Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

CIPL and EU Commission High Level Expert Group on AI (HLEG)

Roundtable on the HLEG AI Assessment List

Bojana Bellamy, President, Centre for Information Policy Leadership

27 June 2019, Brussels

BRIDGING REGIONS
BRIDGING INDUSTRY & REGULATORS
BRIDGING PRIVACY AND DATA DRIVEN INNOVATION

ACTIVE GLOBAL REACH

75+
Member Companies

We **INFORM** through publications and events

We **NETWORK** with global industry and government leaders

5+
Active Projects & Initiatives

We **SHAPE** privacy policy, law and practice

We **CREATE** and implement best practices

20+
Events annually

15+
Principals and Advisors

ABOUT US

- The Centre for Information Policy Leadership (CIPL) is a global privacy and security think tank
- Based in Washington, DC, Brussels and London
- Founded in 2001 by leading companies and Hunton Andrews Kurth LLP
- CIPL works with industry leaders, regulatory authorities and policy makers to develop global solutions and best practices for data privacy and responsible use of data to enable the modern information age

Twitter.com/the_cipl

https://www.linkedin.com/company/centre-for-information-policy-leadership

www.informationpolicycentre.com

2200 Pennsylvania Ave NW
Washington, DC 20037

Park Atrium, Rue des Colonies 11
1000 Brussels, Belgium

30 St Mary Axe
London EC3A 8EP

Industry Session – Questions for discussion

- Do you rely on a specific AI framework (i.e. HLEG or DPA guidelines, CIPL Accountability wheel, ISO, Code of Conduct, specific certifications, your own bespoke framework)?
- What are your views on the HLEG guidelines and assessment list?
- Are you already sharing (or are you ready to share) your best practices to drive the market up on development and use of AI?
- Are you using/ developing specific AI privacy preserving technologies?
- What are your views on an EU AI regulation?
- Should a precautionary principle apply in case of high risk ?
- Will you be participating in the piloting process? Why and why not?

Agenda

11:00 **Industry Session**

12:00 **Lunch**

13:00 **Opening Remarks**

- **Bojana Bellamy**, President, Centre for Information Policy Leadership

13:15 **Presentation of the Assessment list and Piloting Phase**

- **Nathalie Smuha**, Coordinator of the HLEG on AI, DG Connect, EU Commission
- **Andrea Renda**, Senior Research Fellow and Head of Global Governance, Regulation, Innovation & Digital Economy, CEPS

13:45 **Presentation of the ICO AI Auditing Framework**

- **Ali Shah**, Head of Technology Policy, ICO

14:00 **Constructive feedback on the Assessment List**

16:30 **End of Roundtable**

GDPR and AI

GDPR is technology neutral and applies fully to the use of personal data in AI

In addition, several GDPR provisions are specifically relevant for AI:

Art. 5(1)(a): Lawful, fair and transparent processing

Art. 13(2)(f): Informed of existence of ADM and meaningful information about logic involved (data collected directly)

Art. 14(2)(g): Informed of existence of ADM and meaningful information about logic involved (data collected indirectly)

Art. 15(1)(h): Right to access information about existence of ADM and meaningful information about logic involved

Art. 22: Right not to be subject to a decision based on ADM producing legal/similarly significant effects

Art. 22(3): Right to obtain human intervention

Art. 35: Conduct a DPIA for high risk processing, in particular when using new technology

