Review of the Balance of Competences between the United Kingdom (UK) and the European Union (EU): information rights

Submission by Prof. Louise Amoore and Dr Volha Piotukh
(Department of Geography, Durham University, UK)

Background

This submission is largely informed by the research conducted for the *'Securing against Future Events: Pre-emption, Protocols and Publics' (SaFE)* research project funded by the Economic and Social Research Council (ESRC) and led by Prof. Amoore, as well as by Prof. Amoore's previous research into the use of data for security purposes. The *SaFE* project examines new approaches to security informed by developments related to big data, big data analytics and cloud computing, and their implications, including those for privacy and data protection. In particular, during our research, we have been closely following the reform process of the EU data protection framework and have engaged with all the key stakeholders.

This submission is focused on the key questions related to data protection on which we have specialist academic expertise. It does not, therefore, cover any issues related to the freedom of information.

Review questions

Q2. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) strikes the right balance between individuals' data protection rights and the pursuit of economic growth?

Recently, the relationship between data protection and economy growth is invoked more and more often and in different contexts. It was also the case at the *'European Big Data Conference: Towards a Data-Driven Economy for Europe'* that we attended (1 October 2013, Brussels), where the discussions revealed certain differences in positions within the European Commission (EC) itself in terms of the tension between the EC digital agenda (with its arguable reliance on data maximisation and the need for data protection to be 'in line with business opportunities') and the support for the data protection reform (with its principle of data minimisation and conceptualisation of personal data as a human right, with data subject and individual citizen 'still at the centre'). All too often, data protection is considered as an obstacle/challenge, an issue that came to prominence in light of the active lobbying on behalf of big US digital tech companies that marked

the process of reform of the European data protection framework (e.g., Albrecht, 2014)[1], something that we also discussed with a number of stakeholders as part of our research. In this respect, the shifting of focus towards considering a strong and effective data protection regime as a 'competitive' advantage should not be underestimated (e.g., EU Justice Commissioner Viviane Reding's speech *'The EU Data Protection Reform: Helping Businesses Thrive in the Digital Economy' (SPEECH/14/37* of 19 January 2014) and Preliminary Opinion of the European Data Protection Supervisor (EDPS) *'Privacy and Competitiveness in the Age of Big Data: The interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'*, March 2014).

However, we would like to suggest that the question of a balance between data protection and economic growth implies a false dichotomy between privacy and economy, which is even more evident now that data protection is recognised as a fundamental right under Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) (this was arguably less evident previously with the DP Directive stemming from the development of the single market). After all, data protection is a matter of what we value as a liberal democracy. Thus, in the words of Peter Hustinx former European Data Protection Supervisor (EDPS):

> the right to respect for private life and the right to the protection of one's personal data - are both fairly recent expressions of a universal idea with strong ethical dimensions: the dignity, autonomy and unique value of every human being, which also implies the right of every individual to develop his or her own personality and to have a fair influence on matters that may have a direct impact on them.

In this light, it is more appropriate to talk about, for example, the tension between data protection and rights of others, or the conflict between privacy and technology or about imbalances in terms of value generated by the use of personal data and benefits for data subjects as consumers (e.g., Preliminary Opinion of the European Data Protection Supervisor (EDPS) *'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'*, March 2014).

However, this is not the approach that is usually taken in assessing the economic impact of legislation, including the proposed EU Data Protection (PD) Regulation (see also the answer to Q. 4 below). Economic impact assessments also tend to disregard/downplay impacts that are difficult/impossible to quantify, but are not any less 'real' or important because of that, for example, the impact of such issues as confidence/trust (see also answer to Q. 10 below).

[1] Albrecht, J.P. 2014. Uniform protection by the EU – the EU Data Protection Regulation salvages informational self-determination. *In*: H. Hijmans and H. Kranenborg (eds). *Data Protection Anno 2014: How to Restore Trust? Contributions in honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*. Cambridge: Intersentia, pp. 119-128.

