HM Government

Review of the Balance of Competences between the United Kingdom and the European Union

Information Rights

December 2014

Review of the Balance of Competences between the United Kingdom and the European Union

Information Rights

Contents

Executive Summary

This report examines the balance of competences between the European Union (EU) and the United Kingdom (UK) in the area of information rights. It is led by the Ministry of Justice. It is a reflection and analysis of the evidence submitted by experts, non-governmental organisations, business people, Members of Parliament, and other interested parties. It includes evidence submitted in writing or orally, as well as a literature review of relevant material. Where appropriate, the report sets out the current position agreed within the Coalition Government for handling this policy area in the EU. It does not predetermine or prejudge proposals that either Coalition party may make in the future for changes to the EU or about the appropriate balance of competences.

The report examines the rapid changes in technology that have taken place over the past decade and the impact this has had on safeguarding personal data. In particular, it considers how the Data Protection Directive has struggled to adapt to technological changes such as cloud computing, the growth of online commerce, international data flows and social networks. The challenge of future-proofing new legislation in light of the diverse and unpredictable uses of data is also considered.

Chapter One describes the development of EU competence in both data protection and access to information.

Section 1.1 outlines the current state of competence in both areas and explores evidence received on the significance of Article 16 of the Treaty on the Functioning of the European Union.

Chapter Two summarises and considers the evidence received on the impact of the EU's competence on the UK. The chapter is divided into two parts:

- Evidence on the impact of EU competence on the UK; and
- Evidence on the level at which action should be taken.

Section 2.1 covers evidence on the impact of EU competence on the UK. In the area of data protection, a range of respondents felt EU competence had been advantageous to the UK. Many suggested that the current Directive struck a good balance between the interests of data controllers and citizens, and that in some cases this has been due to the UK's particular implementation of the Directive. However, almost all respondents felt the Directive has not kept pace with rapid technological changes. This is particularly relevant in light of complex developments such as cloud computing.

In the area of access to information, a number of respondents including those from legal institutions, think tanks and the insurance industry, were of the view that EU competence has had a positive impact on the UK's national interest to the extent that it has increased the transparency of EU institutions. Transparency helps UK businesses to hold the EU to account, predict the impact of its legislation, and influence policy before it becomes legislation. A few respondents highlighted operational problems with both the Access to Documents Regulation and the Environmental Information Directive.

Section 2.2 considers evidence on the level at which action should be taken. In the domain of data protection, respondents generally argued that action needed to be taken at an EU or international level. Some considered this was a necessity because modern data flows did not recognise national borders. Others also based their argument on the advantages of common standards to businesses and consumers. However, views were mixed about where the balance should be struck between allowing Member States flexibility and pursuing greater uniformity of standards.

In the domain of access to information, a range of respondents thought there was no need to extend EU competence in this domain, and that efforts should be focused on improving the EU's implementation of the existing Access to Documents Regulation. However, some suggested there was an opportunity for the UK to promote its freedom of information culture across Europe. While some respondents argued that EU legislation could reduce a perceived overuse of exemptions from disclosure in the UK, others stressed that any EU legislation would only be valuable if European standards were raised to those of the UK.

Chapter Three looks at the future opportunities and challenges in the area of information rights. The evidence submitted identified several major future challenges for the UK and the EU.

In the domain of data protection, respondents identified the proposed EU Regulation as a key opportunity and challenge for the future. While some respondents welcomed the Commission's action in this area, they queried whether the proposed provisions struck the correct balance in protecting individuals. Many highlighted the instrument's prescriptive nature. This may have a negative impact on several business sectors.

Flexibility was seen by many as a vital element for any legislation that aims to cover a wide range of sectors and organisations, of all sizes, across 28 different Member States. Flexibility is also important for any legislation which aims to stand the test of time in the face of unpredictable technological advances and changes in the way we process and provide our personal data.

Other challenges were identified, such as the rise of Big Data, cloud computing, and the Internet of Things (IoT). Respondents again emphasised the need for any future framework to be sufficiently flexible to adapt to these changes. Many respondents also evoked a need for flexibility to allow for different circumstances of organisations such as Small- and Medium-Sized Enterprises (SMEs), industry sectors, and different cultures in Member States.

In the domain of access to information, respondents highlighted an increasing potential tension with data protection requirements; the increasing volume of data being collected and consequently increasing number of requests for access to, and the challenges of identifying official information as the public sector becomes increasingly diversified.

Four broad cross-cutting themes are identified throughout the report:

(i) The need to be aware of interaction between principles of data protection and access to information;

(ii) The need to make sure any legislation is future proofed, given the potential for further unpredictable changes in data use;

(iii) The need to find a balance between an approach towards greater common standards, and sufficient flexibility for different sectors, and the different circumstances in Member States;

(iv) The need for greater understanding and engagement with stakeholders in this complex, diverse, and rapidly-changing field.

Introduction

This report is one of 32 reports have been produced as part of the Balance of Competences Review. The Foreign Secretary launched the Review in Parliament on 12 July 2012, taking forward the Coalition commitment to examine the balance of competences between the UK and the EU.

It will provide an analysis of what the UK's membership of the EU means for the UK national interest. It aims to deepen public and Parliamentary understanding of the nature of our EU membership and provide a constructive and serious contribution to the national and wider European debate about modernising, reforming, and improving the EU in the face of collective challenges. It has not been tasked with producing specific recommendations or looking at alternative models for Britain's overall relationship with the EU.

This review is broken down into a series of reports on specific areas of EU competence, spread over four semesters between 2012 and 2014. More information can be found on this review, including a timetable of reports to be published, at www.gov.uk/review-of-the-balance-of-competences.

Scope and Structure of this Report

This report explores the development of EU competence in the field of information rights, the impact of how that competence has been exercised up to the present day, and also possible future developments. Taking its lead from the key rights that now appear in the EU Treaties, this review will focus on data protection rights and the right to access official information.

The Treaty on European Union states in Article 4.2 that national security remains the sole responsibility of each Member State. Therefore, this review does not propose to examine information rights in the context of national security.

- Chapter One outlines the history of the development of the EU's information rights policy for both data protection and access to information. This chapter also looks at the current nature of competence in these areas.
- Chapter Two assesses the impact on the UK's national interest of the current state of competence in information rights.
- Chapter Three considers the future of EU competence and identifies potential challenges and possible options.

Engagement with Interested Parties

The analysis in this report is based on 48 pieces of evidence in response to a Call for Evidence by the Ministry of Justice from 28 March 2014 to 1 July 2014. It also draws on notes of workshops held during the Call for Evidence period and existing material such as parliamentary reports and academic literature. Four workshops were held to collect evidence: one in London, one in Edinburgh, one in Belfast, and one in Brussels. The report also takes account of evidence submitted to previous Calls for Evidence.

A list of those who submitted evidence can be found in Annex A, with details of those who participated in the workshops in Annex B. A list of further evidence drawn upon can be found in Annex C.

Areas of Overlap with Other Reports

The report has drawn on themes touched on by other Review of the Balance of Competences between the United Kingdom and the European Union reports such as:

- Subsidiarity and Proportionality (published in parallel);
- Environment and Climate Change (2013);
- The Single Market (2013);
- Police and Criminal Justice (published in parallel); and
- Fundamental Rights (2014).

Definition of EU Competence

For the purposes of this review, we are using a broad definition of competence. Put simply, competence in this context is about everything deriving from EU law that affects what happens in the UK. That means examining all the areas where the Treaties give the EU competence to act. This includes the provisions in the Treaties giving the EU institutions the power to legislate, to adopt non legislative acts, or to take any other sort of action. It also means examining areas where the Treaties apply directly to Member States without needing any further action by the EU institutions.

The EU's competences are set out in the EU Treaties. These provide the basis for any actions the EU institutions take. The EU can only act within the limits of the competences conferred on it by the Treaties, and where the Treaties do not confer competences on the EU, they remain with the Member States. There are different types of competence: exclusive, shared, and supporting.

- In areas where the EU has exclusive competence, only it can act. Example areas are the customs union and common commercial policy.
- In areas of shared competence, such as the Single Market, environment, and energy, either the EU or Member States may act, but if the EU has already acted first, the Member States are prevented from doing so afterwards.
- In areas of supporting competence, such as culture, tourism, and education, both the EU and the Member States may act. Prior action by the EU in this case does not prevent the Member States from taking action of their own.

When exercising competence, the EU must act in accordance with fundamental rights (such as freedom of expression and non-discrimination) as set out in the Charter of Fundamental Rights. It must also act in accordance with the principles of subsidiarity and proportionality.

Under the principle of subsidiarity, if the EU does not have exclusive competence, it can only act if it is better placed than the Member States to do so because of the scale or effects of the proposed action. Under the principle of proportionality, the content and form of EU action must not exceed what is necessary to achieve the objectives of the EU treaties.

Chapter 1: Information Rights in Context

1.1 This chapter contains an overview of the development of competence in data protection and access to official information. It does not deal with information rights in the context of national security, as national security remains the sole responsibility of each Member State and is therefore outside the scope of this report.

1.2 In relation to data protection, reference is made to common concepts which are explained below.

Data Protection – Common Concepts

- Personal data means any information which can identify a living individual, otherwise known as a data subject. It can include your name, address, and date of birth. It can also extend to information about purchases you have made, your health history, or even your library records.
- In the UK, the rights contained in the Data Protection Directive have been transposed into domestic law through the Data Protection Act 1998 (DPA 1998). They include a right for individuals to access the information held about them; a right to object to it being processed; a right to object to having decisions taken based on automated processing; a right to rectify inaccurate data or have it erased, and a right to claim compensation for breaches of these rights.
- Data Protection rights are reinforced by corresponding obligations of data controllers to guarantee the above rights. Further responsibilities on controllers include the obligation to have lawful grounds for processing and to respect sensitive data in particular. They also include the obligations to be transparent about processing, to disclose personal data in a fair and lawful manner, and to have appropriate security measures.
- A data processor is a person or body processing personal data on behalf of the data controller but not making the key decisions.

Data Protection

The UK Dimension

1.3 In the UK, it has long been established that personal information should be protected in certain contexts. We expect doctors to protect confidential information about their patients, and lawyers about their clients. Principles such as these existed long before any law dedicated to data protection was passed.

1.4 We can trace the development of legislation in this area back to at least 1970 and the establishment of the Younger Committee.[1] This Committee conducted a survey about public attitudes to privacy. More and more personal information was beginning to be held on computer systems, and the survey indicated that people's fears were growing about what their data would be used for and who could access it.

1.5 In the meantime, certain protections began to be provided in consumer law regarding the use of personal data for decisions about creditworthiness. The Consumer Credit Act of 1974 allowed individuals to access information held about them by credit reference agencies and, if necessary, amend it. In the fields of healthcare and education, similar rights of access to information were created in statute.

1.6 In 1976, the Lindop Committee was established and charged with exploring what could be done to improve the protection of personal data.[2] The Committee reported in 1978 and recommended the creation of an independent body which would draw up statutory codes of conduct for various sectors, both private and public.

1.7 The UK also took note of important international developments which were happening at the same time. The passing of the Data Protection Act 1984 (the background to which is explained in more detail below) is evidence of this.

The International Dimension

1.8 Many developments in the 20th century led some countries to adopt data protection measures. This was in part in response to the growing use of computers to store and process personal data, which meant rules were needed to protect it from being stolen or disclosed to those without authorisation.

1.9 Personal data also needed to be kept accurate: many automatic decisions were being taken which had an impact on people, such as those concerning pensions, insurance, or creditworthiness. As more and more countries enacted data protection legislation, fears grew in some quarters that these measures would stifle the flow of data that was becoming increasingly important for international trade.

