Information Accountability Foundation

18 November 2021

The following comments are pursuant to the Department for Digital, Culture, Media, and Sport ("DCMS") consultation entitled "Data: A new direction."

Who We Are and the Scope of Our Comments[1]

The Information Accountability Foundation (IAF) is the preeminent global information policy think tank, creating collaborative scholarship and education on the policies and processes necessary to use data responsibly in an observational age, while enabling a trusted digital ecosystem that serves people. The IAF is the incorporation of the Global Accountability Dialog, the multi-stakeholder project that developed the "Essential Elements of Accountability." The IAF believes:

- It's critical that organizations are able to think with data and engage in knowledge creation in order to enable and achieve the benefits of a global digital ecosystem.
- To be trusted, organizations must be accountable, responsible, and answerable, and be prepared to demonstrate their accountability.
- Frameworks based on risk assessment and effective data governance enable beneficial, data-driven innovation while protecting individuals and society from the potential harms that may arise from data processing in the digital age.

Since 2014, the IAF has focused on public policy models and the governance of innovative uses of data pertaining to people in advanced analytics and artificial intelligence (AI). Based on its expertise, the IAF's comments will address questions in Chapters 1 and 2 of the Consultation.

[1] These comments were prepared by IAF staff and do not necessarily reflect the views of the IAF Board of Directors, funders, or members of the IAF extended community.

Initial Comments

The IAF welcomes the DCMS Consultation. The current pattern of data protection law development in the UK and elsewhere, and the application of these laws, has led to confusion about when advanced analytics for knowledge creation may be used where there is no distinct legal basis for processing personal data for this purpose. Increasingly this sort of data processing leads to the creation of new insights key to digital innovation. This void has led organizations to delay or forgo the creation of these insights which is inconsistent with the UK Government's goal of unleashing the power of data. Regulators and policymakers often have taken a very strict view of data protection, in part, because some overly aggressive applications involving personal data have left them with a sense that every processing that touches data pertaining to people is equally worthy of the same restrictive controls. However, not every processing of data pertaining to people is an assault on individual sovereignty and human dignity. In addition, the absence of processing because it might not be clear if it is permissible may lead to the people beneficial aspects of this data use not being realized or to an infringement of human dignity. The failure to create insights, even with all appropriate safeguards in place, is a source of reticence risk that can be mitigated with better policy design. Overly aggressive behaviors can be mitigated so that pathways to innovation that serve people can be created. In the end, effective controls so innovation can take place is what is at issue in the Consultation. While a clarification of requirements and even the reduction of some requirements or the way they have been applied is certainly welcome, to achieve trusted data innovation and meet the goals of unleashing the power of data, more mature accountability program investments than would be expected in a compliance focused privacy management program are required. Care needs to be taken to both reduce the compliance burden on organizations and to advance the type of accountability mechanisms necessary to achieve a trusted digital environment. **Comments on Chapter 1 – Reducing Barriers to Responsible Innovation**

There is dissonance between the ability for digital ecosystems to generate new insights that have the potential to lead to new knowledge and the subsets of privacy related to individual autonomy and sovereignty. This dissonance has acted as a brake on digitally driven innovation. As data use through advanced analytics creates even more opportunity, this dissonance has the potential to have an even greater negative impact.

This constraint does not relate just to scientific research. It also relates to the creation of knowledge through analytical processes by the private sector for purposes related to health, transportation, product development, product improvement, better understanding of customers, acquisition of potential new customers, and any data driven applications where data is used to suggest correlations that might be explored for their validity. To remedy this dissonance, it is important to understand two constructs.

- Advanced analytics, especially, artificial intelligence (AI) consists of two processes: knowledge creation and knowledge application. Knowledge creation is the generation of insights about people that originates with data that pertains to people in general and not a specific individual or set of individuals. Knowledge application is the utilization of knowledge created on a specific or identifiable set of individuals. The process of "knowledge creation" has been called "thinking with data," and the process of "knowledge application" has been called "acting with data."

- Knowledge creation is conducted for two difference research purposes: (1) scientific, and (2) commercial.

Understanding the difference between knowledge creation and knowledge application and the purposes for which they are being undertaken is critical to understanding how they should be regulated.

