Written evidence submitted by Dr C N M Pounder, Amberhawk Training Limited (DPDIB03)

ISSUES ASSOCIATED WITH THE DPDI No 2 BILL

This brief four page commentary guides the Committee in its exploration of the Data Protection and Digital Information No. 2 Bill ("No. 2 Bill") in seven areas.

The author has been a data protection practitioner from when the Data Protection Act 1984 commenced; he has also appeared before Parliamentary Committees to give oral evidence on privacy matters. Amberhawk Training Limited has existed for over a decade and trains data protection officers or those who have detailed data protection responsibilities.

A comprehensive CV for the author is available on https://amberhawk.com/wp-content/uploads/2022/11/CV-Chris-Pounder.pdf).

1. The absence of Keeling Schedules

It is difficult to comment on legislation that modifies existing legislation if no Keeling schedule is available.

Ministers have had over a year from the publication of the No.1 Bill to organise the preparation of Keeling Schedules for the No.2 Bill and UK_GDPR but have failed to do so. I cannot see how the Committee can efficiently perform its functions without them as the Committee will become increasingly reliant on Ministerial comments which are then difficult to scrutinise properly.

The Committee should make a statement regretting the absence of a Keeling Schedules for the interaction between the No.2 Bill and the DPA2018 or UK_GDPR.

2. Human Rights position

Although the Information Commissioner (ICO) is not antagonistic towards the DPDI No 2 Bill, this is not the case with respect to the proposed changes to the human rights regime in the UK. The No.2 Bill is integrally linked to the proposed Bill of Rights(BoR) through the expected changes to Articles 8 and 10 of the Human Rights Act 1998.

If anything is going to impact on the European Commission's Adequacy Decision it is the BoR legislation; the Adequacy Decision itself mentions "human rights" over 80 times and compliance with Strasbourg jurisprudence is expected by the Agreement.

There has been no consideration of the BoR and No.2 Bill interaction, yet the ICO is on the record as stating:

- *"Changes in how the concepts of necessity and the public interest are assessed in human rights law will inevitably have an knock on effect on their assessment in data protection law".*

- *"The concept of necessity is fundamental across the DPA/UK_GDPR (Article 5 principles, Article 6 lawful bases, Article 9 conditions for processing special category data, Article 23 exemptions, and Schedule 1)".*
- *"…likely impact could make it more difficult for the ICO to protect individuals data"* (e.g. *"if public authorities are be able to rely on public interest grounds in a presumptive way": (para 3.27).*

Further detail can be found in my blogs: " ***UK Bill of Rights set to undermine UK_GDPR and Adequacy***"; https://amberhawk.typepad.com/amberhawk/2022/07/uk-bill-of-rights-set-to-undermine-uk_gdpr-and-adequacy.html and "***DPDI No 2 Bill should be paused until the UK Bill of Rights position is resolved"***: https://amberhawk.typepad.com/amberhawk/2023/03/dpdi-no-2-bill-should-be-paused-until-the-uk-bill-of-rights-position-is-resolved.html.

3. The cost savings associated with the DPDI No.2 Bill

The Government's figures, if analysed properly, show the savings associated with this Bill are insignificant. For instance, as there are 67.1 million data subjects in the UK so the cost of maintaining current UK_GDPR standards is calculated as *£7.00 per year* per data subject. This equates to 13.5 pence per data subject per week, or just under *2p per day*.

As there are 1.07 million controllers, the average saving for each controller can be calculated at £439 per year per controller. This is **about £8.40 per week per controller**; about the price of a bottle of plonk.

A full financial analysis can be found on "***New DPDI Bill savings inflated by 324%" (from the No. 1 Bill***). The loss of Adequacy Agreement would cost UK over £2 billion (per decade). Further detail on: https://amberhawk.typepad.com/amberhawk/2023/03/new-dpdi-bill-savings-inflated-by-324-loss-of-adequacy-costs-uk-over-2-billion.html

4. Definition of personal data

The definition of personal data in the No. 2 Bill is defective; it certainly does not comply with data protection standards established in 1981 let alone in the definition in the GDPR. This undermines the substantive provisions in the UK_GDPR/ DPA2018 as they are defined in terms of personal data.

The definition's defects are discussed in my two blogs, one of which shows the definition does not fully cover personal data captured by facial recognition cameras (a current privacy hot potato).

