Centre for Information Policy Leadership
Hunton Andrews Kurth LLP

3 July 2019

Comments by the Centre for Information Policy Leadership on the UK's Committee on Standards in Public Life Review of Artificial Intelligence and Public Standards

The Centre for Information Policy Leadership (CIPL) is an independent global data privacy and cybersecurity think tank with over 70 member companies. Its mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world.[1]

CIPL welcomes the opportunity to contribute to the Review of Artificial Intelligence and Public Standards which has been launched by the UK's Committee on Standards in Public Life.[2]

Although a great deal has been written about Artificial Intelligence in recent years, CIPL believes that this Review is the first to focus on the ethical issues which are, and increasingly will be, raised by the use of AI specifically by public authorities and those delivering public services. CIPL congratulates the Committee for this important initiative.

This submission does not aim to be comprehensive. Instead, we draw attention to some of the relevant work that CIPL has already undertaken. We hope that some of the information and analysis we have assembled may be of assistance to the Committee, particularly our observations about the relationship between AI and data protection regulation. We also suggest that there may be some ideas, approaches and techniques which could usefully be adopted and adapted by the Committee for its Review.

Delivering Sustainable AI Accountability in Practice

CIPL has been conducting extensive research on the interplay between AI and data protection through its project on "Delivering Sustainable AI Accountability in Practice".[3] This on-going project aims to provide a detailed understanding of the opportunities presented by AI, its challenges to data protection laws and practical ways to address these issues through best practices and organisational accountability. CIPL published its first White Paper "Artificial Intelligence and Data Protection in Tension"[4] in October 2018.

---

[1] CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth and is financially supported by the law firm and 77 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this paper should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] Review of AI and Public Standards, UK Committee on Standards in Public Life, available at https://www.gov.uk/government/collections/ai-and-public-standards.

[3] See CIPL Project on Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice: https://www.informationpolicycentre.com/ai-project.html.

[4] See CIPL white paper on "Delivering Sustainable AI Accountability in Practice: Artificial Intelligence and Data Protection in Tension", 10 October 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_ai_first_report_-_artificial_intelligence_and_data_protection_in_te....pdf.

This paper includes:

- an Introduction to Artificial Intelligence, noting that the term encompasses a wide variety of current and prospective technological innovations, each of which presents distinct challenges to existing norms, policies and laws;
- a summary of the capabilities of Artificial Intelligence, looking particularly at the functions, potential and implications of machine learning, deep learning and Natural Language Processing (NLP);
- an overview of public and private uses of Artificial Intelligence, noting some of the changes in major sectors influenced by emerging AI technologies. These include healthcare, transportation, financial services, marketing, agriculture, education, cybersecurity, law enforcement and public services;
- an analysis of some of the tensions that AI brings – or will very soon bring – for data protection law and compliance.

This tensions identified in this latter section of the CIPL paper include:

- problems with definitions of "personal data";
- potential conflicts with limitations on collection, purpose specification and use of personal data;
- problems with excessively narrow approaches to data minimisation and data retention;
- challenges of transparency and openness, especially where the "black box" phenomenon calls into question how to provide notice about "the unpredictable and the unexplainable";
- the need for data quality, comprehensiveness and correction mechanisms;
- the particular challenges of laws which specifically address profiling and automated decision-making.

The paper concludes by elaborating six key observations, all of which have relevance to the Committee's Review:

- not all AI is the same;[5]
- AI is already widely used in society and is of significant economic and societal value;
- AI requires substantial amounts of data to perform optimally;
- AI requires data, including sensitive personal data, to identify and guard against bias;
- the role of human oversight of AI will need some re-definition for AI to deliver the greatest benefits;
- AI challenges some of the basic requirements of data protection law.

Ethical Implications of Artificial Intelligence

The CIPL White Paper notes repeatedly that the development and deployment of various AI techniques in various contexts increasingly raises ethical issues which go much wider than the focus of data protection regulation. There are also some very difficult tensions between benefits and risks. These concerns tie in with emerging debates about data ethics.

[5] A point forcibly made by the recent ICO/Turing Institute's "Project Explain" paper which emphasises the importance of context in explaining AI decisions.

For example, the 40th International Conference of Data Protection and Privacy Commissioners in October 2018 adopted a Declaration on Ethics and Data Protection in Artificial Intelligence.[6] CIPL very much welcomed this focus of attention and much of the substance of the Declaration. But we had reservations about some of the detailed points where we feared excessive threats to beneficial innovation. Accordingly CIPL published a Response to the Declaration[7] in January 2019. The Response argued the need for novel, flexible, risk-based and creative approaches to addressing the challenges, even if this means some departures from conventional interpretations of privacy principles. Moreover, while respect for privacy rights must be a key consideration in the development of AI, such rights are not absolute and must be balanced against other human rights, such as those respecting life and health, and the benefits of the AI to individual users and society as a whole.