Both knowledge creation and knowledge application make use of data pertaining to people. Knowledge creation in and of itself is significantly less impactful on individuals. Knowledge application can lead to decisions and actions that impact individuals and brings more into consideration traditional privacy concerns. Knowledge creation does not have the same concerns and results. As such, knowledge creation and knowledge application should not be treated the same way. Therefore, regulatory approaches, including the regulation, oversight, and enforcement, should treat these two processes differently. Both processes require controls, but since the risks are not the same in knowledge creation and knowledge application, the controls should not be the same.

Like knowledge creation for scientific purposes, knowledge creation for commercial purposes requires its own set of controls. To begin, an organization must: have a legitimate objective to conduct knowledge creation, conduct and document a risk assessment, and establish an internal oversight mechanism. Additional transparency obligations should be applied. For example, they could include:

- The types of knowledge creation data activities the organization engages in, how data are used to achieve each knowledge creation purpose and the types of third parties to which personal data may be transferred (or received) in order to achieve each purpose,
- Descriptions of the governance processes employed (e.g., policies and procedures) regarding knowledge creation data activities;
- A description of the assessment process the organization uses

Data Subject Rights (DSR) may apply differently in knowledge creation and knowledge application. For example, there should be a limited ability to object to data processing that is part of knowledge creation.

Treating knowledge creation and knowledge application the same has the unintended consequence of overburdening the organizations that are the engines for digital innovation (e.g., innovators in medical devices, transportation, education, design, and services.) There is a great deal of concern about surveillance market players, but they are not the only knowledge creation innovators.

The IAF has advocated for many years that there should be a distinction between knowledge creation (thinking with knowledge) and knowledge application (acting with knowledge). This key concept was expressed in the Unified Ethical Frame for Big Data Analysis and was continued in the IAF's assessment projects in Asia, the Americas and Europe.

While some examples of controls and impacts to DSR have been mentioned, the IAF thinks a multi-stakeholder dialogue, similar to the original Global Accountability Dialog, is necessary to build out the set of controls and DSR impacts that an organization must have in place to support the creation of a new legal basis for the conduct of knowledge creation for commercial purposes.

Defining Knowledge Creation and Scientific Research

The Consultation asks whether scientific research should be defined in the statutory language. The IAF believes that it should. The IAF also believes the statutory language should include and define knowledge creation. There has been a ten-year Unified Ethical Frame for Big Data Analysis debate on how broadly the term research should be. This topic was explicitly discussed at the 2013 International Conference of Data Protection and Privacy Commissioners. Some believed that all research endeavors, whether in the private sector or at universities, should be included as research. Others believed that research is conducted at universities, led by faculty, and results published for public review. This discussion was triggered in part by a paper published by the Centre for Information Policy Leadership entitled "Big Data and Analytics: Seeking Foundation for Effective Privacy Guidance."[2] There was no consensus in that session, and there has been no consensus since then. However, it is key to recognize much of the world's data innovation will be created by the private sector. The IAF believes that it is

[2] Martin Abrams, IAF Executive Director was one of the authors. As a member of the "Advisory Committee" for the conference, he organized the referenced session.

imperative to define and reflect these two processes in public policy and to develop and require the appropriate rules for each to achieve trust.

Scientific Research and Knowledge Creation Have Different Impacts on People than the Application of Learning

Data protection law in many jurisdictions treats all processing with data pertaining to people as equally impactful on individuals. That just is not the case. "Big Data and Analytics: Seeking Foundation for Effective Privacy Guidance" first suggested that knowledge creation was different from knowledge application.[3] The processing conducted for the purpose of discovering new knowledge does not have a direct impact on any individual absent of a failure in security safeguards. It is only when the insights from knowledge creation are applied to make a decision about, or take an action on, an individual or individuals does the processing become impactful.

Policy discussions that have taken place in Europe, Asia and North America have referred to these processes as "thinking with data" and "acting with data." The process to apply data science that might create insights into correlations related to credit and housing (thinking with data) is different from the process to make a decision to grant credit or provide housing (acting with data). There should be controls for both, but they are different controls. The controls for acting with data, or knowledge application, have been well developed in the UK GDPR. The specific controls for knowledge creation, such as appropriate, non-discriminatory objectives and security safeguards, still need to be developed. The general parameters for

controls could be part of a revised UK GDPR with the requirement that detailed controls come from a multi-stakeholder process. Such controls also could be part of a code of conduct for knowledge creation.

