





Public
Law
Project

Rise of the Robots: The Harm Behind the Hype

Challenging Artificial Intelligence use and decisions

Wednesday 1 February 2024



GARDEN COURT CHAMBERS

 @gardencourtlaw



CURRENT STATE OF PLAY WITH AI / ADM AND GOVERNMENT

Mia Leslie

Research Fellow - Public Law Project

THE HARM BEHIND THE HYPE

Robodebt was a fiasco with a cost we have yet to fully appreciate

Published: November 16, 2020 10:57am GMT

DAVID MARIUZ/AAP

Email

Twitter

Facebook

LinkedIn

Print

436

4k

The Robodebt class action bought by Gordon Legal has been settled at a cost to the government of around \$1.2 billion. According to federal Labor frontbencher Bill Shorten, this is the [biggest class action](#) in Australian legal history.

This [comprised](#) refunds of \$721 million to 373,000 people, \$112 million in compensation and \$398 million in cancelled debts.

As is well-known, “Robodebt” is the label commonly applied to the initiative starting in 2016 designed to increase recoveries by government of “overpayments” made to social security recipients, retrospectively dating back to 2010.

“If a Robodebt-like scandal were to happen in the UK, the current framework would not guarantee people clear access to information about how such an automated system worked”

THE HARM BEHIND THE HYPE

FROM POLITICO PRO

Dutch scandal serves as a warning for Europe over risks of using algorithms

The Dutch tax authority ruined thousands of lives after using an algorithm to spot suspected benefits fraud – and critics say there is little stopping it from happening again.



SIGNIFICANCE OF AI USE BY GOVT

*“we are looking at high-volume data that is mostly about poor people,
and we are turning it into prediction tools about poor people”.*

- Professor Karen Yeung,
JHAC oral evidence: New technologies and the application of the law

Algorithmic Transparency Recording Standard

Algorithmic transparency pilots

[Cabinet Office: Automated Digital Document Review](#)

11 January 2024 Standard

[GOV.UK Data Labs \(Cabinet Office\): Related Links](#)

1 June 2022 Standard

[Department for Health and Social Care and NHS Digital: QCovid algorithm](#)

1 June 2022 Standard

[Information Commissioner's Office: Registration Inbox AI](#)

6 July 2022 Standard

[Food Standards Agency: Food Hygiene Rating Scheme – AI](#)

6 July 2022 Standard

[Hampshire and Thames Valley Police: DARAT](#)

14 October 2022 Standard

[West Midlands Police: exploratory analysis of sexual convictions](#)

14 October 2022 Standard

Central Government awareness of AI usage

The Cabinet Office's response to a Parliamentary Question on awareness of AI and ADM in the public sector:

“...the government currently has no comprehensive view of the full range of automated decision-making tools currently used by public authorities”

PLP'S TAG REGISTER

- As of 1 February 2024, there are **55 automated tools** in the register
- **38** are classed as **low transparency**, **16** as **medium transparency**, and **1** as **high transparency**
- **83.6%** of these tools were only uncovered or more fully understood through the submission of **Freedom of Information requests**
- **49.1%** of these tools have **publicly available** government assessments on their impact on the protected characteristics of individuals

The changing legal and regulatory landscape

- AI Regulation
 - Government's 'pro-innovation' AI Regulation White Paper
 - Analysis of consultation feedback expected
- The Data Protection and Digital Information (DPDI) Bill
 - Proposed changes to safeguards in data protection framework
 - HoL Committee Stage Feb/March

What is AI?

EU AI Act: *An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as content, predictions, recommendations, or decisions that can influence physical or virtual environments.*

Basically, AI has two key elements:

- an algorithmic system; and
- it is used to replicate human intelligence.



Public
Law
Project

Rise of the Robots: The Harm Behind the Hype

Challenging Artificial Intelligence use and decisions
Discrimination and Equality

Nicola Braganza KC, Garden Court Chambers



GARDEN COURT CHAMBERS

 @gardencourtlaw

My 4 Key Points

- ❖ Equality Act 2010, private law claim
- ❖ Section 149 Equality Act, Public Sector Equality Duty
- ❖ ECHR Article 14 taken with another substantive human right

*“The **enjoyment of the rights and freedoms** set forth in this **Convention** shall be secured **without discrimination on any ground** such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth **or other status.**”*



1st Key Point - Don't underestimate!

Proxy Discrimination

- Closely corresponding factors, eg excluding civil partners from renting B&B rooms available to married couples, *Preddy v Bull* [2013] UKSC 73
- Predictive policing based on postcodes/geographical areas, focusing on areas with higher Black and Asian communities



1st Key Point - Don't underestimate!

Trained Proxy Discrimination

- an inherently discriminatory criterion is directly embedded and coded into the algorithm, eg mortgage application assessments, marital status correlation with repayment data, excluding civil partnership => sexual orientation

Learnt Proxy Discrimination

- Machine learning algorithms can also draw their own correlations between datapoints.
- The algorithm, rather than the human trainer, creates the indissociable proxy.