1.10 In 1980, the Organisation for Economic Cooperation and Development (OECD) issued a set of guidelines for how personal data should be protected. The OECD stated that its member countries have a common interest in protecting both personal data and the global free flow of information.

1.11 In 1981, the Council of Europe introduced a new international binding agreement on data protection, which is commonly known as Convention 108.[3] The aim of this Convention is to reconcile data protection with the free flow of information. Focusing on the automatic processing of personal data, it set out many key principles that remain central to data protection law today. These include the principles that personal data be processed fairly and lawfully, that it be processed only for specific purposes, and that it be accurate and kept up to date. It established rights of access to personal data, rights to rectify and erase personal data, and it also designated authorities who could cooperate to ensure the protection of personal data across borders.

---

[1] In 1970, the UK Government appointed Kenneth Younger to chair a Committee on Privacy which reported in 1972. HMG, *Younger Committee's Report on Privacy (*Cm 5012) (1972).

[2] In July 1975, the UK Government announced the setting up of a Data Protection Committee under the Chairmanship of Sir Norman Lindop. HMG, *The Lindop Report* (Cm 7341) (1978).

[3] The UK signed Convention 108 in 1981 and ratified in 1987. Regulation 98/59/EC of the Council on Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981.

1.12 The Convention's general principles were incorporated into the Data Protection Act 1984. This established in UK law the rights for individuals to have access to data that was held about them and to correct any inaccuracies.

The EU Dimension

1.13 Specific EU competence in the area of data protection is a relatively recent development: key steps were taken to a similar timescale as the developments described above. A Treaty right to data protection and associated legislative competence was only explicitly provided for in the Treaty on the Functioning of the European Union (TFEU) by the Treaty of Lisbon, which came into effect in 2009.

1.14 The original Treaties of 1952 and 1957, which established the European Communities, were silent on whether EU law guaranteed minimum rights for individuals in the field of data protection. Instead, the original Treaty provisions gave the EU express competence to legislate in order to establish a single market.

1.15 However, the European Court of Justice (ECJ) increasingly recognised the importance of interpreting EU law to include minimum safeguards to the rights of individuals in circumstances where the operation of the Single Market had a potential effect on those rights. Without such protection, it was considered that the movement towards a single market would not enjoy the necessary public confidence. Accordingly, in the course of giving effect to such rights, the Court recognised that the right to protection of personal data is a general principle of EU law.

General Principles of EU law

General principles are part of the EU's primary law, with which the EU institutions and Member States are bound to comply.[4] They derive from the traditions of national legal systems and have been recognised in EU law by the ECJ. General principles are applied by the ECJ and domestic courts when determining the lawfulness of legislative and administrative measures within the scope of EU law. This means that the EU and, in certain circumstances, its Member States, must comply with the general principles. General principles are also an aid to interpretation in cases where the meaning of EU rules is open to doubt. Other examples of general principles of EU law are subsidiarity and proportionality, which are the subject of a separate report in the fourth semester of the Balance of Competences Review.[5]

1.16 Having recognised the right to protect personal information in this way, the ECJ has taken it into account when interpreting and ruling on the validity of acts of the EU and its Member States.

1.17 Following these developments in the recognition of data protection rights at EU level, the EU asserted competence to legislate in the field of data protection for the first time in 1990. The legal base for proposing legislation (which led to the 1995 Directive) was the then Article 100a of the Treaty Establishing the European Community. Accordingly, the EU's competence to legislate on data protection, prior to the coming into force of the Lisbon Treaty, was an expression of its competence to take appropriate measures to encourage the free movement of goods and services within the EU.

---

[4] Yassin Abdullah Kadi, and Al Barakaat International Foundation v Council of the European Union, Commission of the European Communities, United Kingdom of Great Britain and Northern Ireland, Case C-402/05 and Case C-415/05, [2008] para 308.

[5] HMG, *Review of the Balance of Competences between the United Kingdom and the European Union: Subsidiarity and Proportionality* (published in parallel).

1.18 To that extent, the EU's ability to legislate took effect subject to the wider limitations on its competence. Accordingly, the 1995 Directive recognised that Member States have sole responsibility for safeguarding their national security, and permitted them to legislate to impose restrictions on obligations and rights under the Directive where necessary for this purpose.

1.19 That said, and despite its status as a single market measure, subsequent ECJ case law made it clear that, in its view, there did not need to be a specific link to free movement in order for the Directive to apply in a given situation.[6]

Case Study: Lindqvist Case C-101/01

Mrs Lindqvist, who worked for the Catholic Church, had set up internet pages at home on her personal computer in order to help parishioners prepare for their confirmation. The pages contained information about 18 colleagues in the parish, such as their names, employment details, hobbies and telephone numbers. The pages were linked to the Swedish Church's website.

The Swedish public prosecutor charged Mrs Lindqvist with breaching Swedish data protection rules. The Swedish court referred several questions to the ECJ, including on the nature of Article 3(2), which exempts household processing from the scope of the Directive.

In the course of considering the referred questions, the ECJ looked at the legal base in Article 100a TFEU. It held that the use of Article 100a TFEU to enact the Directive 'does not presuppose the existence of an actual link with free movement between Member States in every situation referred to by the measure founded on that basis'.[7] In short, although enacted as a free movement measure, the Directive is also capable of regulating processing that is done for non-free movement purposes.

1.20 These case law developments exerted a clear influence on the approach taken when the Treaty of Lisbon was negotiated. That Treaty sought to recognise the EU's right to legislate on data protection in clear terms. It did so in the form of Article 16, which provides:

Article 16 TFEU[8]

1.21 Everyone has the right to the protection of personal data concerning them.

1.22 The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.

1.23 The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

---

6 Rechnungshof v Osterreichischer Rusterfunk and Others and Christa Neukomm, Case C-138/01, [2003]; Bodil Lindqvist v Kammaraklagaren, Case C-101/01, [2003].

7 Kathleen Gutman, *The Commission's 2010 Green Paper on European Contract Law: Reflections on Union Competence in Light of the Proposed* (2010).

8 Treaty on the Functioning of the European Union (TFEU).

1.24 The following chapter sets out the UK Government's view on what Article 16 means for the current state of competence for the EU, and other views that were submitted in evidence.

Access to Official Information

1.25 High levels of public disinterest or even distrust of the EU had been noted in the lead up to the negotiation of the Maastricht Treaty. For this reason Declaration 17 annexed to that Treaty recommended that the EU Commission and Council work together to improve public access to information of the main EU institutions. This was inspired partially by a wish to regain this lost public confidence and interest through transparency and greater accountability.

1.26 The result was a Code of Conduct, which was adopted formally and came into force in 1994, on public access to Commission and Council documents.[9] This created a right of access to Council and Commission documents, subject to exceptions, and a right of review if documents were refused. There were subsequent disputes in EU court proceedings about the correct legal basis for the Code of Conduct and whether it was right for the access arrangements to be limited to Council and Commission documents.

1.27 Article 255 of the 1995 Treaty of Amsterdam provided a specific right of access to official documents of EU institutions for EU residents. It also provided the Council with a power to set out general principles and limits to the right in further legislation. The Article 255 right and legal base have since been replicated and replaced by Article 15(3) of the TFEU during the negotiation of the Treaty of Lisbon.

1.28 Article 15(3) of TFEU now gives EU residents a right of access to documents held by the EU's main institutions, bodies, offices, and agencies. That Article also provides that the European Parliament and the Council may establish general principles and limits on how the right may be used. These should be set out in a Regulation, passed using ordinary legislative procedure.

1.29 The UK retains exclusive competence to pass legislation relating to access by the public to information held by public authorities in the course of their duties.

1.30 The EU has exercised its competence under Article 15(3) by enacting the Public Access to Documents Regulations (1049/2001) which regulate the right of access to documents held by EU institutions. The Regulations resemble domestic Freedom of Information legislation, particularly the idea that rights of access are subject to exemptions which protect important interests, for example; personal data, national security, commerical sensitivity. The recent Danish Presidency made proposals to update the Regulation but these were unsuccessful.

[9] Council Decision 93/731/EC of the European Council on Public Access to Council Documents,1993 and Council Decision 94/90/EC of the European Council on Public Access to Commission Documents, 1994.

Environmental Information

1.31 In 1984 the UK's Royal Commission on Environmental Pollution recommended that there should be a presumption in favour of unrestricted access for the public to information which the pollution control authorities obtain or receive by virtue of their statutory powers.[10] In line with the formulation recommended by the Royal Commission, the government proposed a resolution during the UK Presidency of the European Community in 1986 calling for access to environmental information to be made available throughout the Community. In 1987 the Council of the European Communities passed a resolution to this effect.

1.32 The direct result of the 1987 resolution was Council Directive 90/313,[11] which was followed by the UK legislation implementing that Directive in 1992. For the first time the public had a statutory right of access to environmental information held by public authorities.

1.33 A succession of United Nations (UN) inspired agreements led to similar conclusions, starting with the first UN conference on the environment in Stockholm in 1972, which decided that traditional and contemporary mass communications media should be used to disseminate information.[12] Twenty years later the Rio conference agreed a new set of principles, recognising that citizens should be involved in environmental issues, through having access to information held by public authorities.[13]

1.34 At a regional level the United Nations Economic Commission for Europe (UNECE) sponsored the Aarhus Convention in 1998, granting the public rights and imposing on public authorities obligations regarding access to information, public participation in decision making and access to justice.[14]

1.35 Aarhus was implemented at EU level by the repeal and replacement of the original Environmental Information Directive in February 2003. The new Directive was transposed by the UK Environmental Information Regulations 2004, which came into force on 1 January 2005.[15]

1.36 The UK, as a Member State, retains competence to take whatever necessary legislative measures are required in order to ensure compliance with the obligations in the Directive. Whilst the Directive sets out the general framework of the right of access to environmental information, it leaves to the Member States the task of defining the practical arrangements under which information is effectively made available to the public.

---

10 HMG, *Tackling Pollution – Experience and Prospects* (Cm 9149) (1984).

11 Council Directive 90/313/EEC on the Freedom of Access to Information on the Environment, 1990.

12 United Nations, *Report of the United Nations Conference on the Human Environment* (1972).

13 United Nations, *Conference on Environment and Development (UNCED)* (1992).

14 United Nations, *Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters* (1998). Usually known as the Aarhus Convention.

15 HMG, *Environmental Information Regulations (EIR)* (2004) Available at: http://www.legislation.gov.uk/uksi/2004/3391/contents/made, accessed on 24 November 2014. EIR is a UK Statutory Instrument (SI 2004 No. 3391).

1.1 Information Rights in Context: Current Competence

1.37 Evidence received as part of this review suggested that competence in relation to access to official information is, relatively speaking, uncontested. That is less true of data protection. With that in mind this section focuses on the range of views on the latter.

1.38 Accordingly, this chapter largely focuses on the current state of EU competence under Article 16 of the TFEU in relation to data protection.[16] It also examines the evidence received about current competence in access to official information.

The UK Government's Perspective

1.39 Article 16(1) provides each individual whose personal data is processed within the EU (regardless of nationality or place of residence) with a right to protection of their personal data.

1.40 Article 16(2) then empowers the Council and Parliament to make rules about the use (or 'processing') of personal data by Union institutions or Member States, when either are 'carrying out activities which fall within the scope of Union law'.[17]

1.41 Any rules made using this power are subject to the ordinary legislative procedure. This means there is qualified majority voting in the Council, which must come to a codecision with the European Parliament.

1.42 However, the EU's competence in making data protection rules under Article 16(2) is limited. There are four key limitations, one category of which is specific to the UK, Ireland and Denmark.[18] This category is described in more detail below in relation to Protocol 21.

