Balance of Competences Consultation Response

Information Rights

June 2014

This is a joint response from the Law Society of England and Wales and the Law Society of Scotland (the Law Societies).

The Law Society of England and Wales is the independent professional body, established for solicitors in 1825, that works globally to support and represent its 160,000 members, promoting the highest professional standards and the rule of law.

The Law Society of Scotland is the professional body for Scottish solicitors, established in 1949. It is not only the representative and regulatory body for all practising Scottish solicitors but also has an important duty to work towards the public interest.

Introduction

I. The Law Societies' Privacy, Technology Law and EU Committees have considered the Call for Evidence on EU Information Rights. The Law Societies are contributing to a number of Calls for Evidence as part of the Review of the Balance of Competences. This submission should be read in the wider context of all our consultation responses.

II. UK membership of the EU has brought significant benefits to solicitors, law firms and their clients, most particularly through the ability to trade, provide services and establish across the EU and to seek effective redress to cross-border legal issues.

III. The legal services sector plays a key role in the UK economy, assisting the UK's competitive advantage and in improving the efficiency of doing business. Legal services directly contributed £28.6 billion to the UK economy in 2011. This included almost £4 billion of exports – a substantial volume of which was generated through trade with EU Member States.

IV. UK legal practitioners represent clients who are involved in cross-border legal issues due to the exercise of their free movement rights provided in the Treaties. This forms a significant part of their business and source of expertise. It is for these reasons that the Law Societies and the legal profession have an interest in the stability of the UK's position within the EU and the future role of the UK at the heart of EU law-making.

V. The Law Societies accept that there is a debate as to the appropriate level of EU competence in various policy areas and will input into the parts of the Review of the Balance of Competences of most relevance to the legal profession.

General remarks

1. In responding to this call for evidence and assessing advantages and disadvantages, we assume that there would be some national legislation in place to protect individuals' right to privacy and data protection. Consequently we believe that EU action in this area should be assessed against the added value it brings to national legislation only.

2. Our response to this consultation is based on our members' experience with data protection, as data controllers themselves, and from advising clients on their data protection rights and obligations. We also note that 'hard' empirical evidence is generally not available to inform most of the questions posed by the Review. However, where possible we have sought to identify relevant statistics and reports.

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?

3. There are a number of benefits that arise from data protection legislation. Individuals benefit from additional personal information rights; greater confidence in how their personal data will be handled by commercial and public providers of various services and the probability that they have suffered less from misuse of personal data or poor information handling. This trust is essential for all sectors of society, including the legal profession which depends on its clients having faith in their data being kept confidential.

4. A single set of rules, applied EU-wide, is also of great advantage to organisations, which operate in all or many EU member states and hold and control large datasets and databases. There are clear cost savings and efficiencies in having a single model for holding such data.

5. This may in some instances primarily concern large organisations such as banks and telecom operators, but increasingly also includes SME's. This is particularly the case for innovative IT-focussed start-ups who see the whole of Europe, if not the whole world, as their market. They would likely abandon the UK, or indeed the EU, if faced with the task of embedding 28 different sets of Data Protection rules in their apps/products. In that scenario, it would make financial sense for them, for instance, to develop their offering in the US, a comparably-sized market with one set of DP rules

6. The most often cited disadvantage of the EU legal framework for data protection is its complexity. This can be disadvantageous for both individuals and data controllers.

7. For individuals it may be difficult to enforce rights arising from a framework that can be difficult to understand. There is evidence, for example the Bichard Inquiry, that some individuals may have suffered from organisations (particularly in the public

sector) misunderstanding their rights to share data. The detriment may however equally occur in cases where a data controller unlawfully passes on personal data to a third party and the individual concerned does not complain because he or she is unaware of their legal position.

8. For data controllers the complexity create difficulties because of uncertainty around what their obligations are and the cost associated with compliance. It should be said however that it is not possible to predict what the administrative requirements and compliance costs might be in a scenario of domestic legislation only. All legislation, be it EU or domestic, should be proportionate and fit for purpose.

9. The key driver for EU legal developments in the area of data protection has been the need to ensure the free flow of data in the context of trade within the internal market. The possible disadvantage of current EU data protection legislation in terms of its complexity is partly linked to the continuing large differences in national implementation of the 1995 EU Directive.

