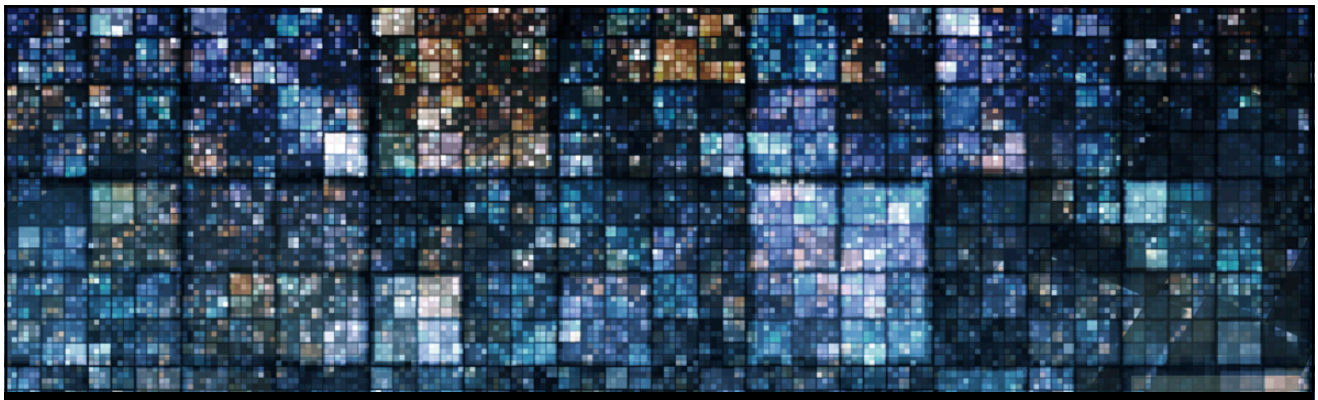
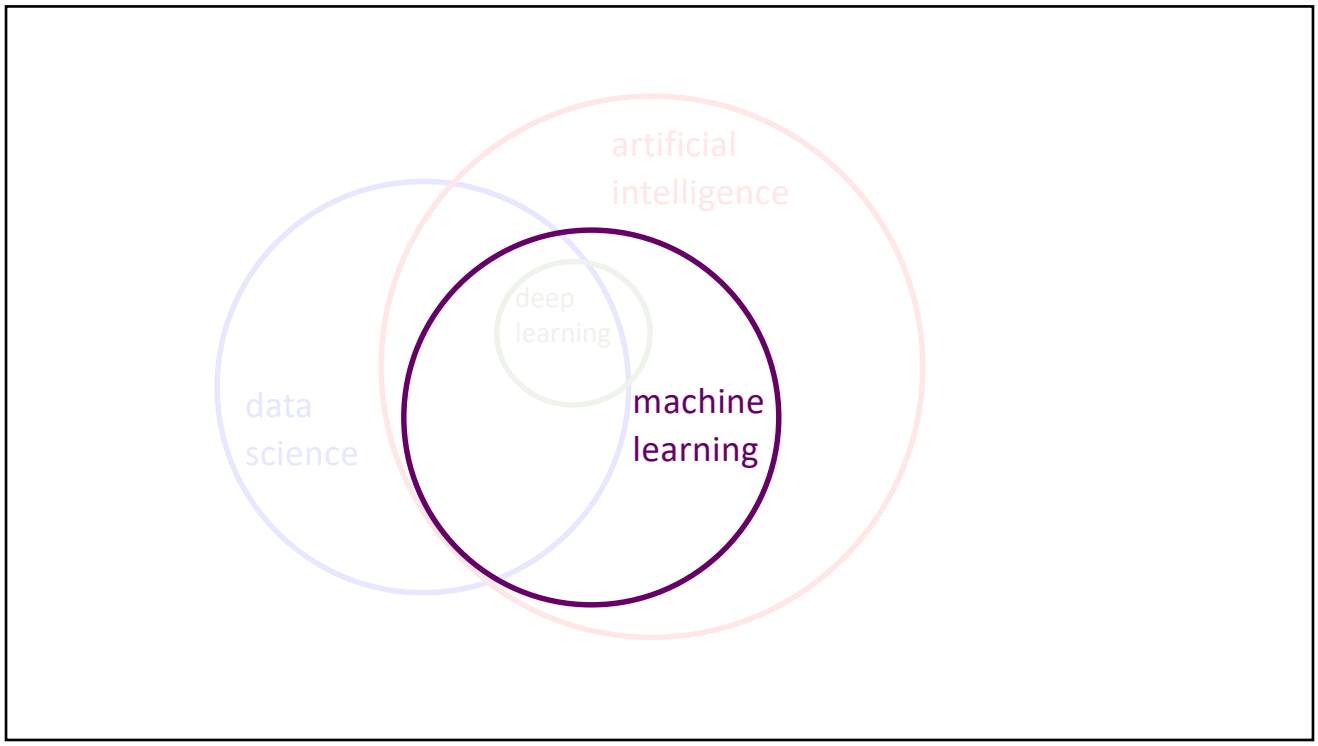


