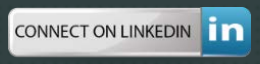
cornerstone barristers

Legal AI and Data Protection

Estelle Dehon

Barrister at Cornerstone Barristers



General Data Protection Regulation

Source: Slane Cartoons https://www.slanecartoon.com/

What is the GDPR?

- Framework of rights and duties designed to safeguard personal data
- Focuses on information entered and stored electronically, but also extends to some real-world filing systems
- Designed for a digital world, to bring good practice to businesses and give control back to individuals

Mechanics of GDPR

General Data Protection Regulation 2016/679

- 14 April 2016 - adopted
- 27 April 2016 - signed
- 4 May 2016 - published in the Official Journal
- 25 May 2016 - came into force
- **25 May 2018** – became enforceable

GDPR – How does it Help?

- Values people’s personal information
- Requires Privacy by Design
- New definition of “profiling” in data protection law
- New focus on transparency
- Making us think carefully about consent

Definitions: Personal Data

- Article 4(1) GDPR
  - “personal data” means any information relating to an identified or identifiable natural person (‘data subject’)
  - an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Definitions: Big Data

- “Big data” is used to refer to massive datasets which are difficult to analyse using traditional methods because they are:
  - High-volume
  - High velocity (real-time data which changes quickly)
  - High variety (from a number of different sources)

- “Data mining” – very instructive metaphor

Definitions: Machine Learning

- “Machine Learning” is a sub-field of AI: computers are given the ability to learn without being explicitly programmed when exposed to new data:
  - achieved through the construction of algorithms which produce models from example ‘training’ data which are then used to make predictions on further data
  - can be supervised or unsupervised
- “Deep learning” is a subset of machine learning
  - involves use of neural networks to simulate the way in which the human brain processes information through neurons and synapses

Definitions: Artificial Intelligence

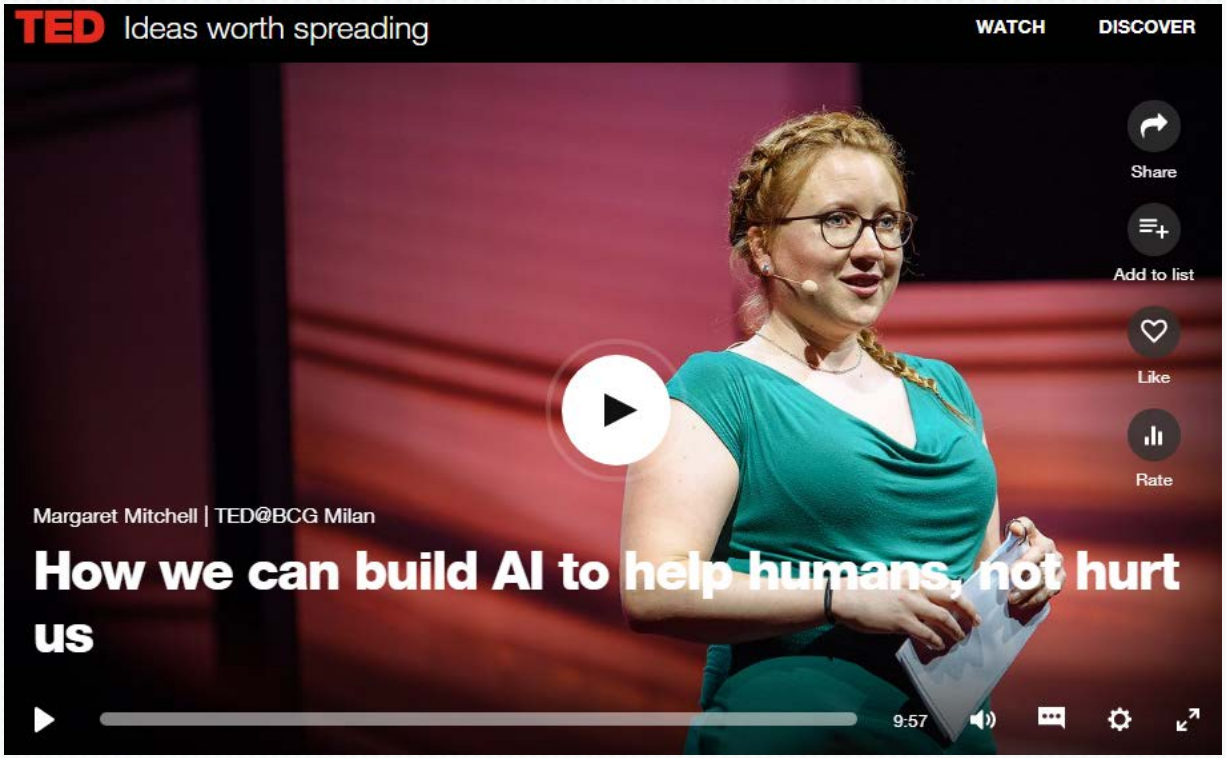
- “AI” is an overarching term for systems that employ computer intelligence, often to analyse data and model an aspect of the world
  - modelling is used to predict or anticipate future events
  - from playing (and winning) games such as Chess or Go against humans
  - assess a judge’s approach to a particular issue in published judgments to predict win/loss on a case
  - analyse opponent’s previous arguments to predict what she will argue in a case
  - assign a risk score evaluating risk of re-offending