1st Key Point - Don't underestimate!

Latent Variable Proxy Discrimination

- Algorithms are infinitely better than humans at amassing data & analysing it for correlations.
- Inherently discriminatory rules created by humans may be recognisable as discriminatory, but not necessarily so for those created by algorithms.

See, 'Directly Discriminatory Algorithms' Jeremias Adams-Prassl, Reuben Binns, Aislinn Kelly-Lyth, M.L.R. 2023 86(1) 144-175



1st Key Point - Don't underestimate!

A 'machine learning tool' could:

“learn a perfect proxy for race - a combination of variables that fully captures the correlation between race and measured recidivism, such that including race over and above this combination would have no effect on risk classification”

B. Davies & T. Douglas, 'Learning to Discriminate: The Perfect Proxy Problem in Artificially Intelligent Criminal Sentencing'

- e.g. formerly boys-only secondary school, began admitting girls in 2010. Employer only recruits a job applicant if (i) a graduate of that school & (ii) born before the year 1990 - neither inherently discriminatory on sex, if applied individually - some school's graduates are women & half the population born before 1990. But no woman meets both criteria applied together = cumulative criteria = ID



Intro to 2nd Key point - Types of discrimination

- **Direct discrimination:** “*difference in treatment of persons in analogous, or relevantly similar situation*” “*based on an identifiable characteristic, or “status”* *DH v Czech Republic* (2008) 47 EHRR 3 at [175]
- **Indirect discrimination:** disproportionately prejudicial effects of a general policy or measure which, though couched in neutral terms, discriminates against a group *DH v Czech Republic* (2008) 47 EHRR 3
- ***Thlimmenos v Greece* 34369/97:** without an objective and reasonable justification, the state fails to treat differently persons whose situations are significantly different.
- **Equality Act 2010 specifically defines the concepts.**



Article 14 - 4 stages

- Does the subject matter of the complaint fall **within the ambit** of one of the substantive Convention rights?
- Does **the ground** upon which the complainants have been treated differently from others constitute a “**status**”?
- Have they been **treated differently** from other people **not sharing** that status who are similarly situated or, alternatively, have they been **treated in the same way** as other people **not sharing** that status whose **situation is relevantly different** from theirs?
- Does that different or similarly in treatment have **an objective and reasonable justification**, in other words, does it pursue a **legitimate aim** and do the means employed bear “**a reasonable relationship of proportionality**” to the aims sought to be realised?

Baroness Hale in *R (DA) v SSWP* [2019] UKSC 21

Approved in *A and B v CICA* [2021] UKSC 27



2nd Key Point - Indirect or Direct Discrimination? Don't Rule out Direct Discrimination

S13 Equality Act 2010 – Direct discrimination

- less favourable treatment on grounds of ...
- No defence

S19 Equality Act 2010 – Indirect discrimination

- A applies to B a provision, criterion or practice “PCP” puts, or would put, persons with whom B shares the characteristic at a particular disadvantage when compared with persons with whom B does not share it, it puts, or would put, B at that disadvantage, and
- A cannot show it to be a proportionate means of achieving a legitimate aim.



2nd Key Point – Can you run it as Direct Discrimination?

- Take the ADMS using geographical areas to flag high crime risk
- areas with larger Asian and black populations are over-represented
 - => ‘predictive policing’
 - => Increased policing => higher arrest rates among those groups
 - => Arrests fed back into the predictive policing algorithm, confirming the original prediction.
 - = ‘runaway feedback loops in predictive policing’
- The model becomes increasingly confident in its own predictions.
 - => **justification made out!**



Intro to 3rd Key Point – Burden of proof

R (DA) v SSWP [2019] UKSC 21 Lord Wilson

“In the DH case the Grand Chamber proceeded to explain in para 177 that, once the applicant had shown a difference in treatment of persons in relevantly similar situations, **the burden of proof lay on the state** to establish that it was justified; and in para 178 that what shifted the burden on to the state was ‘prima facie evidence’”

DH (2008) 47 EHRR 3 at [177]

“Lastly, as to the burden of proof in relation to Article 14, the Court has held that once the applicant has shown a difference in treatment, it is for the Government to show that it was justified.”



3rd Key Point – Burden of Proof – An essential tool!

S136 Equality Act 2010

- A *prima facie* case direct discrimination => the burden of proof shifts to the respondent to provide an adequate non-discriminatory explanation for its actions
- Rather than having to show use of the algorithm can be objectively justified, as required in Indirect Discrimination, the decision-maker will have to show that the unfavourable algorithmic output was *not* because of a protected characteristic. Much more difficult.
- Burden of proof shifts in Indirect Discrimination to justification.



4th Key Point – Get proactive!

- Direct evidence of discrimination is rare. In AI even more difficult.
- AI discrimination won't be intentional, a product of unconscious bias
No need for intent, *Nagarajan v London Regional Transport* [1999] IRLR 572
- Establishing discrimination is difficult and tribunals and courts should be prepared, where appropriate, to draw inferences of discrimination from the surrounding circumstances or any other appropriate matter, *Amnesty International v Ahmed* [2009] ICR 1450.