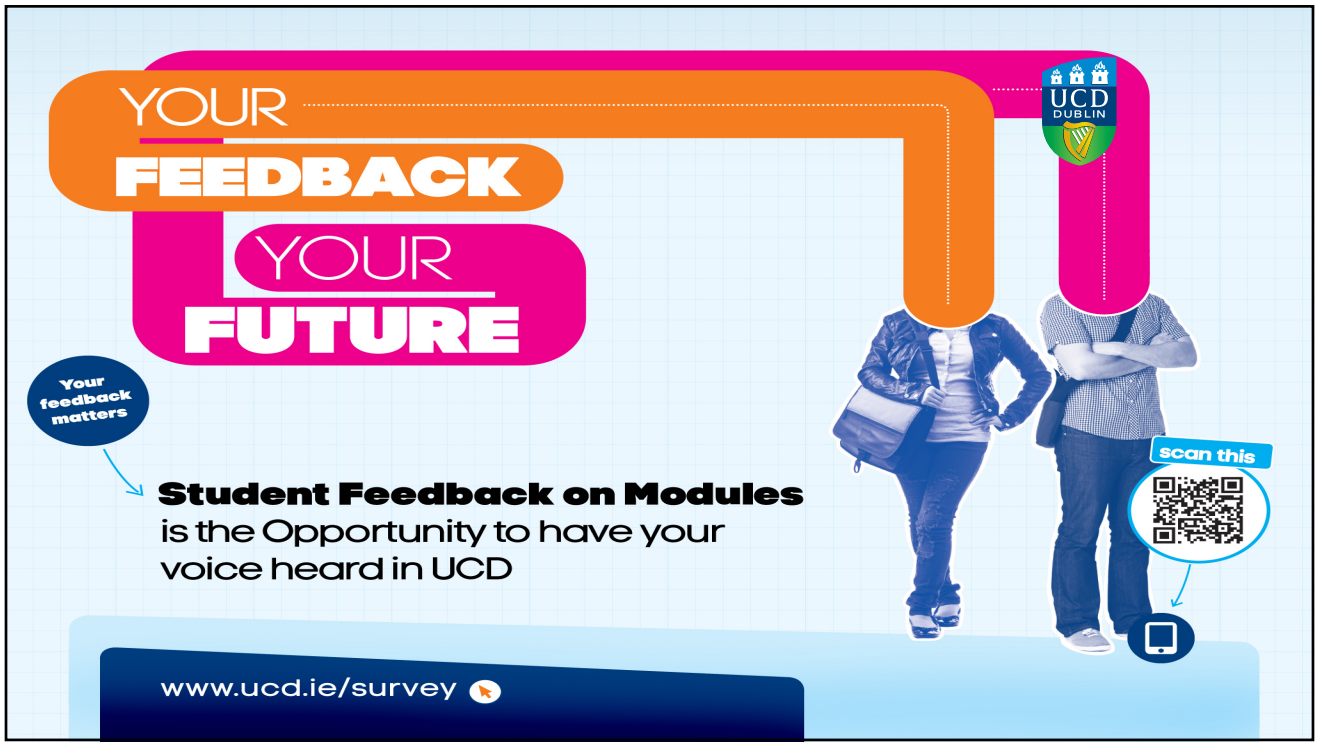
COMP47590
Advanced Machine Learning
GDPR