Machine Learning and Privacy

- Increase the fairness, decrease the fear:
  - Move from…..

Machine Learning and Privacy

- Increase the fairness, decrease the fear:
  - To….



Privacy by Design

- “Steve Jobs Describes the GDPR in 2010!”

Steve Jobs on privacy, Steve Jobs at the D8 Conference (Video)

Privacy by Design

- “Steve Jobs Describes the GDPR in 2010!”
  - AllThingsD conference, at time of controversy around the use of location tracking on devices
  - Jobs said:

    “We take privacy extremely seriously… **Privacy means people know what they’re signing up for — in plain English, and repeatedly**.”
  - Jobs used privacy as a strong basis for a trusted brand

Privacy by Design & Default - Article 25 GDPR

- Implement appropriate technical and organisational measures and procedures
- Implement mechanisms to ensure that, by default, personal data are:
  - only processed where necessary for each specific processing purpose
  - not collected or retained beyond the minimum necessary for those purposes

Privacy by Design

- GDPR embraces this positive power of privacy
  - To build trust and confidence with clients
  - To give good customer experience & outcomes
  - To improve working practices (especially around security)
- Design in sensible privacy measures:
  - By default personal information is only collected/ used/stored fairly and where necessary
  - By default personal information is collected/kept/ used securely

GDPR & Profiling

- New definition of “profiling” in data protection law
  - 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

What is Profiling?

Article 4(4) GDPR

- Three components:
  - A form of automated processing;
  - Performed on personal data, but can also involve non-personal data
  - Has the aim of evaluating personal attributes of an individual or individuals

How we Profile

- Profiling enables aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted

- UK Information Commissioner: "No longer simply a matter of placing individuals into traditional interest buckets based on purchases…Profiling in today's digital economy involves sophisticated technologies and is widely used in a variety of different applications, until recently with relatively limited publicity."

How we Profile

- Tends to be achieved through algorithms analysing information about individuals
  - Can involve big data as the basis for assessment
  - Can involve scraping “public” information from the internet
  - Data can be assessed through machine learning (can involve new algorithms being created)
- Accomplished using various data sources

Profiling and the GDPR

- Profiling involves a number of types of processing of personal information
  - Obtaining personal information from various sources (including potentially public sources)
  - Analysing or assessing that information
  - Creating new data in the form of the profile
  - Storing both the base data and the new data
  - Sharing the base data or the new data
- All of these processes must comply with the GDPR principles and have a lawful basis