1.43 The first limitation is that rules can only be made to regulate EU institutions or Member States when they are carrying out activities 'within the scope of Union law', that is, activities that relate to something that the EU can legislate on more generally.[19]

1.44 This limitation also affects the issue of shared competence. There may be activities that fall within an area that the EU could legislate on but has yet to do so. The UK considers that such activities are not carried out 'within the scope of Union law'.[20] Therefore, data protection rules could not be made under Article 16(2) to regulate the use of personal data for those activities or areas.

1.45 On competence and matters of national security, Declaration 20 annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon recognised that whenever rules laid down on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. The conference recalled that the legislation presently applicable, in particular the 1995 Data Protection Directive, contains specific derogations on these subjects.

1.46 Article 346(1)(a) TFEU is also significant. It provides that no Member State is obliged to disclose information if it considers that disclosure would be contrary to its essential security interests.

---

16 TFEU.

17 TFEU, Article 16(2).

18 Similar limitations on competence imposed by Article 6a of Protocol 21 of the treaties, as regards the UK and Ireland are imposed as regards Denmark by Article 2a of Protocol 22 of the treaties.

19 TFEU, Article 16(2).

20 Idem.

1.47 The second limitation is contained in Article 6a of Protocol 21 to the EU Treaties on the position of the UK and Ireland in respect of the area of freedom, security, and justice (Protocol 21 annexed to the TFEU).[21] The EU's power to legislate in relation to activities in this area is set out under Title V of TFEU. Generally speaking, Protocol 21 allows the UK to 'opt into' Title V rules. If the UK does not opt into those rules in this way, then they will not apply to the UK.

1.48 Rules passed under Title V powers may include those concerning police or judicial cooperation between Member States in criminal cases involving the interests of more than one Member State. Activity authorised by those rules might require Member States to share personal data. Normally, data protection rules under Article 16(2) TFEU would apply to govern how the personal data are used in such instances.

1.49 However, Article 6a of Protocol 21 states that if the UK does not participate in police and judicial cooperation rules (Articles 82 to 89 TFEU), then more general EU data protection rules that would ordinarily apply to that activity will not apply either. In brief, this means that if the UK is not a participant in EU police and judicial cooperation rules, the UK retains competence to make its own rules on those topics and may apply its own data protection standards accordingly.

1.50 The third limitation is that Article 16(2) of TFEU does not cover the protection of personal data in the context of the Common Foreign and Security Policy (CFSP). Rules relating to the processing of personal data relating to activities within the scope of the CFSP and rules relating to the free movement of such data should be made under Article 39 TEU. This states that it is for the Council to adopt a decision laying down such rules. To date, no measures have been made under Article 39.

1.51 The final limitation is that any exercise of competence by the EU under Article 16 TFEU must comply with Article 8 of the Charter of Fundamental Rights, which, following the Lisbon Treaty, enshrined existing rights.[22] More information on the Charter can be found in the Balance of Competences Fundamental Rights report.[23]

1.52 Article 8 provided a right to the protection of personal data. This might appear to duplicate the right given by Article 16(1). However, it would be possible for the EU to breach the Charter right if it were to enact legislation under Article 16(2) which failed properly to give adequate protection to personal data.

1.53 In giving effect to the Article 8 right, the ECJ has held that the right reflects the fundamental right to respect for private life in Article 8 of the European Convention on Human Rights, and the right to protection of personal data. These were both already part of EU law before the Lisbon Treaty came into force.[24]

---

[21] Treaty on the Functioning of the European Union.

[22] Charter of Fundamental Rights of the European Union (2010) OJ C83/02.

[23] HM Government, *Review of the Balance of Competences between the United Kingdom and the European Union: Fundamental Rights* (2014).

[24] Volker und Markus Schecke GbR v Land Hessen Case C-92/09 [2010] and Hartmut Eifert v Land Hessen, Case C-93/09, [2010]. The ECJ interprets the right in Article 8 of the Charter by reference to pre-Lisbon case law such as Tietosuojavaltuutettu v Satakunnan Markkinaporssi and Satamedia Oy Case C-73/07, [2008]. In case Patrick Kelly v National University of Ireland (University College, Dublin), Case C-104/10, [2011], paragraph 55, after referring to EU acts such as Council Directive 95/46/EC of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data The Court states: 'The protection of personal data is also provided for in Article 8 of the Charter of Fundamental Rights of the European Union'. In case Michael Schwarz v Stadt Bochum, Case C-291/12, [2013] paragraph 27, refers to case law of the Strasbourg Court when considering the concept of personal data for the purpose of Article 8.

1.54 The ECJ has shown that it is willing to examine EU legislation closely and critically in light of the Article 8 right.

1.55 For example, in the case of Volker[25] the Court held that EU Council regulations were incompatible with Article 8 of the Charter to the extent that they required the publication of the names of all people in receipt of funding from the European Agricultural Guarantee Fund and the European Agricultural Fund for Rural Development.[26]

1.56 By way of contrast in Schwarz, the Court considered it was compatible with Article 8 of the Charter for a Regulation to require that when people applied for passports, their fingerprint data should be collected and stored. The requirements were a proportionate means of protecting against the fraudulent use of passports.[27]

Perspectives from the Evidence

1.57 The evidence submitted in response to the Call for Evidence suggests that there are a variety of opinions about the significance and effect of Article 16 in particular, what it says about the current competence of the EU and how it ought to be exercised.

1.58 In particular, some respondents suggest that free movement principles should continue to have a significant influence on the content of future rules enacted under Article 16(2).

1.59 In contrast, other respondents suggest that the new Treaty right is now more closely aligned with the idea of data protection as a fundamental right, standing independent of free movement or single market imperatives.

The EU Charter of Fundamental Rights

In 2000, the Council, Parliament and Commission jointly proclaimed the Charter of Fundamental Rights as a non-binding document which brought together the fundamental rights which were already recognised by the EU, but did not contain any new rights or change the scope and meaning of those existing rights. The Charter includes the right to respect for private and family life (Article 7) and the protection of personal data (Article 8). The Charter became legally binding when the Treaty of Lisbon came into force in 2009. More information on the Charter can be found in the Balance of Competences Fundamental Rights report.[28]

[25] Volker und Markus Schecke GbR v Land Hessen, Case C-92/09, [2010] and, Hartmut Eifert v Land Hessen, Case C-93/09, [2010].

[26] Regulation 1290/2005/EC, of the European Council on the Financing of the Common Agricultural Policy, 2005 Article 44a.

[27] Michael Schwarz v Stadt Bochum, Case C-291/12, [2013].

[28] HMG, *Review of the Balance of Competences: Fundamental Rights* (2014).

Relationship between Article 16, the Single Market and Fundamental Rights

1.60 The evidence confirmed the analysis set out above by supporting the impression that the emphasis of EU competence in data protection has shifted since the EU first asserted competence to legislate in the field, back in 1990. At this time, the EU's competence to legislate on data protection was an expression of its competence to take appropriate measures to encourage the free movement of goods and services within the EU.

1.61 As set out in the previous chapter, the ECJ has since made clear in its case law that, in its view, there does not always need to be a specific link to free movement activity in order for the data protection Directive to apply in a given situation.[29]

1.62 In its evidence submitted to this Review, the law firm Lewis Silkin noted this development in the court's jurisprudence, highlighting that the shift away from the Single Market had occurred before the advent of the new legal base in Article 16.[30] Instead, in its view, EU case law had already expanded the scope of competence so that data protection rights no longer arose only in a single market context.

1.63 Following on from this view, the British Bankers' Association, Association for Financial Markets in Europe and the International Regulatory Strategy Group argued that Article 16 confirmed, definitively, that competence in the field of data protection will not be based simply on single market objectives.[31]

1.64 Even if that is an accurate picture and no technical single market constraint is now placed on the EU's competence, there remains a question as to whether competence nevertheless still ought to be exercised with free movement objectives in mind.

1.65 Some respondents contend that, even if Article 16 is not limited by reference to them, single market objectives should remain central in this way when the EU exercises its competence to enact data protection rules.[32]

1.66 The Wealth Management Association implied caution against turning away from the Single Market and is eager that data protection in the future does not hamper business.[33] Similarly, the RSA Insurance Group suggests that an entirely new legal base that is not linked to the Single Market risks creating a regime where privacy and economic growth are too often in conflict to enjoy the confidence of firms looking to operate across and beyond the EU.[34] The Digital Policy Alliance also appears to support a free-movement based approach. The Digital Policy Alliance does add that 'any increase to the EU's competence to legislate using a principles-based approach […]could have a beneficial impact on the internal market at large and the UK economy in particular'.[35]

---

29 Rechnungshof v Osterreichischer Rusterfunk and Others and Christa Neukomm, Case C-138/01, [2003]; Bodil Lindqvist v Kammaraklagaren, Case C-101/01, [2003].

30 Lewis Silkin, *submission of evidence*, p4.

31 British Bankers' Association, Association for Financial Markets in Europe and the International Regulatory Strategy Group (referred to as British Bankers' Association), *submission of evidence*, p5.

32 The Wealth Management Association, RSA Insurance Group, the Digital Policy Alliance, *submission of evidence*.

33 Wealth Management Association, *submission of evidence*, p2.

34 RSA Insurance Group, *submission of evidence*, p5.

35 Digital Policy Alliance, *submission of evidence*, p5.

1.67 The Information Commissioner's Office (ICO) appears to propose that single market objectives can be balanced with a regime that protects individual rights. It contends that there is a reasonable justification for creating a new legal base not expressly linked to the Single Market, given that the range of personal data processing and its potential impact has changed significantly over the last twenty years. In the ICO's view, these rights ought to be set out as a freestanding right whilst still respecting the important relationship with the Single Market.[36]

1.68 Both the Law Society and the Liberal Democrats Home Affairs, Justice, and Equalities Committee, do not consider that the new legal base is, or should be, exercised only with free movement objectives in mind, go on to make observations about the relationship between the new Article 16 and the EU Charter of Fundamental Rights.

1.69 The Law Society is of the opinion that the new legal base can be seen as an indication of an increased focus on rights protected by the Charter. In particular, the Law Society's evidence identifies a perceived need to make sure that the right to data protection in the TFEU and the right to data protection in the Charter resembles one another so that there is equivalence between the protections given by both.[37]

1.70 Both, the Law Society and the Liberal Democrats Home Affairs, Justice, and Equalities Committee expound the view that the ECJ is increasingly prepared to look at competence in the data protection field, and how it has been exercised, against the backdrop of the rights guaranteed by the Charter, increasingly citing it in its case law.

[36] Information Commissioner's Office, *submission of evidence*, p8.

[37] The Law Society of England and Wales, The Law Society of Scotland, *submission of evidence,* p8.

Case Study: Google Spain

In 1998, a Spanish newspaper published information about proceedings against Mr Gonzalez for the recovery of social security debts. In 2010, Mr Gonzalez complained that when a Google search was entered in his name it was possible to obtain links to the information. He argued that the proceedings had been resolved for some years and were now irrelevant. The data should be removed from the papers web pages and links removed from Google's search engine. He relied on existing rights given by the Data Protection Directive to block processing of 'incomplete or inaccurate' personal data (Article 12) and to object to processing of any personal data on 'legitimate compelling grounds' (Article 14).

The claim was brought against both Google Spain and Google Inc, a related company headquartered in the United States. Only the latter operates the search engine and does so from outside the EU. The Spanish Data Protection Authority ruled that the newspaper did not have to remove the content. However, it found against Google Spain and Inc concerning the search result links to the content. Google Spain and Inc appealed to the Spanish Court which referred a series of questions about the application of the Directive to the ECJ.