See "***DPDI No.2 Bill defines "personal data" below the international standards established in 1981***" https://amberhawk.typepad.com/amberhawk/2023/04/definition-of-personal-data-in-dpdi-no-2-bill-results-in-non-compliance-with-coe-convention-no108.html) and

"***Facial recognition CCTV is excluded by DPDI No2 Bill's definition of personal data***": https://amberhawk.typepad.com/amberhawk/2023/04/facial-recognition-cctv-excluded-from-new-data-protection-law-by-definition-of-personal-data.html).

5. Voluntary data sharing between public bodies

The Digital Economy Act 2017 provides Ministerial powers to set up voluntary data sharing arrangements between public bodies. Yet the terminology used by Ministers infers that such sharing is compulsory or that public bodies are expected to share their personal data in every instance (even though data sharing is voluntary).

The issue that has not been considered is that although the direction of travel is for voluntary data sharing for a public good, this conflicts with circumstances when Parliament has given powers (e.g. to national security, law enforcement and HMRC) to demand personal data.

The overlap between the voluntary and compulsory approach towards data sharing has yet to be explored. For instance, should a voluntary approach for disclosure to a public body be permitted when Parliament has provided explicit statutory powers to that public body so it can demand the same personal data?

Adoption of the voluntary approach to data sharing avoids the statutory safeguards insisted by Parliament. This raises the question of "*What is the point of Parliament providing statutory powers to demand personal data, subject to statutory safeguards, if both statutory requirements and safeguards can be avoided by using a voluntary approach towards data sharing*?".

In other words, voluntary data sharing could bypass the safeguards Parliament has determined.

A public sector body relying on a voluntary approach towards data sharing could inform the recipient of a request that (a) there is no obligation to share personal data or (b) powers given the that public body by Parliament to demand personal data cannot be used (that is why it has asked for voluntary data sharing).

See: "***DPDI Bill removes "public interest" test in push to legitimise general public sector data sharing"***; https://amberhawk.typepad.com/amberhawk/2022/08/dpdi-bill-removes-public-interest-test-in-push-to-legitimise-general-public-sector-data-sharing.html

6. Marketing

The proposed use of the "*legitimate interests*" lawful basis to support marketing activities overturns nearly 40 years of data protection law when applied to third party marketing. Consent for third party marketing has been the norm ever since the early Tribunal decisions under the DPA1984.

Additionally, the Government has not reproduced in the Bill, the safeguards that were associated with consent for third party marketing (e.g. it should be as easy to withdraw consent as to give it). Under the No 2 Bill, there is no requirement for data subjects to change their mind re third party marketing if it falls within "*legitimate interests*".

The result is that the marketing arrangements could be open to considerable abuse unless (a) consent and not legitimate interest is restored as the lawful basis for third party marketing and (b) controllers who rely on legitimate interests for their own marketing provide an easy and simple way for those who did not see the "opt-out" to change their mind.

In summary, the Government have been carefree in its drafting; it risks creating a spammer's paradise.

7. Absence of the Identity Assurance Principles

As background, I refer to the "*Nine Identity Assurance Principles*" that were published in 2015 by Government for inclusion in any future digital identity projects. The Nine Identity Assurance Principles can be found on the Government website at: https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles).

The objective was to avoid a repeat of the ID Card debacle a decade earlier; so the Government asked a number of privacy experts (including the ICO and myself) to debate and draft a set of objectives for a safe ID system. As a result, these Identity Assurance Principles emerged to provide a benchmark for a privacy compliant digital identity scheme.

In summary, consideration of the Identity Assurance Principles will allow the Committee to identify which Principle is not being incorporated and assess the consequences of that lack of consideration.

In the No.2 Bill none of the Identity Assurance Principles have been considered, even though the Secretary of State has to produce something called a "***DVS Trust Framework***". It is difficult to see how a Trust Framework that excludes these Principles, is indeed to be trusted.

Further detail on: https://amberhawk.typepad.com/amberhawk/2023/02/governments-digital-identity-proposals-ignore-obvious-privacy-concerns.html

Dr. C. N. M. Pounder
Director: Amberhawk Training Limited
Website: ***Amberhawk*** - ***www.amberhawk.com***
Blog: ***Hawktalk*** - ***http://amberhawk.typepad.com***
Twitter:***@hawktalk_blog***
27 April 2023