Specific Recognition in the Law

The IAF believes a revised UK GDPR should have specific legal bases in Article 6 for both scientific research and knowledge creation. As in other legal bases, there should be specific controls so that processing for these two purposes is trustworthy. The IAF does not believe these processes should be covered by either legitimate interests or for public purposes. These comments will discuss legitimate interests below.

[3] The paper referred to "Knowledge Creation" and "Knowledge Application." Discussions in Canada and Hong Kong have used the terms "Thinking with Data" and "Acting with Data."

Further Processing

With appropriate controls, both scientific research and knowledge creation are not impactful on people until further action is taken with the knowledge and the insights that flow from the research. The benefits from new knowledge developed for non-nefarious purposes are not calculatable always immediately, but they always have been the life blood of progress. The completeness of data sets for research directly impacts the accuracy of results. The IAF believes strongly that both scientific research and knowledge creation clearly should be compatible with further use. This view is consistent with a risk-based system.

The Consultation says the UK government proposes to clarify in the legislation that data subjects may give their consent for broader areas of scientific research when it is not possible to fully identify the purpose at collection. While the IAF does not believe consent is the appropriate legal basis for scientific research or knowledge creation, as discussed above, providing such a broad consent option may be useful in the context of a research application where there is a clear desire to use the data for further research.

Further use raises the issue of transparency. If transparency's main purpose is informing data subjects of their rights, and research is complex, the transparency never can be adequate. If the purposes are to prevent secret processing or to empower oversight, society has the capability for building new, and more effective, transparency instruments, but they still will be too complex for individuals. The question should address the impactfulness of the research itself on individuals. The IAF does not believe that research, knowledge creation, is a violation of an individual's sovereignty.

Legitimate interests

A stated intent of both the EU and UK GDPR was to not force consent as the legal basis for processing where it did not fit. Many expected that legitimate interests would replace consent in those instances where processing is legitimate and serves the needs of stakeholders including the data subject, other individuals, society as a whole, as well as the business doing the processing. Legitimate interests required organizations to balance their legitimate interests against the full range of rights and freedoms of the data subject. Nowhere in that equation were the interests of other stakeholders impacted by the processing considered. When many of the places where legitimate interests would have been justified based on these other stakeholders, ranging from smart cars to smart medical devices, this legal basis did not fit because the balancing was bilateral and not multilateral.

Furthermore, legitimate interests require the individual to have the ability to exercise the right to object, and the individual must be fully informed before exercising the right to object. The

ICO has raised this transparency issue in its enforcement action against Experian and its work on adtech. The ICO has expressed the view that data science is too hard to understand and therefore that the right to object to data science is too hard to exercise. The ICO's view is too extreme; it is going too far to say that all data science is too hard to understand. Restricting legitimate interests when processing is hard to understand impacts almost all data science. Rather, the IAF has suggested the solution is that there should be consumer facing privacy notices that are very approachable, combined with complete notices that are intended to facilitate oversight. Those complete notices should be available to individuals, but individuals are not the target audience.

The IAF therefore argues that legitimate interests are not encumbered just by a flawed balancing test, but also that it is flawed because the right to object has become another form of consent. The DCMS suggested a limited set of legitimate interests for which assessments would not be necessary. The IAF believes that assessments are useful, but that they need to be the right type of assessments.

Instead, the IAF has suggested a more multilateral legitimate interests balancing instrument in its 2017 paper "Legitimate Interests and integrated Risk and Benefits Assessment." There was regulatory participation in the project that led to publication of that paper, but the balanced assessment process was not part of the subsequent regulatory guidance.

Neither pre-approved legitimate purposes nor a more balanced assessment solves the problem of the right to object and how it might be informed. The IAF also has suggested projects to enrich transparency beyond notices. This issue of transparency linked to the right to object will be a problem until either the right to object and transparency are unlinked or other forms of transparency are accepted.

