EURIM DIGITAL POLICY ALLIANCE

informing policy for a competitive, inclusive, networked society

Response of the Digital Policy Alliance to the Ministry of Justice Call for Evidence on the review of the Balance of Competences between the United Kingdom and the European Union

(Information Rights)

June 2014

"We must restrict the anonymity behind which people hide to commit crimes. As citizens, we have a right to privacy. We have no such right to anonymity."

Edgar Bronfman, Jr.

"I believe that any violation of privacy is nothing good."

Lech Walesa

"Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies."

Bill Gates

Background

The Digital Policy Alliance (EURIM) is an independent, not-for-profit, politically neutral, broad-based membership organisation, informing policy for a competitive, inclusive, networked society.

The cross-party policy voice of the internet and technology sector, we focus on digitally-related topics including ubiquitous broadband, cyber security and e-crime, data protection, lifelong learning and telehealth, next generation Internet and Smart UK. Our working groups produce plain language briefings for Parliamentarians, Ministers, civil servants and industry members, and we promote our findings to policy decision-makers and influencers through a programme of targeted events.

The Digital Policy Alliance (EURIM) is the policy voice of the internet and technology sector.

QUESTIONS

1. What evidence is there that the EU's competence and the way it has used it (principally the Data Protection Directive) has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

In an interconnected age and when the UK is in urgent need of economic growth, the Internet is one of the most important ways to deliver it. Developing a common regional data protection framework to apply across the EU and that is likely to be adopted by other non-EU Countries (Switzerland, EFTA, EU Candidate Nations and beyond), is already a strategic objective for the UK Government. It is also in line with the position taken by the Foreign and Commonwealth Office at the Seoul Cyberspace conference that took place in October 2013.

Companies in the UK using 'big data' and trading via the Internet undoubtedly bring significant economic benefits to the UK. Foreign-based companies seeking to operate within the UK are more likely to comply with a common regional set of data protection rules rather than having to comply with diverging legislative frameworks in 28 separate jurisdictions, and there is a danger that they might avoid a UK market that has separate rules.

Against this backdrop we have found no evidence to suggest that the EU's competence and the way it has used it thus far have been disadvantageous. The Single Market has brought benefits to business, e.g. by providing some degree of harmonisation and predictability, (and could be yet more beneficial were it to be fully implemented). It has also benefited consumers, with improved services while also making it easier for individuals to seek redress from any EU Member State.

The fact that there has been no major outcry from business regarding the current EU Data Protection Directive reinforces the above conclusions. Business is focused on the need to drive value from across the Single Market to maximise shareholder value, and common rules are helpful in this regard. Growth in the EU digital economy has unfolded and is continuing under the current EU Data Protection Directive regime, with many of the World's companies choosing the UK as their Regional HQ. Without the EU Data Protection Directive, and/or without the UK being part of the EU, things could easily have been different.

The EU's competence in the data protection domain can therefore be seen as beneficial to the UK's employment market, economic growth and future prosperity. If the UK's aim to be at the forefront of the Digital Age is to be realised, then supporting EU policy in this domain as part of the UK Government's wider International engagement strategy is entirely logical. Applying 'UK only' rules when the rest of the world is interconnecting apace, is a recipe for enforcement problems and would add complexity and cost to business. They would also complicate the position of the City of London as a major hub for global online business.

Such disadvantages as there may be (and we have found no evidence of any) are far outweighed by the advantages of cross border legal certainty and a common framework that reduces red tape in line with HMG stated goals, espoused by the Department for Business, Innovation and Skills (BIS).

We have, however, found evidence of unsatisfactory notification activities between undertakings within the UK under the current regime.

2. 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?

We have found no evidence to suggest that the balance is wrong, if indeed "balance" is the appropriate way to consider the whole issue. The Executives and Judiciaries of both the UK and the EU Institutions share a common objective and are better envisioned as being on the same side but to slightly differing degrees. "Balance" implies that the parties are on opposite sides when this is not so. Effective remedies in the Internet age demand common international approaches – and this is already HMG policy.

The EU Institutions have been at the forefront of recognising data protection as a fundamental right for individuals. Unfettered economic growth without adequate protection for citizens would be politically unacceptable. We are unaware of any "misuse" by the EU of the Data Protection Directive. However the draft legislative proposals require further work to be fully workable.

Business and individuals can and do work together for the delivery of benefits to the consumer, e.g. supermarket store cards. Businesses store data on individual preferences and use this to offer customers benefits such as cost savings on products. The individual's data has value to business, and where this value is shared between them this is most likely to build greater cooperation between consumers and businesses everywhere. Some UK supermarkets are active in other EU member states and are already operating on this 'shared value' basis. A common regime for data protection, uniformly applied, would further help the development of 'shared value' models.