Q3. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) is meeting the challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks?

Like other frameworks developed a decade ago or earlier (see the answer to Q. 7 regarding the revision of the Organisation's for Economic Co-operation and Development (OECD) *'Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' ('Privacy Guidelines')*), the EU DP framework does not effectively meet the above challenges. In fact, modernisation of data protection principles with a view of "making them future-proof and fit for the digital age"[2] is one of the main reasons behind its comprehensive reform. See Q. 10 for the detailed discussion of the current technological challenges.

Q4. What evidence is there that proposals for a new EU Data Protection Regulation will be advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

There is little doubt that the current EU DP framework is in need of reform. The three main reasons for the reform process, namely modernisation, harmonisation and alignment with a new EU institutional framework, are sound. The strengthening of the rights of the data subject is clearly advantageous for the individuals, while the increased harmonisation and removal of administrative burdens is advantageous for businesses and the public sector. In terms of overall impact, in 2012 the EC[3] and the UK Information Commissioner's Office (ICO) (2012)[4] have produced rather divergent assessments. We do not intend to evaluate these documents in detail, but would like to stress that, just because certain impacts are not easily monetised, it does not mean that they are not important and that the final balance sheet has to be in the negative. Opportunities related to the single digital European market are a case in point (e.g., in the areas of cloud services and privacy-enhancing technologies), as are reputational advantages to businesses and synergies between enhanced data security through stronger data protection and cyber security, which is one of the UK national security priorities[5].

[2] http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf
[3] http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
[4] https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/eu-data-protection-reg-impact-assessment.pdf
[5] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf; https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

Q7. How could action, in respect of information rights, be taken differently at national, regional or international level and what would be the advantages and disadvantages to the UK?

To ensure adequate protection of the rights of the individual, action must be taken at all levels: national, regional and international. In this respect, while national data protection authorities, e.g., the UK ICO, play and will continue to play the key role by issuing guidance, monitoring compliance and taking enforcement action (and, in light of the new technological developments and associated challenges, they will need more powers and more resources than ever before if these challenges are to be addressed effectively), borderless technologies and networks, a globalised economy and the transnational nature of data flows mean that national measures alone are insufficient and that action is required at regional and international levels. The effectiveness of this action depends to a large extent on harmonisation of regulation and effective co-operation between national authorities, something that can be best achieved at the EU level and something that the proposed DP Regulation sets to strengthen. The weight of the EU as a whole is also important in strengthening data protection standards internationally and in encouraging other countries to improve their policies and practices of relevance, which is crucial in light of the ever increasing data flows with non-EU countries, some of which have much weaker data protection standards, and the need to protect the rights of all EU citizens in the process. This is something that the proposed DP Regulation also attempts to do by expanding its scope to include companies not established in the EU, if they offer goods or services in the EU or monitor the online behaviour of data subjects residing in the EU. Recent EC Communication COM(2013) 846 *'Rebuilding Trust in EU-US Data Flows'* of 27 November 2013 states that "EU rules on collection, processing and transfer of data should be promoted internationally" (p. 8). Indeed, in light of the importance of the issue of public trust, a strong data protection regime can become a EU competitive advantage (see, for example, EU Justice Commissioner Viviane Reding's speech *'The EU Data Protection Reform: Helping Businesses Thrive in the Digital Economy'* (SPEECH/14/37 of 19 January 2014) and Preliminary Opinion of the European Data Protection Supervisor (EDPS) *'Privacy and Competitiveness in the Age of Big Data: The interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'*, March 2014)). See also answer to Q 10 regarding the significance of the EU single digital market for enabling future technological and business developments, especially in light of the already established US hegemony in many of the areas of the digital markets, such as big data analytics and cloud computing.