Dr. Brian Mac Namee

Information

Email:	Brian.MacNamee@ucd.ie
Course Materials:	All material posted on UCD CS moodlehttps://csmoodle.ucd.ie/moodle/course/view.php?id=663 Enrolment key **UCDAdvML2017**


artificial
intelligence
deep
learning
data
science
machine
learning

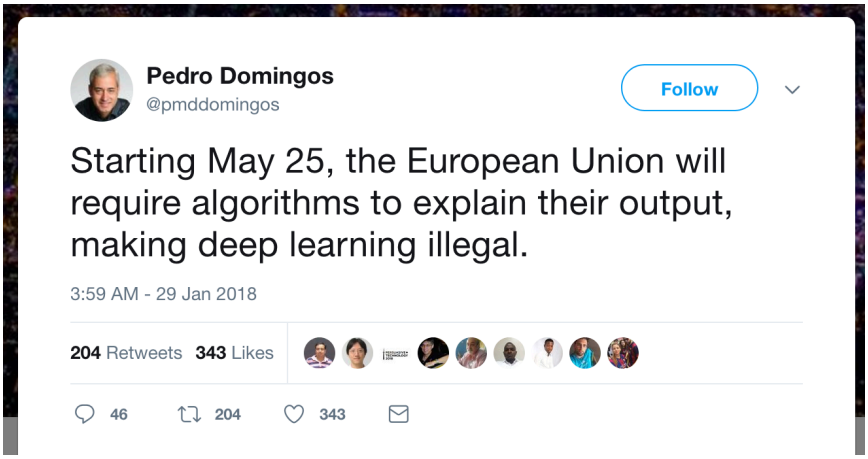

YOUR
FEEDBACK
YOUR
FUTURE
UCD
DUBLIN
Your feedback matters
Student Feedback on Modules
is the Opportunity to have your
voice heard in UCD
scan this
www.ucd.ie/survey

Section Outline

In this section we will cover:

- What is GDPR?
- Impact of GDPR on ML?

Will Deep Learning Become Illegal?



https://twitter.com/pmddomingos/status/957825455666618368?lang=en

GDPR, What Is it?

GDPR, What Is It?

General Data Protection Regulation comes into force on 25th May 2018 and replaces the 1995 data protection directive

- The technological landscape has changed dramatically since the 1995 directive and GDPR aims to address this by providing a modernised, single set of data protection and privacy rules across Europe

For Data Controllers GDPR emphasises **transparency**, **security**, and **accountability**, while at the same time standardising and strengthening the rights of an individual to data privacy

https://www.cs.ucd.ie/gdpr/gdprcompsci/

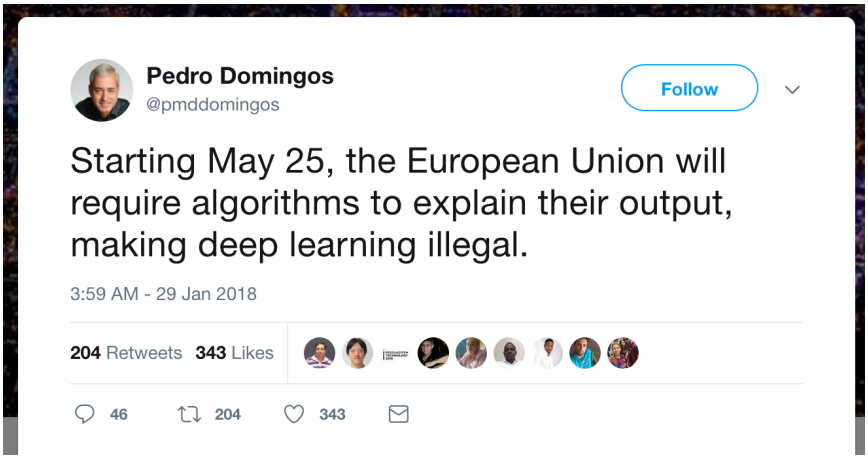
GDPR, Profiling & Automated Decision Making

GDPR also outlines regulations surrounding **profiling** and **automated decision making**

- Using data and machine learning models to make decisions

GDPR, Impact On ML

Will Deep Learning Become Illegal?



https://twitter.com/pmddomingos/status/957825455666618368?lang=en

Will Deep Learning Become Illegal?

Why might deep learning become illegal?

- General data protection
- Prohibition on profiling and automated decision making
- Right to explantion

https://twitter.com/pmddomingos/status/957825455666618368?lang=en

Will Deep Learning Become Illegal?

Why might deep learning become illegal?