The ECJ found that:

- Operators of search engines which provide links containing details about named individuals are themselves 'data controllers'. As a result, the 1995 Data Protection Directive will apply where a search engine enables links which contain personal data.
- EU data protection rules can apply when the processing of personal data is done by an entity outside the EU, if that entity has a sufficiently close commercial relationship with a related company based in the EU.
- Search engines, and other data controllers, do not have to comply in all circumstances with requests for the removal of links under Articles 12 and 14. There must be good reasons underlying the request (although prejudice is not needed), and public interest arguments can defeat the right.
- It may be possible to object to the creation of a link to personal data via an internet search result even if it was originally lawful to publish the linked-to data elsewhere. That right to object may apply even where there is no right to prevent the data from continuing to be included on the linked-to website.

Source: Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, [2014].

1.71 The view of the Law Society is that both the Google Spain[38] ruling and the Digital Rights Ireland[39] case can be seen as indications of the ECJ taking a firmer stance on the protection of personal data (Article 8 of the Charter) and the right to privacy (Article 7 of the Charter). The Liberal Democrat Home Affairs, Justice, and Equalities Committee also comments that the overruling of that Directive in Digital Rights Ireland on the basis of Articles 7 and 8 of the Charter shows how firmly these rights are now anchored in the Treaties and, therefore, EU law.[40]

[38] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, Case C-131/12, [2014].

[39] Digital Rights Ireland Ltd. V Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Siochana, Case C-293/12, [2012].

[40] The Liberal Democrat Home Affairs, Justice, and Equalities Committee, *submission of evidence*, p4.

1.72 These observations raise the question as to whether in the future the ECJ may, by placing greater emphasis on Articles 7 and 8 of the Charter, take a more expansive approach to what EU data protection competence, and the rules created using it, can achieve. No evidence was received as to whether such a development of this sort would or would not be desirable. The wording of Article 6(1) TEU is clear, however, that the Charter does 'not extend in any way the competences of the Union as defined in the Treaties'.[41]

1.73 The evidence also raised an important related discussion point, centring round the concept of the 'direct effect' of EU Treaty rights. The issue is whether Article 16 of the TFEU has such an effect.

Direct Effect of Treaties

Some provisions of the TFEU are sufficiently clear, precise and unconditional that they confer rights directly on individuals. They have 'direct effect'. This means that in order to demonstrate a breach of EU law, an individual need only show that the TFEU Article itself has been breached. There is no need to demonstrate a breach of either national law or any other EU legislation, such as a regulation or directive. Examples of TFEU Articles which have direct effect are:

- Article 18 (discrimination on grounds of nationality);
- Article 21 (free movement of EU citizens); and
- Article 45 (free movement of workers)

On the other hand, some provisions in the TFEU do not confer directly applicable rights on individuals. As such, it is not possible for an individual to rely upon the wording of the Article directly in order to demonstrate a breach of EU law. An example of an Article without direct effect is Article 19 TFEU on discrimination.

1.74 Hijmans and Scirocco, quoted in the Liberal Democrat Home Affairs, Justice, and Equalities Committee submission, state that there are strong arguments in favour of Article 16(1), the Treaty right to data protection, having direct effect.[42] They note the similarity in wording to Article 18 EC on citizenship which the ECJ has already deemed to have direct effect. They conclude that if Article 16 does have direct effect, then this is a further restriction on what data protection legislation enacted under Article 16(2) can do. That is because to give direct effect to the Treaty right would very clearly underscore the idea that legislation made under Article 16(2) must very clearly bolster, and must not cut across, the primary Article 16(1) right.[43] It is well recognised that countervailing views exist, albeit that no specific evidence expressing those was submitted.

1.75 Durham University suggests that the language of the Treaty, which mirrors the language of the Charter, actually creates a specific right similar to Charter rights. Since the Directive is no longer tied to the Single Market, data protection has become recognised as a fundamental right.

---

41 TEU.

42 Hielke Hijmans and Alfonso Scirocco, 'Shortcomings in EU Data Protection in the Third and The Second Pillars, Can The Lisbon Treaty be Expected to Help?' *Common Market Law Review* Vol. 46 (2009), p.1517.

43 The Liberal Democrat Home Affairs, Justice, and Equalities Committee, *submission of evidence*, p4.

Regulation of the Public/Private Sectors

1.76 Some respondents also chose to make observations on a different dimension relating to current competence. These relate to whether the new legal base enables processing in all sectors to be regulated by EU rules or whether it can only be used to regulate processing in certain sectors. The focus of these observations is on how far rules created under Article 16 TFEU can extend to both the public and private sector.

1.77 The Digital Policy Alliance describes competence as extending to all forms of processing in both public and private sectors, including police and judicial cooperation.[44] The Commission Legal Service is also of the firm opinion that Article 16 TFEU is sufficient ground for both public and private sectors. This view reflects the position of the ECJ in its judgments. Further, Hunton and Williams note that Member States appear to have accepted the Commission's view without challenge. On this view, the legal base for data protection legislation set out in Article 16 is simply a restatement of the position under current case law.[45]

1.78 In contrast, Experian[46] and the Finance and Leasing Association[47] are of the opinion that the scope of Article 16 TFEU may be narrower than current case law. All question whether Article 16 TFEU can be used to legislate for private sector processing. Hunton and Williams observe that Article 16 TFEU is oddly worded and that there remains a possible argument that it does not provide a basis for the regulation of data protection in the private sector.[48] Experian describes the legal base as 'obscure' in nature, unclear as to whether it encompasses private sector and individuals' data.[49] Similarly, the Finance and Leasing Association comments that the full scope of Article 16(2) TFEU is not clear, adding that it would appear primarily to target personal data processed by and between public authorities rather than private sector data.[50]

1.79 The Finance and Leasing Association adds that Article 16 TFEU does not preclude the EU from continuing to regulate data protection in the private sector on the basis of internal market provisions.[51] Experian suggests, however, that since Article 16 TFEU does not clarify that the basis of internal market provisions could be used to regulate private sector data, it is not clear that this is so, adding to potential confusion over competence.[52]

Other Influences on the Boundaries of Competence

1.80 The Newspaper Society suggests that, whilst data protection legislation enacted under current competence may appear to be defined and limited by the boundaries of that competence, the reality is that it provides significant scope for regulators to expand the impact of legislation on the ground.[53] For example, legislation restricts the application of data protection rights in the area of press freedom. However, in the Society's view, the powers which the same legislation gives to regulators to take action have the potential to cut across those limits.[54]

---

44 Digital Policy Alliance*, submission of evidence*, p6.

45 Hunton & Williams, *submission of evidence*, p9.

46 Experian, *submission of evidence*, p9.

47 Finance and Leasing Association, *submission of evidence*, p4.

48 Hunton & Williams, *submission of evidence*, p9.

49 Experian, *submission of evidence*, p9.

50 Finance and Leasing Association, *submission of evidence*, p4.

51 Idem.

52 Experian, *submission of evidence*, p9.

53 Newspaper Society, *submission of evidence*, p2.

54 Idem.

1.81 The British Computer Society posits that as technology has advanced and creates legislative gaps it is important that competence is exercised in such a way as to deal with these new challenges.[55]

Access to Official Information

1.82 Hunton and Williams comment that, save for the specific provisions on access to environmental information, there is less uniformity across Member States in the area of access to information than in data protection. Scandinavian attitudes, for example, appear to be very different to those of some of the Member States in the south and east of the EU.[56] There is not the same sense of a shared value as exists in respect of the protection of privacy.

1.83 Hunton and Williams comment further that businesses are far more impacted by data protection legislation than by rights of access to information.[57] For the latter, the burden tends to fall mainly on the public sector.

Environmental Information

1.84 The ICO notes that the Environmental Information Regulations 2004 and the Environmental Information (Scotland) Regulations 2004 (EIR) potentially cover a wider range of public authorities than the Freedom of Information Act 2000 (FOIA) and the Freedom of Information (Scotland) Act 2002 (FOISA).

1.85 This is one of a number of differences between the EU and domestic regimes. For environmental information the range of exemptions is more limited than those provided for under the domestic acts (for example, all exemptions are subject to a public interest test). By contrast, the UK Parliament decided that the right of access under the Freedom of Information Act 2000 should not require disclosure of certain classes of information that might be said to fall within the EU regime.

1.86 It also notes the recent Court of Appeal judgment in relation to the use of the FOIA veto and the finding that the veto cannot apply under the EIRs, although this is the subject of an appeal.[58]

1.87 The ICO observes that the Access to Documents Regulation does not appear to provide comparable rights of access to the UK's FOIA and FOISA and the Directive on Access to Environmental Information.[59]

---

[55] British Computer Society, *submission of evidence*, p5.

[56] Hunton & Williams, *submission of evidence*, p3.

[57] Idem.

[58] R (Evans) v Her Majesty's Attorney General and the Information Commissioner, Case C1/2013/2250, [2014].

[59] The Information Commissioner's Office, *submission of evidence*, p6.

Chapter 2: Impact on the UK's National Interest: Summary of Responses

Summary

A broad range of respondents thought that the Data Protection Directive has been advantageous to the UK. For many, this was due to the flexibility of the Directive and its interpretation by the UK. However, where respondents were supportive of the Directive and action at EU level in the area of data protection, it is also important to note that many thought there was room for improvement.

For example, there was a near consensus that the Directive had failed to keep pace with technological change and has struggled to adapt to the growth of online commerce, international data flows, and social networks. A number of respondents also believed that uniformity of standards could be best worked towards at EU level, but some cautioned about excessive uniformity.

The evidence showed that in many cases respondents believed there was a good existing balance between protecting individual data protection rights and pursuing economic growth. It was suggested that the Directive had advanced privacy rights for UK citizens and set a globally recognised standard. Respondents acknowledged there were costs to businesses, but many did not think they were disproportionate. Some concern was expressed about perceived limitations on rights and on the free flow of data, and about the complexity of the instrument for both individuals and organisations.

Views were more divided over the benefits of having standardised rules across the EU and the benefits of having the flexibility to take account of the different circumstances of Member States. Common standards were widely recognised as a way for businesses to reduce costs, and the EU was best placed to improve harmonisation. However, a number of respondents considered the Directive's success was due in part to the UK's implementation of the Data Protection Act 1998.

In the area of access to information, the evidence suggested EU competence has had a positive impact on the UK's national interest, in so far as it has increased the transparency of EU institutions. Transparency helps UK businesses hold the EU to account, predict the impact of its legislation, and influence policy before it becomes legislation. A few respondents highlighted operational problems with the Access to Documents Regulation and the Environmental Directive.

Most respondents considered there was no need to extend the EU's competence in this area, and that efforts should focus on improving implementation of the existing legislation. However, some suggested there was an opportunity for the UK to promote its Freedom of Information culture across Europe.

Introduction

2.1 This chapter summarises evidence received on the impact of EU competence on information rights in the UK. This Review does not seek to draw conclusions but will set out the evidence to highlight the diverse ways EU competence may affect UK citizens and organisations.

2.2 This chapter is divided into two sections:

- Section 2.1 sets out the evidence on how EU competence has impacted on individuals and organisations for Data Protection and Access to Information; and
- Section 2.2 sets out the evidence received on the most appropriate level at which action should be taken for each area whether at the UK level, EU level, or international level.

2.1: What Impact Does the EU's Competence on Information Rights have on the UK?

Data Protection

2.3 This section explores evidence about the impact of EU competence on data protection primarily through the 1995 Data Protection Directive, which was introduced to bring about common data protection standards across the EU. The Directive has a broad scope and provides a general data protection framework to be implemented by each Member State through its domestic legislation. This means differences in interpretation between Member States may still exist as highlighted in the box below. In the UK, the Directive has been transposed into law through the Data Protection Act 1998.