10. Further standardisation of data protection legislation thus has the potential to decrease the disadvantages in terms of compliance cost. This makes sense in an increasingly international and digital business environment. For companies wishing to establish or expand within the internal market it is simpler to have one set of data protection rules to comply with.

11. This may also bring advantages in terms of protecting citizens' rights better in a digital age where national action alone would not be able to create an equal level of protection. According to research conducted for the World Economic Forum[1] two in three respondents believed that using the Internet put privacy at risk. Since the internet is global it seems sensible that attempts of furthering rights online should be taken on a level that covers as many as many states as possible.

12. The advantages and disadvantages for lawyers, their clients and the courts are largely mirrored by the general impact of the EU information rights regime on businesses, individuals and the public sector. Further, one specific problem that the legal profession has experienced in regards to the 1995 Directive relates to access to information in cross-border litigation. Courts when faced with discovery requests have tended to apply divergent interpretations of 'legitimate interest' and whether this exemption permits the transfer of information containing personal data. This is another example of where divergent Member State interpretation of the Directive can bring problems, suggesting the need for greater consistency at EU level.

13. In addition, information rights is a growing legal discipline and lawyers are prominent in providing advice and support to businesses and individuals. Handling sensitive personal data, managing information and maintaining a high degree of confidentiality are traditional skills and strengths of lawyers. Many UK law firms offer their services cross border or work for clients wishing to trade within the internal market and can

[1] The Internet Trust Bubble, Global Values, Beliefs and Practices, 2013

therefore add value through familiarity with the EU data protection framework. The development of statutory information rights builds on this tradition.

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?

14. The assumption behind the exercise of the EU's single market competence in relation to information rights appears to be that individual data protection rights and economic growth are mutually reinforcing. Consequently, some degree of EU level data protection is needed to maintain trust in business. Similar assumptions have underpinned the development of similar frameworks including the UK's Data Protection Act 1984, Council of Europe Convention 108 and the 1980 Organisation for Economic Co-operation and Development (OECD) Privacy Principles guidelines.

15. From time to time there have been suggestions that such legislation has stifled innovation in the development of IT services. The emergence and rapid growth of the Internet against the backdrop of pre-Internet regulation (for example DPA 1984) and of e-commerce on the World Wide Web alongside Directive 95/46 is strong 'big-picture' evidence that data protection rights, innovation and economic growth are entirely compatible.

16. More recently the World Economic Forum's multi-year *Rethinking Personal Data*[2] initiative has argued that personal data is an untapped opportunity for socioeconomic growth but that unlocking its full potential means that a number of information rights issues including privacy and data ownership need to be further addressed.

17. This implies that it is essential for there to be a legal framework in place that instils trust in users. There is also a risk that EU data protection regulation could stifle economic growth if the framework is not modernised to further Internet-based innovation.

18. As such reforms are ongoing it remains to be seen whether the new framework will 'strike the right balance'. An overly process-driven and bureaucratic approach to individual data protection rights could adversely affect economic growth without providing any benefit to individuals. Equally, economic growth could be harmed if individuals possessed such minimal substantive rights that they could not trust the public and private sectors to protect their data properly.

[2] http://www.weforum.org/issues/rethinking-personal-data

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?

19. EU action to facilitate the exchange of data with third countries has been helpful in moving towards a level playing field for European data controllers. This is particularly the case for the adequacy decisions on third countries' data protection standards. Disparities however still exist in how Member States have implemented the 1995 Directive's other provisions concerning the transfer of data to third countries.

20. Consequently, and in view of technological developments, there is a need to refresh the legal framework in order to strengthen trust in international flows of data. The World Economic Forum[3] argues that '*just as tradeable assets like water and oil must flow to create value, so too must data…But for data to flow well, it requires the same kinds of rules and frameworks that exist for other asset classes.*' It further suggests that the reality has been different and that '*individuals are beginning to lose trust in how organisations and governments are using data about them, organizations are losing trust in their ability to secure data and leverage it to create value, and governments are seeking to strengthen trust to protect an individual's privacy'*.

21. The Societies are also aware of concerns that have been expressed, particularly resulting from the revelations by Edward Snowden, as to how secure systems are in third countries for the processing of data of or about EU nationals. We note that work is ongoing to revise certain safe-harbour agreements as an essential element of continued trust of European-based users, be they private individuals or corporates, of online and internet-based services. This is also an important issue for many solicitors and their clients. For example many outsourcing organisations used in disclosure exercises are located in third states.