It must also be considered that current positive developments in the USA, such as this year's comprehensive review of policy issues at the intersection of big data and privacy, which was requested by the US President Obama and resulted in the two important Reports: *'Big Data: Seizing Opportunities, Preserving Values'* and '*Big Data and Privacy: A Technological Perspective'*, have been to a certain extent influenced by the EU's position, and, in particular, by its

calls to restore trust in the EU-US data flows following the allegations regarding the mass surveillance of European citizens, and the reform process of the EU data protection framework. The US review's recommendations include, *inter alia*, extending privacy rights to non-US citizens and the advancement of the *Consumer Privacy Bill of Rights*, measures that were also put forward in the above mentioned EC Communication. Indeed, EU institutions were instrumental in revealing the inadequacies in the way in which the Safe Harbour regime, established by Decision 2000/520/EC to serve as a legal basis for data transfers from the EU to the US companies who declare their adherence to the privacy principles, was functioning (e.g., EC COM(2013) 847 *'On the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU'* of 27 November 2013)).

With regard to the international level of regulation, one should also note the recently revised OECD *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ('Privacy Guidelines')*, the advantage of which lies in their geographical scope, which extends beyond Europe. The revision of the *'Privacy Guidelines'* containing "the first internationally agreed upon set of privacy principles" (OECD 2013 *'OECD Privacy Framework*', p. 19) took place in light of "changing technologies, markets and user behaviour and the growing importance of digital identities" (OECD 2013 *'Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines',* p. 4). The revised Guidelines advocate a risk-based approach to privacy protection and call for the increased interoperability of the privacy standards, as well as introducing such measures as national privacy strategies, privacy management programmes and data security breach notifications (OECD 2013 'OECD Privacy Framework', p. 4). Despite the importance of the revised *'Privacy Standards'* and the impact of the original version of standards, they represent a framework document rather than a set of specific and detailed privacy protection provisions and are not legally binding, which means that they remain open to 'cherry-picking'.

Another option worth considering is that of self-regulation. However, according to our research findings, there is a growing appreciation among public authorities and commercial entities that, although it should encouraged and supported, self-regulation alone is insufficient and ill-equipped to ensure privacy and data protection, as the US experience has demonstrated. This is especially the case in light of the current technological advancements and the growing imbalance between citizens as consumers and 'data giants', exploiting the economies of aggregation (e.g., EDPS *'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'*, March 2014). Instead, the focus should be on co-regulation, whereby a legal framework provides for and encourages development of codes of conduct, a position supported by the former EDPS Peter Hustinx among

others (e.g., Swire, 2014[6]). Equally, there is a growing appreciation that, the importance of technological solutions (e.g., privacy-enhancing technologies) notwithstanding, technology alone cannot protect privacy effectively (e.g., 2014 *'Big Data and Privacy: A Technological Perspective'* Report). At the same time, the US big data and privacy review has recommended to "strengthen U.S. research in privacy-related technologies" and argued in favour of the U.S. leadership on these issues (pp. 50, 52). Currently, the leading global provider of research funding related to privacy-enhancing technologies is the European Research Council, with UK universities and businesses among the leading national beneficiaries. Indeed, the European single digital market envisages important opportunities for innovation and trade in privacy-enhancing software technologies (e.g., EC COM(2007) 228 *'Promoting Data Protection by Privacy Enhancing Technologies (PETs)*).

Overall, we highlight the need for a strong, harmonised, legally-binding regional data protection framework, supported by effective enforcement and co-operation among national data protection authorities, a framework that would also encourage complementary self-regulation mechanisms and further development and application of appropriate technological measures. If adopted, the revised EU data protection framework could indeed become such a framework.