Art. 35(3)(a): DPIA required in the case of Art. 22 ADM

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

AI and Machine Learning: Challenges and Tensions with Data Protection Principles

Challenges associated with AI

•Fairness •Ethical Issues •Public Trust •Legal Compliance •Tensions

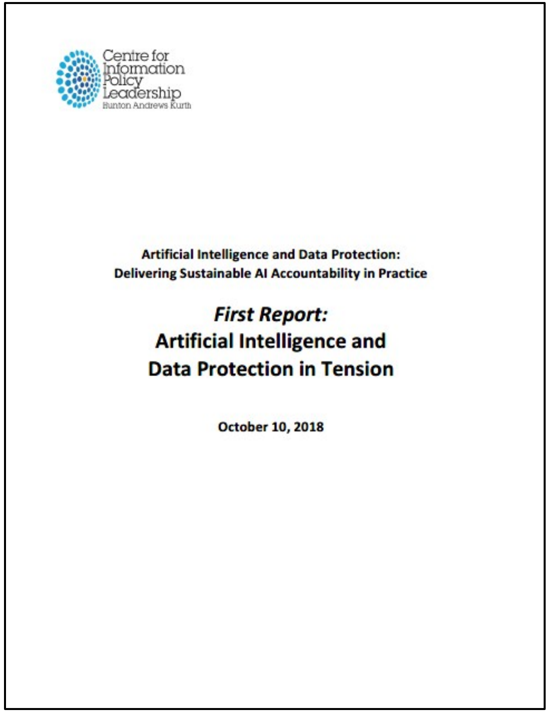
Tensions To Resolve

Data Protection Requirements	Artificial Intelligence
Collection limitation / Data minimisation	Needs sufficient volumes of data for research, analysis, operation, training and to avoid bias
Purpose specification & Use limitation	Uses data for new and unforeseen purposes beyond original scope
Legal basis for processing	Insufficient/limited variety of legal bases may undermine full range of AI applications
Retention limitation	Needs to retain for AI training, deployment and oversight
Transparency	Operates in a black box and may produce unexplainable and unanticipated outcomes
Individual rights	Cannot always facilitate access, correction or explanation of the logic involved
Rules on ADM	Based on ADM & No human involvement

CIPL Project on Accountable AI

CIPL Project on Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice

https://www.informationpolicycentre.com/ai-project.html



Centre for Information Policy Leadership
Hunton Andrews Kurth

Artificial Intelligence and Data Protection:
Delivering Sustainable AI Accountability in Practice

First Report:
Artificial Intelligence and
Data Protection in Tension

October 10, 2018

- First Report - **Artificial Intelligence and Data Protection in Tension** (October 2018) https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf

- Second Report in progress (estimated release October 2019)

First Report

Describes in clear and understandable terms:

(1) **What AI is** and how it is being used all around us today;

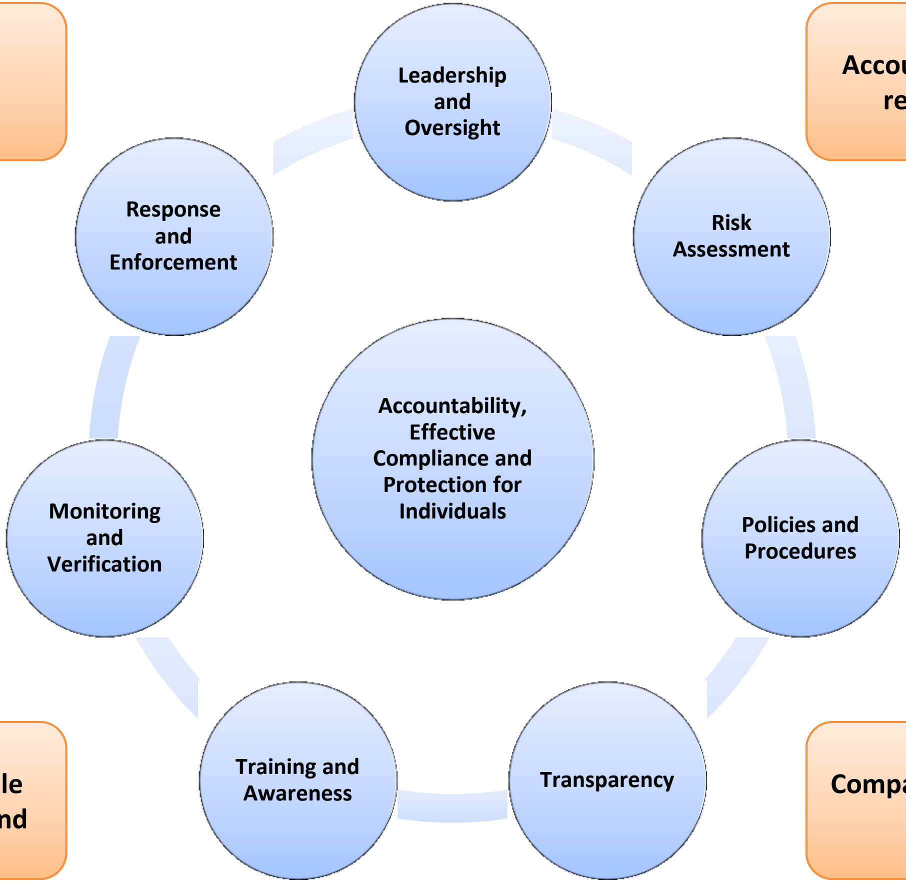
(2) **The role that personal data** plays in the development, deployment and oversight of AI; and

(3) **The opportunities and challenges** presented by AI to data protection laws and norms.