Again, the Committee may find some parts of our detailed Response to be useful for its current Review.

Impact of Data Protection

The scope of the Committee's Review is wider than data protection, addressing some applications which will never involve any personal data at all. It is also narrower, focusing on the use of AI by public services alone. But the messages from the CIPL White Paper suggest that many innovatory and potentially beneficial uses of AI – perhaps the majority – will be severely threatened unless creative and flexible approaches are adopted towards data protection requirements. Such an approach needs to be adopted by regulatory bodies, but also by those (such as DPOs) overseeing compliance inside organisations. This is not to suggest that a creative, flexible approach means any sort of automatic green light. But nor should there be an automatic red light just because some sort of AI application is involved.

What will be important is to address these issues openly from the outset and establish true accountability of organisations when using AI: (1) having credible mechanisms to assess and demonstrate whether benefits outweigh downsides and (2) implementing an effective control system for each application which addresses both compliance and ethical considerations. As a minimum, regulatory bodies will expect such arrangements from accountable organisations if they are to be expected to adopt any sort of creative and flexible approach.

The remainder of this submission includes suggestions which the Committee could adopt to move towards such a situation.

[6] ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence, 23 October 2018, available at https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

[7] See comments by the Centre for Information Policy Leadership on the International Conference of Data Protection and Privacy Commissioners Declaration on Ethics and Data Protection in Artificial Intelligence, 25 January 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_icdppc_declaration_on_ethics_and_data_protection_in_artificial_intelligence.pdf.

Lessons from Data Protection

CIPL believes that there are many parallels and that it may in fact be possible to draw some lessons from successes with data protection as well as from innovations which have sought to address some of the limitations of a "traditional" approach.

- A Principles-based approach: Although, as noted above, AI is increasingly calling into question the substance of some of the core data protection principles, CIPL believes that the basic concept of a principles-based approach is sound and has largely survived the test of time. Given such rapid changes in technology and the focus on public services, CIPL believes that it would be sensible for the Committee to articulate principles which public sector and third parties providers would be expected to observe when developing and deploying AI applications. This would avoid some of the drawbacks associated with excessively prescriptive legislative requirements, anticipate that public bodies can largely be expected to observe such principles without the need for legal enforcement and will enable rapid refinement in the light of experience.

  At this stage, CIPL hesitates to suggest a comprehensive set of such principles, although – as noted below – some of them will follow from the Standards Challenges which the Committee has already articulated. We do suggest, however, that it would be desirable and efficacious to set out some principles in explicitly negative terms – i.e. unacceptable processes and outcomes which the Committee believes that public service providers should avoid when using Artificial Intelligence.

- Accountability – Accountability is one of the Seven Principles of Public Life and, on any analysis, it will inevitably feature as a key element for ensuring clarity about how any AI application is being used. For over 10 years, CIPL has been the leading advocate of incorporating the Accountability Principle as a central component of any regulatory framework for data protection. It has now been incorporated into GDPR and into other data protection laws around the world, although its full implications have yet to be fully tested.

  The Accountability Principle requires organisations a) to implement a comprehensive privacy management program, that operationalises legal requirements into measurable rules and controls, b) be able to verify and continuously improve on implementation of such program and c) be able to demonstrate to regulator, oversight body, or individuals or general public the effectiveness of the program.

  The Committee may find it helpful to draw upon two papers on the subject which CIPL published in July 2018:

  - The Case for Accountability:[8] How it Enables Effective Data Protection and Trust in the Digital Society

[8] "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society," 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

- Incentivising Accountability:[9] How Data Protection Authorities and Law Makers Can Encourage Accountability

The two papers are summarised in a short introductory paper.[10] In the papers, CIPL strongly advocates that both private sector and public sector organisations should be required to implement and demonstrate accountability. The following diagram was used to show the essential elements of accountability which organisations must implement and continuously deliver and improve:

