c) Vital interests
- d) Not-for-profit bodies
- e) Made public by the data subject
- f) Legal claims and judicial acts
- g) Substantial public interest conditions
- h) Health or social care
- i) Public health
- j) Archiving, research and statistics

# FRT in public spaces

- FRT in public spaces is where data is scanned and checked against a ‘watch list’, if found, there’s usually human decision before action
- If system is completely automated higher standard needed
- If private company consent and option to opt out important
- To be accountable when using FRT must be able to explain
  - the lawful basis relying on;
  - why FRT is necessary in the circumstances or in the public interest;
  - why less intrusive options were ruled out;
  - assessment of the likelihood that objectives of FRT will be met;
  - how effectiveness has been measured

# FRT Checklist ([www.ico.org](http://www.ico.org))

- Conduct a [Data Protection Impact Assessment \(DPIA\)](#) addressing need, lawful basis for use and the impacts on the rights and freedoms of individuals whose personal data are captured for every deployment
- Document justification for FRT
- Have sufficient volume and variety of training data
- Chosen an appropriate resolution for the cameras
- Positioned cameras in areas with lighting to ensure good-quality images
- Identify false & true matches, false +ves and –ves and amend if rates high
- Consider if an Equalities Impact Assessment (EIA) is required
- Complied with the Surveillance Camera code of practice where required.

# Surveillance Case example 1

- Both fixed and mobile cameras should be focused and individuals should not unintentionally made the subject of surveillance.
- A café installs a surveillance system which captures the entrance of the premises to improve its security, as there have been reports of break-ins in the local area.
- When reviewing the system, the café owner realises that the camera's field of vision also captures footage of a nearby flat and can see into the property.
- The café owner adjusts the field of vision so that the focus of the recording is restricted only on the café entrance to avoid any unnecessary privacy intrusion to nearby residents.

# Surveillance case example 2

- An education authority is considering whether to use (FRT) to verify pupils' identities at the cash register during lunch to facilitate cashless catering
- FRT involves processing **biometric data** which presents risks to rights and freedoms, esp. bias & discrimination
- First action must be **Data Protection Impact Assessment (DPIA)**
- Must **evidence that FRT is necessary & proportionate**
- Will rely on **consent**, must be freely given, specific, informed and unambiguous
- If a pupil/parent refuses they must be given a **genuine alternative** (swipe card, pin number, cash)
- Also, must apply Protection of Freedoms Act 2021, about parental consent

# Technology in society

- Digital technology has a dual role as a utility and entertainment; it is part of the social fabric of our lives
- Technology pervades workplaces, education, homes, and environmental infrastructure
- No one knows the social, psychological, and intellectual implications of such a reliance on technology
- Predictions abound that it will enhance intelligence and performance, and change behaviour, but also that it diminishes some skills & attributes
- Beliefs about the value/perils of technology are not new
- Since the beginning of industrialisation, technology has been both valued & feared as a force for change