Implementing Accountability

Organisations must be able to demonstrate accountability – internally and externally

Accountability is not static, but dynamic, reiterative and a constant journey

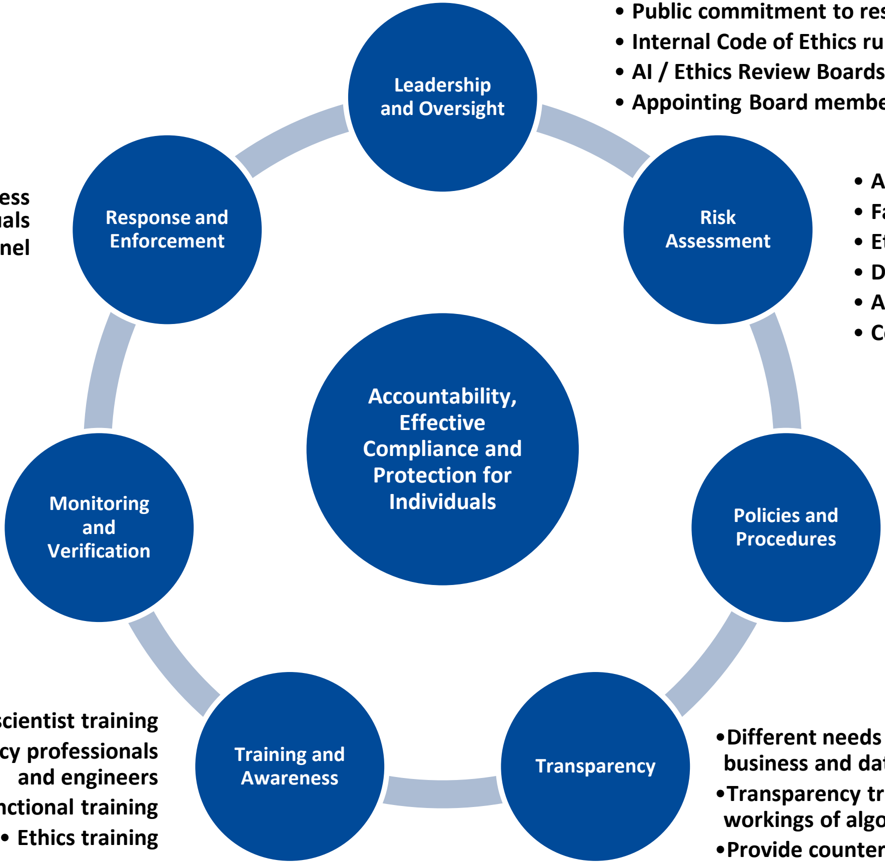


Accountability translates legal requirements into risk-based, verifiable and enforceable corporate practices and controls

Company values and business ethics shape accountability

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

What Does an Accountable AI Governance Model Look Like?



Accountability, Effective Compliance and Protection for Individuals

Leadership and Oversight

- Public commitment to respect specific principles in AI development
- Internal Code of Ethics rules
- AI / Ethics Review Boards /Committees (internal or external)
- Appointing Board member for AI oversight • Privacy engineers

Risk Assessment

- Algorithmic Impact Assessment
- Fairness assessment tools
- Ethics Impact Assessment
- DPIA for high risk processing
- Anonymisation techniques
- Consider external guidance / developments

Policies and Procedures

- Verification of data input and output
- Algorithmic bias testing
- Pilot testing AI models before release

Transparency

- Different needs for transparency to individuals, regulators, business and data partners and internally
- Transparency trail – explainability of decision and broad workings of algorithm
- Provide counterfactual information

Training and Awareness

- Data scientist training
- Cross functional training – privacy professionals and engineers
- Ad hoc and functional training
- Ethics training

Monitoring and Verification

- Audit of input and output
- Human in the loop – human review of individual decisions
- Reliance on different audit techniques

Response and Enforcement

- Complaints-handling and redress mechanisms for individuals
- Feedback channel

Artificial Intelligence Guidance to Date

UK ICO, Big Data, Artificial Intelligence, Machine Learning and Data Protection (September 2017)

- https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

CNIL, How Can Humans Keep the Upper Hand?: The Ethical Matters Raised by Algorithms and Artificial Intelligence (December 2017)

- https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

Datatilsynet (Norwegian Data Protection Authority), Artificial Intelligence and Privacy (January 2018)

- https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf

ICDPPC, Declaration on Ethics and Data Protection in AI (October 2018)

- https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

European Commission High Level Expert Group on AI, Draft Ethics Guidelines for Trustworthy AI (December 2018)

- https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57112

Singapore PDPC, A Proposed Model Artificial Intelligence Governance Framework (January 2019)

- https://www.pdpc.gov.sg/Resources/Model-AI-Gov

Council of Europe, Guidelines on Artificial Intelligence and Data Protection (January 2019)

- https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8

OECD Council Recommendation on Artificial Intelligence (May 2019)

- https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#_ga=2.251645126.1726117956.1559308992-1610692363.1559308992