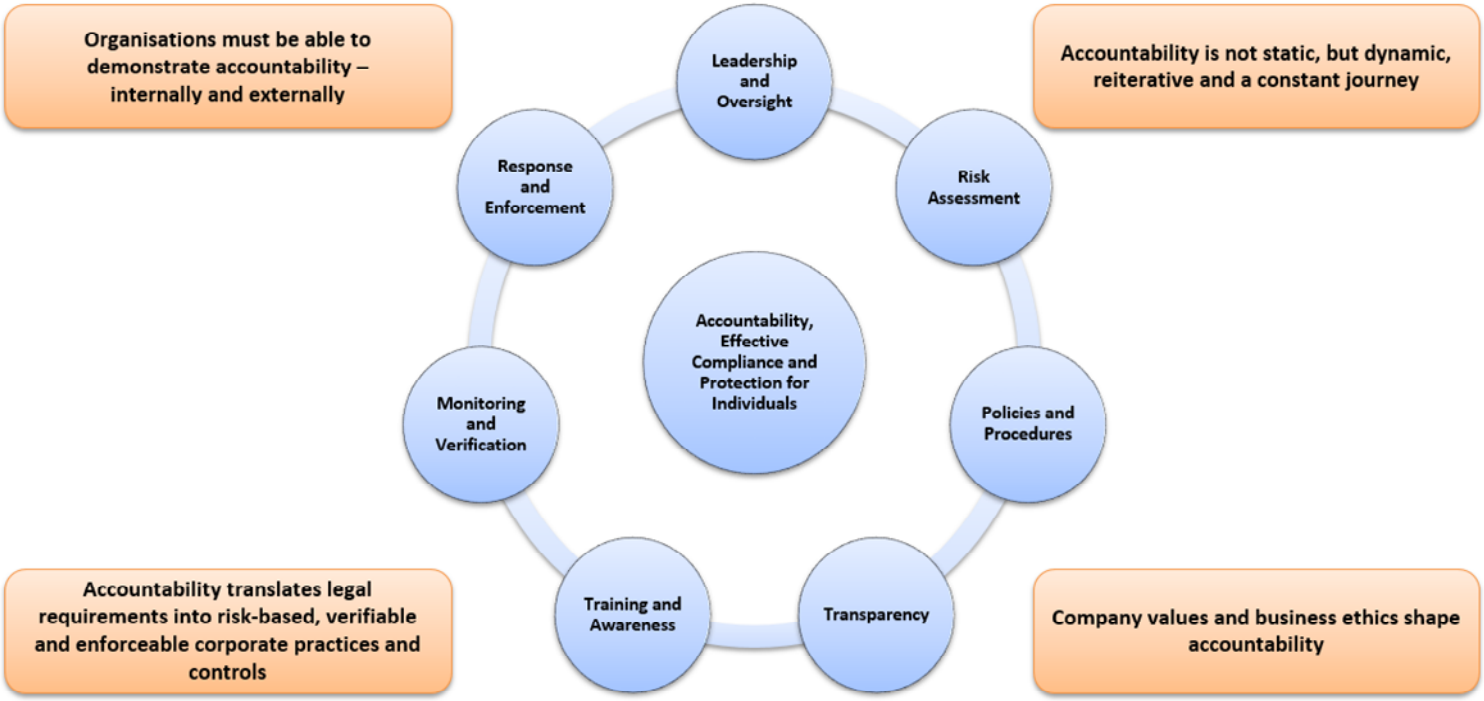

Figure I: CIPL Accountability Framework

- Governance, Leadership and Oversight – It is now widely recognised that data protection is a cultural challenge which cuts across many fragmented parts of an organisation. Good governance is essential to "get it right" so that leadership and oversight is needed at – or very near to – the top. The same must be true for acceptable use of Artificial Intelligence. Problems are inevitable if those at the top of public bodies do not have a good idea of which

[9] "Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_2_-_incentivising_accountability_-_how_data_protection_authorities_and_law_makers_can_encourage_accountability.pdf.

[10] Introduction to CIPL papers on the Central Role of Organizational Accountability in Data Protection", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/introduction_to_two_new_cipl_papers_on_the_central_role_of_organisational_accountability_in_data_protection.pdf.

AI techniques are being used, what they are doing and how they are being governed and monitored.

For many central UK public bodies, the Accounting Officer may need to certify annually that effective controls are in place to ensure that the AI Principles are being met. Similar controls may be needed for other bodies, such as NHS Trusts, police forces and local authorities.

There may also be a need for external oversight. In the absence of a statutory regulator, there may be a role for the National Audit Office and other audit mechanisms.

- A risk-based approach – Since 2014, CIPL has argued the case for building into data protection laws an approach that puts particular emphasis on situations where the risks are most likely or most serious. GDPR contains provisions which reflect this thinking, with particular reference to "risky" types of processing. CIPL's most recent paper on the subject - Risk, High Risk, Risk Assessments and Data Protection Impact Assessments[11] – unpacks the topic in more detail.