Fairly processed, fair and fairness

The DCMS consultation has raised the issue of the terms "fairly processed," "fair" and "fairness" in the context of AI. The IAF believes fair should be looked at from a broader context than just AI.

Under modern data protection in an observational age that fuels advanced analytics, where the law and application are supposed to be risk-based, these three terms are applicable to almost all processing of data pertaining to people. Risk means asking the question what negative outcomes, if any, warrant attention by both organizations and regulators, and where attention by regulators is warranted, which regulators are implicated.

In paragraph 67 of the Consultation, the DCMS references the distinction the UK GDPR makes between data used for research purposes and non-research purposes. Earlier in these comments, the IAF referenced the differences between knowledge creation and knowledge application. This is the point raised in paragraph 67. The distinction is made because research is not directly impactful on a person while the application of research purposes are. This distinction goes directly to the difference between fair outcomes and fair processes.

Fair processing requires that data be collected and processed in a lawful manner, be adequate for the purposes, be subject to appropriate controls, and be processed in a transparent manner. Data protection agencies are the parties to oversee and enforce whether data used for any complex processing is processed fairly. Part of processed fairly is that organizations understand the risks they create for others and put in place processes to address those risks. Therefore, data protection agencies should have the authority to determine whether companies understand the risks and are addressing them, e.g., are conducting risk assessments to determine if there are outcomes that are unfair and if they are, mitigating them. However, as suggested in the Consultation, there are other regulators who are better equipped to make judgements on whether outcomes are fair.

Fair outcomes are based on societal norms and associated laws and regulations. For example, discrimination based on race in housing and lending are prohibited by law. Advanced analytics that contribute to prohibited discrimination would be a violation of fair housing and lending laws. It is the job of the organization to have assessment processes that identify the risk to people being subject to discrimination because of discriminatory processes. The ICO should have the power to enforce against inadequate processes that do not effectively assess fairness. The violation of the housing and lending laws is enforced by other agencies, not the ICO. This is the distinction. Of course, the ICO should retain the ability to enforce aspects of the UK GDPR that tie to fairness of, for example, the application of DSRs.

This distinction only will become more important. AI will lead to winners and losers in a modern economy. For example, autonomous trucks may make for safer highways, but they also will lead to a need for fewer drivers. Data protection authorities do not decide on the balance between safer highways and truck driver employment. The IAF believes that the ICO and other data protection authorities should have the power to oversee required processes by organizations to identify the risk of unfair outcomes, and other regulators should make appropriate decisions on whether knowledge application creates prohibited outcomes as determined by laws and societal norms.

These sections have responded to questions:

- Q1.2.1. Consolidating and bringing together research-specific provisions will allow researchers to navigate relevant law more easily. strongly agree
- Q1.2.2. Creating a statutory definition of 'scientific research' would result in greater certainty for researchers. Strongly agree but suggest a definition for knowledge creation
- Q1.2.3. Is the definition of scientific research currently provided by recital 159 of the UK GDPR a suitable basis for a statutory definition? no
- Q1.2.4, Identifying a lawful ground for personal data processing for research processes creates barriers for researchers. Strongly agree
- Q1.2.5. Clarifying that university research projects can rely on tasks in the public interest as a lawful ground would support researchers to select the best lawful ground for processing personal data. neither agree nor disagree

- Q1.2.6. Creating a new, separate lawful ground for research (subject to suitable safeguards) would support researchers to select the best lawful ground for processing personal data. strongly agree; however, there should also be a lawful basis for knowledge creation
- Q1.2.8 It would benefit researchers to clarify that data subjects should be allowed to give their consent to broader areas of scientific research when it is not possible to fully identify the purposes of the personal data processing at the time of collection. Consent should not be legal basis for research, however in some situations broader consent may be useful so we agreeQ1.2.9. Researchers would benefit from clarity that further processing for research purposes is both (i) compatible with the original purpose and (ii) lawful under article 6(1) of the UK GDPR. Strongly agree
- Q1.4.1. Do you agree with the proposal to create a limited, exhaustive list of legitimate interests for which organisations can use personal data without applying the balancing test? Neither agree nor disagree
- Q1.4.2. Do you agree with the suggested list of activities where the legitimate interests balancing test would not be required? Neither agree nor disagree
- Q1.4.3. What, if any, additional safeguards do you think would need to be put in place? See discussion in legitimate interests section
- Q1.4.4. Do you agree that the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities? Neither agree nor disagree
- Q1.5.1. Do you agree that the current legal obligations with regards to fairness are clear when developing or deploying an AI system? Strongly disagree
- Q1.5.2. Do you agree that the application of the concept of fairness within the data protection regime in relation to AI systems is currently unclear? Strongly agree