Guidance from the European Commission High Level Expert Group on AI

European Commission

INDEPENDENT

HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE

SET UP BY THE EUROPEAN COMMISSION

AI

ETHICS GUIDELINES FOR TRUSTWORTHY AI

Identifies the **ethical principles** that must be respected in the development, deployment and use of AI systems:

- Respect for human autonomy, prevention of harm, fairness and explicability
- Pay attention to more vulnerable groups (children, disabled individuals, employees, consumers)
- Acknowledge that in spite of substantial benefits, AI systems also pose certain risks and wider impacts on society

Provides **seven requirements to realize** Trustworthy AI (technical and non-technical means)

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Environmental and societal well-being
- Accountability

Provides a **Trustworthy AI assessment list** to operationalize key requirements

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

The HLEG Guidelines and GDPR

Key requirements of Trustworthy AI	Overlap with GDPR provisions
Human Agency and Oversight	Legitimate interest balancing test (**art. 6(1)(f)**)/ Transparency (**art. 13 & 14**)/ ADM (**art. 22**) and Right to obtain human intervention (**art. 22(3)**) / Risk assessment and DPIA (**art. 35**)
Technical Robustness and Safety	Security (**art. 32**) / Risk assessment and DPIA (**art. 35**) / Data accuracy (**art. 5(1)(d)**)
Privacy and Data Governance	Data protection principles (**art. 5**) / Legal grounds for processing (**art. 6**)/ Legal grounds for sensitive data (**art. 9**)/ Rights of the data subject (Chapter III) and in particular Transparency (**art. 13 & 14**) and Right to information on ADM and logic involved (**art. 15(1)(h)**) and Right not to be subject to an ADM decision (**art. 22**) and right to human intervention (**art. 22(3)**) / Accountability (**art 24(3)**) / Data protection by design (**art. 25**)/Processor due diligence (**art. 28(1)**) / Security (**art. 32**) / DPO (**art. 37 & 38**)
Transparency	Transparency (**art. 13 & 14**)/ ADM (**art. 22**)
Diversity, Non-Discrimination and Fairness	Fairness Data protection principle (**art. 5.1(a)**) / Risk assessment and DPIA (**art. 35**) / Right to information on ADM and logic involved (**art. 15(1)(h)**)
Societal and environmental wellbeing	Risk assessment and DPIA (**art. 35**) / Transparency (**art. 13 & 14**)
Accountability	Accountability (**art 5(2) & 24(3)**) / Risk assessment and DPIA (**art. 35**) / Processor due diligence (**art. 28(1)**) / DPO (**art. 37 & 38**)

European
Commission

Towards Ethics Guidelines for Trustworthy AI in Europe

Nathalie Smuha

European Commission, DG Connect (Dir. A – AI & Digital Industry)
KU Leuven, Faculty of Law (Dept. International & European Law)

Background

EU STRATEGY ON ARTIFICIAL INTELLIGENCE

published in April 2018

Boost AI uptake

Tackle socio-economic changes

Ensure adequate ethical & legal framework

In this context: appointment of Independent High-Level Expert Group on Artificial Intelligence (AI HLEG) in June 2018

European Commission

High-Level Expert Group and mandate

Chair:
Pekka Ala-Pietilä

52 members from:

Industry

Academia

Civil society

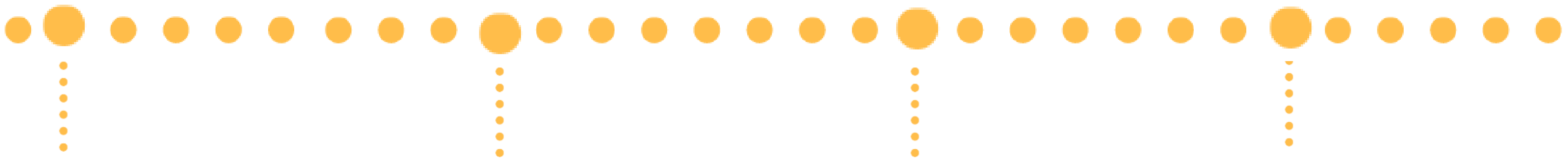
Two deliverables

- Ethics Guidelines for Artificial Intelligence
- Policy & Investment Recommendations

Interaction with European AI Alliance

- Broad multi-stakeholder platform counting over 3000 members to discuss AI policy in Europe

Ethics Guidelines for AI – Process



18 December 2018

First draft published

December 2018- February 2018

- Open consultation
- Discussion with Member States
- Discussion on the European AI Alliance

March 2019

Revised document delivered to the Commission

April 2019

Final document published & welcomed through Commission Communication

Ethics Guidelines for AI – Intro

Human-centric approach: AI as a means, not an end

Trustworthy AI as our foundational ambition, with three components

Lawful AI

Ethical AI

Robust AI

Three levels of abstraction

from principles (Chapter I)

to requirements (Chapter II)

to assessment list (Chapter III)