  Any risk-based approach needs clarity about the threats and harms which could materialise and which need to be mitigated. The CIPL paper suggests how organisations should assess the likelihood and severity of any harms that might result from risky processing. The Committee may find it especially helpful to look at CIPL's thinking (at page 26) on the different types of harm. It is likely that similar harms will be identified as arising from unacceptable AI. The harms we classified were:

  a) Material, tangible, physical or economic harm to individuals, such as:

  - bodily harm;
  - loss of liberty or freedom of movement;
  - damage to earning power and financial loss; and
  - other significant damage to economic interests, for example arising from identity theft.

  b) Non-material, intangible distress to individuals, such as:

  - detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;
  - chilling effect on freedom of speech, association, etc.;
  - reputational harm;
  - personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
  - unacceptable intrusion into private life;
  - unlawful discrimination or stigmatisation;
  - loss of autonomy;
  - inappropriate curtailing of personal choice;

[11] "Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR", 21 December 2016, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf.

- identity theft; and
- deprivation of control over personal data.

c) Societal harm – affecting Society in ways which go above and beyond individual harms, for example:

- damage to democratic institution;
- excessive state or police power; and
- loss of social trust ("who knows what about whom?").

- Impact Assessments – Whether or not a full risk-based approach is adopted, the Committee may wish to explore the benefits of Privacy and Data Protection Impact Assessments. These have been developed by various Data Protection Authorities (with the ICO playing a leading role) to encourage, and in some cases require, organisations to identify and document exactly how proposed data processing will impact individuals' lives. The GDPR now requires the use of DPIAs in certain risky situations. CIPL finds that some of the leading private sector organisations have started leveraging successfully the DPIA methodology to conduct a wider human rights impact assessment or even an AI impact assessment.

  The Committee could, for example, outline how the Impact Assessment concept could be modified and then used by public authorities before they use Artificial Intelligence in defined circumstances.

- Accountable AI practices – As a second stage of its Accountable AI Project, CIPL has embarked on finding emerging best practices that private sector organisations have started to build and deploy when developing AI technologies and applications. We have started to map some of those against CIPL's accountability framework to show that the same architecture of accountability may prove useful for those specific, additional AI controls and tools.

  We include the work so far on mapping of these nascent best practices, in case it proves useful to the Committee when coming up with examples of possible best practices in the public sector, too.