Examples of Data Protection Practice in Some Member States

Data Protection Officers

There is no requirement in the Data Protection Framework Decision (DPFD) or the UK's Data Protection Act 1998 for organisations to appoint a data protection officer. However Member States do have discretion to implement data protection law above the minimum standard.

This is evident in Germany where, unlike in the UK, a data protection officer is a requirement for all companies which employ more than nine employees who are permanently engaged in automated data processing or at least 20 persons who are engaged in non-automated data processing. A breach of this requirement can lead to a significant fine from the German data protection authority.[1]

Registration with the Supervisory Authority

In the UK, there is an obligation on data controllers who process personal data to register, at a fee, with the Information Commissioner. Data Controllers have to inform the Information Commissioner's Office about their data processing activities. Unlike in the UK, German data protection legislation does not require data controllers to register with the data protection authority. Even though the German data protection legislation provides for notification, such notification tends to be the exception rather than the rule.

Similarly, in Spain a register for controllers is not maintained. However, the Spanish supervisory authority holds a registry of databases containing personal information. Registration for databases containing personal information is carried out through a specialist software package that is very detailed and identifies in full not only the data controller, but also any data processors supporting it.[2]

1 Data Protected Linklaters, *Germany* (2014). Available at: https://clientsites.linklaters.com/Clients/dataprotected/Pages/Germany.aspx, accessed 24 November 2014.

2 DLA Piper, *Data Protection Laws of the World* (2013).

2.4 This section focuses on several key themes that were repeated throughout the evidence:

- Whether the Directive strikes a good balance between protecting rights and promoting economic growth;
- Whether the Directive strikes a good balance between harmonisation of standards and allowing flexibility of interpretation by Member States;
- Whether the Directive has had a positive impact on individuals in the UK;
- Whether the Directive has had a positive impact on businesses and organisations; and
- Whether the Directive has kept up with new technology, the rise of online social networks, e-commerce, and increased data flows, and the impact this has on the UK.

Evidence on the General Balance between Economic Growth and Rights

2.5 One of the themes brought out in the Call for Evidence is that for every right exercised by individuals, there is a corresponding obligation on businesses. Obligations often translate into costs, but it is seldom straightforward to place a value on the benefits of individual rights. Respondents were invited to provide evidence concerning the balance which the Directive struck between the pursuit of growth and the protection of individual rights in the UK.

2.6 Many respondents including those from organisations such as banking, finance and technology industries felt that EU action, through the Data Protection Directive, struck the right balance between protecting individuals' data protection rights and allowing for economic growth. The Advertising Association and Direct Marketing Association found that there was a 'good balance' in the Directive, while the British Bankers' Association believed that the balance was largely correct.

2.7 Experian viewed the Directive as 'an excellent demonstration of where the EU's competence has attained a balance between the individual's data protection rights and the pursuit of growth.'[3] The Cookie Collective observed that the Directive is viewed internationally as one of the best data protection regimes and suggested this is evidence that it has found the best possible balance.

> The Data Protection Directive has provided the best available balance between the rights of individuals and the pursuit of growth. This can be evidenced by the fact that it is held up internationally as one of the best regimes in the world.[4]

2.8 However, a number of respondents argued that the balance tipped too heavily in favour of one goal over the other. Krowdthink Ltd, a social networking start-up, held that there was an imbalance in the Directive that had been to the advantage of business over the individual.[5] Conversely, the National Farmers Union warned that the Directive placed too many financial and administrative burdens on businesses, potentially harming growth.[6]

---

3 Experian, *submission of evidence*, p6.

4 Cookie Collective, *submission of evidence*, p1.

5 Krowdthink Ltd., *submission of evidence*, p1.

6 National Farmers Union, *submission of evidence*, p1.

2.9 The Faculty of Advocates highlighted the costs that the Directive imposed on controllers. However, it felt that the balance was not disproportionately slowing down the growth of its members' practices.[7]

2.10 Some respondents challenged the very notion of a balance between the protection of rights and the pursuit of growth. While the ICO believed the current balance was 'reasonable', it cautioned that the two objectives were not necessarily in competition with each other.[8] Similarly, the Digital Policy Alliance was concerned that the notion of a balance between the two inaccurately implied they are opposing goals.[9]

2.11 Several participants at the Edinburgh workshop emphasised the difficulty of comparing two dissimilar objectives. Some participants at the Edinburgh workshop pointed out that the societal benefits served from protecting individuals' personal data were not easily monetised that they could be weighed against the cost to business.[10] In its evidence, the law firm Hunton and Williams also challenged the notion of such a balance, suggesting it may lead to placing too much focus on short-term business costs. In many areas, they argued a lack of measures to protect individual rights may often incur long-term economic and social costs that should be taken into account.[11]

Evidence on the Balance between Harmonisation and Interpretation or Flexibility

2.12 The UK's particular implementation of the Directive was cited by many respondents as a primary reason why the UK achieved a reasonable balance between protecting individuals' personal data and the pursuit of economic growth. This suggests there is another balance to evaluate: the balance which the Directive strikes between permitting flexibility to allow for Member States' different circumstances, and pursuing a greater level of uniformity of standards across the EU. The evidence indicated both approaches offered advantages to the UK.

2.13 Many respondents felt an increased commonality of standards through the Directive had been advantageous to the UK. The Digital Policy Alliance believed a common set of rules benefited the UK and the EU in terms of investment from foreign based companies. A common set of rules as set out in the current Directive is more attractive than twenty-eight different sets, and the Digital Policy Alliance argued that such companies might have avoided the UK, had it operated its own separate rules.[12]

2.14 The Cookie Collective acknowledged that, owing to national differences, there was not full harmonisation of the Directive but that there is still a 'core common ground'. It stated that EU action has helped bring Member States closer towards a single market for data flows. This degree of harmonisation benefits businesses that are transferring data across Member States.

> Without the core common ground provided by the Data Protection Directive, it would be much more difficult for UK businesses reliant on cross border movement of personal data to operate and compete for business in key EU markets.[13]

---

7 Faculty of Advocates, *submission of evidence*, p2.

8 Information Commissioner's Office, *submission of evidence*, p3.

9 Digital Policy Alliance, *submission of evidence*, p3.

10 *Record of 28 May 2014 stakeholder event*, Edinburgh, p2.

11 Hunton & Williams, *submission of evidence*, p6.

12 Digital Policy Alliance, *submission of evidence*, p2.

13 Cookie Collective, *submission of evidence*, p1.

2.15 The Law Society regarded harmonisation of rules across the EU as advantageous in terms of saving costs for businesses who operate across several Member States and process personal data. Lack of harmonisation may increase costs or confusion. It gave the example of how differing interpretations of 'legitimate interest' create problems for cases of cross border litigation.[14]

2.16 The British Computer Society also acknowledged that the efforts made by the EU to advance harmonisation have helped to reduce uncertainty but not to eliminate it. In its evidence, it observed that Member States still apply the Directive in different ways across the EU. These divergent approaches led to extra costs for businesses.[15] In its evidence to the Single Market Review, Vodafone suggested that differences in privacy laws across Member States were holding back the future development of pan-European services.[16]

2.17 CIFAS echoed the observation that a persistent lack of harmonisation or fully common standards increases the costs and difficulties for UK businesses operating in other Member States. In addition to these costs to the UK economy, CIFAS said that the sharing of data intended to prevent fraud had been limited due to a lack of consistency in the implementation of the Directive.[17]

2.18 Respondents from the financial and credit sector, advertising industry, and health and medical research sector gave examples of where the UK's particular implementation of the Directive has been advantageous.

2.19 In its evidence, the Finance and Leasing Association emphasised the importance of processing personal data to the UK credit industry. By storing and processing personal data, credit providers are better equipped to make responsible lending decisions and to better manage risk.[18] In 2013, its members provided £88.9bn of credit to UK businesses and households. The Finance and Leasing Association argued that there are different cultural attitudes concerning data protection across Member States and praised the flexibility the Directive gave Member States. In its evidence, it welcomed the UK's implementation of the instrument through the Data Protection Act 1998 and the Information Commissioner's approach to enforcement, which allows for robust action to be taken when the Act is breached.[19]

> The FLA regards the Data Protection Act as a sound piece of legislation that protects consumers' fundamental human right to respect for their private and family life, their home, and their correspondence.[20]

2.20 Experian echoed the advantages that data processing by the credit industry brings to the UK in terms of facilitating suitable credit decisions, avoiding excessive indebtedness, and guarding against fraud. It also observed the importance of processing data to comply with the EU Consumer Credit Directive.

---

[14] Law Society of England and Wales, Law Society of Scotland, *submission of evidence*, p3.

[15] British Computer Society, *submission of evidence*, p5.

[16] Vodafone, *submission of evidence to the Review of the Balance of Competences between the United Kingdom and the European Union: Single Market Report* (2013).

[17] CIFAS, *submission of evidence*, p2.

[18] Finance and Leasing Association (FLA), *submission of evidence*, p1.

[19] Ibid, p2.

[20] Idem.

2.21 In its evidence, Experian highlighted the rights which an individual already had to access their credit file, before the Data Protection Directive. This could have led to confusion when the Data Protection Directive, and its provision allowing individuals to access personal data held on them, came into force. For example, consumers may have confused their UK right to access their credit report with their EU right to obtain all information that was held about them. Consequently, they would have had to hunt through vast amounts of data to try to discover which information was included on their credit report.[21]

2.22 To avoid this confusion Experian noted that the UK Government provided clarification in its implementation of the Directive. The UK is, as far as Experian knows, the only Member State where consumers can choose between exercising a full access right and a right to access their credit report only. Experian considers that this clarification would not have been possible had there not been flexibility in the Directive. It felt that this flexibility had also allowed for a variety of stakeholders to have their say and help facilitate a regime that reflects the UK's circumstances.[22] This has been highly advantageous to the UK. Firstly, it has led to innovation in how organisations use data, and secondly it has contributed to growth in the digital sector.

> The flexibility for the UK Government to establish and modify Data Protection law to suit the UK economy has promoted a strong growth in online and digital industries and services, which has undoubtedly been beneficial to consumers and the public sector.[23]

2.23 Respondents from the advertising industry provided further evidence to show that it is the Directive's flexibility and the UK's implementation of it that have helped strike a balance between protecting individual rights and pursuing economic growth.

2.24 The Direct Marketing Association and Advertising Association acknowledged that the Directive imposed greater burdens on organisations than the then UK Data Protection Act 1984 did. The two associations welcomed the exemptions in the Directive, and the 'pragmatic implementation' of the Directive by the UK and regulation by the ICO, concluding that this combination had allowed businesses to succeed in the UK.[24]

2.25 The Internet Advertising Bureau agreed that pragmatic implementation and regulation by the UK Government and the ICO had contributed to the success of businesses based on data processing. In its evidence, the Internet Advertising Bureau gave the example of the UK's interpretation of what processing data on the grounds of 'legitimate interest' meant, arguing that other Member States interpret it too restrictively.[25] It also welcomed the ICO's risk-based approach to enforcement. The Internet Advertising Bureau emphasised the importance of the digital advertising sector to the UK, observing that, with an annual growth of 15.2%, it was the fastest growing advertising sector. Expenditure on digital advertising made up a greater proportion of total advertising spending in the UK than in any other country in the world.[26]

---

[21] Experian, *submission of evidence*, p4.

[22] Idem.

[23] Experian, *submission of evidence*, p6.

[24] Direct Marketing Association and the Advertising Association, *submission of evidence*, p3.

[25] Internet Advertising Bureau, *submission of evidence*, p3.

[26] Idem p1.