European Commission

Ethics Guidelines for AI – Principles

4 Ethical Principles based on fundamental rights

Respect for human autonomy

Prevention of harm

Fairness

Explicability

Ethics Guidelines for AI – Requirements

- Human agency and oversight
- Technical Robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination and fairness
- Societal & environmental well-being
- Accountability

To be continuously implemented & evaluated throughout AI system's life cycle

European Commission

Ethics Guidelines for AI – Assessment List

Assessment list to operationalise the requirements

- Practical questions for each requirement – 131 in total
- Test through piloting process to collect feedback from all stakeholders (public & private sector)
  - “Quantitative” analysis track -> open survey
  - “Qualitative” analysis track -> in depth interviews
  - European AI Alliance

Piloting Phase: 26 June – 1 December

European Commission

Next steps

- ❑ Feedback gathering on assessment list from 26 June till December 2019
- ❑ Revised version assessment list in early 2020
- ❑ Commission will then decide on Next Steps
  - Self-regulation / (Self-)certification?
  - Standardisation?
  - Sectorial Guidelines?
  - Regulation?

Policy & Investment Recommendations

Second deliverable: different audience (Commission & Member States)

- Ensuring Europe’s competitiveness and policies for Trustworthy AI
- Looking at key impacts and enablers
- Presented at AI Alliance Assembly on 26 June 2019
- After the summer: recommendations for strategic sectors

European Commission

Thank you

Icons made by Freepik from www.flaticon.com

AI Audit Framework

Ali Shah - Head of Technology Policy
ali.shah@ico.org.uk

Information Commissioner's Office

UK Independent Regulator Upholding Information Rights

DPA 2018/GDPR

PECR - e-IDAS - NIS

ICO Priorities

Information Commissioner's Office

Technology Strategy 2018-2021

ico.

Information Commissioner's Office

1. To ensure effective education and awareness for ICO staff on technology issues.

2. To provide effective guidance to organisations about how to address data protection risks arising from technology.

3. To ensure the public receive effective information about data protection risks arising from technology.

4. To support and facilitate new research into data protection risks and data protection by design solutions.

5. To recruit and retain staff with technology expertise to support delivery of the strategy.

6. To establish new partnerships to support knowledge exchange with external experts.

7. To engage with other regulators, international networks and standards bodies on technology issues related to data protection.

8. To engage with organisations in a safe and controlled environment to understand and explore innovative technology.

ICO Priorities

- Cyber Security
- Anonymisation
- Age Appropriate Design Code
- Ad-Tech
- Facial Recognition Technology