Finally, data protection as a fundamental right can also be complemented by protection of the data subject as a consumer. Thus, the aforementioned preliminary EDPS opinion *'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'* justifiably points out that, in the digital economy, personal data is an important asset. Thus, according to some estimates, in 2011, the data of EU citizens was worth EUR 315bn, and its value was predicted to grow to almost EUR 1tn by 2020 (Viviane Reding, SPEECH/14/37 of 19 January 2014 *'The EU Data Protection Reform: Helping Businesses Thrive in The Digital Economy'*). At the same time, there are significant "risks to the consumer posed by concentrations and the abuse of market dominance where firms process massive amounts of personal data" (p. 7), which are not fully appreciated or addressed. It suggests that competition and consumer protection rules can and should be used to protect the data subject as a consumer against exclusionary conduct, exploitation and misleading commercial practices, including describing a product or service as 'free', while in reality the consumer has to provide a payment in the form of her personal data. Importantly, such measures are not there to replace or substitute the data protection, but to complement it. In sum, we urge careful attention to the issue of commercial value of personal data and, particularly, to the close relationship between protection of data subjects and access to the resource that is their data.

[6] Swire, P. 2014. Peter Hustinx and three clichés about EU-U.S. data privacy. *In*: H. Hijmans and H. Kranenborg (eds). *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*. Cambridge: Intersentia, pp. 191-198.

Q8. Is there any evidence of information rights being used indirectly to expand the competence of the EU? If so, is this advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

Two developments are of particular relevance: TFEU and the jurisprudence of the Court of Justice of the European Union (ECJ). With respect to the latter, we would like to point to the 2014 ECJ Judgment in Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* as indicative of difficulties encountered by national authorities when data are collected, stored or processed outside their territory, e.g., in the 'cloud'. This judgement demonstrates a much welcome appreciation that use of advanced analytics constitutes data processing, which is advantageous to the extent that it is one of the few examples of institutions attempting to keep pace with technological advances. This judgement also shows the importance of the European institutions as an additional source of expertise and a much needed added level of protection.

Q10. What future challenges or opportunities in respect of Information Rights might be relevant at a UK, EU or international level; for example cloud computing?

According to our research, the main challenges to privacy and data protection arise from the high speed of technological developments, and, in particular, from the rise of big data and big data analytics and cloud computing, combined with the outdated privacy and data protection frameworks. These challenges are significant and diverse, and they are just beginning to be recognised.

According to the OECD, over recent decades the environment for privacy has changed dramatically in view of such developments, as: "the volume of personal data being collected, used and stored"; "the range of analytics involving personal data"; "the frequency and complexity of interactions involving personal data"; and "the global availability of personal data" (OECD 2013 *'OECD Privacy Framework'*, pp. 3-4). These developments are closely associated with the rise of the big data phenomenon, characterised by four Vs: increased volume, variety, velocity and veracity. Following our research findings, we have suggested that what is 'big' about big data is specifically the way it appears to exceed human capacities to make sense of it. This suggests that the focus should be not so much on the big data as such, but on the big data analytics. Therefore, it is not just big data, but big data combined with big data analytics that "brings with it the possibility of finding information, trends, insights that were not previously obvious or capable of being ascertained" (OECD 2013 *'OECD Privacy Framework'*, p. 83). This, in turn, generates both "economic and social value" and "privacy implications" (OECD 2013 *'OECD Privacy Framework'*, p. 83). Of course, not all big data is personal data. The reliance of big data analytics on as large data

sets as possible and the difficulty of knowing in advance how they will be used (as this largely depends on the capabilities of analytical models and algorithms in question), create tensions with the key principles of data protection, such as collection limitation and purpose specification (of course, even "collection and storage of data also creates privacy risks" Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*, p. 17)).