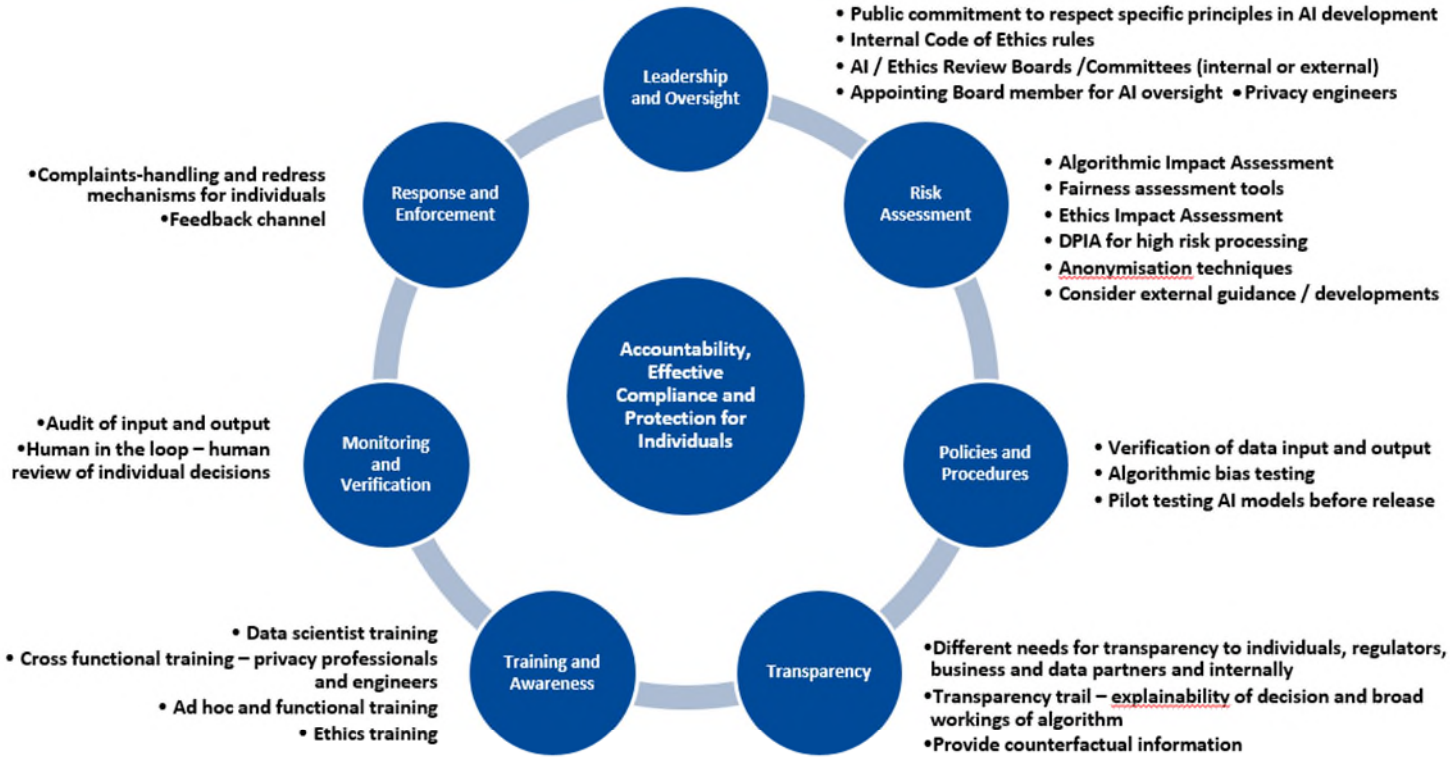

Figure II: AI Best Practices Mapped to CIPL's Accountability Framework

The Standards Challenges

CIPL is grateful to the Committee for sight of its paper which provisionally identifies six challenges which AI poses for public sector bodies.

These six challenges are broadly consistent with issues which have been discussed at length in various contexts by CIPL. The challenges need to be elaborated, but we are confident they will provide a solid foundation for a way forward.

We do, however, wish to make at this stage four comments on the paper:

- Context – The Committee may need to say more about features of public services which makes it especially important to establish a control framework to govern AI use. These include the monopolistic nature of many such services with no competitors and little need to safeguard reputation, the widespread use mandatory powers to collect and use information and the far-reaching nature of many public sector decisions which affect freedoms, rights and autonomies.
- Challenge 2 – The need to avoid bias goes further than demographic bias. Bias and discriminatory inferences can also arise from many other data sources – e.g. financial, health and consumption data and information about political and other opinions and behaviours.
- Challenge 5 – The risks of abuse are not limited to malicious acts. They can also come from ignorant, incompetent and sloppy administration on the part of officials and from inadequate resourcing.

- Extra Challenge – The paper is silent on the risks to democratic norms. Where AI means that decisions are made without adequate understanding about their rationale or where responsibility lies, there could be real threats to the principle of informed choice which must lie at the heart of the democratic process.

Principles of Good Decision-Making

As the Committee has made clear, AI will fundamentally change the way public bodies operate and deliver services. The impact on individual citizens from decisions which are made or assisted by AI use will be of particular concern. Although there will undoubtedly be many benefits, there will also be scope for unjustified or unfair processes and outcomes which could have dire effects.

The quality of decision-making by public bodies as it affects individuals tends to be a topic which is only debated when individual scandals surface. There is little systemic review. There is, however, disturbing evidence of existing failures to achieve "Right First Time", not least in the very high success rates of those who appeal to tribunals or other review mechanisms on such matters as social security, immigration and school exclusions. It is to be hoped that AI will improve this situation with greater "accuracy". But there are also risks that increasing reliance on AI may eliminate or marginalise human discretions, judgements and flexibilities. There are already frequent calls for more user-friendly and more humane public bureaucracies. It would be unfortunate if the quest for rationality reduced the human input further still.

Although adopted nearly 10 years ago before AI was on the agenda, CIPL draws the Committee's attention to the seven Principles which the Administrative Justice and Tribunal Council put forward for decision-making public bodies:

- Make users and their needs central, treating them with fairness and respect at all times;
- Enable people to challenge decisions and seek redress using procedures that are independent, open and appropriate for the matter involved;
- Keep people fully informed and empower them to resolve their problems as quickly and comprehensively as possible;
- Lead to well-reasoned, lawful and timely outcomes;
- Be coherent and consistent;
- Work proportionately and efficiently;
- Adopt the highest standards of behaviour, seek to learn from experience and continuously improve.

These Principles, which are elaborated in AJTC's 2010 report, drew upon the experience of the Parliamentary & Health Services Ombudsman in addressing maladministration by public bodies.

The Principles may need to be revived and made to resonate even more strongly as Artificial Intelligence is more and more used by public bodies which every day are making tens of thousands of decisions of real importance to citizens and their families.