- **General data protection**
- Prohibition on profiling and automated decision making
- Right to explantion

https://twitter.com/pmddomingos/status/957825455666618368?lang=en

General Data Protection

GDPR concerns personal data only

- **Direct Personal Data** is any identifier that leads to a clear conclusion about a person's identity
  - name, picture, phone number, email or postal address
- **Indirect Personal Data** in isolation does not give clear reference to a specific person but a possibility to identify this person using a unique combination of the given information what allows the individual to be distinguished from others
  - username, IP address, place of employment, job title

https://www.cs.ucd.ie/gdpr/gdprcompsci/

General Data Protection

Eight rules of data protection

- Obtain and process information fairly
- Keep it only for one or more specified, explicit and lawful purposes
- Use and disclose it only in ways compatible with these purposes
- Keep it safe and secure
- Keep it accurate, complete and up-to-date
- Ensure that it is adequate, relevant and not excessive
- Retain it for no longer than is necessary for the purpose or purposes
- Give a copy of his/her personal data to an individual, on request

https://www.dataprotection.ie/docs/A-Guide-for-Data-Contollers/y/696.htm

General Data Protection

Rights for individuals under the GDPR include:

- subject access
- to have inaccuracies corrected
- to have information erased
- to object to direct marketing
- to restrict the processing of their information, including automated decision-making
- data portability

Will Deep Learning Become Illegal?

Why might deep learning become illegal?

- General data protection
- **Prohibition on profiling and automated decision making**
- Right to explantion

https://twitter.com/pmddomingos/status/957825455666618368?lang=en

Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Prohibition On Profiling & Automated Decision Making

Is there a prohibition on profiling and automated decision making

- Only when the decisions "*produce legal effects*" or "*similarly significant effects*"
- Allowed under three conditions

Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

the part of the controller, to express his or her point of view and to contest the decision.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Will Deep Learning Become Illegal?

Why might deep learning become illegal?

- General data protection
- Prohibition on profiling and automated decision making
- **Right to explantion**

https://twitter.com/pmddomingos/status/957825455666618368?lang=en

Right To Explanation

What is a *right to explanation*:

- **system functionality** the logic, significance, envisaged consequences, and general functionality of an auto- mated decision-making system
- **specific decisions** the rationale, reasons, and individual circumstances of a specific automated decision

Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, Sandra Wachter, Brent Mittelstadt, Luciano Floridi
https://academic.oup.com/idpl/article/7/2/76/3860948

Article 22

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

decision.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Right To Explanation

Does GDPR impose a right to explanation?

- The consensus seems to be no - Article 22 is vague (some will say purposefully so)
- What about Recital 71?

Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, Sandra Wachter, Brent Mittelstadt, Luciano Floridi
https://academic.oup.com/idpl/article/7/2/76/3860948

Recital 71

"[a person who has been subject to automated decision- making] *should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*"

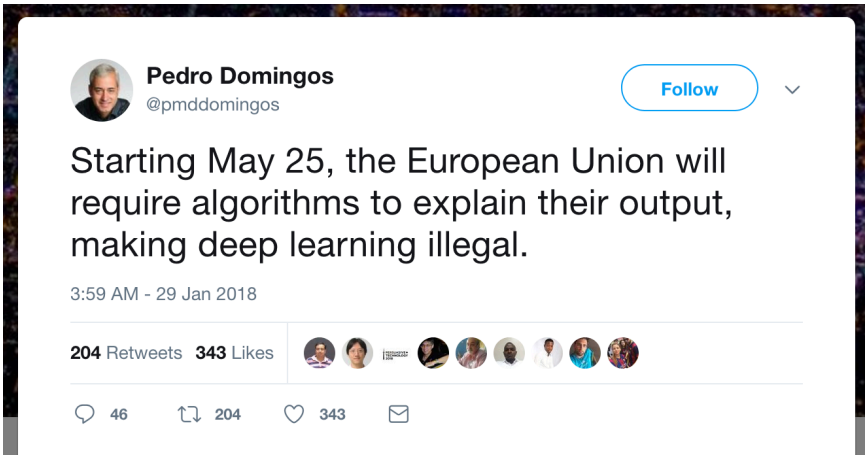
Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, Sandra Wachter, Brent Mittelstadt, Luciano Floridi
https://academic.oup.com/idpl/article/7/2/76/3860948
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Recital 71

If legally binding, this provision would require an explanation of specific decisions

However, recitals provide guidance on how to interpret the Articles, but are not themselves legally binding

Will Deep Learning Become Illegal?



https://twitter.com/pmddomingos/status/957825455666618368?lang=en

Summary

Summary

GDPR

- The GDPR is new EU data protection legislation which comes into effect on May 25th 2018
- This will impact the application of machine learning, but perhaps not as dramatically as some suggest
- Explanation will perhaps become more important

Questions