RESPONSE TO THE ARTICLE 29 WORKING PARTY'S CONSULTATION REGARDING OPINION 06/2014 ON THE NOTION OF LEGITIMATE INTERESTS OF THE DATA CONTROLLER UNDER ARTICLE 7 OF DIRECTIVE 95/46/EC

BACKGROUND

This response is submitted by the Centre for Information Policy Leadership (the "Centre"). Nothing in this submission should be construed as representing the views of any individual Centre member. Understanding the circumstances in which legitimate interest can be relied upon as a processing ground is vital to the development of new products, services, systems and technologies, and for ensuring individuals are adequately protected. The members of the Centre are all global businesses, and are all committed to using personal data responsibly. It is for this reason that the Centre is providing input on the Article 29 Working Party's (the "29WP") opinion on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC (the "Opinion").

EXECUTIVE SUMMARY

1. The Centre welcomes the Opinion and the 29WP effort to re-establish the legitimate interest processing ground on an equal footing with the other grounds in Art 7(f) of the Directive. The legitimate interest processing ground serves a valuable purpose for data controllers. It provides flexibility, coupled with necessary organisational accountability, in times of rapid technological change and evolving forms of data processing. It also demonstrates how an enhanced focus on organisational accountability can appropriately account for the role of individuals. It also emphasises the shift of larger focus to organisational accountability, while at the same time retaining a focus on individual. Given the narrow construction of the other lawful processing grounds, it is important that the legitimate interest ground retains this flexibility and that its use is not unduly curtailed.

2. A flexible approach to transparency and accountability principles is required, allowing businesses to direct their limited resources to more intrusive processing activities and those that pose greater risks to individuals. Information about the use of legitimate interest and internal documents that record how a controller has applied the balancing test should not be made available proactively to individuals, but only in specific circumstances, justified by a risk-assessment, or in response to a specific complaint from the individual, and supported by technical capabilities to do so.

3. While the Centre recognises the importance of safeguarding the rights and freedoms of individuals, offering individuals an unconditional right to opt-out, even as an additional safeguard, may be unworkable and it may undermine the precise basis for relying on the legitimate interest ground.

RESPONSE

4. The Centre welcomes the Opinion and considers it an important step forward in the interpretation and application of European data protection law. Arguably, the legitimate interest ground has been "neglected" by privacy practitioners in the years since the adoption of the EU Data Protection Directive. Its uneven application and a lack of guidance in Member States has resulted in data controllers being reticent in relying on the legitimate interest ground and instead over-relying on other grounds, even when the legitimate interest ground may have been more appropriate in the circumstances. The Opinion is particularly welcome at a time when the proposed EU Data Protection Regulation is being heavily debated in the European institutions. Finally, during a time of increased global debate about the evolving role of notice and consent in the modern information age, and when legalistic and long-worded

consents are not delivering the right protection, nor transparency for individuals, the Opinion offers real alternatives and paves a way for a more modern application of data protection law.

5. The Centre also considers the Opinion useful as it confirms the accountability model that the Centre has pioneered and advocated for many years. It confirms the need to shift the burden onto organisations to implement proactive privacy management programs and be able to demonstrate compliance with data privacy requirements and internal privacy programmes. The legitimate interest ground is an example of a proactive and responsible approach to the processing of data, and pre-supposes the existence of a data privacy program which addresses accountability through oversight; risk assessment; rules and procedures; training and awareness, monitoring and verification; response to breaches/ complaints and internal enforcement. Also, legitimate interest requires organisations to consider data processing from the perspective of individuals and to assess the risks to individuals. It is a real example of a risk-based approach to privacy and how privacy risk assessment plays a part in the everyday decision-making of accountable organisations.

Relationship with other processing grounds

6. The Centre supports the clarification of the circumstances in which legitimate interest may be relied upon. In particular, the Centre welcomes the recognition that reliance on legitimate interest should not be reserved for exceptional cases. Centre members highlight the flexibility offered by the legitimate interest ground, coupled with the requirement that data controllers must be accountable. This is particularly important in a period of rapidly advancing technology where new processing activities are constantly evolving and where increasingly business processes are digitised. The experience of Centre members shows that there are many instances where organisations process personal data for every-day, routine, legitimate and established business purposes that are clearly in the legitimate interest of the processing organisation, and that do not prejudice the interests or fundamental rights of individuals and do not raise unmitigated risks for individuals. Hence, it is important to preserve the flexibility of the legitimate interest ground in a way that is more streamlined and not unduly burdensome for organisations of all sizes.

7. Equally, there are instances where organisations may rely on the legitimate interest ground for more complex or less routine processing purposes, and in circumstances where the balancing test is more complicated, the safeguards more detailed and in general there is a need for more scrutiny and organisational accountability. In these cases, a more detailed process for assessing whether the legitimate interest ground can be relied upon is warranted, along with a greater level of accountability requirements.

8. Finally, it is important to preserve the flexibility of the legitimate interest ground and not make it overly burdensome, given the current trend to construe narrowly the other processing grounds. Also, the Centre strongly believes that as the modern information age embraces the Internet of Things, advanced analytics and connected devices, there will be challenges to the viability and applicability of some of the more established grounds for processing (e.g. consent, contract). As a consequence, there will be an ever increasing number of processing operations that may have to rely on the legitimate interest ground (of course, always subject to balancing test, appropriate safeguards and other accountability requirements). From a policy perspective, the Centre believes that this is desirable and should be encouraged, as it may deliver more effective privacy protection for individuals and more effective compliance on the ground.