Furthermore, a crucial challenge and opportunity lies in the increasing ability to combine different datasets and to leverage both structured (e.g., transactions) and unstructured data (e.g., text, sensor data, image) data for analysis. The opportunities envisaged by data industries and their clients centre on the capacity to build a more 'complete picture' of a person – whether a consumer purchasing products, an unemployed citizen seeking welfare, or a customer of financial institutions seeking credit. The mining of multiple forms of data, some of it traditional, others coming from open source social media, is seen as a valuable new opportunity for governments and private companies alike. However, these opportunities bring new challenges for regulation. First, the analytics processes produce new forms of derived or inferred data that cannot always be clearly defined as 'personal data' (see Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*). Second, contemporary techniques used for analysis actually significantly challenge the capacity for anonymisation (e.g., EDPS *'Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy', March 2014*; *'Big Data and Privacy: A Technological Perspective'*), let alone deletion, or 'the right to be forgotten'. The ability to link different disparate pieces of data to identifiable individuals "by combining the anonymised data with information contained in other databases" has been demonstrated on several occasions (OECD 2013 *'OECD Privacy Framework'*, p. 97; Ohm, 2010:1704[7]). It has been argued in this respect that "[o]nce any piece of data [is] linked to a person's *real* identity, any association between this data and a *virtual* identity breaks anonymity of the latter" (Narayanan and Schmatikov, in Tene and Polonetsky, 2013:251; original emphasis). Third, a key challenge is regulating data quality and accuracy and, particularly, ensuring that discrimination does not take place either in data extraction/ingestion, or in the profiles that are subsequently generated. As the automated mining and analysis of data intensifies, it will become ever more difficult to guarantee that profiling has not taken place on the basis of data pertaining to health, race, ethnicity, gender, sexuality or disability. For example, processes of text mining and sentiment analysis infer individual characteristics from a large array of data elements, not all of which 'belong' to the same data

[7] Ohm, P. 2010. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, **57**, pp. 1701-1777.

subject. Even with statistical algorithms, there is a fundamental problem of "uncertainty that discovered properties of groups apply to a particular individual in a group", while "[m]aking incorrect conclusions about individuals may have adverse consequences for them" *('Big Data and Privacy: A Technological Perspective'*, p. xii). Furthermore, patterns and relationships revealed through big data mining may not be representative of reality *('Big Data and Privacy: A Technological Perspective'*, p. 25).

Finally, in light of the new technological advances, the conventional categories of data protection, such as consent, access, redress and correction are also challenged. For example, as OECD identify "obtaining meaningful consent is increasingly challenging", especially as "individuals often have no choice other than to simply 'take it or leave it'" (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*, p. 14; *'Big Data and Privacy: A Technological Perspective'*, p. xii). Perhaps more significantly, though, the nature of data analysis affects such data subject rights as access and correction, particularly in light of "[r]apid dissemination, indexing, caching and mirroring of data" (OECD 2013 *'OECD Privacy Framework'*, p. 100), and in relation to derived or inferred data, "even in situations where individuals are made aware of their impact" (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*, p. 6; also Amoore, 2014[8])). It should be stressed that while "disclosure of personal data by individuals is made very easy" (and often by default), "exercising access rights or seeking correction of these data can be burdensome" (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*, p. 12), which is why the aforementioned ECJ decision is so important.

Overall, the use of big data analytics creates transparency issues and often results in the so-called 'transparency paradox': while it "enables greater insights about individuals, the machinery behind it is anything but transparent" (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)*3, p. 15). Therefore, it is becoming recognised that more needs to be done "to increase the transparency of algorithmic effects" and to ensure that individuals can better understand both how the data were arrived at and impacts of data uses (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of*

[8] Amoore, L. 2014. Security and the claim to privacy. *International Political Sociology*, **8**(1), pp. 108-112.

Current Thinking', DST/ICCP/REG(2014)3, pp. 10, 12; also Amoore, 2013[9])). Indeed, "since in a big data world it is often not the data but rather the inferences drawn from them that give cause for concern, organizations should be required to disclose their decisional criteria" (Tene and Polonetsky, 2013:239[10]).

Some of the above challenges will be addressed if the proposed DP Regulation is adopted, as it provides for: more emphasis on data minimisation; better user control, including explicit consent, when required, a right to be forgotten and data portability; emphasis on 'privacy by design' and 'privacy by default'; clearer allocation of responsibilities; more transparency and stronger supervision and enforcement. However, further measures are required to ensure, for example, "consistency of purposes when personal data are processed by multiple entities" (Working Party on Security and Privacy in the Digital Economy, 2014, *'Summary of the OECD Privacy Expert Roundtable: Protecting Privacy in Data-Driven Economy: Taking Stock of Current Thinking', DST/ICCP/REG(2014)3*, p. 18). In addition, technological solution should be implemented (e.g., *'Big Data and Privacy: A Technological Perspective'*) with a view to complementing legislative measures (such measures are encouraged in the Proposed DP Regulation) and to operationalise the politically and ethically significant emphasis on increased transparency discussed above.