2.26 In addition, the value of flexibility and of the UK's interpretation of the Directive was highlighted by respondents from the health sector. The Wellcome Trust concluded that this had allowed for a balance to be found between advancing medical research and protecting individuals' data. It cited the UK's choice to include medical research in the definition of 'medical purposes', thereby facilitating the processing of health data, as an example of how the UK's interpretation of the Directive had been advantageous for the medical research sector.[27]

The UK's implementation of the Data Protection Directive allows world-leading health research with personal data to take place in the UK.[28]

2.27 The NHS European Office also found that, while common standards were useful, the flexibility the Directive gave Member States was beneficial to deal with the complexities of research.[29]

2.28 However, a number of respondents took a different view and suggested there were ways in which the UK's implementation had disadvantaged the UK.

2.29 One respondent argued that the UK's implementation of the Directive had been disadvantageous to both individuals and the economy. They cited, as an example, the differing interpretations of risks posed by pseudonymous data, which broadly speaking was information that did not directly identify an individual. The respondent suggested that the lack of a common definition for when data are fully anonymous and no longer personal has impeded the development of globally competitive online businesses and start-ups in the UK and the wider EU.

2.30 Hunton and Williams suggested that during implementation of the Directive, there were high thresholds on rights such as the right to object to processing and the right to claim compensation. This has made it more difficult for some individuals to exercise them.[30]

2.31 The National Archives stated that the UK's transposition may have gone beyond the Directive in certain respects, causing difficulties for archives. In particular, the National Archives felt it had limited their ability to host personal data on online archives.[31]

2.32 Although the Wellcome Trust described the UK's implementation of the Directive as 'largely positive' for medical research, it argued the Data Protection Act 1998 was overly complex. It suggested that organisations in the research sector have struggled to interpret the scope of definitions and provisions for data that have been encrypted or pseudonymised. It thought that this confusion has partially led to a risk-averse culture of sharing data and thus delayed beneficial research. However, it acknowledged a lack of evidence as to whether such confusion is even avoidable and whether the Directive or the Data Protection Act were the main factors contributing to this complexity in the highly specialised area of research.[32]

---

27 Wellcome Trust, *submission of evidence*, p2.

28 Idem.

29 NHS European Office, *submission of evidence*, p2.

30 Hunton & Williams, *submission of evidence*, p6.

31 The National Archives, *submission of evidence*, p1.

32 Wellcome Trust, *submission of evidence*, p2.

Evidence on the Impact on Individuals

2.33 Most stakeholders viewed the Data Protection Directive as having a positive impact on individuals in the UK. The advantages to UK citizens revolve largely around privacy matters but also consumer rights. While no evidence was received that the Directive disadvantages individuals, several respondents argued that sometimes data protection rights may not be fully exercised or enforced. The complexity of the Directive may also hinder individuals fully exercising their rights.

2.34 Concerning advantages the Directive gives UK citizens, one respondent gave examples of the right to correct inaccurate personal information held about them and the right to object to direct marketing. The ICO also held that complaints by individuals were addressed effectively through the Directive's provisions for independent regulatory bodies such as itself.[33]

2.35 The National Farmers' Union observed in their evidence that the Directive has been advantageous to individuals in terms of increasing the protection of their personal data.[34] Furthermore, the Open Rights Group believed that the EU's action had been vital for UK citizens' rights and has also promoted data protection principles across the world. The Digital Policy Alliance also viewed the EU as being 'at the forefront of recognising data protection as a fundamental right'.[35] The ICO further welcomed the inclusion of data protection in the Charter of Fundamental Rights and emphasised how this has promoted the data protection rights of individuals.

2.36 While no evidence was received to suggest that the Directive had disadvantaged individuals in the UK, a couple of respondents pointed out areas where they felt it was not working effectively enough in their interests. For example Krowdthink Ltd was concerned that an imbalance in the Directive towards data controllers led to data being collected by default.[36]

2.37 The Law Society drew attention to the complexity of the Directive and considered the possibility that it hinders some individuals from exercising and enforcing their rights. Due to the complexity of the instrument, individuals may not fully understand when they can exercise their right to complain about their data being misused.[37] The complexity may also play a part in the misuses occurring.

Evidence on the Impact on Businesses and Organisations

2.38 While many respondents concluded that the balance between protecting individual rights and pursuing economic growth was largely proportionate, opinions were divided about the extent to which data controllers had been disadvantaged. On the one hand, evidence from the submissions suggested that the potential advantages of the Directive for data controllers could include the value of consumer trust for their business and potential efficiency gains through the requirement for document processing. On the other hand the evidence suggested that disadvantages could include restrictions on processing which may limit important data sharing or discourage it by causing controllers to become too risk-averse. As with individuals, the complexity of the instrument may cause problems for controllers, particularly under-resourced SMEs.

---

[33] Information Commissioner's Office, *submission of evidence*, p2.

[34] National Framers' Union, *submission of evidence*, p1.

[35] Digital Policy Alliance, *submission of evidence*, p1.

[36] Krowdthink Ltd., *submission of evidence*, p1.

[37] Law Society of England and Wales, Law Society of Scotland, *submission of evidence*, p2.

2.39 As advantages, in addition to the evidence already seen about the benefits of harmonisation, some respondents highlighted the value of trust for an organisation. The Law Society viewed a consumer's trust in an organisation as an essential component for all sectors. It felt the Directive had led to individuals having 'greater confidence in how their personal data will be handled by commercial and public providers of various services'. They observed this was particularly relevant for the legal profession, for which client confidentiality is a key consideration.

2.40 The Faculty of Advocates agreed on the importance of trust in the legal profession, and that the Directive helps advocates discharge their duty of client confidentiality. In their evidence, they noted the duty of confidentiality was formulated before the advent of sophisticated and complex data processing, and that the Directive adds value through its guidance on how to protect privacy while processing personal data.

2.41 Hunton and Williams stressed the importance of the public's trust for all organisations and that the Directive has also increased the transparency of data processing practices. Trust emerges as a concern in a 2010 survey of consumers by FDS International. Commissioned by the Office of Fair Trading, the study found that 19% of a large sample of UK internet users did not shop online. One-third of these cited concerns about the security of their personal data as a reason for avoiding online commerce.[38]

2.42 Hunton and Williams also suggested that the recognition of the importance of record-keeping may have led to efficiency gains for businesses.

2.43 On ways in which the Directive may disadvantage organisations, a couple of respondents evoked the concept of risk. One respondent feared the Directive's stipulations may lead to organisations adopting a risk-averse approach when processing personal data and they may avoid using it in ways that otherwise may have been beneficial. However, they cautioned that this needed to be balanced against the risk of improper disclosures.[39]

2.44 The NHS European Office gave the example of data-sharing being unduly limited despite being in the patient's best interests. It cited the second Caldecott Review, which stated that the duty to share information and the duty to protect patient confidentially may sometimes be equally important.[40] The NHS European Office felt that a balance needed to be made between these two duties. It also observed that although many professions may process data for health purposes, there were different rules. In particular, it observed that those working in social services often needed to rely on consent, unlike medical professionals. NHS European Office emphasised that this may become a significant issue given the increasing proportion of the elderly in Britain. According to NHS European Office data-sharing should be facilitated between professions connected to the health and care sector.[41]

> [I]t is important that data can lawfully be shared with any professional that is involved in caring for the individual.[42]

2.45 The National Farmers' Union believed the Directive does not sufficiently take into account differing degrees of risk. This is particularly problematic for SMEs, with resources which may often be strained and where processing of personal data is relatively low-risk. The

[38] Office of Fair Trading, *OFT Response to the Call for Evidence on a Common European Sales Law for the European Union – A Proposal for a Regulation from the European Commission* (2012).

[39] Hunton & Williams, *submission of evidence*, p.6

[40] F. Caldicott, I*nformation: To Share or Not to Share? The Information Governance Review* (2013).

[41] NHS European Office, *submission of evidence*, p1.

[42] Idem.

financial and administrative costs of compliance with the Directive were highlighted by the National Farmers' Union in its evidence. It gave the example of organisations having to appoint staff and purchase special computer software in order to be able to fulfill their obligations. The National Farmers' Union concluded the requirements were 'burdensome and inconsistent with the risks addressed by the Directive […] this will adversely affect the pursuit of economic growth'.[43]

2.46 In a survey led by the Federation of Small Businesses in October 2013, data protection was revealed to be the third most burdensome area of EU compliance for SMEs polled (Q20, 14%).[44] The 1995 Directive also featured in a *Joint List of the most burdensome EU legislative acts for SMEs* in 2010.[45]

2.47 The Faculty of Advocates drew attention to the complexity of the Directive. Compliance, coupled with the risks of sanctions, imposes resource costs on organisations. This can be particularly burdensome for self-employed data controllers, including members of the Faculty, whose day- to- day work may not involve close familiarity with the data protection framework.[46] The British Bankers' Association also found the Directive's complex provisions, along with differing Member State approaches, had generated confusion and did not help controllers.[47]

2.48 Although the British Bankers' Association still considered that the Directive largely struck the right balance between the pursuit of economic growth and the protection of personal data, it felt there were requirements that still placed too high burdens on data controllers. In its evidence, it cited prescriptive notice requirements and restrictions on using cloud services.[48] It argued these stipulations were limiting growth and expansions into new markets, as well as potentially barring new firms entering the market. One respondent gave the example of claims firms making requests to access personal data and creating considerable costs for data controllers.

2.49 Restrictions on international transfers were signalled out as being particularly disadvantageous to organisations by a couple of respondents. While the Internet Advertising Bureau cited the Safe Harbour Decision as an important example that allows organisations to transfer data to the US,[49] other methods came under criticism. The British Bankers' Association observed that 'ticking the box' through using model contractual clauses was emphasised too much over 'ensuring meaningful measures of accountability are in place'.[50] In addition, Hunton and Williams noted that too much of an administrative burden was involved in obtaining approval of a Binding Corporate Rule, which allows companies to transfer data to affiliates outside the European Economic Area.[51] This, it concluded, was disadvantageous to businesses.

---

[43] National Farmers Union, *submission of evidence*, p1.

[44] Research by Design, *FSB 'Voice of Small Business' Survey Panel* (2013). Available at: http://www.fsb.org.uk/policy/assets/regulation.pdf, accessed on 5th September 2014.

[45] European Commission, *Results of the Public Consultation of the Top 10 Most Burdensome Legislative Acts for SMEs* (2013).

[46] Faculty of Advocates, *submission of evidence*, p2.

[47] British Bankers' Association, *submission of evidence*, p2.

[48] Idem.

[49] Internet Advertising Bureau, *submission of evidence*, p2.

[50] British Bankers' Association, *submission of evidence,* p1.

[51] Hunton and Williams, *submission of evidence*, p6.

2.50 Transatlantic Trade and Investment Partnership (TTIP) will see an increase in data flows between the EU and US. However, there is a general concern that the differences in the EU and US privacy frameworks may be hard to reconcile. In the EU, general data protection legislation is underpinned by the fundamental right to privacy as enshrined in the Charter of Fundamental Rights, whereas in the US there is no such statutory recognition of privacy as a fundamental right.

TTIP

TTIP is a trade and investment agreement under negotiation between the EU and the US. The main aim of TTIP is to increase trade and investment between the US and EU by reducing tariffs, aligning regulations and standards, improving protection for overseas investors, and increasing access to services and government procurement markets by foreign providers. TTIP is also designed to drive growth and create jobs.

Independent research shows that TTIP could boost:

- the EU's economy by €120bn;
- the US economy by €90bn;
- the rest of the world by €100bn.

Source: European Commission, *In Focus: Transatlantic Trade and Investment Partnership (TTIP)* (2014).

