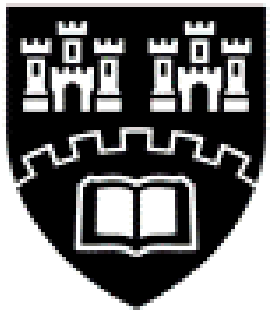

Northumbria University
NEWCASTLE

Privacy and Crime Fighting: the European Context

Gemma Davies, Associate Professor, Northumbria University

The Rise of Privacy

- **Leander v Sweden (1987) 9 EHRR 433**
- "both the storing and the release of [private] information held by the police… amounted to an interference with … [an individual's] … right to respect for private life as guaranteed by Article 8(1).”
- **S and Marper v United Kingdom [2009] 48 EHRR 50**
- “[t]he mere storing of data relating to the private life of an individual amounts to an interference within the meaning of art. 8’
- The policy in operation in England and Wales to indefinitely retain the biometric data of non-convicted persons violated Article 8 ECHR and could not be justified by the application of a “margin of appreciation”.
- The retention system in operation at that time was “blanket and indiscriminate” and “overstepped any acceptable margin of appreciation”.
- **M.K. v. France [2013] Application no. 19522/09**
- Article 8 applied with even greater force when data underwent automatic processing and/or use for policing purposes.

Recent cases

- **Catt v United Kingdom [2019] ECHR 76**
- Police's collection and retention of data of a peaceful protestor was an unlawful interference with article 8 of the Convention because it was not necessary in a democratic society.
- The case highlighted the need to carry out meaningful reviews of retained data and that it must be held for legitimate policing purposes.
- **Gaughran v United Kingdom [2020] ECHR 144**
- UK police’s indefinite retention of DNA profile, fingerprints and photographs of person convicted of a minor offence without a possibility of review constituted an infringement of Article 8 ECHR.
- UK had overstepped the acceptable margin of appreciation and the retention of the information constituted a disproportionate interference with the applicant’s right to respect for private life and could not be regarded as necessary in a democratic society.

R (Bridges) v Chief Constable of South Wales Police & Information Commissioner

- 11 August 2020
- UK Court of Appeal
- Use by police of automated facial recognition (“AFR”) technology
- Recognised the system constituted an interference with Article 8 that was NOT in accordance with law
- BUT would be proportionate if sufficiently narrow local policy was framed.

- Caution needs to be exercised by LEAs
- Mass surveillance is likely to be disproportionate if it can be shown that less intrusive and better targeted measures available

- Watch this space…

European Cross-border investigations

- Swedish Initiative
- GDPR
- Law Enforcement Directive
- Mutual Legal Assistance
- European Investigation Order

Access to stored electronic data

- Traditionally from an EU perspective, mutual legal assistance treaties, and more recently the European Investigation Order allows for the lawful collection of electronic information in cross-border proceedings.
- Pressure mounted within the EU to allow law enforcement authorities' access to data outside existing judicial cooperation channels.

- The Clarifying Lawful Overseas use of Data Act 2018 (CLOUD Act) – introduced after Microsoft-Ireland case
- E-evidence (or cross-border access to electronic evidence) proposal 2018

- Vera Jourová, EU Commissioner for Justice, Consumers and Gender Equality: "**While law enforcement authorities still work with cumbersome methods, criminals use fast and cutting-edge technology to operate. We need to equip law enforcement authorities with 21st century methods to tackle crime, just as criminals use 21st century methods to commit crime.**"

E-evidence proposal

1. Prosecutor in Member State A makes a request
2. Approved by a judge (for transactional or content data)
3. Served on the legal representative of the service provider in Member State B
4. Who sends evidence directly to police in Member State A

Access to e-evidence and privacy

- The proposal introduces the concept of extra-territorial application of law.
- The authorities, on whose territory a provider has been requested to produce or preserve data by an authority of another Member State, will not be aware about the request and, thus, will not have the possibility to object to it unless the data subject is not resident in the issuing state and the request relates to content data.
- That is the case even if the offence concerned does not amount to a criminal offence on the territory concerned.
- Only the service provider of the concerned Member State (or the legal representative therein) will be aware of the order. It will be only up to them to check the order for errors, privilege or other issues.
- This seems to put mutual trust to the test as human rights concerns are in the care of the issuing state.

- Watch this space…

Brexit and the exchange of data

- Exchange of data with a “third country” (any non-EU or EEA Member State) is subject to a guarantee that the personal data will receive an “adequate” level of protection.
- **Schrems** - EU-US Safe Harbour agreement.
- **Schrems II** the court invalidated the adequacy rating of the US ‘Privacy Shield’
- **Privacy International** case – bulk communications data collection in the UK “general and indiscriminate”
- Practices relating to national security measures, although outside of the competence of the EU, fall within the remit of the court as they pertain to EU data protection.
- Data adequacy decision not certain - UK willingness to agree to follow EU rules also unclear.
- Without a data adequacy decision UK LEAs will need to satisfy EU partners that there are adequate data protection safeguards
- The Information Commissioner’s Office is advising that “**EU senders of data will probably require a contract or binding legal instrument or some other way of assessing appropriate safeguards are in place.**”
- Watch this space…