Finally, it should be mentioned that the benefits of value extraction from personal data are often not realised for individuals (Tene and Polonetsky, 2013; EDPS '*Privacy and Competitiveness in the Age of Big Data: The Interplay between Data Protection, Competition Law and Consumer Protection in the Digital Economy'*, March 2014), which is something that can be addressed in the way discussed in the answer to Q.7. Furthermore, it has been suggested that, as "[b]ig data's 'products of analysis' are created by computer programs that bring together algorithms and data so as to produce something of value", "[i]t might be feasible to recognize such programs, or their products, in a legal sense and to regulate their commerce" (*'Big Data and Privacy: A Technological Perspective'*, p. 49).

The National Institute of Standards and Technology (NIST) of the US Department of Commerce defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, *2011 Special Publication 800-145,* p. 2). There are different service and deployment models, with the former ranging from Software as a Service (SaaS) to Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), and the latter

[9] Amoore, L. 2013. *Politics of possibility: risk and security beyond probability*. Durham and London: Duke University Press.
[10] Tene, O. and J. Polonetsky. 2013. Big data for all: privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property*, **11**(5), pp. 239-273.

including private, public, community and hybrid clouds. While for some cloud computing represents a technological revolution, for others it is just another form of outsourcing. Potential for innovation and economic benefits of cloud computing notwithstanding, it is widely acknowledged that cloud computing presents a number of data protection challenges (e.g., *Article 29 Data Protection Working Party (Art. 29 WP) Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196);* 2012 *EDPS Opinion on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'))*. Many of these challenges stem from the lack of control over data and lack of transparency regarding the entities, processes and jurisdictions involved and, relatedly, a lack of clarity regarding the applicable rules and distribution of responsibilities; these challenges also tend to get compounded as one moves through the cloud hierarchy from IaaS to PaaS and through to SaaS. Lack of control over data manifests itself in a variety of ways: vendor lock-in; sharing of resources and lack of isolation, for instance, in a multi-tenant cloud; possible access of third parties resulting from data centres being located in (a) different jurisdiction(s); and inability for data controller to intervene when necessary (*Article 29 Data Protection Working Party (Art. 29 WP) Opinion 05/2012 on Cloud Computing (01037/12/EN WP 196)).* At the same time, it is essential that the "level of data protection on a cloud computing environment [is] not inferior to that required in other data processing context" (2012 *EDPS Opinion on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'*, p. 3). The consistent and effective application of the existing data protection provisions can address many of these issues (see, for example, the UK ICO 2012 *'Guidance on the Cloud Computing'*). However, future consolidation of the cloud computing market, already predominantly dominated by US companies, and the growing imbalance in the relationship between cloud providers and cloud clients are likely to have a further negative impact (2012 *EDPS Opinion on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'*). The way to effectively address the above concerns would be through a combination of the development of well-regulated EU cloud capabilities and a strengthened data protection framework. The first aspect is envisaged by the EC COM(2012) 529 of 27 September 2012 *'Unleashing the Potential of Cloud Computing In Europe'*, which provides for the three key actions: safe and fair contract terms and conditions; clear standards; and the European Cloud Partnership. These actions represent real opportunities for the UK digital enterprise, which otherwise may find it more difficult to compete with the established cloud giants on its own. The second aspect is addressed, to a certain extent (for the remaining issues, see, for example, the above mentioned EDPS Opinion), in the proposed EU DP Regulation, which provides, *inter alia*, for: an extended scope of application, therefore better covering cloud services; clearer rules with respect to the duties and responsibilities of cloud providers; and stronger safeguards with respect to international data transfers.