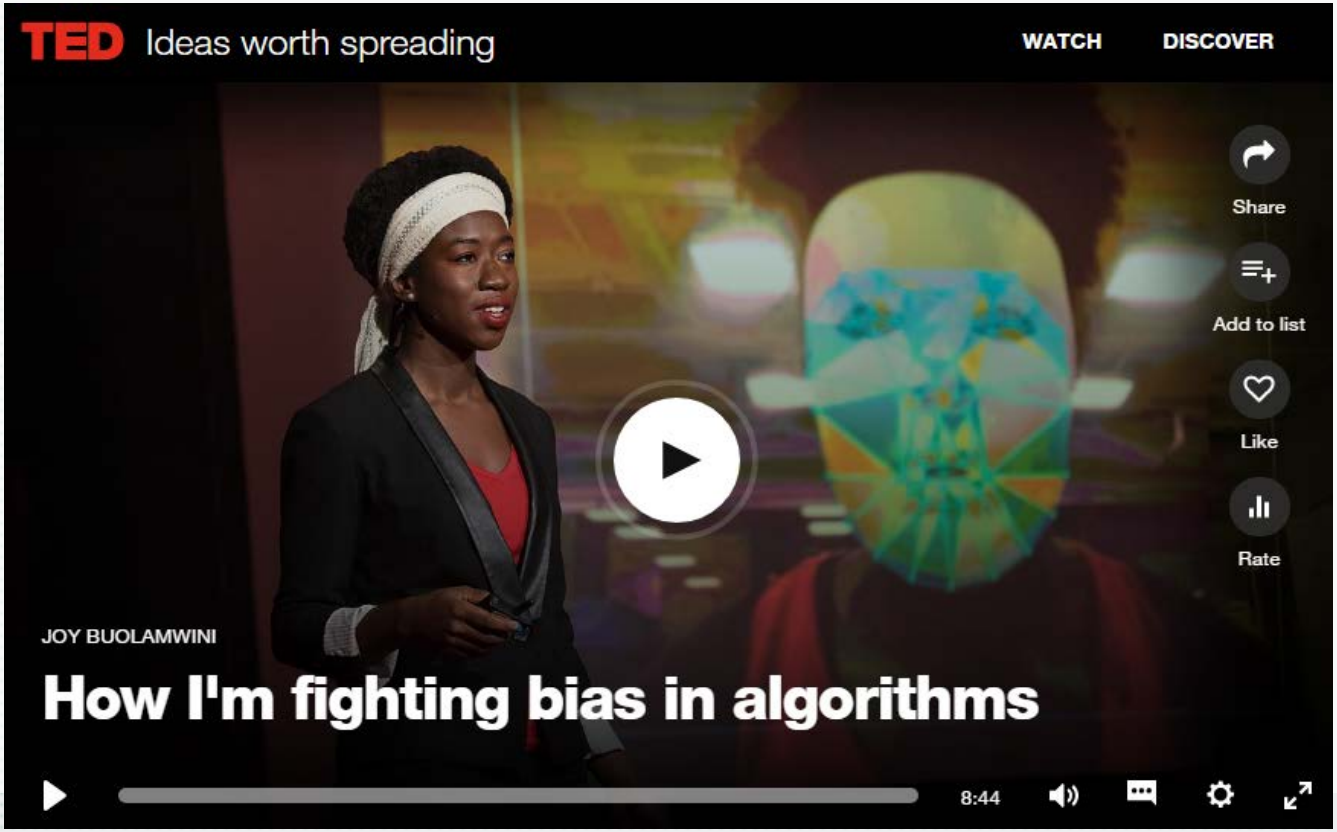
Profiling and the GDPR: Transparency

- Profiling is often not as transparent as other forms of processing

- Need to tell people when you are profiling
  - Especially if there are seemingly unrelated transactions
  - Cross-device tracking
  - Tell people of the potential consequences
  - Tell them if will use information in an unexpected way

