HUNTON & WILLIAMS
30 ST MARY AXE
LONDON, EC3A 8EP

TEL +44 (0)20 7220 5700
FAX +44 (0)20 7220 5772

BOJANA BELLAMY
DIRECT DIAL: +44 (0)20 7220 5703
EMAIL: BBELLAMY@HUNTON.COM

RESPONSE TO THE INFORMATION COMMISSIONER'S OFFICE BIG DATA AND DATA PROTECTION PAPER

1. BACKGROUND

This response is submitted by the Centre for Information Policy Leadership (the "Centre"). Nothing it contains should be taken as representing the views of any individual Centre member. The Centre strongly supports the attention given by the ICO to big data analytics, and recognises the enormous societal and economic benefits that can flow from big data and advanced analytics. The members of the Centre are all global businesses, each of which is committed to using personal data responsibly. It is for this reason that the Centre chose to provide input on Questions 1 and 3 of the ICO's paper on big data and data protection (the "paper").

2. RESPONSE

The Centre welcomes the ICO's consideration of issues arising from big data and welcomes the paper, which is in many aspects reasonable, considerate and well balanced. The Centre congratulates the ICO for taking on the task of producing the first regulatory guidance on the topic of big data, which can be used by privacy practitioners and which also has a capacity to influence the thinking of regulators and policymakers more broadly. This is especially important at the time when the topic of big data and analytics is being much debated on both sides of the Atlantic and the US administration is consulting on the approach to big data and regulation in the US.

In particular, the Centre finds helpful the ICO guidance around fairness and transparency; the fact that the use of big data will often determine fairness (use for research and trend analytics v. use in order to make decisions impacting individuals); the focus on reasonable expectations of individuals; the pragmatic approach to anonymisation; the reiteration of flexibility afforded in determining that subsequent or new purposes for which big data and analytics are deployed are not incompatible with the original purpose; the reiteration of legitimate interest ground for processing and eponymous Article 29 guidance; the mention of risk based approach; the important role of trust, as a business driver; and the link between data privacy and information governance at the C-suit level. Finally, the examples are always useful to illustrate a point, but also to show the variety of big data and analytics scenarios.

The Centre would like to make some observations regarding certain aspects of issues raised and specifically answer questions 1 and 3, as well as reflect on the format of the eventual guidance by ICO.

2.1 Question 1

Does this paper adequately reflect the data protection issues arising from big data or are there other relevant issues that are not covered here? If so, what are they?

The Centre finds the ICO paper places too great an emphasis on consent as a condition for processing personal data, and insufficient emphasis on legitimate interest ground and related alternative protections. Consent cannot provide individuals with appropriate and workable protections in all circumstances – a fact the ICO recognises in its report. Even where a consent in a single processing scenario theoretically appears to work, it is doubtful that a repeated and frequent recourse to consent will be workable for individuals in an information age, where big data and analytics will be performed constantly and automatically, by all types of organisations, on many devices and in all kinds of scenarios – in online, employment, customer, and government contexts.

The Centre believes that additional analysis by the ICO concerning when and how consent remains viable in the big data context and when it does not would be beneficial. Such further analysis would reveal that, increasingly and cumulatively, in many circumstances, consent may not be viable and cannot deliver the necessary and effective privacy protections for individuals. Where this is the case, we believe that alternative safeguards do exist that, nevertheless, keep the focus on the interests of the individual in delivering effective data protection.

- The "legitimate interest ground" for processing discussed by the ICO is such an alternative safeguard. It should be given more prominence and its application and relevance in the big data context should be further elaborated in the paper.

- Another related safeguard is the so-called risk-based approach to privacy (the ICO alludes to in the paper in the context of the draft EU Data Protection Regulation). Its application should be further explored and elaborated. Risk assessments, just like the legitimate interest ground for processing, place the responsibility for data protection on the organisation rather than the individual in appropriate circumstances. They are inherently linked to organisational accountability and are integral components of what accountable organisations can and must do. Organisations are in a better position to assess and understand the impact of their proposed information use. Thus, they should be allowed and required to use tools to assess the potential risks and harms of their proposed information uses on individuals in a given context, implement appropriate safeguards based on these assessments, weigh any residual risk against the benefits of the proposed processing and then make responsible decisions about whether and how to proceed with the proposed processing, taking full accountability for their actions (or inaction) both vis-a-vis individuals and privacy regulators.

Legitimate Interest Ground for Data Processing

Legitimate interest is likely to become an increasingly important ground for data processing in the era of big data, as it can:

a) Facilitate data collection, use, sharing and disclosure in circumstances where consent is not feasible, practicable or effective.

b) Enable new uses of information for new purposes, beyond the original purposes at the time of collection, provided such uses are not harmful to individuals and appropriate safeguards are implemented.

c) Stay consistent with organisational accountability, pursuant to which organisations implement safeguards in the entire lifecycle of information, from collection to use, sharing and destruction.

d) Ensure the protection of individuals' privacy, while allowing organisations and society at large (including its people) to pursue the benefits of new technologies, products and services.