and

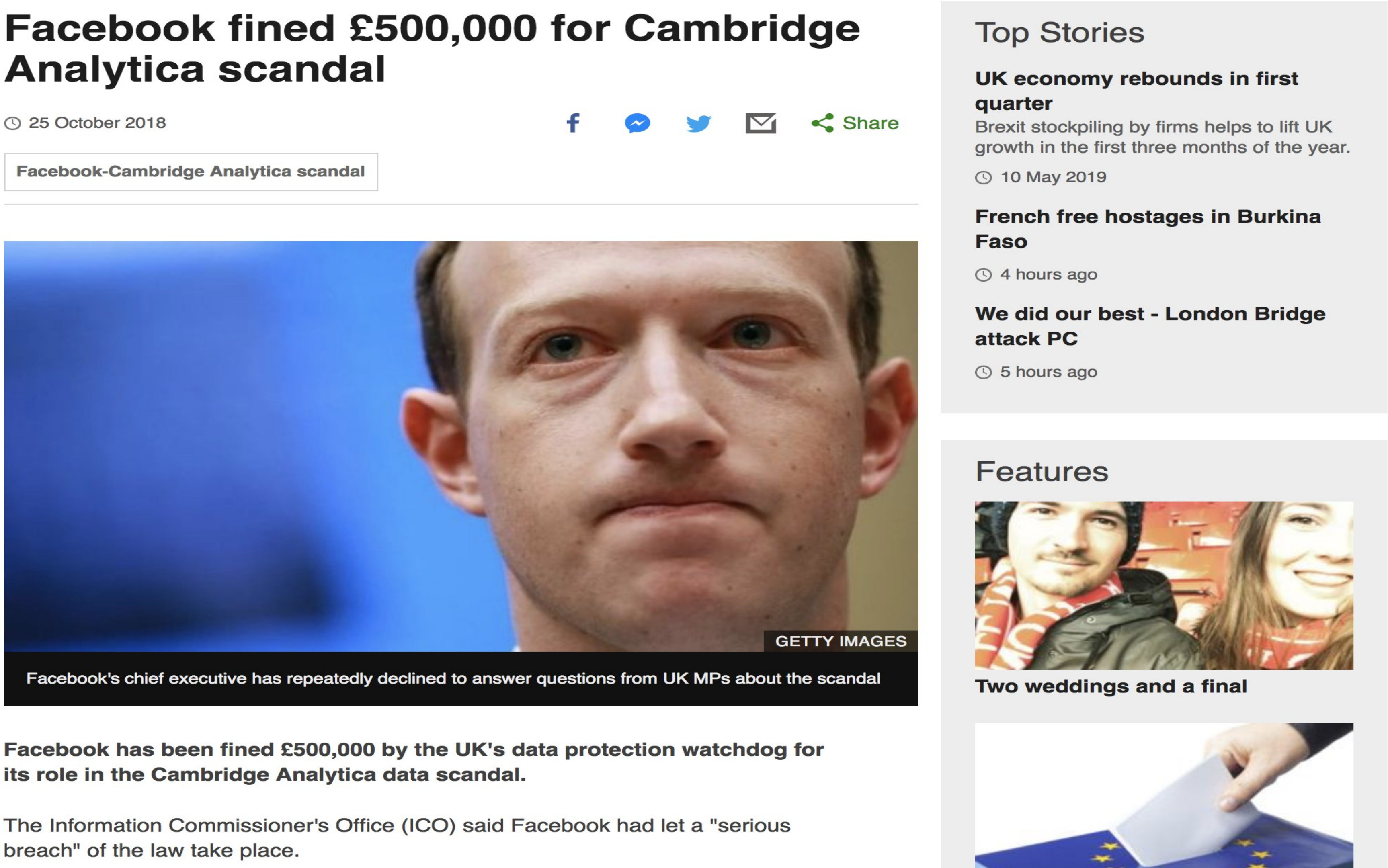
- AI

by 2030

$15.7tr economic contribution

26% increase in GDP

Source: PwC https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html



Facebook fined £500,000 for Cambridge Analytica scandal

25 October 2018

Facebook-Cambridge Analytica scandal

Facebook's chief executive has repeatedly declined to answer questions from UK MPs about the scandal

Facebook has been fined £500,000 by the UK's data protection watchdog for its role in the Cambridge Analytica data scandal.

The Information Commissioner's Office (ICO) said Facebook had let a "serious breach" of the law take place.

Top Stories

UK economy rebounds in first quarter

Brexit stockpiling by firms helps to lift UK growth in the first three months of the year.