4th Key Point – Get proactive collecting evidence!

- Equality Impact Assessments
- Data Protection Impact Assessment
- Freedom of Information requests
- Statistics?
- Press on the EIAs: are there gaps? additional lines of enquiry?
- Where is the transparency; testing and review of impact?
- Ask difficult questions - don't be put off!



Because – “mere assertion” in defence is not enough!

“It is clear that, if the SS were able to demonstrate that the objective of the exclusion was to create fairness, this would be a legitimate aim. Furthermore, we do not consider that the SS is required to demonstrate exhaustively that that was the aim of the relevant exclusion. It would be enough **if the contemporaneous documentation could generally be said to support the objective of fairness**. But in our view the SS has to go **beyond mere assertion**. In this legal context a particular policy might be asserted to be fair, but if in fact **the accompanying material does not support that assertion** the court may be unable to conclude that the relevant exclusion was legitimate”

Smith v SSHCLG [2022] EWCA 1391, a planning inspector’s reliance on the new definition of Gypsies and Travellers in Planning Policy for Traveller Sites



R (ota Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058

Facts: -

Pilot project by SWP on automated facial recognition (AFR) technology, processing facial biometric data of members of the public. Surveillance cameras used to capture digital images of people, which were then processed and compared with images of those on police watchlists. If no match made, the image was immediately & automatically deleted.

Held (appeal allowed in part): –

Use of AFR technology interference was not “in accordance with the law” ECHR Art 8(2) (“binary question”): no clear guidance on where technology used & who could be put on a watchlist.

A data protection impact assessment was inadequate & not compliant with the Data Protection Act 2018 s64(3).

Breach of PSED as SWP had not taken reasonable steps to investigate whether the technology had a racial or gender bias.



Bridges cont'd

“The reason why the PSED is so important is that it requires a public authority to give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population.”

The police force had never investigated whether AFR had an unacceptable bias on grounds of race or gender.”

The fact that the technology was being piloted made no difference to the duty.



Bridges – What if there is no evidence to show a need for concern?

“181. We acknowledge that what is required by the PSED is dependent on the context and does not require the impossible. **It requires the taking of reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact** of a proposed decision or policy on people with the relevant characteristics, in particular for present purposes race and sex.

82. We also acknowledge that, as the Divisional Court found, there was no evidence before it that there is any reason to think that the particular AFR technology used in this case did have any bias on racial or gender grounds. **That, however, it seems to us, was to put the cart before the horse.** The whole purpose of the positive duty (as opposed to the negative duties in the Equality Act 2010) is to ensure that **a public authority does not inadvertently overlook information which it should take into account.**” [emphasis added]



Thank you.

020 7993 7600

info@gclaw.co.uk

@gardencourtlaw

<https://www.gardencourtchambers.co.uk/barristers/nicola-braganza/sao>

nicolab@gclaw.co.uk



GARDEN COURT



CHAMBERS



Human Rights and AI

Louise Hooper, Garden Court Chambers

1 February 2024



Surveillance and profiling

- **Surveillance tech:**
 - Automated facial recognition: Webcams, CCTV
 - Computer use- keystrokes, voice recognition, websites visited, content created
- **Emotion recognition tech:**
 - Facial expression recognition
 - Eye tracking
 - Voice stress analysis
 - Functional magnetic resonance imaging



Surveillance and profiling

- **Profiling:**
 - Predictive algorithms e.g. COMPAS sentencing algorithm in the US, OASyS recidivism assessments, welfare fraud, migration and border control.
 - Safety tech in schools.
- **Combination of the above**



Human Rights Claims: some challenges

- HRA 1998: unlawful for a public authority to act in a way which is incompatible with a Convention right.
- Is the client a ‘victim’?
- Time limits
- Can the litigation be funded?
- Is it in the client’s interests?
- Who is the public authority?



What is a public authority for the purposes of the HRA?

Obvious:

- a government department or
- local authority.

But...

‘...In the interests of efficiency and economy, and for other reasons, functions of a governmental nature are frequently discharged by non-governmental bodies...’

Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank [2003]
UKHL 37 [2003] UKHRR 919, HL

So...query whether non-governmental body performing a governmental function is a public authority for HRA.