2.51 The British Bankers' Association provided comments on TTIP and noted that there is potential for increased data flows between the US and EU under TTIP which would encourage growth in the digital economy and attract investment. However, the British Bankers' Association felt that the current Commission draft imposed too many disproportionate burdens, which may hamper TTIP. The British Bankers' Association highlights the need for negotiations on data protection and TTIP to remain separate, which reflects the UK Governments view.

> It is important that any advances made on EU developments are not hampered by negotiations on other politically sensitive topics within TTIP, and that the overall balance of interests is not lost sight of as the negotiations proceed.[52]

Safe Harbour

Safe Harbour is an agreement between the EU and the US under which participating US organisations commit to complying with key principles, which, if complied with, equate to an adequate level of data protection pursuant to the 1995 Directive. This recognition is achieved by compliance with the relevant Safe Harbour principles. The US Department of Commerce maintain a public list of participating companies, and each firm must verify their continuing compliance on an annual basis to remain on the list.

[52] British Bankers' Association, *submission of evidence*, p8.

2.52 Some respondents drew attention to the Safe Harbour agreement between the EU and US and queried whether data protection rights are being enforced through it. Under Safe Harbour, data may be transferred to participating US organisations that have self-certified compliance with the Safe Harbour principles. Lewis Silkin noted it was 'unclear if there was any substance in the protection.'[53] Durham University observed there were 'inadequacies' in the current functioning of Safe Harbour,[54] and Krowdthink Ltd argued the scheme is 'poorly policed'.[55]

2.53 In March 2014, The House of Lords European Union Committee conducted an enhanced scrutiny of the European Commission's communication on rebuilding trust in EU-US data flows and the functioning of the Safe Harbour Decision. The Committee concluded that the Safe Harbour scheme should not be suspended as recommended by the European Parliament for Civil Liberties, Justice and Home Affairs (LIBE). The Committee recognised that despite some weaknesses, the Safe Harbour arrangements offer benefits to citizens and businesses. The Committee supported the Commission's efforts to strengthen the provisions of Safe Harbour. It also made recommendations aimed at strengthening transparency and increasing awareness and accessibility of Safe Harbour for businesses and citizens.[56]

2.54 The European Commission made clear its intentions to conclude an agreement with the US on reforming Safe Harbour by summer 2014. However, at the date of publishing this Report no final agreement has been announced. An update from the Commission is still pending.

The UK Government Position

2.55 In so far as it needs updating at all, the Government's view is that Safe Harbour should be reformed rather than suspended. Safe Harbour helps to facilitate the flow of international data and encourages the adoption of data protection principles by companies in the United States, which is important for consumers. The Government recognises that the Safe Harbour provisions can be improved to strengthen transparency and accessibility for individuals and businesses.

Evidence Concerning the Extent and Impact of the Directive's Ability to Keep Up with new Technology, the Rise of Online Social Networks, Commerce, and Increased Data Flows

2.56 Many respondents indicated that the Data Protection Directive had been outpaced by new technologies and new trends of data use, although a small minority of respondents such as the Digital Policy Alliance[57] and the Advertising Association[58] felt the Directive has in the main met the challenges of the last two decades. Several participants at the Brussels stakeholder workshop acknowledged that the Directive was drafted in the days when the word 'filing systems' was a more common term.[59] Nevertheless, they still concluded the Directive has been successful in standing the test of time.

---

[53] Lewis Silkin, *submission of evidence*, response to Q7.

[54] Durham University, *submission of evidence*, response to Q7.

[55] Krowdthink Ltd., *submission of evidence*, response to Q3.

[56] House of Lords European Union Committee to Simon Hughes MP, Minister of State for Justice (7 May 2014). Available at: http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/safeharbour/boswell.pdf, accessed on 25 November 2014.

[57] The Digital Policy Alliance, *submission of evidence*, p2.

[58] Advertising Association and Direct Marketing Association, *submission of evidence*, response to Q1.

[59] *Record of 18 June 2014 stakeholder event*, Brussels.

2.57 The Advertising Association and Direct Marketing Association agreed and attributed this to the approach behind it being deliberately technologically neutral.[60] This flexibility had allowed space for innovation to address new changes. Both associations also recognised the benefit of other instruments, such as the E-privacy directive which can be used to address specific gaps.[61] The Digital Policy Alliance agreed the Directive had been relatively effective in its ability to meet new challenges, and that this may be due to its relative lack of prescriptiveness.[62]

2.58 Nevertheless, many respondents believed the Directive was failing to meet various technological, social, and economic developments. This was deemed by some to have negative consequences for data controllers who struggle to interpret the rules in light of new, complex processing situations. There may also be a negative impact on individuals, who may not understand whether their personal data are being sufficiently protected or even how the data is being processed.

2.59 Among those who felt the Directive was out of date in regard to recent technological changes were the Faculty of Advocates, the Finance and Leasing Association,[63] and many participants at the London stakeholder workshop. Experian agreed and also stressed the myriad of new ways in which consumers are now using the Internet.[64] The ICO acknowledged that there may be doubts about the Directive's efficient applicability in a changed world that has seen such a rise in international transfers of personal data, and the development of cloud computing.[65]

2.60 Evidence from the Nottingham University Business School echoed these doubts and stressed that the Directive was facing challenges nowadays that could not have been foreseen during its implementation.[66] Among these challenges is the growing use of personal data, which is now employed more and more in increasingly international supply chains. The Business School argued that even now data is being under-utilised, its value underestimated, and that there remains the possibility still for further unpredictable developments in the way it will be used.[67]

2.61 Several respondents highlighted the impact that a failure of the Directive to keep up pace with changes could have on the UK. The National Farmers Union called attention to the growth of online activities. It noted that individuals may suffer as a consequence from insufficient regulation of online personal data that is being unlawfully processed.[68]

---

60 Advertising Association and Direct Marketing Association, *submission of evidence*, response to Q1.

61 Directive 2002/58/EC of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications), 2002.

62 The Digital Policy Alliance, *submission of evidence*, p3.

63 Finance and Leasing Association, *submission of evidence*, response to Q3.

64 Experian, *submission of evidence*, response to Q3.

65 Information Commissioner's Office, *submission of evidence*, response to Q3.

66 Nottingham University Business School, *submission of evidence*, response to Q3.

67 Idem.

68 National Farmers Union, *submission of evidence*, p1.

2.62 Another respondent called attention to the risks that the growing use of encrypted or pseudonymised data may pose to individual rights. The increasing frequency of data transfers may also create cumulative risks. This potentially spiralling risk is particularly relevant in the context of cloud computing, where there may be many processors and sub-processors. In contrast, this respondent considered that the Directive was largely coping with the rise of online social networks. This was due to the efforts of the Article 29 Working Party and the European Network and Information Security Agency.[69]

2.63 Other respondents chose to put the emphasis on the complexity of online developments and technological changes. A lack of clear rules can lead to confusion, with a negative impact on both individuals and data controllers.

2.64 The British Computer Society gave evidence that many technology companies felt the Directive was out of date and could not be applied effectively to new situations. Despite being intended to be technology-neutral, the Directive's definitions for concepts such as 'data controller', 'data processor', and 'consent' could not always effectively be adapted to fit cloud computing or online activities such as social networks, media, and marketing.[70]

2.65 Several participants at the Northern Ireland workshop echoed this concern and spoke of the possibility of data controllers without control.[71] The Directive did not predict cloud computing or the growth in outsourcing processing services, and consequently there is a potential imbalance between the responsibilities of a controller and a processor under the Directive and what their capabilities are in reality.

Access to Information

2.66 The previous chapter set out the two significant pieces of EU legislation in the area of access to information. Respondents to this review focused their evidence primarily on these two pieces of legislation.

2.67 The first is the Access to Documents Regulation, which allows EU residents to view documents of the main EU institutions. It only applies to documents held or written by an EU institution. This can include documents created by the UK that have been sent to an EU institution and are in its possession. However, it does not affect UK official documents that are only in the possession of the UK Government.

2.68 The second piece of EU legislation in this area is the Environmental Information Directive which places certain obligations on Member States' public authorities, or private bodies performing certain public functions, including the obligation to respond to requests for environmental information.[72] This Directive was transposed into UK Law through the Environmental Information Regulations 2004 and the Environmental Information (Scotland) Regulations 2004 (EIRs). These provide a general right of access to recorded environmental information, which includes data about air, water, soil, land, plants, animals, energy, noise, waste, and emissions such as pollution and radiation. Environmental information also includes information about decisions, policies, and activities that affect the environment.

---

[69] Caspar Bowden, *submission of evidence*, p3.

[70] British Computer Society, *submission of evidence*, response to Q3.

[71] *Record of 11 June 2014 stakeholder event*, Belfast.

[72] Council Directive 2003/4/CE on Public Access to Environmental Information in the UK, 2003.

2.69 A number of respondents such as the Digital Policy Alliance, the RSA Insurance Group and Gene Watch UK, were of the opinion that EU competence in the area of access to information has had a positive impact on the UK's national interest. Some respondents highlighted operational problems with the Access to Documents Regulation and the Environmental Directive and suggested ways the current exercise of EU competence could be improved.

Access to Documents Regulation

2.70 Respondents from a broad range of sectors highlighted the positive impact of the Access to EU Documents Regulation to the extent that it increases the transparency of EU policy-making.

2.71 The Liberal Democrats Home Affairs, Justice, and Equalities Committee felt that the rights afforded by the Regulation were vital for building trust in the EU and holding it to account.[73] The ICO also stated that the Access to EU Documents Regulation 'is an important tool to understand the operation of the EU and hold decision-makers to account.[74]

2.72 For example, the RSA suggested that the Regulation has helped UK businesses to follow the progression of other EU pieces of legislation.[75] This in turn allows UK businesses to evaluate more effectively the consequences of EU policy-making to themselves and to their customers.

2.73 Furthermore, the Regulation potentially gives UK organisations the opportunity to influence EU policy-making. GeneWatch UK emphasised that access to EU documents allowed them to influence EU policy before it became legislation.[76] They gave an example of successfully requesting documents concerning draft EU policy to regulate genetic tests, which subsequently led them to argue for stronger provisions in the interest of consumers.

2.74 Although no respondent believed the Access to Documents Regulation had been disadvantageous on balance for the UK, several cited various weaknesses in the Regulation that have caused problems for citizens and businesses attempting to access official EU information.

2.75 Many respondents submitted evidence indicating it was often difficult to obtain documents through the Regulation. The Direct Marketing Association and the Advertising Association argued that the process lacked transparency.[77] Their evidence suggested that there were particular problems in obtaining documents concerning discussions in the Council of Ministers. Although the two associations found the European Parliament's policy-making to be more transparent, they observed that amendments to texts were not always made available. They also felt that the trilogue process between the Parliament and Council lacked openness. In their view, this lack of transparency reduced stakeholders' ability to influence discussions, and potentially leads to outcomes that are disproportionate and insufficiently evidence-based.

---

[73] The Liberal Democrats Home Affairs, Justice, and Equalities Committee, *submission of evidence*, p5.

[74] The Information Commissioner's Office, *submission of evidence*, response to Q5.

[75] RSA, *submission of evidence*, response to Q5.

[76] GeneWatch UK, *submission of evidence*, response to Q5.

[77] Advertising Association and Direct Marketing Association, *submission of evidence*, response to Q5.

2.76 Experian echoed these observations about how the Regulation works in practice, noting that the EU restricts many documents during the legislation process.[78] The Faculty of Advocates commented that its faculty members had sometimes been refused access to official EU documents.[79] The British Bankers' Association also suggested that the right of access under the Regulation may contain too many exceptions.