- Q1.5.3. What legislative regimes and associated regulators should play a role in substantive assessments of fairness, especially of outcomes, in the AI context? This question does not lie within the IAF competencies.
- Q1.5.4. Do you agree that the development of a substantive concept of outcome fairness in the data protection regime – that is independent of or supplementary to the operation of other legislation regulating areas within the ambit of fairness – poses risks. Strongly agree

Comments on Chapter 2 – Reducing burdens on businesses and delivering better outcomes for people

History of the Accountability Principle

21st century interpretations of the data protection accountability principle were kick-started by the multi-stakeholder "Global Accountability Dialog" in 2009. The working paper for that project, "Data Protection Accountability: The Essential Elements A Document for Discussion," laid out five essential elements:

1. Organisation commitment to accountability and adoption of internal policies consistent with external criteria.
2. Mechanisms to put privacy policies in place, including tools, training, and education.
3. Systems for internal ongoing oversight and assurance reviews and external verification.
4. Transparency and mechanisms for external participation.
5. Means for remediation and external enforcement.

The essential elements set the basis for establishing that accountability required organisations to be responsible and answerable. These became the basis for how privacy management programmes began to be thought about. This concept of responsible and answerable is the foundation for regulator guidance in Canada, Hong Kong, Colombia and Australia and numerous new laws that require accountability. Unfortunately, the EU GDPR places greater emphasis on answerable, leading to the 'box-ticking' exercise the Consultation discusses, even though many of the actual requirements in the GDPR, such as data protection impact assessments, are the tools described in essential element 2.

Privacy Management Programmes

The Consultation suggests DCMS would like to establish a regulatory structure that is more risk based and is about encouraging innovation by organisations that act in a responsible fashion. It goes on to suggest these goals could be accomplished by requiring organisations to have

comprehensive privacy management programmes and references the 2012 Canadian guidance "Getting Accountability Right with a Privacy Management Programme." While guidance and not a legal requirement, the Canadian regulators have made it clear that part of enforcement reviews will be an examination of an organisation's comprehensive programme, including privacy impact assessments (PIAs).

The IAF's experience is that the PIA process is more mature in Canada than in most other jurisdictions. The IAF has conducted multi-stakeholder projects in Canada to develop enhancements in assessments in order to address the issues that arise with advanced analytics and AI. One of the learnings of these projects is that Canadian companies can better adapt to those requirements because of the maturity of the privacy programmes that have resulted as a result of the 2012 guidance.

The Consultation references the flexibility in Singapore that has come with recent amendments to that country's data protection law. Before Singapore amended its law, it heavily encouraged business to move up an accountability maturity model that required assessments. For a business to take advantage of the flexibility, it first must be fairly high on the maturity model. To be high on the maturity model. organisations must have an accountable individual with the skill sets required of a data protection officer.

The IAF discussion in Chapter 1 on innovation and the law makes it clear that flexibility requires effective controls. The effective controls are exercised best when organisations have comprehensive programmes. So, rather than a comprehensive program being a replacement for effective controls, it is the locus for such controls. While privacy management programmes emphasize responsible use of data to be trustworthy, answerable still must be included in them.

The IAF suggests that a revised UK GDPR place greater emphasis on comprehensive accountability programs. The revised UK GDPR still should include many of the assurance requirements that exist in the current law, but they instead should be linked to the requirement to be responsible and to be demonstrable. Those elements, which are contained in Section 156 of the Consultation, need to be linked to the controls necessary for trust in innovative data use.