What is a public authority for the purposes of the HRA? 2

- Considerations that should be taken into account include:
 - the extent to which, in carrying out the relevant function, the body is **publicly funded**,
 - or is **exercising statutory powers**,
 - or is **taking the place of central government or local authorities**,
 - or is **providing a public service**, and
 - whether and to what extent the **state has surrendered or delegated any of its functions or powers** to the organisation

- See further:

YL v Birmingham City Council and others [2007] UKHL 27 (care home not a public authority), *R (Susan Weaver) v London & Quadrant Housing Trust* [2008] EWHC 1377 (Admin) (housing association was a public authority) cf *R(Macleod v Governors of Peabody Trust* [2016] EWHC 737 (Admin) , *Holy Monasteries v Greece* (1995) 20 EHRR 1



In Accordance with the Law

*‘3 ...the Convention concept of legality entails more than mere compliance with the domestic law. It requires that the law be **compatible with the rule of law**. This means that it must be **sufficiently accessible and foreseeable for the individual to regulate his conduct accordingly**. More importantly in this case, there must be **sufficient safeguards against the risk that it will be used in an arbitrary or discriminatory manner**. As Lord Kerr put it in *Beghal v Director of Public Prosecutions (Secretary of State for the Home Department and others intervening)* [2015] UKSC 49; [2015] 3 WLR 344, at para 93, “**The opportunity to exercise a coercive power in an arbitrary or discriminatory fashion is antithetical to its legality**” in this sense.*

R (on the application of Roberts) (Appellant) v Commissioner of Police of the Metropolis and another (Respondents) [2015] UKSC79



Necessary in a democratic society

Weber and Saravia v Germany:

In the context of justifying secret surveillance measures on national security grounds the ECHR held:

- Fairly **wide margin of appreciation** in choosing means for achieving the legitimate aim of protecting national security.
- ‘...nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist **adequate and effective guarantees against abuse**’
- This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law.



Striking the right balance between individual rights and the benefits of new technology

*‘the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests...The Court considers that **any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.**’*

S and Marper v United Kingdom [2008]



Transparency - CJEU- public interest v commercial interests

- Patrick Breyer, MEP sought information about the reliability, ethics and legality of emotion recognition tech of the EU's emotion recognition project for border control 'iBorderCtrl'
- The tech:
 - Involves the use of AI powered lie detection technology with the intention of replacing border guards
 - Interview bot: asks questions and analyses emotional response
 - Returns a risk score
 - If potentially dangerous – check by a real person
- The commercial interests of the REA and its consortium members outweighed the public interest. The CJEU upheld that “general considerations” of overriding public interest invoked by Breyer were not enough to establish that the need for transparency in this situation was “particularly pressing”.



Facial Recognition: *Glukhin v Russia* (4.7.23)

The use of facial recognition technology in administrative offence proceedings in order to identify, locate and arrest a peaceful protestor was capable of having a chilling effect on rights to freedom of expression and assembly.

In implementing facial recognition technology there is a need for:










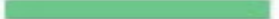








- i) detailed rules governing the scope and application of measures
- ii) strong safeguards against the risk of abuse and arbitrariness.

This increased when live facial recognition technology was used and whilst not ruling out the use of such technology at all the Court found the use in the instant case could not be regarded as necessary in a democratic society.

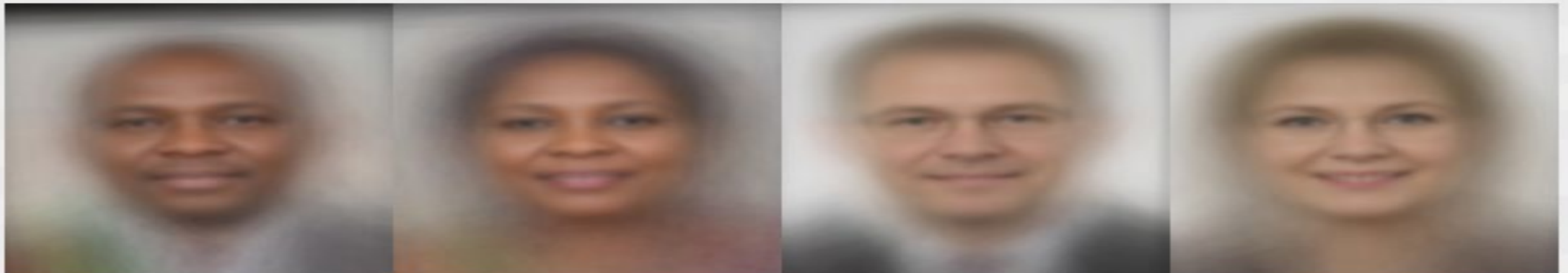
Violation of Articles 8 (private life) and 10 (freedom of expression)



Gender shades- Joy Buolamwini, Timnit Gebru

Gender Classifier	Darker Male	Darker Female	Lighter Male	Lighter Female	Largest Gap
 Microsoft	94.0% 	79.2% 	100% 	98.3% 	20.8% 
 FACE++	99.3% 	65.5% 	99.2% 	94.0% 	33.8% 
 IBM	88.0% 	65.3% 	99.7% 	92.9% 	34.4% 

<http://gendershades.org/overview.html>



Other jurisdictions: Poland and Sweden: facial recognition and biometrics in schools

- The requirement to provide biometrics at school for identification and lunch payment verification has been found illegal in Poland on the grounds that there was no legal basis for the measures.
- In Sweden, facial recognition technology in schools for the purpose of recording attendance has been found to breach not just data protection rights, but also wider rights to privacy and integrity of the person.