As such, further work by the ICO on this subject should expand on the role of legitimate interest ground in the context of big data.

2.2. Question 3.

This paper refers to a number of practical measures and tools that can help to protect data privacy in the context of big data analytics: anonymisation, privacy impact assessments, privacy by design, data portability and privacy seals. Are other practical measures and tools needed? If so, what are they?

The Centre welcomes the ICO's recognition of anonymisation, privacy impact assessments, privacy by design, and privacy seals as important practical measures to protect privacy in the big data context. In addition, the Centre appreciates the multiple references to the role of risk assessment in delivering effective privacy protections.

However, the Centre wishes to further underline the importance of a risk based approach to privacy. The Centre believes that the ICO should place more emphasis in the paper on the role of risk and that it should analyse the further use and value of a risk based approach and its methodology in the big data context.

Risk assessment and the risk-based approach to privacy

The Centre has long advocated a risk-based approach to privacy and use of privacy risks assessments. The risk-based approach is closely linked with the concept of organisational accountability - risk assessment is one of the essential elements of accountability. It is also an element of the legitimate interest ground for data processing. Building on its earlier work on organisational accountability, the Centre recently launched a multiyear project to develop a comprehensive analytical framework for such risk assessments – the Privacy Risk Framework Project. Specifically, the project seeks to build consensus in collaboration with international privacy regulators, privacy experts and industry members, on what is meant by privacy risks to individuals and society, and to create a practical framework and the tools for organisations to identify, quantify, prioritize and mitigate such risks. In June 2014, the Centre published its first white paper on the subject "A Risk-based Approach to Privacy: Improving Effectiveness in Practice."

Privacy risk assessments can help accountable organisations determine whether and how to proceed with proposed information uses, based on potential risks and harms (both material and intangible) they may cause to individuals. Risk assessment is an integral part of devising proper information security measures and implementing privacy by design. While risk assessment

should be performed in connection with all processing activities, they are uniquely suited to enable responsible data use decisions in the context of big data for the following reasons:

a. Understanding the likelihood and potential severity of harms to individuals that may result from proposed information uses in big data context allows organisations to understand the impact of their actions and to devise appropriate and targeted mitigations and controls, including addressing any concerns from individuals. It also facilitates weighing any residual risk of harms, after mitigations have been implemented, against the countervailing benefits of the proposed use.

b. Privacy-risk assessments place the burden of privacy protection on the organisation. They are especially useful in big data situations where individual control and consent may not be viable due to the absence of direct interaction with the individual (*e.g.,* if the data has been de-identified, or in case of interconnected devices emitting personal data), or due to the repeated frequency of the information processing, or increased complexity of processing.

c. Because risk assessments focus on the risks to individuals (rather than solely on the organisational risks) and seek to remove or limit such risks as much as possible (or to identify uses that should not be pursued), the individual remains at the center of focus even in the absence of individual consent.

d. A risk-based approach can calibrate applicable legal requirements to specific big data contexts and allows for the flexibility in interpretation of the data privacy principles, which ensures that they stand the test of time (the ICO paper emphasises the latter point on multiple occasions). Thus, the risk-based approach is not an alternative, nor does it replace or supersede such requirements. It simply allows for interpretation and contextualisation, emphasising privacy protection measures that are more appropriate to the context at hand.

e. Risk-based approach and risk assessment can be useful in determining the compatibility of the subsequent or new purpose, when determining compliance with a purpose limitation principle. For example, if having performed a risk assessment, an organisation determines that a subsequent or new big data processing would have a great likelihood of causing significant risks of harms to individuals, the organisation may conclude that such subsequent or new processing is not compatible with the original purpose (and vice versa).

f. Risk assessments also reduce inefficient deployment of organisational resources by allowing organisations to prioritise their privacy controls according to the likelihood and severity of harm associated with a proposed data use. Such prioritisation is likely to contribute to the overall effectiveness of internal privacy programs. It also allows for a more holistic approach to information governance and data privacy, ensuring that data privacy shifts from being perceived as an obstacle, to being a business enabler in data driven business processes and the big data world.

A crucial issue is how to identify and agree on the nature, classification and quantification of privacy risks. To yield effective protection, the risk-based approach will take an inclusive approach to harm. It will not only seek to identify and evaluate tangible harms such as bodily injury, financial and other economic harms and loss of liberty, but will also consider intangible

harms such as reputational harm, embarrassment and discrimination and stigmatisation. As part of its ongoing Privacy Risk Framework Project, the Centre is currently working to develop consensus on the identity of the cognizable harms and how to quantify them. We hope our conclusions will be useful to the ICO in the future.

2.3 Presentation of the eventual ICO guidance

To ensure usability and readability of the paper, the Centre suggests that the final guidance document from ICO be presented divided into three sections.

- The first section would introduce the topic, background research and issues identified, which at present are strewn across the paper.
- The second section would focus on the actual core guidance – interpretation of the data privacy principles to the big data context, one by one, including reference for tools for compliance, summarised in a simple visual table.
- The third and final section would cover other best practices, business context and other more aspirational, yet still important parts of the guidance.