

Domestic Data Protection team
DCMS
100 Parliament Street
London
SW1A 2BQ
Via email: DataReformConsultation@dcms.gov.uk

'Data: a new direction': Response to consultation

Written submission from Dr Marion Oswald, Vice-Chancellor's Senior Fellow in Law, Northumbria University; Associate Fellow, Royal United Services Institute; Chair, West Midlands PCC and West Midlands Police data ethics committee; Member of the CDEI Advisory Board; PI of the AHRC-funded Observatory for Monitoring Data-Driven Approaches to Covid-19 (www.omddac.org)

Introduction

1. This submission sets out my personal views and does not represent the views of Northumbria University, RUSI, West Midlands PCC or West Midlands Police, or CDEI.
2. The submission reflects my experience and research in respect of the use of AI and data analytics in the public sector.

Legal frameworks and statutory gateways

3. While the consultation focuses upon key aspects of the UK GDPR, a number of consultation questions (e.g. Q1.5.19, Q1.5.20) ask whether data protection is the appropriate legal framework to deal with the risks identified.
4. In 2014, the Law Commission reported on its scoping project 'Data Sharing Between Public Bodies' (<https://www.lawcom.gov.uk/project/data-sharing-between-public-bodies/>). It concluded that 'there are problems with the form of the law relating to data sharing that could usefully be addressed. We have also found evidence of problems which are not directly due to the form of the law, but could be alleviated by law reform.' (para 1.3). The Law Commission recommended (inter alia) that 'a full law reform project should be carried out in order to create a principled and clear legal structure for data sharing, which will meet the needs of society...The project should include work to map, modernise, simplify and clarify the statutory provisions that permit and control data sharing and review the common law.' (para 1.6)
5. Since that date, the clarity of the situation has not improved. **Statutory 'gateways'** have become increasingly common (such as ss 35, 40, Digital Economy Act 2017; clause 15 of the Police, Crime, Sentencing and Courts Bill, 'Disclosure of Information') with such provisions tending to disapply any obligations of confidence (such as those applying to medical information) whilst stating that the provision does not authorise any breach of the Data Protection Act.
6. Such a **siloed approach** to relevant legal frameworks contributes to **confusion, uncertainty and differing interpretations** as to whether disclosures through such gateways are fair and therefore legal under data protection law or more generally, and/or whether disclosures other than by an explicit gateway are lawful. The increase in statutory gateways may on the one hand create the impression that explicit gateways are always necessary to share data (thus contributing to excessive caution) and on the other, suggest that data transfers can be 'waved through' because a gateway exists, without sufficient consideration given to other important legal principles contained within

human rights, equalities and administrative law (not mentioned in such gateways), in particular whether acquisition and subsequent use and analysis of the information is both necessary and proportionate. The use of gateways can encourage focus on data disclosure and acquisition without equal attention being paid to **how data is then used, including how the outputs of data analysis are deployed in public sector decision-making**. Subsequent use, including by way of analytics to produce further information (e.g. inferences or conclusions about individuals) often raise significant legal and ethical issues.







7. The National Data Guardian has recently expressed her concern over the above-mentioned clause 15 of the Bill: ‘People need to trust that they can share information in confidence with those responsible for their care without worrying how it will be used, by the police or others...Decisions about data use require not only expert data protection knowledge regarding what’s lawful, but practical and professional wisdom and experience to consider what would be ethical and right, balancing potential benefits against the avoidance of future harms.’

<https://www.gov.uk/government/news/data-driven-innovation-why-confidentiality-and-transparency-must-underpin-the-nations-bright-vision-for-the-future-of-health-and-care>

8. The following **diagram attempts to demonstrate the uncertainty** that may still remain despite the use of statutory gateways (previously submitted to the 2013 Law Commission consultation):

Disclosure Gateways

Addressing Art 8 “except as in accordance with the law”

Discloser/ Acquirer	 Specifically Disclosable	 No specific disclosure gateway*	 Statutory bar on disclosure
 Specific power to acquire	✓	?	?
 No specific power to acquire*	?	?	X
 Acquisition specifically forbidden	X	X	X

* - "No specific...": Prerogative/Common Law/implicit power/Ram Doctrine may apply
 ? – Unsure – see below for possible solution (hierarchy of authorities/bodies)

© M. Oswald, 2013

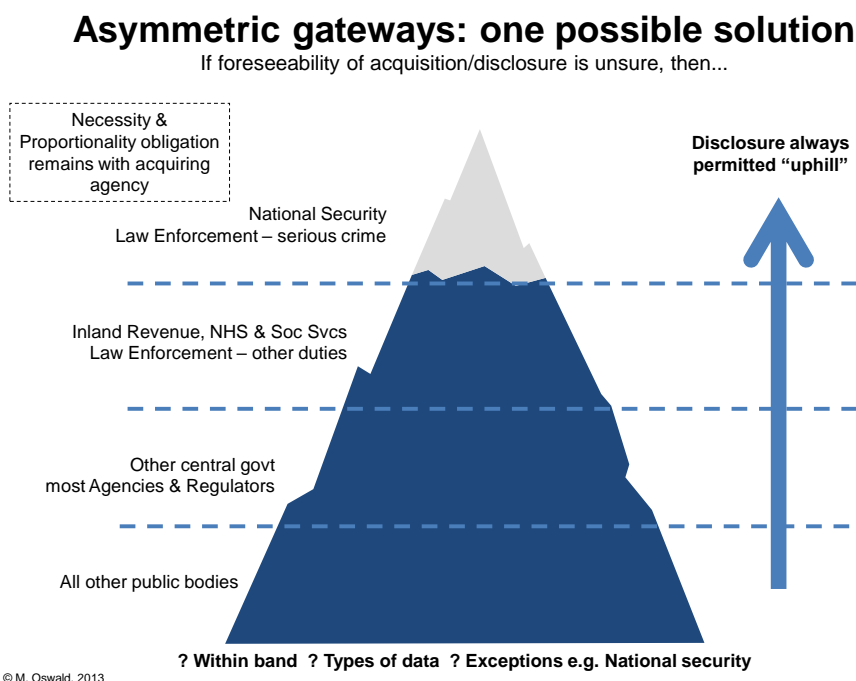
9. Where disclosure is not mandated, a challenge for many public authorities will be to make a judgement on the reasons given by the acquiring authority for its acquisition and use of the data, in order to determine whether or not the disclosing authority has the power to disclose. This may involve an element of **second-guessing** of the acquiring authority’s reasons for its request, a balancing exercise in respect of the potential impact of the disclosure on the holding authority’s own statutory functions and an assessment of the impact of the disclosure and data use on its own reputation.