9. Overall the Centre welcomes the Opinion's approach to legitimate interest. For all of the reasons discussed above, the Centre is mindful of the need to ensure its usage remains flexible in practice (for small businesses as well as large), while at the same time ensuring that individuals are protected when it is relied upon.

Accountability and transparency

10. The Centre broadly supports the 29WP's proposed approach to accountability and transparency, and recognises the importance of documenting the outcome of the balancing

test in order to demonstrate accountability in appropriate circumstances, both internally and externally. However, the Centre would welcome clarification on the circumstances in which this should be carried out. Centre members are concerned about the value and the administrative burden of maintaining detailed documentation for every single processing operation in relation to which legitimate interest is relied upon during the lifecycle of personal data. A more flexible approach would allow businesses to focus their finite resources on situations where, based on a privacy risk assessment, there is a significant privacy risk for individuals, or where processing activities are particularly intrusive, or would not be reasonably expected by individuals.

11. Also, the Opinion recommends that data controllers explain to individuals the reasons for believing that their legitimate interest is not overridden by the rights and freedoms of individuals. Again, the Centre recognises the value of transparency to individuals in appropriate circumstances, but would urge flexibility as to when such individual disclosures should be required. For example, in cases of routine and uncontroversial processing where the legitimate interest ground is relied upon, individuals may be unnecessarily burdened with information if the outcome of the balancing test is communicated to them. Similarly, where an unconditional right to opt-out of processing is not offered to individuals, Centre members question the utility of proactively informing individuals of the outcome of the balancing test.

12. The experiences with individual notifications in the context of data breach notification may offer a helpful analogy. As a best practice, individual notice is prioritized where there is a significant likelihood of material impact to an individual's health, finances, welfare or other status, so that they take action to mitigate any adverse impact. Where there are no essential individual mitigation strategies, or the nature of the impact is not material, individual notice is burdensome to companies, and potentially disruptive to individuals. Further, individual notification may be impractical where a data controller has not processed sufficient data to allow contact with an identifiable data subject (e.g. only IP address, cookie or other online identifier has been processed for a given operation).

13. To conclude, the Centre advocates a more flexible approach to identifying circumstances in which individuals are informed about the use of the legitimate interest ground and the outcome of the balancing test. In the Centre's view, the circumstances should be limited to those identified through a risk-based analysis, or in a response to a specific complaint from the individual.

The right to opt-out

14. The Centre is concerned about the suggestion that data controllers should consider offering an individual a right to opt-out from processing based on legitimate interest, as an additional safeguard and above and beyond a right to objection. The concern is that a requirement to offer an unconditional right to opt-out from processing where legitimate interest is relied upon essentially introduces a "soft" form of consent. This not only confuses the grounds for processing (by introducing a consent option where a legitimate interest ground would apply), but also could prejudice the legitimate interest of the data controller or a third party. The experiences of Centre members demonstrate that offering an unconditional right to opt-out is inappropriate in several scenarios where legitimate interest is typically relied upon. Many of these scenarios are complex, where striking the right balance may be difficult and where additional safeguards (other than unconditional opt-out) may be required. For example:

    a. A foreign legal requirement to screen the names of customers, suppliers or employees against export control or sanctions watch lists, or to comply with anti-money laundering laws, or to implement a whistleblowing and business ethics hotline.

       In all these scenarios, the Centre recognises the importance of safeguards to ensure individuals are not unduly prejudiced by the processing, but considers that offering an opt-out to individuals would entirely defeat the purpose of the processing. Businesses and the wider public have a clear interest in ensuring compliance with these foreign legal requirements, and a requirement to grant an unconditional right to

opt-out would swing the balance too far in favour of individuals and make that interest impossible to achieve.

b. Information security, intellectual property and asset protection measures, or fraud prevention steps, such as scanning a company network, computer and mobile assets, internal websites and email traffic, or the analysis of traffic and transactions.

   Again, the Centre considers that in these common scenarios it is important that safeguards are in place to protect the rights of individuals, but it would be impossible to perform such processing in a meaningful and effective way if a right to opt-out was offered to individuals affected.

c. On a related point, certain processing may be within the reasonable expectation of the individual. Many services are offered in such a manner that the individual should understand that the value proposition of engaging with the service, for example a website /online service, is predicated on an understanding that data will be processed. Some websites/online services may rely on a consent model as a barrier to entry to the website, but it may be more privacy protective to rely on the legitimate interest ground, subject to appropriate risk-based safeguards and accountability mechanisms, .particularly where no identifying or contact information is required. Where a website/online service processes data pursuant to a legitimate interest ground, offering individuals an unconditional right to opt-out (beyond the decision not to engage with the website at all), would be just as illogical as requiring a website operator to run the services without processing any IP address.

   The Centre considers it an important matter of technology policy that one-size-fits-all obligations may unnecessarily constrain the future applicability of the legitimate interest ground and could undermine its value as an alternative to consent and contract as processing grounds.

15. In conclusion, it is important that organisations implement sufficient safeguards to protect individuals, but it is unworkable to provide an unconditional right to opt-out in all circumstances where legitimate interest is relied upon. We note that a separate right to object already exists in all cases of legitimate interest and individuals can exercise that right in accordance with the law. The right to object offers individuals necessary but sufficient protection, without the need to supplement it with an unconditional right to opt-out.