Furthermore, according to our research, the issue of trust is fundamental for the potential of cloud and other digital technologies for innovation and growth to be realised. Indeed, the importance of

trust for the uptake of these technologies was stressed at every major fora of relevance we attended, including the World Cloud Forum in London in 2013 and 2014 and the 3rd European Annual Cloud Conference in Brussels in 2014. At the same time, public trust in both governments and companies handling their personal data has been undermined on both sides of the Atlantic (e.g., Hijman and Kranenborg, 2014[11]; EC MEMO/14/60 of 27 January 2014 *'Data Protection Day 2014: Full Speed on EU Data Protection Reform'*; the US big data and privacy review[12]). Thus, according to the 2011 Special Eurobarometer survey *'Attitudes on Data Protection and Electronic Identity in the European Union'*, "70% of Europeans (EU) are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected"[13]. According to a recent survey by Ipsos MORI/King's College London, in the UK social media sites and media companies are barely more trusted with personal data they have than foreign governments[14]. A robust, harmonised and future-proof data protection framework can go a long way in addressing these concerns and in restoring public trust in governments and private companies and confidence in using online services. Indeed, according to the above mentioned Eurobarometer survey, almost all Europeans – 90% - are in favour of equal protection of rights across the EU.

Q11. Is there any other evidence in the field of EU Information Rights that is relevant to this review?

With regard to other evidence relevant to this review, we draw attention to the relationship between information flows and the principle of freedom of movement of people, goods, services, and finance. Increasingly, a clear regulatory framework for data is necessary precisely because of the growing levels of mobility of people and things across borders. Our research findings suggest that, for example, even a renegotiated and reduced UK relationship with the EU around free trade would still necessitate some level of common framework on data protection. Why is this the case? In order to benefit from the opportunities of global mobility, the UK (as all industrialised states) has moved towards 'risk-based' approaches to border management. Put simply, this involves differentiated treatment depending on the relative risks and opportunities in question. However, risk-based approaches are 'data hungry', they rely on a ready supply of transactional data in order to differentiate areas of high and low risk activity. One example would be trusted traveller programmes, in which people receive low risk status in return for the supply of their biometric and

[11] Hijmans, H. and H. Kranenborg. 2014. Data protection anno 2014: How to restore trust. An introduction. *In*: H. Hijmans and H. Kranenborg (eds). *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*. Cambridge: Intersentia, pp. 191-198.
[12] http://www.whitehouse.gov/issues/technology/big-data-review
[13] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
[14] http://www.statslife.org.uk/opinion/1344-data-privacy-where-do-people-draw-the-line

other relevant data. In this 21st century transnational exchange of personal data for increased freedoms, common frameworks on data protection are required to secure trust and necessary 'buy-in'. In our view, and based on our findings, a 'go it alone' UK position may forgo the advantages of co-operation and secure data exchange/transfer based on common standards providing a high level of data protection, co-operation that is required to ensure security, facilitate mobility and ensure public trust. The latter is particularly important in light of concerns surrounding governments' access to and use of commercial data gathered by businesses *('Big Data and Privacy: A Technological Perspective'*, p. 6), as, for example, in the case of passenger name records (PNRs).

Our research findings also point to the necessarily conjoined processes of data marketisation and data protection. As the returns on 'big data' analysis increase, UK digital industries will seek to capitalise on their competitive advantage across Europe. Our interviews with software suppliers evidence a strong awareness of the need for compliance with data protection principles, particularly for access to European markets. There are, of course, parallels in many other domains – for example, the world's leading financial centres are pioneers not only in terms of marketisation, but also in terms of the regulatory structures that facilitate that market. It is our view that the UK's fledgling and innovative digital industries will significantly suffer if they are perceived to be 'offshore' and outside of the harmonised European regulatory frameworks. For example, the current debates surrounding the European Cloud Partnership also reflect concerns that US providers do not provide adequate protection for consumers.