Welfare benefits: The SyRI system in the Netherlands

- SyRI did not strike a fair balance between the interest of fraud detection and the human right to privacy and inadvertently created links based on bias such as lower socio-economic status or an immigration background
- **Had only been deployed in poor neighbourhoods**
- **Lack of safeguards** = interference was not proportionate or necessary for the purposes of combatting abuse and fraud.
- **Lack of transparency** on grounds that:
 - **neither risk model nor indicators were public or known** to the data subject
 - **no duty in legislation** to inform individuals that
 - Data had been processed or
 - Risk report submitted
- Automated systems **must meet the minimum protections of GDPR or else will not be ‘in accordance with the law’**
- The **absence of transparency** about the existence and workings of automated systems **arguably results in the right to contest an adverse decision and seek a meaningful remedy being ‘illusory’.**



Predictive decision making

- Visas
- Employment
- Exam Results
- Predictive policing
- Welfare benefits
- Facial Recognition
- Access to Services
- Housing allocations



[This Photo](#) by Unknown Author is licensed under [CC BY-ND](#)



What's next?



AI, Human Dignity and ECHR rights

Key recommendations to ensure human dignity and compliance with ECHR rights, include:

- The **right to be informed** of the fact that one is **interacting with an AI system** rather than a human being
- The **right to refuse to interact with an AI system** when this can adversely affect human dignity
- The **right not to be subject to a decision based solely on automated processing** where this produces legal effects on or similarly significantly affects individuals
- The **right to effectively challenge decisions** made by AI systems **or to opt out** of such decisions
- **A right to human review**
- **A right to decide freely to be excluded from AI enabled manipulation, individualised profiling and predictions** including in the case of non-personal data processing
- The **right to non-discrimination and equal treatment** [see article 14]



Draft Framework Convention on AI, Human Rights, Democracy and the Rule of Law

- Risk based approach mirrors EU AI Act
- Chapter II- general obligations to respect human rights and freedoms, maintain integrity of democratic processes and respect for the rule of law
- Chapter III- **principles of design, development, use and decommissioning of AI systems requires transparency and oversight, accountability and responsibility, equality and non-discrimination, privacy and personal data protection, safety, security and robustness and safe innovation.**
- Chapter IV – remedies and procedural safeguards
- Chapter V – **risk assessment and risk management requirements to mitigate risks including adequate training**
- Chapter VI – implementation of Convention must be **non-discriminatory** and ensure the rights of persons with disabilities and children



Draft Framework Convention on AI, Human Rights, Democracy and the Rule of Law

- Requirement for **public consultation** in respect of fundamental questions raised by the design, development, use and decommissioning of AI systems to ensure appropriate public discussion and multi-stakeholder consultation in the light in of relevant social, economic, legal, ethical and environmental implications.
- Parties should **encourage and promote digital literacy and skills for all of the population.**
- The Convention neither limits nor derogates from existing human rights and fundamental freedoms.
- It does not preclude states from granting a wider measure of protection.



Thank you

020 7993 7600

| info@gclaw.co.uk

| [@gardencourtlaw](https://www.instagram.com/gardencourtlaw)



GARDEN COURT CHAMBERS



Public
Law
Project

Rise of the Robots: The Harm Behind the Hype

Challenging Artificial Intelligence use and decisions

BREAK



GARDEN COURT CHAMBERS

 @gardencourtlaw

EFFECTIVE USE OF FREEDOM OF INFORMATION ACT (FOIA) REQUESTS

Mia Leslie

Research Fellow - Public Law Project



Public
Law
Project

FOIA requests and Govt use of AI and ADM

1. Why FOIA is particularly useful to understanding Govt use of AI and ADM
2. Specific challenge(s) of FOIA regime in this context
3. What to ask for and why its useful
 - *Case study* - PLP's sham marriage algorithm investigation



Why FOIA requests?

- Broad application and scope
 - not limited to data collection or processing
- Can be used to (help) identify where AI / ADM sits in policy or process
 - Extent of human involvement in decision-making process
 - Decision support / recommendation function OR decision-making
- Request for specific documents
 - DPIAs and EIAs



Challenge(s) of FOIA regime

Purpose of AI / ADM use

FOIA disclosure exemption

DWP uses machine learning to:

“identify potentially fraudulent benefit claims before they go into payment”

Section 31(1)(a) - the prevention or detection of crime

Home Office uses the Marriage Assessment (Sham Marriage) Triage Tool to:

“identify proposed marriages and civil partnerships in which additional scrutiny is warranted”

Section 31(1)(e) - the operation of immigration controls



Public
Law
Project

FOIA REQUESTS AND THE SHAM MARRIAGE ALGORITHM (TRIAGE TOOL)

The 'hook'

- 7.5 In order to decide which cases needed to be investigated, MRAU used its own triage model, known as the 'dial'. This brought together known intelligence, profiling agreed by Immigration Intelligence and section 24 reports in order to categorise couples as either 'red' (liable to be extended to 70 days for an investigation) or 'green' (could marry at 28 days). MRAU carried out further research on the red cases to add detail. Senior managers told inspectors that they would not seek to adjust the sensitivity of the dial until further evaluation of the outcomes.