10. Connected to the above, one OMDDAC stakeholder reflected that ‘it’s not the law that’s been the problem; it’s the **issue of shared responsibilities**...In ninety-nine percent of situations data

protection law allows you to do what you want to do, provided the safeguards are there.’ (<https://www.omddac.org.uk/news/final-report-omddac-lessons-learned/> fn 52) These uncertainties also relate to the questions around further processing and legitimate interests identified in section 1.3 and 1.4 of the consultation.

11. In my view, a ‘new direction’ purely focused on data protection will not be sufficient to appropriately govern new data-driven and algorithm-informed public sector decision-making. It will be important to take a **holistic approach to the key principles** in all relevant legal frameworks (including human rights, administrative law, equalities law, data protection, regulation of intrusive and investigatory powers, law of evidence) ‘in order to create a principled and clear legal structure for data sharing’ as recommended by the Law Commission. This is because personal data disclosure and acquisition is fundamentally connected to subsequent use, analysis and further disclosure of the results of such analysis, and the use of data analysis within the exercise of state power and discretion. The principles of **administrative law** therefore govern (as they have done for many decades) the exercise of such power and discretion, already providing fundamental principles around the duty to give reasons (relevant to automated decision-making), relevant and irrelevant considerations and fettering discretion (see Oswald 2018 <https://royalsocietypublishing.org/doi/full/10.1098/rsta.2017.0359>).

12. Taking such a holistic approach will provide opportunities to consider new ways of creating ‘a principled and clear structure for data sharing’ along with new ways of overseeing such sharing. One possible solution to the issue of overlapping/conflicting/unclear statutory gateways (that I proposed previously in response to the Law Commission consultation) is a system of **asymmetric gateways based on a hierarchy of statutory agencies (or public purposes)** as laid out in the following diagram:



13. Such a hierarchical approach would provide an opportunity for a **public conversation about the nature of each public function** and the extent to which the transfer and use of personal data (especially sensitive data such as data about children, mobility data and identifiable medical information) is necessary and proportionate for each function, and therefore where each function

should be placed in the hierarchy. Whilst the model describes a hierarchy of public bodies, perhaps the statutory function/purpose for which disclosure is proposed might be a better alternative. The outcome has the potential to create clarity over both **the extent of data sharing and where the limitations should lie**: the default position being that disclosure would be permitted ‘up-hill’ subject to the acquirer justifying the necessity and proportionality and taking responsibility for the data and its use. Disclosure would not be permitted ‘down-hill’ except in specified **exceptional situations**, such as those seen during the pandemic.

14. Research conducted through our OMDDAC project has highlighted the importance of **avoiding assumptions** about whether the public is comfortable with their data being shared across all sections of the public sector (i.e. avoiding a ‘one-size-fits-all’ approach to data-sharing). For instance, our research has shown that survey participants were significantly less willing to share data with the police as compared with their local authority or public health body despite the emergency situation created by the pandemic (<https://www.omddac.org.uk/news/final-report-omddac-lessons-learned/>, 24).

Governance and oversight

15. It goes without saying that **independent scrutiny and governance** must therefore play a crucial role at all stages of such a hierarchical approach, which could contribute to increasing general transparency over the use of algorithms by the public sector. The OMDDAC project concluded that there exists ‘a need for greater levels of transparency and public engagement with regard to the ways in which data is used. It is evident that there exist real public concerns around specific types of data sharing that need to be addressed directly and we encourage a **new public conversation post pandemic** to ensure that the public are better informed, educated and consulted regarding the use of their data. The views of young people – who have been described as ‘the hidden victims of COVID-19’ – must also be incorporated into this conversation.’ (<https://www.omddac.org.uk/news/final-report-omddac-lessons-learned/>, 6)

16. It will be crucial, as the digital environment becomes ever more complex, that scrutiny and governance is ‘**end-to-end**’ i.e. that scrutiny - and thus accountability - becomes a **rolling process**, from project planning/initiation to eventual operationalisation, rather than being limited to ex-post review. New models of review and scrutiny will be needed, and lessons could be learned from the proceedings of the **West Midlands Police and Crime Commissioner and West Midlands Police data ethics committee** (the first of its kind in UK policing) which is an ongoing experiment in scrutinising and advising upon AI policing projects proposed for real operational environments. I discuss these lessons, and the challenges for such an approach, in more detail at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3812576

Dr Marion Oswald

8 November 2021