22. A further issue is that many organisations face practical difficulties when faced with requests for information from regulators/courts in a third state where the transfer of the information sought would be a breach of the applicable national data laws of a Member State.

23. The UK benefits from being able to negotiate, as part of the EU, a large trading block, for the revision of these international bilateral agreements to govern the basis on which such data may be processed in third countries.

24. The major challenge of social networks appears to be users' own behaviour and the corresponding amount of personal information that is now available online. Further, Internet search engines make it possible to easily collect and gather data about individuals, assembling fragments of information that on their own might not infringe an individual's right to privacy. However, pieced together with the help of an online

[3] World Economic Forum, *Rethinking Personal Data: Strengthening Trust* May 2012

search engine, the compiled fragments might provide a disproportionate publicly available amount of information on an individual that there is no legitimate interest in having available. The recent Google ruling (C-131/12) of the Court of Justice of the European Union (CJEU) highlights the need to update the framework. The question of whether search engines should or should not be covered by any obligation to delete personal data was clearly not considered at the time of adoption of the 1995 Directive and it would appear desirable to improve legal certainty on these matters in the new legislation under way. This in particular concerns the uncertainty surrounding some aspects of the Court ruling, notably whether potentially other online services such as online archives, could be interpreted to fall under the Court's definition of a search engine.

25. An updated legal framework and better bilateral agreements between the EU and various third countries may however only be part of the solution (and the latter may not be altogether realistic to achieve). Technological developments and the move towards Internet of Everything, e.g. ubiquitous / mobile and cloud computing and big data analytics, generate an increased quantity of data and increased capacity to analyse it. Massive data collection and analysis may be making the individual monitoring and enforcement of individual information rights less relevant.

26. Possible solutions to this problem include privacy enhancing technologies and privacy by design (baking-in rather than bolting-on) and these appear to be under-emphasised in the current framework. Further there is a need for increased focus on security to ensure that data controllers take the necessary steps to protect their data.

27. This includes a possible need to increase efforts in the area of cyber security and fraud. This is most recently evidenced by BIS' Information Security Breaches Survey 2014, which indicates that whilst the number of cyber attacks is slightly down their severity and cost is up.

28. It needs to be stressed that the speed of development of the Internet and technological solutions will mean that any legal system will struggle to keep up with the challenges that are being posed. There is not one solution; legal and technical solutions need to work together. Equally, EU and national action can and should be complementary. BIS has for example been doing and should continue to do important work on cyber security. This need not conflict with EU action in the area. The two should feed into each other as national action alone and in an isolated manner is not likely to be able to effectively resolve any of the above issues.

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?

29. Under the proposals, individuals would acquire strengthened rights and potentially greater security of their data. Businesses handling data across Europe should experience reduced overheads and cost through harmonisation. They would also benefit from the abolition of the requirement to notify the Information Commissioner that they are processing personal data and could benefit indirectly if the new framework increases their customers' trust. Disadvantages to businesses include some additional costs from implementing a new system and potentially complying with some new requirements.

30. The new Regulation is also an opportunity to strengthen legal professional privilege and lawyer-client confidentiality which are long-established legal principles underpinning the administration of justice. Professional secrecy for lawyers has been recognised in case-law as a fundamental right for its role in securing access to justice and upholding rule of law (Van der Mussele v Belgium (1983) 6 EHRR 163, AM & S Europe Ltd v Commission of the European Communities (Case 155/79) [1983] QB 878, and Campbell v United Kingdom (1992) 15 EHRR 137). This needs to be clearly reflected in the new data protection legal framework as advocated by both the Law Societies and the Council of European Bars and Law Societies. This privilege should clearly cover all registered lawyers, including in-house lawyers and not just those in private practice.

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?

31. According to the latest Report from the Commission on public access to European Parliament, Council and Commission documents (relating to 2012), nearly 23% of applications were from academia. The second most active category of applicants were law firms at just under 14% (up from 11% in 2011). On the basis that academics and lawyers are acting rationally to their own advantage or that of their institutions or clients it can be inferred that the right to access documents of the EU institutions has been advantageous to at least some groups in the UK. This view is reinforced by the report's breakdown of the geographical origin of requests. This shows that the second highest percentage of requests came from the UK and that, unlike most other countries, this percentage has been increasing year by year from 7.24% of all requests in 2010, 8.59% of requests in 2011 and 10.17% in 2012.