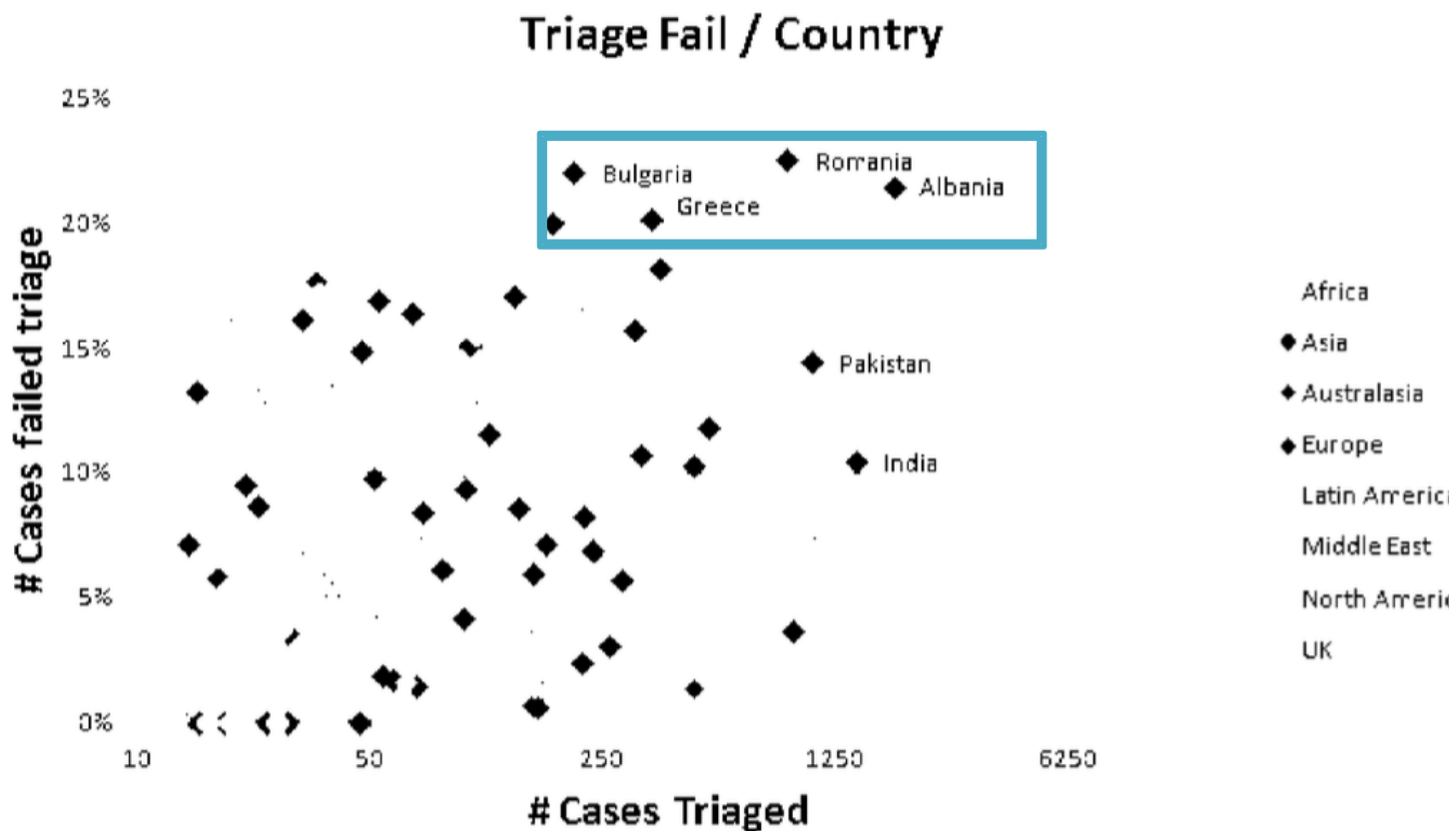


FOIA REQUESTS AND THE SHAM MARRIAGE ALGORITHM (TRIAGE TOOL)

- (1) Does the MRAU still use a triage model or similar system to decide which marriage referrals should be investigated as potential shams?
- (2) Does the model use nationality as a factor in assessing marriage referrals? If so, please provide a copy of the relevant Ministerial authorisation for the purposes of the Equality Act.
- (3) Please provide copies of any equality impact assessments or data protection impact assessments completed in relation to the model.
- (4) Please provide copies of any internal policies, guidance or standard operating procedures which deal with the process of handling marriage referrals and the use of the model.