10 May 2019

French free hostages in Burkina Faso

4 hours ago

We did our best - London Bridge attack PC

5 hours ago

Features

Two weddings and a final

ICO AI Audit Framework

Dr Reuben Binns – ICO AI Research Fellow

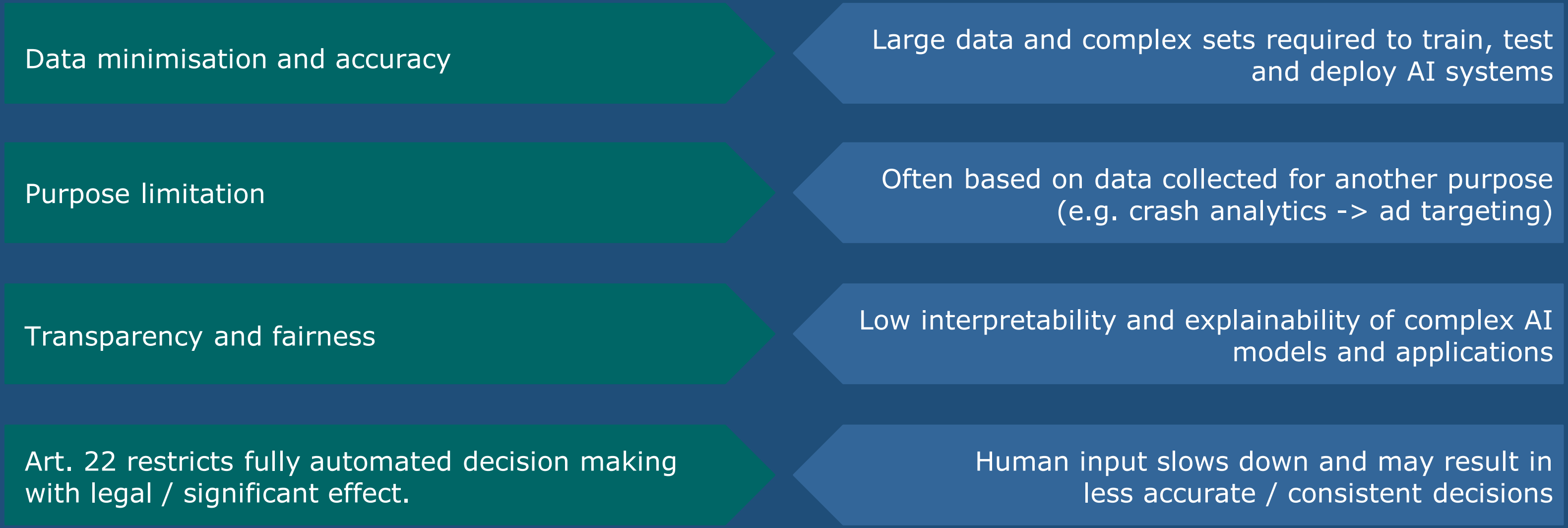
Background

- GDPR put much more focus on automated processing and decisions making through new technologies such as AI.
- It also strengthened individuals' rights (e.g. the right to object to profiling), as well as the ICO powers (e.g. compulsory audits and fines)
- The ICO made AI one of its top three strategic priorities and appointed its first Postdoctoral Research Fellow in AI to develop its AI Auditing framework.

Framework objectives

- Develop a solid methodology for the ICO to supervise the use of personal data in AI systems.
- Support the development of internal knowledge, capabilities, and toolkits to support the work of the ICO, and in particular the assurance and investigations teams.
- Inform additional external guidance for organisations on how to manage data protection risks in AI systems; and support innovation and adoption of “safe” AI.

SOME EXAMPLES OF TENSIONS BETWEEN DATA PROTECTION AND AI



Data minimisation and accuracy	Large data and complex sets required to train, test and deploy AI systems
Purpose limitation	Often based on data collected for another purpose (e.g. crash analytics -> ad targeting)
Transparency and fairness	Low interpretability and explainability of complex AI models and applications
Art. 22 restricts fully automated decision making with legal / significant effect.	Human input slows down and may result in less accurate / consistent decisions

1. GOVERNANCE AND ACCOUNTABILITY

RISK APPETITE	LEADERSHIP ENGAGEMENT AND OVERSIGHT	DATA PROTECTION BY DESIGN AND DEFAULT	MANAGEMENT AND REPORTING STRUCTURES
COMPLIANCE AND ASSURANCE CAPABILITIES	POLICIES AND PROCEDURES	DOCUMENTATION AND AUDIT TRAILS	TRAINING AND AWARENESS

2. AI-SPECIFIC RISK AREAS

FAIRNESS AND TRANSPARENCY IN PROFILING	ACCURACY	FULLY AUTOMATED DECISION MAKING MODELS	SECURITY AND CYBER
TRADE-OFFs	DATA MINIMISATION AND PURPOSE LIMITATION	EXERCISE OF RIGHTS	IMPACT ON BROADER PUBLIC RIGHTS

FAIRNESS AND TRANSPARENCY IN PROFILING

- Bias and discrimination
- Sensitive inferences
- Interpretability of AI systems
- Explainability of AI decisions to data subject (ICO project ExplAIn)

ACCURACY

- Accuracy of AI outputs and performance measures

FULLY AUTOMATED DECISION MAKING MODELS

- Meaningful human review in non-fully automated decision making AI systems
- Human review of decisions made by fully automated decision making AI systems

SECURITY AND CYBER

- Testing and verification challenges and model integrity
- Privacy attacks on Machine Learning models
- Existing security risks exacerbated by the use of AI

TRADE-OFFs

- Trade-offs between:
  - Precision vs recall
  - Accuracy vs privacy
  - Fairness vs accuracy
  - Fairness vs privacy
  - Accuracy vs generalisability

DATA MINIMISATION AND PURPOSE LIMITATION

- Managing training data
- Re-using AI models for new purposes

EXERCISE OF RIGHTS

- Right to:
  - Be forgotten (right to erasure)
  - Data portability
  - Have inaccurate data corrected

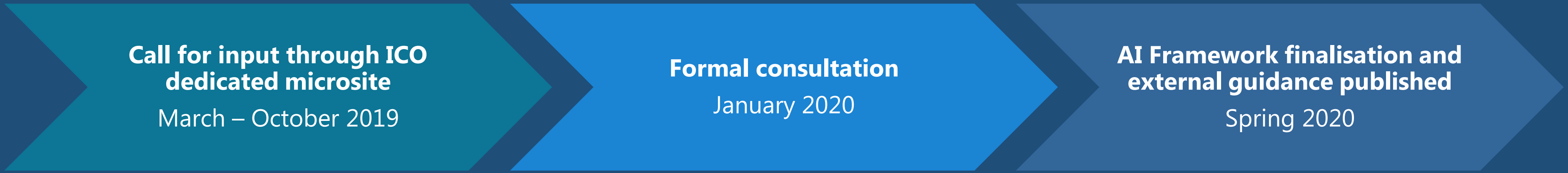
IMPACT ON BROADER PUBLIC RIGHTS

- Public legitimacy
- Autonomy
- Freedom of association
- Freedom of speech
- Individual distress: offensive ad targeting

OVERALL RISK MANAGEMENT CONSIDERATIONS AND COMMON THEMES ACROSS FRAMEWORKS ELEMENTS (E.G. OUTSOURCING RISKS)

Where next for the AI framework?