32. A right to access EU institutions' documents is a key element in fostering public trust for the EU public bodies and enabling scrutiny over them. The Societies therefore support the right of access subject to legitimate public and private interest.

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

33. UK citizens' ability to access official information about public authorities in the UK is governed by the Freedom of Information Act and the Freedom of Information (Scotland) Act 2002, the Environmental Information Regulations and the Environmental Information (Scotland) Regulations 2004 (which implement Directive 2003/4/EC) and the common law. The Freedom of Information Act regimes and Environmental Information Regulations regimes complement each other well and share many common characteristics. We do not perceive any requirement for further EU action in the area of citizens' rights to information of UK public authorities.

34. Clearly, access to official EU documents requires EU action. We are however not in a position to comment on whether the action the EU has taken in this regard is insufficient or excessive.

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?

35. Personal data flows across national and regional boundaries. Independent national frameworks offer the potential for a framework that meets the distinctive needs of that nation. However, there will be costs associated with negotiating and implementing bilateral agreements and complying with the resulting obligations. These bilateral agreements will also need to take account of potential further transfers of data to a third country and so forth. This spiralling complexity could put a break on personal data flows. This would have a detrimental impact on global commerce and national prosperity.

36. A way of avoiding the spiralling complexity involved in accounting for onward data transfers in bilateral agreements between nations is for regional frameworks to be established. For the UK this would imply a framework at the level of the EU. The possible disadvantage to nations is that each nation is likely to have to compromise its preferred national approach depending on the greater or lesser degree of commonality between national frameworks. In practice, regional groupings of nations may however share a common view about the principles involved. An alternative approach would be to establish independent national frameworks for handling data within each nation and establish entirely separate and common principles for handling data that originated in another country. Distinguishing data in this way could be extremely difficult and costly in practice. As well as the need for some compromise, the development of regional frameworks also limits the scope for independently negotiated bilateral agreements between nations within the region and other nations. For example, an independent bilateral agreement between the UK and the USA or China about personal data flows would not be compatible with this model (and is not compatible with the EU Data Protection Directive).

37. Finally, if a global framework could be achieved, the necessary compromise between independent nations would be even greater than in the regional model. Given fundamental differences of approach between countries like the United States and countries like Germany and France it is unlikely that it could be achieved. This suggests that a regional model could enable the right balance between flexibility at the national level and co-ordination at the trans-national level to enable trans-national data flows. It would also suggest, however, that agreements between regions, for example the EU and the US, should have a more important role to play than they currently do.

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?

38. The Law Societies are not aware of any evidence of this.

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?

39. Considering the Treaty of Lisbon has only been in force since 2008, and that the proposed Data Protection Regulation has not yet been adopted, it is not possible to draw any firm conclusions on the impact at this stage.

40. The change however can be seen as an indication of an increased focus on and perceived need to further protect personal data consistent with the inclusion of the Charter of Fundamental Rights into the Treaties.

41. The Google ruling, as referenced above, and, possibly more significant, the data retention ruling (joint cases C-293/12 and C-594/12) can be seen as indications of the CJEU taking a firmer stance on the protection of personal data (Art. 8) and the right to privacy (Art. 7). In the data retention ruling, the CJEU determined that the EU legislator had exceeded the limits on its authority imposed by the principle of proportionality and the need to balance the public interest with individuals' fundamental rights[4].

[4] http://curia.europa.eu/juris/documents.jsf?num=C-293/12

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?

42. With the growth of an Internet of Things, ubiquitous, intelligent and wearable computing, the need for provisions governing transient data processing by individuals (currently exempt from the data protection principles under the domestic purposes exemption) may need to be reconsidered. Whilst it might not be appropriate directly to regulate individuals undertaking potentially highly intrusive and covert data processing it may be necessary to regulate the enablers of such surveillance.

43. The challenge / opportunity would be to develop principles of privacy by design and to find a way to regulate them into the design of products and services in such a way that the users of those products and services did not themselves have to be regulated in order to secure respect for others' information rights. It may, for example, become possible to undertake 'on-the-fly' processing of visual and auditory data about an individual using knowledge-bases that contain no personal data about that particular individual but which nevertheless yield highly accurate data about them.

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

44. The Law Societies are not aware of any other such evidence.