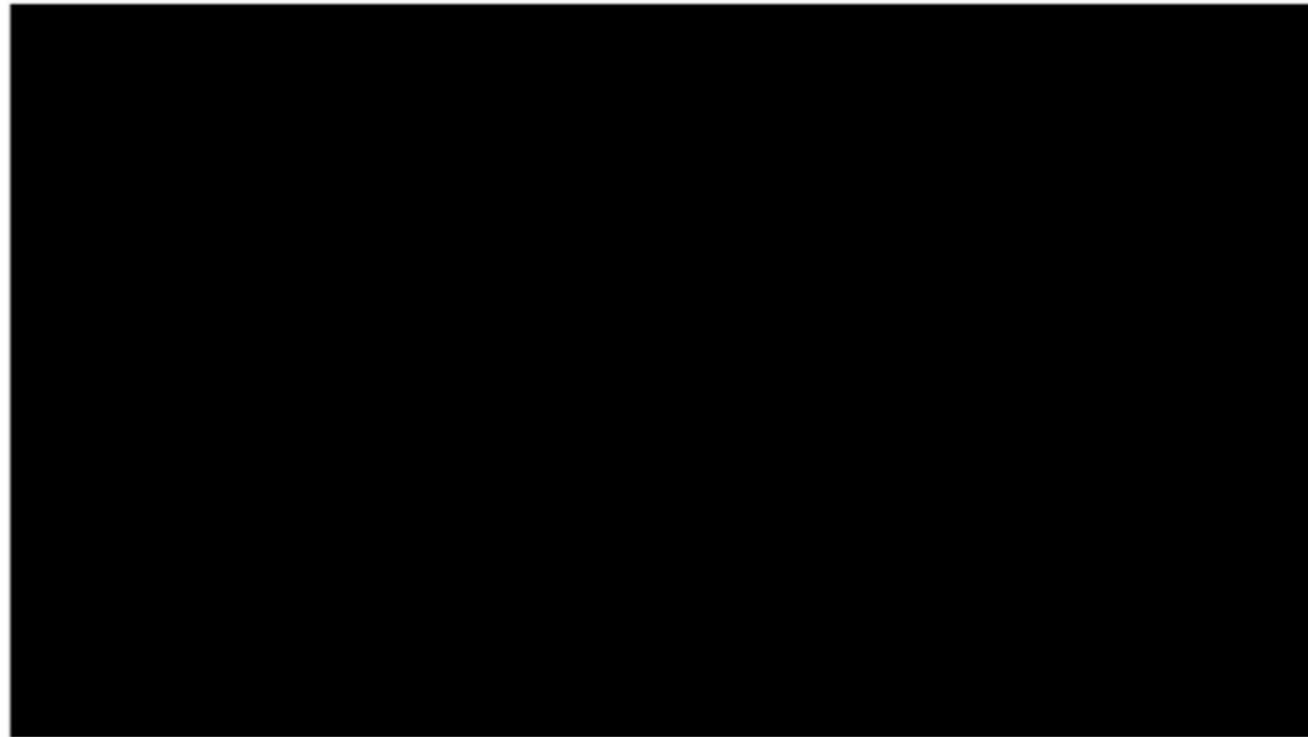


EQUALITY IMPACT ASSESSMENT DISCLOSURE



EQUALITY IMPACT ASSESSMENT DISCLOSURE

The triage process uses the following eight criteria:



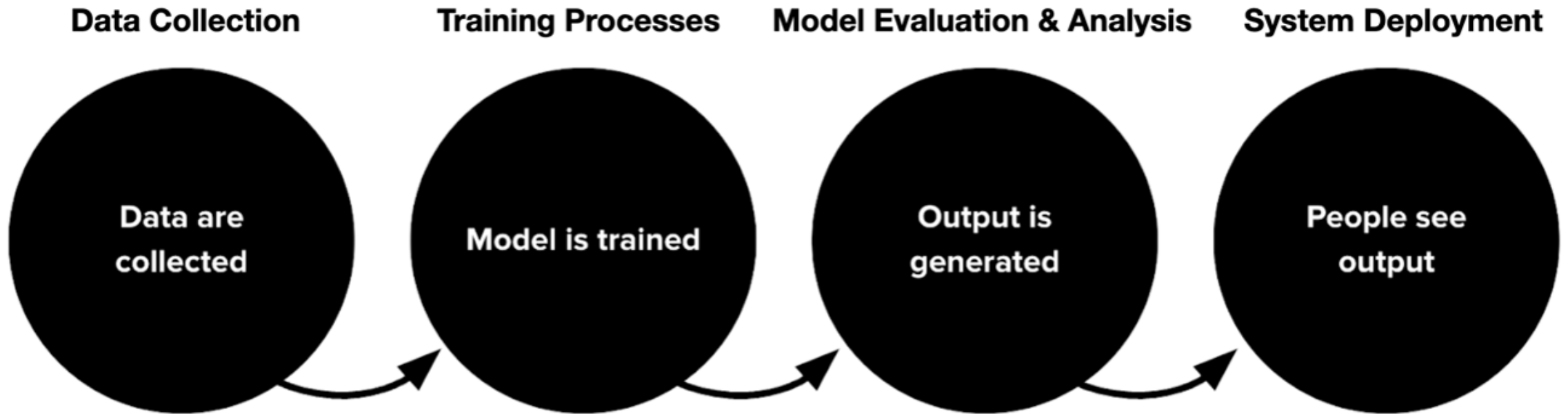
Public
Law
Project

Data Protection and automated systems

Ravi Naik

Legal Director

Ravi@awo.legal



Source: *Margaret Mitchel: The Pillars of a Rights-Based Approach to AI Development* (5 December 2023)