While core elements of accountability are required to be able to demonstrate compliance, trusted digital innovation requires enhanced accountability. For example, an assessment of "fairness" in advanced analytics requires a different sort of governance relative to the data used to address all stakeholder interests and to appropriately mitigate all risks. This approach was best illustrated in IAF work with the Hong Kong Privacy Commissioner on an Ethical Accountability Framework. The IAF's work on many of the projects highlighted in this response, whether it is to address ethical data use or AI, have suggested that Data Stewardship Accountability is required. The challenge is that while it may be desirable to clarify

accountability elements for a compliance-based privacy management programme, the Government will need to find ways to promote the adoption of enhanced accountability if it is to achieve the goal of trusted data innovation.

Prior Consultation with the ICO

The Consultation raises the question of whether prior consultation with the ICO should be required for processing that is characterized as high risk and suggests that such a requirement should be removed from a revised law. The IAF has been concerned that prior consultations are not scalable if organisations are pursuing innovative data uses and bringing all those processing's to the regulator for approval. At the same time, the IAF has found that stakeholders do not trust organizations to conduct assessments in a manner where a thumb is not placed on the scale in the organization's own favor. There is a conundrum between oversight scalability and devices to ascertain honesty.

Internationally, there has been a great deal of discussion about ethical review boards, both internal within organisations and externally at a third-party provider of those services, as it relates to advanced processing that raises tangible risks to individuals. To be trusted, such review boards would have to be independent from those promoting the processing. So, if there is an ethical review committee within an organisation, there need to be provisions that require the committee to be independent of the persons promoting the potentially risky data use and to have both the diversity in representation and the skills necessary to ascertain that the decisions reached are respectful of all stakeholders impacted by the processing. Additionally, such committees should have some basis in law or regulation.

These sections have responded to the following questions:

- Q2.2.1. 'The accountability framework as set out in current legislation should i) feature fewer prescriptive requirements, ii) be more flexible, and iii) be more risk-based? Neither agree nor disagree.
- Q2.2.2. 'Organisations will benefit from being required to develop and implement risk-based privacy management programmes.? Strongly agree.
- Q2.2.3. 'Individuals will benefit from organisations being required to implement a risk-based privacy management programme? Strongly agree.
- Q2.2.4. 'Under the current legislation, organisations are able to appoint a suitably independent data protection officer?' Neither agree nor disagree.
- Q2.2.5. Do you agree with the proposal to remove the existing requirement to designate a data protection officer? Neither agree nor disagree.

- Q2.2.7. 'Under the current legislation, data protection impact assessments requirements are helpful in the identification and minimisation of data protection risks to projects? Strongly agree
- Q2.2.8. Do you agree with the proposal to remove the requirement for organisations to undertake data protection impact assessments? Strongly disagree

Conclusion

The IAF has chosen to comment only on Chapters 1 and 2 of the Consultation. Data pertaining to people used responsibly will drive innovation that will be beneficial for people. There also may be innovations that may be less responsible and, in some cases, harmful to individuals, groups and society as a whole. Regulation is intended to bring friction to the system to maximize the benefits and reduce the potential for harm.

The current version of the UK GDPR has produced friction points that have inhibited beneficial data uses for innovation by creating roadblocks that over emphasize some perceived harms. For that reason, the IAF supports some improvements in the UK GDPR to encourage beneficial and responsible data driven innovation. These improvements are not intended to eliminate friction but rather to better channel that friction. For example, the IAF strongly supports enhanced impact assessments so the interests of all stakeholders are considered by organisations when using data in an innovative manner.

While only commenting on the first two Chapters, IAF has concerns about unintended frictions in other Chapters that will not be productive. The UK ICO is a very important and respected agency within the international data protection community. It's global positioning is beneficial to the responsible application of global data protection regulations and by extension commerce. The government should be careful to assure that the ICO remains independent within a legal framework that defines overarching goals for the agency but does not make the ICO subject to the political goals, real or perceived, of a particular government. Such a structure could impact the UK's global stature and impede the free movement of data that would be harmful to UK economic growth and innovation goals.

These comments were prepared by the IAF staff and do not necessarily reflect the views of the IAF board of trustees, contributors, or broader community. If there are any questions, they should be directed to Martin Abrams at mabrams@informationaccountability.org or +1.972.955.5654.