This kind of activity is made possible through the 'legitimate interest clause,' which allows for the processing of data for any legitimate business purpose so long as this does not harm or disproportionately interfere with the privacy of the citizen. This has enabled new ranges of economic activity to develop, e.g. in financial services, security and web analytics. Importantly, this approach has proven successful in striking the right balance between individuals' data protection rights and the pursuit of economic growth. There is, however, a need for thought leadership with regard to the exercise of informed consumer choice lest this present problems.

3. 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?

We do not see any evidence that the EU's competence in data protection issues and the way it has used the legislation has been a problem. A more general problem, not unique to Europe, is the fact that very prescriptive laws such as in the proposed GDPR always struggle to keep up with the pace of technological evolution, and the legislative process to amend them is also too lengthy to keep up with the "art of the possible". You cannot sensibly legislate in advance for that which you cannot foresee, and this inconvenient truth will not go away. The Digital Policy Alliance (DPA) therefore concludes that a legislative approach based on principles rather than being prescriptive is the best way to help meet the challenges posed.

The way in which the EU Commission identified problems caused by Google's 'Streetview' activities highlights well the kinds of challenges posed by the increasing international flow of data, technological developments, and the growth of online commerce and social networks. Identification of problems at national level across the EU related to uneven implementation of the current

Directive is an issue that must be resolved. The DPA believes that comments of the European Court of Justice made obiter dicta (statements made in the course of a judgment that are not necessary for a decision) on even enforcement throughout the EU would be most valuable.

4. 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 has already been significant comment by others about the EU Commission's Regulatory Impact Assessment for the proposed new draft Regulation, including widely varying estimates as to likely costs or benefits.

A study by Deloitte estimates a potential loss to GDP across the EU of €173 billion and the loss of 2.8 million jobs. There is a case to be made on both sides, and we do not seek to engage in this debate because of the difficulty in finding definitive evidence. The DPA nevertheless urges action to update a statute which dates from nearly 20 years ago and was originally likely to have been first drafted 5 years earlier than that…

The UK and the rest of the EU share a common goal in trying to get this important legislation right, and there is some concern that the proposed Regulation in its current form requires further improvement. If delay is necessary to improve future legislation (whatever form it takes) for the benefit of all EU citizens then we would support this. One idea we have heard of could be that the new Commission considers setting up a special taskforce, as it did so effectively with the Better Internet for Kids programme (possibly even a multi-stakeholder platform). This could potentially assist by giving technical inputs and suggesting ideas as to the best way forwards.

A particular question for the attention of future lawmakers is how possible is it to really anonymise data? How much thought has been given to this given the capabilities of the underlying technology? Has there been adequate discussion to understand whether or not the concept of anonymised data can robustly be translated into practice? New software tools exploiting big data techniques with powerful data analytical processing capabilities have a reasonably high chance by deduction of being able to 'fill in the blanks' even on scrubbed data. This complicates the positions of data controllers and subjects alike, but in an age when any laptop can see a picture of your house, we should be seeking to future proof legislation insofar as this is possible. The DPA believes that whatever form a new data protection statute will take, a principles-based approach has to be at its core.

Notwithstanding the above, we wish to applaud the efforts of the EU Commission and Parliament for tackling this complex area. We fully accept that this is difficult and complicated work and it cannot be ignored.

5. What evidence is there that the right to access documents of the EU institutions has been advantageous or disadvantageous to individuals, business, the public sector or any other groups in the UK?

There is evidence that the right of access to documents of the EU Institutions has been of benefit to UK individuals and companies. No disadvantages have been brought to our attention and if there are any we are unaware of them.

6. How would UK citizens' ability to access official information benefit from more or less EU action?

We have no comment on this question.

7. 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?

The Foreign and Commonwealth Office will already know how difficult it is to get an international agreement as regards Internet governance. A common set of global data protection rules applied uniformly and equally would be the ideal solution – it is also a pipe dream.

The next best option has to be a regional approach, uniformly applied across the EU, which will be adopted progressively by other nations. The EU External Action Service (EEAS) has been seeking to raise data protection standards as part of Free Trade Agreement negotiations, which is to the UK's benefit and yet which is largely unknown and unseen in the UK.

At the national level the UK cannot realistically maintain a position of 'data independence' in an interconnected world. It is essential that adequate technical knowledge is at the disposal of those making the decisions as to the scope and type of legislation to adopt for the future. The DPA considers that this could only benefit the entire legislative process and create better law.