Timeline



Call for input through ICO dedicated microsite

March – October 2019

Formal consultation

January 2020

AI Framework finalisation and external guidance published

Spring 2020

https://ai-auditingframework.blogspot.com/

AIAuditingFramework@ico.org.uk

THANK YOU

https://ai-auditingframework.blogspot.com/

AIAuditingFramework@ico.org.uk

Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

Feedback on the Assessment list
Questions for discussion – General Feedback

- Does the list sufficiently enable the operationalisation of AI?
- Is the list adaptable to be relevant to different recipients, i.e., developers, users, third party acquirers…?
- Can the list be used horizontally across all applications to ensure a foundation in all domains?
- Is the list flexible enough to be tailored to specific use cases? Is it sufficiently scalable?
- Can the list be easily integrated into existing frameworks and governance mechanisms (CIPL Accountability Wheel, ISO, privacy management programs, BCR…)? Does the list cover topics already addressed by other frameworks?
- Is the assessment list easily understandable and deployable in organisation or does it need to be further translated into simpler and more operational language?
- How would this list be implemented within your organisation? Which steps? (promotion, implementation, control, audit), which stakeholders involved? Which timing? Which resources?
- Is the assessment list fit for use in particular sensitive areas or in projects raising difficult questions (i.e. human rights or societal impacts of the AI system)?
- Can the assessment list be self sufficient or does it need to be coupled with additional risk assessment or compliance frameworks?
- Are there gaps in the assessment list? (e.g. training and awareness)

Feedback on the Assessment list
Questions for discussion – Privacy and Data Governance

- Are the questions consistent with key data protection and GDPR concepts (risk-based approach, DPIA, data minimisation, privacy-by-design, legal base, retention limitation, DPO), is there overlap or contradiction?
- Does this list rely too much on "consent and control" of the individuals in all cases?
- Does the list sufficiently take into account the risk-based approach?
- What about due diligence on third party acquired data/ use of third party developed AI systems? Should more detailed assessment criteria be included in the list?

Feedback on the Assessment list
Questions for discussion – Transparency

- Is the possibility for effective alternative solutions to compensate for the lack of transparency sufficiently taken into account with possible examples?

- Are the design of product and services and user experience sufficiently taken into account?

- Do the questions take into account the different level of understanding of recipients (developers, BtoB user, BtoC user) and among users (e.g. children, vulnerable persons) for the transparency and explainibility requirements?

- Do the questions allow for modulation of transparency and explainibility depending on the potential impact of AI on individuals? In particular when they are not legally significant?

- Is there transparency to regulators?

Feedback on the Assessment list
Questions for discussion – Diversity, Discrimination and Fairness

- Do the questions sufficiently take into account the lack of common definition of fairness especially in the context of AI?
- Do the question sufficiently take into account the fact that bias are also included in purely human decision?
- Do the questions sufficiently take risks into account (i.e. should potential bias be taken into account in case of very limited impacts on rights and obligations of individuals)?
- Do the questions take into account the difference between socially acceptable bias and socially non-acceptable bias?
- Are the questions are too “result-oriented” where they should more on a continuous improvement mode and “best efforts” taking into account risks, benefits and costs?
- Do the questions take into account the fact that systems are not stable, but that they change, are updated and can become biased?
- Do the questions take into account processing the need to feed the AI system with sensitive data to verify whether it is biased?

Feedback on the Assessment list
Questions for discussion – Accountability

- Does the notion of accountability in the assessment question match the notion of accountability under the main data protection regimes (including GDPR)?

- Do the questions take into account the iterative and continuous improvement characters of accountability?

- Does it sufficiently include the notions of risk and scalability?

- What could be the role of the DPO/privacy office ?

- Should the requirement to establish review board be more prominent?

Thank You

Bojana Bellamy
bbellamy@HuntonAK.com

Centre for Information Policy Leadership
www.informationpolicycentre.com

Hunton Andrews Kurth Privacy and Information Security Law Blog
www.huntonprivacyblog.com

FOLLOW US ON LINKEDIN
linkedin.com/company/centre-for-information-policy-leadership

FOLLOW US ON TWITTER
@THE_CIPL