Microsoft Cloud Computing Research Centre

3rd Annual Symposium, 8th September 2016

Machine Learning with Personal Data

Christopher Millard
c.millard@qmul.ac.uk

Dimitra Kamarinou
d.kamarinou@qmul.ac.uk

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

ML with Personal Data - Overview

- Automated decision making & profiling in GDPR
- Categories of profiling
- Data protection principles:
  - Lawfulness
  - Fairness
  - Transparency
- Human bias vs ML decisions

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Legal Provisions

- Data Protection Directive (DPD)1995 Art 15
- General Data Protection Regulation:
  - 4 years of deliberations
  - adopted May 2016 – takes effect in Spring 2018
  - builds on DPD principles
  - covers not only profiling but any automated processing

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Automated decision making & profiling

- What is profiling?
- ML – patterns in data – profiles
- GDPR – right not to be subject to a decision based…
  - solely on automated processing (including profiling)
  - which produces legal effects / significantly affects individual

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Categories of profiling

Pre-defined template of 'desired' profile	➢ Individual personal data checked against template
No pre-defined template	➢ Individual personal data → descriptive & emerging profile

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Lawfulness

- Elements of profiling process
- Is automated decision-making / profiling ever allowed?
- Legal requirements
  - ➢ right to human intervention
  - ➢ right to express point of view
  - ➢ right to contest decision
- Data Protection Impact Assessments
  - ➢ data protection by design
  - ➢ data protection by default

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Human bias ≠ ML objectivity (examples)

- Prejudice / stereotypes / metabolism
  - *Implicit bias in shortlisting CVs (2009)*
  - *Israeli judges at parole board (2011)*
  - *The case of Airbnb (2014)*
  - *Identifying gifted students in Florida (2016)*
- Algorithms: ability to disregard prejudicial factors?

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Fairness

- Discrimination: differentiation ≠ unfair treatment
  [at least, not necessarily!]
- Training data sets / input data:
  - Quality
  - Quantity
  - Labelling – reliability
- Direct / indirect bias
- Data Minimization
- Correlation ≠ Causation

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Transparency

- Opacity
- 'Black box' / Trade secrets / Unintelligible to layman
- Logic of automated decision making
- 'Meaningful' information about logic
  - Criteria in algorithm
  - Access to personal data: meaningful?
  - Impact of logic on profile

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

And finally…

- EU data protection law assumes that automated decision-making processes are risky and that individuals need to be protected against unfair machines
- How long will it be before it can be demonstrated that particular ML processes are more transparent and less prone to bias than the thought processes of human decision makers?
- At that point, should individuals be given a right to appeal to a machine against decisions made by a human?

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies

Microsoft Cloud Computing Research Centre

3rd Annual Symposium, 8th September 2016

Machine Learning with Personal Data

Christopher Millard
c.millard@qmul.ac.uk

Dimitra Kamarinou
d.kamarinou@qmul.ac.uk

UNIVERSITY OF CAMBRIDGE

Queen Mary University of London
Centre for Commercial Law Studies