We set out earlier in this paper our initial thoughts on actions needed to create a new EU information rights regime comprising:

1 a new principles-based statute with:

2 more direct input from the technology sector to ensure adequate 'future proofing',

3 drafted so as to attach different rules to different classes of data, and

4 uniform implementation of the statute across the EU.

8. 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?

As yet there is no evidence of this and from a business perspective, access to a single market is vitally important.

Some have argued that recent actions by the ECJ have sought to extend the competence of the EU. However a "principles based" approach necessarily means scope for interpretation by the judiciary who should have the ultimate oversight. Questions regarding the composition of the ECJ are outside our competence.

9. What is the impact on EU competence of creating an entirely new legal base for making data protection legislation that is not expressly linked to the EU's single market objectives?

The question relates to the introduction of legislation under a different legal system to that used for the original DP Directive. Article 16 of the Treaty on the Functioning of the European Union provides a new legal basis for the regulation of data protection, applicable to the processing of all personal data in the public or private sectors, including police and judicial cooperation. This new legal basis is being invoked for the proposals for the revised Data Protection Directive and the GDPR.

The 1995 Directive was adopted when the Internet was far less widely used than it is today. The DPA believes that because of greatly increased flows of personal data, a stronger and more coherent data protection framework providing for greater consistency is now necessary. The legal approach which most efficiently delivers the benefits of an Internal Market, with improved harmonisation and assuring legitimate exchange of personal data, which is clear and simple to understand and apply, and will be uniformly enforced throughout the Union, is the logical way to proceed. Any increase to the EU's competence to legislate using a principles-based approach along these lines could have a beneficial impact on the internal market at large, and on the UK economy in particular.

We should be pushing to ensure an appropriate system of checks and balances between law makers, law enforcers, the judiciary and the public they represent.

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

This is the subject for a whole book, or at least a consultation in its own right. It is also fundamentally important to this consultation. Put simply, in an interconnected international economy it is not clear through which jurisdictions personal data (or parts of a larger data "whole") may have passed, lending credence to the vital need for an international approach and as much agreement as possible.

The World Trade Organisation (WTO) and International Telecommunication Union (ITU), as well as the Internet Governance Forum (IGF) could have roles to play in addressing this, as will the EU and the UK (as a nation state and as a part of the EU) – thereby providing the UK with two voices in the forthcoming debates. Future discussions with other trade partners, improved policy coordination, striving for a more uniform international framework in respect of information rights – all of these represent future opportunities and challenges which are relevant to this discussion. Of particular interest to the UK could be the India-EU Free Trade Agreement (FTA) discussions, and this was on the agenda when Prime Minister Cameron visited India last year, with discussion believed to be on-going. Whilst the EU position in this area remains unclear, this is unhelpful to the successful conclusion of negotiations where the UK could turn out to be Europe's principal beneficiary.

We should also recognise fully the consequences of the data choices we are in the process of making. Cloud computing, for example, is seen by all national administrations as a way to stimulate economies in Europe – but if the benefits of cloud computing are so neutralised that business chooses not to implement on the scale envisioned (or adopt it at all…) because of data protection concerns, the policy choices made will be questioned.

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

It was J F Dulles who stated in 1947 that "Europe must cooperate or Europe will perish." Today's EU membership for the first time in centuries comprises democracies, at peace, and with similar value systems to our own (though differing levels of ability to actually implement EU legislation). We sometimes forget to acknowledge this. Spending time to assist those countries less fortunate than ourselves via the provision of expertise would be a wise investment if we want to build a broader international consensus and help to ensure that the UK either drives the data protection debate, or at least preserves its ability to meaningfully inform discussion. Going it alone on data protection is an amusing academic exercise but no more than this. Alternatively we could join the bus late… but we have tried that in Europe before.

We believe that the data protection issues of the future will be increasingly international in character. The most appropriate strategy in the UK is to continue to push for a common global framework for Information Rights that can be effectively nationally enforced. Such an agreement is unlikely to ever come to pass, but at least a regional approach is a positive step in such a direction. It is also already UK Government policy. The quest for a common framework is already proving difficult enough, as the European Parliament's vote to suspend the Safe Harbor agreement demonstrates.

The general direction of travel we are seeing worldwide is in the direction of more rights for citizens, and this to our mind includes the right to have more control over their own data, with the Courts as the ultimate destination for disputes - howsoever that might be reflected in legislation.

The issue of "Balance" *is* relevant to this consultation – but in the context of data risks versus data rewards and how best to achieve this, since we all share a common goal of seeking improvement.

David Happy and Richard Ward

Digital Policy Alliance

June 2014