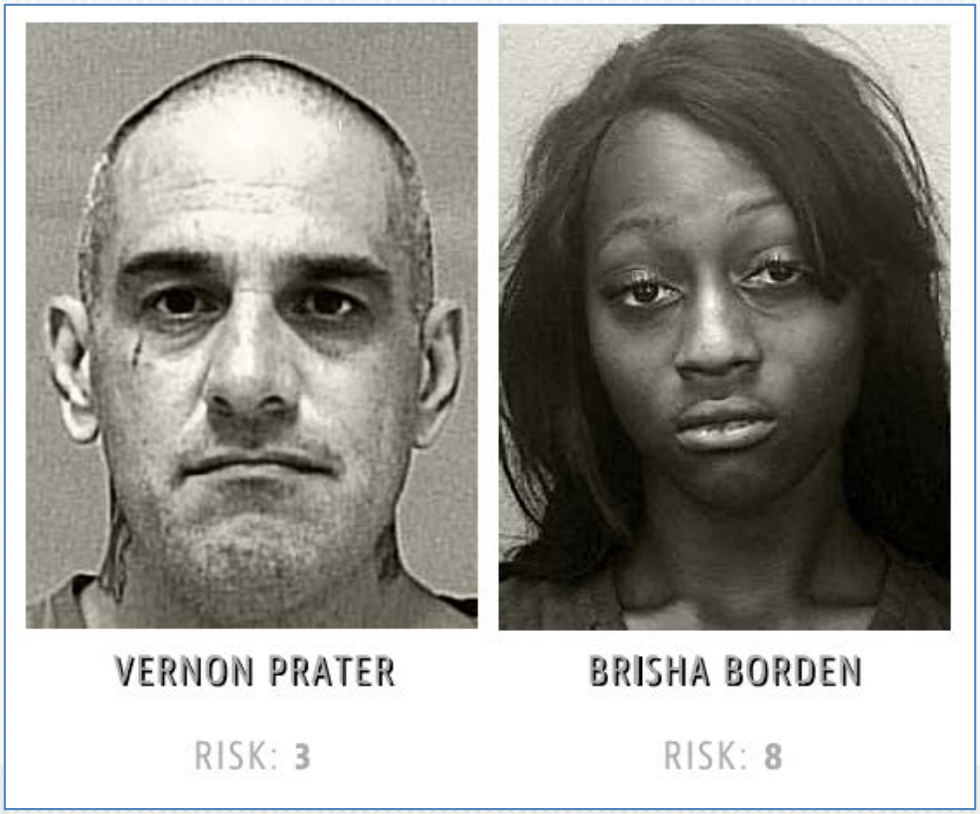
Profiling and the GDPR: Fairness

- Profiling can include hidden biases and emphasise existing stereotypes or social segregation



Profiling and the GDPR: Fairness

- ProPublica exposé on Machine Bias in the risk assessment AI implemented in Broward County, Florida



Profiling and the GDPR: Fairness

- Need to guard against algorithmic bias
  - **Recital 71** data controllers should “use appropriate mathematical or statistical procedures for profiling” in order to ensure fair processing
  - By design have full spectrum inclusion – data sets
  - By design have ways to check is bias is developing: eg review of risk assessments
  - Care needed with off the shelf products – privacy and fairness designed in?

Profiling and the GDPR: Automated Decision-Making

- Individuals have the right not to be subject to a decision based solely on automated decision-making (including profiling), which produces legal effects concerning the individual or “significantly affects” him or her: Article 22(1)
  - One of the strongest rights/prohibitions in the GDPR
- “Significantly affects”
  - A consequence more than trivial, maybe unfavourable
  - Choose not to take your case because AI assesses low probability of success?

Consent

- Definition of “consent”
  - 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Consent

- Conditions for consent
  - withdrawal as easy as giving consent
  - only appropriate if you can offer people real choice and control over how you use their data;
  - if you intend to process the personal data anyway on another basis, asking for consent is misleading and inherently unfair;
  - power imbalance may make consent difficult;
  - consent can’t be a precondition of service;
  - good transparency = good consent

GDPR - Appropriate Safeguards

- Organisations may want to consider a number of safeguards:
  - ways to test big data systems
  - introduction of innovative techniques such as algorithmic auditing
  - accountability/certification mechanisms for decision making systems using algorithms
  - codes of conduct for auditing processes involving machine learning
  - measures for identifying and rectifying inaccuracies
  - a process for human intervention (in case needed)

Image Source: https://www.roboticsbusinessreview.com

Estelle Dehon

Cornerstone Barristers

estelled@cornerstonebarristers.com

0207 421 1849