Data Protection Regulations

- i. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**United Kingdom General Data Protection Regulation**), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019
- ii. Data Protection Act 2018

Parliamentary Bills

Data Protection and Digital Information Bill

Government Bill

Originated in the House of Commons, Sessions 2022-23, 2023-24

Last updated: 29 January 2024 at 19:33

Commons



Lords



Final stages



[See full passage](#)

[Details](#)

[News](#)

[Stages](#)

[Publications](#)

Long title

A Bill to make provision for the regulation of the processing of information relating to identified or identifiable living individuals; to make provision

Data Protection Regulations

- i. UK General Data Protection Regulation
- ii. Data Protection Act 2018

Application

Personal data

‘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;

Article 4(1) GDPR

Application

Personal data

‘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;

Article 4(1) GDPR

Application

Data controllers

‘controller’ means

the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Article 4(7) GDPR

Application

Data controllers

‘controller’ means

the natural or legal person, **public authority**, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Article 4(7) GDPR

Application

Access requests

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
 - (a) the purposes of the processing;
 - (b) the categories of personal data concerned;
 - (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (f) the right to lodge a complaint with a supervisory authority;
 - (g) where the personal data are not collected from the data subject, any available information as to their source;
 - (h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Article 15 GDPR

Application

Access requests

1. The data subject shall have the right to obtain from the controller **confirmation** as to whether or not personal data concerning him or her are being processed, and, where that is the case, **access** to the personal data and the following information:
 - (a) the **purposes** of the processing;
 - (b) the **categories** of personal data concerned;
 - (c) the **recipients** or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
 - (d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
 - (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
 - (f) the right to lodge a complaint with a supervisory authority;
 - (g) where the personal data are not collected from the data subject, any available **information as to their source**;
 - (h) the **existence of automated decision-making**, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject

Article 15 GDPR

Information Commissioner's Office



Complaints

Section 165 DPA

(1) Articles 57(1)(f) and (2) and 77 of the GDPR (data subject's right to lodge a complaint) confer rights on data subjects to complain to the Commissioner if the data subject considers that, in connection with personal data relating to him or her, there is an infringement of the GDPR.

(4) If the Commissioner receives a complaint under subsection (2), the Commissioner must—

- (a) take appropriate steps to respond to the complaint,
- (b) inform the complainant of the outcome of the complaint,
- (c) inform the complainant of the rights under section 166, and
- (d) if asked to do so by the complainant, provide the complainant with further information about how to pursue the complaint.

(5) The reference in subsection (4)(a) to taking appropriate steps in response to a complaint includes—

- (a) investigating the subject matter of the complaint, to the extent appropriate, and
- (b) informing the complainant about progress on the complaint, including about whether further investigation or co-ordination with another supervisory authority or foreign designated authority is necessary.

Information Commissioner's Office



Technology | Science | Culture | Gear | Business | Politics | More ▾

Privacy

It looks like the UK's data regulator has given up, blaming coronavirus

Information Commissioner's Office has effectively downed tools as a result of the pandemic, raising concerns about outstanding cases and ongoing privacy issues



By **NICOLE KOBIE**

Tuesday 19 May 2020



Information Commissioner's Office



ICO Realities: 5 Year Analysis (2018-23)

- **Annual Report Numbers:**

Year	DP Fines (at £ 2022)	DP Notices	PECR Fines (at £ 2022)	Income (at £ 2022)
18/19	22 (£3.5M)	0	23	£46M
19/20	15	2	7 (£2.6M)	£56.1M
20/21	3 (£44.4M)	1	35	£59.8M
21/22	4 (£0.7M)	0	33 (£3.2M)	£67.4M
22/23	2 (£7.6M)	1	19 (£1.88M)	£67.4M

- **Cross-Cutting Analysis:**

- ‘Complaints’ Average: GDPR/DP 37,279; PECR 109,254
- 2019/20 Report stated c. **75% budget on “proactive engagement”**
- Asserted great impact to **soft approach** e.g. California 2020 visit:

“The reception was **universally warm** and welcoming and helped us build **strong relationships** with key stakeholders. The UK’s brand of **pragmatic and proportionate regulation** was widely **praised by businesses** and lawmakers, as was our willingness to find new regulatory solutions to problems.”

Thank you

020 7993 7600

| info@gclaw.co.uk

| [@gardencourtlaw](https://www.instagram.com/gardencourtlaw)



GARDEN COURT CHAMBERS