2.77 A couple of respondents raised concerns involving data protection. Caspar Bowden suggested that the Regulation required applicants to submit too much personal data with their request.[80] He gave the example of being required to give his postal address when requesting documents to be sent by email.

2.78 The British Bankers' Association also highlighted the need to guarantee that the EU institutions, as well as Member States, fully protect sensitive consumer information from being released under the Access to Documents Regulation or Member State Freedom of Information Acts.[81]

Environmental Directive

2.79 On the Environmental Information Directive, which was implemented through the EIR and the EIRs, there were differing views about its effects. Some participants at the stakeholder workshop in London saw EU competence in this domain as beneficial.[82] For instance, some highlighted the potential recourse the Directive offers to those who seek environmental information and may have been refused under the domestic Freedom of Information Acts. The ICO also highlighted that there are 'important features' in the Environmental Information Directive, including a public interest test for all exceptions.[83]

2.80 However, other participants in the London workshop emphasised the relatively low usage of the rights under the EIRs and the Environmental Information Directive compared to the Freedom of Information Acts, which benefit from a higher profile.[84]

2.81 The Scottish Government acknowledged in its evidence the potential benefits for harmonisation of access to environmental information.[85] However, it concluded that the Directive does not add to the rights already set out in FOISA, and that the overlap between the two often creates confusion. In addition, it noted that the Directive is sometimes excessively bureaucratic and offered the example of the requirement to do a public interest test for refusals to release information even when the authority does not hold the information.

78 Experian, *submission of evidence*, response to Q5.

79 The Faculty of Advocates, *submission of evidence*, p4.

80 Caspar Bowden *submission of evidence*, response to Q5.

81 British Bankers' Association, *submission of evidence,* p5.

82 *Record of 29 April 2014 stakeholder event,* London.

83 Information Commissioner's Office, *submission of evidence,* response to Q1.

84 Idem.

85 Scottish Government, *submission of evidence,* para 22.

2.82 The Scottish Government also highlighted that, unlike FOIA and FOISA, the Environmental Directive was not intended to take Scottish or wider UK circumstances into account. In its evidence, the Scottish Government emphasised different practices and opinions about what information should be released. It noted that unclear exemptions in the legislation can lead to problems and gave examples of situations when the Directive and EIRs have hindered the restriction of information that should not be released. This included cases of commercially sensitive information, legal advice, and information that needs to be verified before release, such as official statistics.

Other Areas in the Information Rights Domain

2.83 Stakeholders at the Northern Ireland event stated that the INSPIRE Regulation 2009 has had a positive impact on the Open Data agenda.[86]

2.84 The Liberal Democrat Home Affairs, Justice, and Equalities Committee emphasised the value of the data collected by the EU. It concluded that 'the current untapped potential for re-use to innovate, create new products and services and help policy makers make better decisions is unparalleled. The overall economic gains from opening up this resource could amount to €40bn a year'.[87]

2.85 The Committee welcomed in particular the European Commission's decision to grant free access to data collected by the Copernicus system of earth observation satellites and sensors. It concluded that this data will be advantageous to a broad range of stakeholders, including UK citizens, businesses, researchers, and will help inform policy decisions.

[86] *Record of 11 June 2014 stakeholder event,* Belfast.

[87] The Liberal Democrat Home Affairs, Justice and Equalities Committee, *submission of evidence,* p3.

2.2: What is the Most Appropriate Level for Action?

2.86 The previous section set out differing views on where EU action, or its absence, has been advantageous and disadvantageous to the UK. This section now explores the evidence for taking action at different levels, whether on the UK level, the EU level, or internationally, and whether this would be advantageous to UK national interest.

2.87 While on the whole the evidence suggested competence should remain unchanged, many emphasised the need for national flexibility. Several participants at the Edinburgh workshop argued this is particularly relevant for access to information. They observed that the crossborder flow of data makes coordinated action more necessary for data protection, but access to information may require a culturally oriented approach, given the diverse views, often context dependent, of what should or should not be disclosed.

Data Protection

2.88 In the previous section, while most respondents felt EU action had had a positive impact on the UK several tensions emerged through the evidence provided. There were conflicting views about where the balance should be struck between protecting rights and pursuing economic growth, and even about whether it is right to see the two as opposing objectives locked in competition. Furthermore, respondents from the medical research, fraud prevention, and credit sector offered a reminder that the free flow of data is vital for pursuits other than economic growth.

2.89 Above all, the evidence showed conflicting views about the degree of harmonisation and its impact on the UK. Evidence from Krowdthink summarises the challenge involved when considering where the balance of competence should lie:

> It's a reality that every country has different cultural norms that filter into what is and what is not acceptable for cultural norms online. However, the Internet transcends national boundaries, and that is its major asset.[88]

2.90 There were varied views on the extent to which harmonisation is desirable. This reflects the many aspects of the debate about where and how action should be taken.

2.91 Two main cross cutting themes were identified:

- Where to strike the balance between harmonisation and flexibility; and
- What level is most appropriate for meeting the challenges of globalisation and new technological, commercial, social developments?

2.92 It was widely recognised amongst respondents that these two questions were vital for determining where action should be taken. The remainder of this section will explore arguments for action on the national, EU, and international level.

[88] Krowdthink Ltd., *submission of evidence,* response to Q6.

Harmonisation and Flexibility

2.93 Harmonisation is a theme that cuts across several aspects of the debate. It cuts across the argument about where the balance should lie between the pursuit of economic growth and individual rights. In the previous section, we set out evidence from a number of respondents who argued that the current degree of harmonisation has advanced individual rights by extending them across the EU and promoting them beyond its borders. We saw evidence that it also reduces compliance costs for businesses and organisations that operate in up to 28 different Member States and do not want 28 different sets of rules. However, a number of businesses considered that the Directive's flexibility, and the UK's implementation of it, were key reasons for its success in creating an environment where both economic growth and the protection of rights could be pursued.

2.94 Beyond purely economic considerations, harmonisation also cuts across the wider argument about where the balance should lie between promoting the free flow and use of data and protecting individual rights. For example, a reduction in barriers to data sharing among Member States was felt to have facilitated the free flow of data. CIFAS gave evidence that insufficient harmonisation was still harming the sharing of data to prevent fraud. However, respondents from the health and medical research sector argued that Member State flexibility has been vital to allow important research using personal data to go ahead.

2.95 These examples illustrate the inherent tension and the balance that must be struck between harmonisation and flexibility. On the one hand, a high degree of harmonisation of rules can promote economic growth and the free flow of data through its removal of barriers. Insufficient harmonisation limits these potential benefits.

2.96 On the other hand, excess harmonisation that fails to take into account crucial national or cultural differences may also limit important data-sharing that is beneficial to the public and wider world. These differences may be substantial. Polcak observed that there are multiple interpretations across Member States even about what constitutes personal data, for example, whether it can include Close Circuit Television (CCTV), Internet Provider addresses, and phone numbers.[89]

2.97 As the Nottingham University Business School wrote in its evidence, 'each system must be able to fit locally and globally at the same time which looks mutually exclusive'.[90] The view that respondents take on harmonisation strongly influences not only the level where they believe action would best be taken, but also the extent and form of that action.

Technological, Commercial, and Social Changes

2.98 The previous section also discussed the extent to which the Data Protection Directive is coping with immense commercial and technological change, and the impact which any failure to keep up has on the UK. The last twenty years have seen the rise of cloud computing, the realities of which do not always correspond to traditional data protection concepts and terms such as 'controller' and 'processor'. There has been also the rise of social media, the growth of online commerce, and a considerable increase in international data flows and usage.

---

[89] R. Polcak, 'Aims, Methods and Achievements in European Data Protection,' *International Review of Law, Computers, & Technology* Vol. 23 Issue 3 (2009), p179-188.

[90] Nottingham University Business School, *submission of evidence,* response to Q7.

2.99 This theme of immense change was highly relevant for many respondents, who considered it as a rationale for why action should or should not be taken on the domestic, regional or EU, or international level. Many highlighted the international character that data processing and sharing has taken and indicated an international approach would be ideal. Others underlined the growing interconnectedness of data use with other imperatives for the UK, such as trade and free movement of goods. Many sectors are highly dependent on data. As the Internet Advertising Bureau wrote in their evidence: 'Data is global by nature, and the free flow of data across borders is fundamental to the functioning of the data-driven economy'.[91]

Evidence for Action to be taken at a UK Level

2.100 The evidence submitted in relation to this issue was based largely on the value of common rules to businesses, organisations, and individuals, and the significance of modern, cross border flows and their relation to the UK economy.

2.101 Several participants at the Brussels workshop emphasised the value that the free flow of data throughout the EU brought to the UK, and that domestic legislation by itself could not secure this.[92] The Digital Policy Alliance's view summarised the views of many: 'At a national level, the UK cannot realistically maintain a position of "data independence"'.[93]

2.102 Other respondents elaborated further on this, underlining the interconnectedness of data use and the UK's relations with the EU. Academics from Durham University pointed out that the flow of data is connected to the freedom of movement of people, goods, services, and finance. They concluded that even if the UK were to reduce its relations with the EU to free trade only, the UK would still need to comply with various EU data protection requirements. They gave an example of the UK's risk-based approach to border management, which relies heavily on the supply of data to determine levels of risk.[94]

2.103 The National Archives agreed that freedom of movement of goods and people was dependent on the flow of personal data. The law firm Hunton and Williams considered how data protection may often overlap or interact with other EU regulation areas, for instance the regulation of e-commerce. When areas overlap, it could be more advantageous to have a common approach on a similar level, rather than simply the domestic level.

2.104 The Digital Policy Alliance further considered the value that harmonisation of rules across the EU brings to foreign-based companies. They argued that many might cease doing business in the UK market if the UK broke away from the common set of requirements.[95] This was echoed in the Law Society's evidence.[96] One respondent also commented that there may be administrative burdens on businesses if competence for data protection were to be repatriated.

---

[91] Internet Advertising Bureau, *submission of evidence,* p3.

[92] *Record of 18 June 2014 stakeholder event,* Brussels.

[93] Digital Policy Alliance, *submission of evidence,* p5.

[94] Durham University, *submission of evidence*, response to Q11.

[95] Digital Policy Alliance, *submission of evidence*, p2.

[96] The Law Society of England and Wales and the Law Society of Scotland, *submission of evidence,* response to Q2.

Evidence for Action to be taken at an International Level

2.105 Several respondents stated that as data flows were increasingly international, action would be best suited at the international level. Given the rise of borderless cloud computing, British Naturism[97] pointed out that individuals may face a choice of continuing to use the internet or ceasing to do so in order to protect their personal data. They believed that action was necessary on an international scale with minimum standards that must be enforced.

2.106 However, others concluded that it would not be possible to achieve such a regime. The Digital Policy Alliance believed an international approach would be beneficial but considered it 'a pipe dream', due to difficulty in obtaining international agreements in relation to the internet.[98] The Law Society agreed and cited the considerable cultural differences in approach to data protection between some EU Member States such as Germany and France and countries like the US.[99] The Law Society thought that a regional model, such as at the EU level, could enable the right balance between flexibility at a national level and coordination at a transnational level to enable data flows.

Evidence for Action to be taken at the EU Level

2.107 Many respondents argued that the EU should take action in the area of data protection. This was partially due to the conclusions above that it was unrealistic for the UK to have competence, given the cross-border and integrated nature of data flows. Respondents further argued the EU was better placed to harmonise a common set of rules and also to promote its standards globally.

Harmonisation

2.108 Many stakeholders submitted evidence that harmonisation through the EU is beneficial to the UK. In addition to evidence noted so far, the Digital Policy Alliance concluded that action on the EU level was the second best option to global action and perhaps the most realistic.[100] The Law Society noted that action on the EU level was desirable for organisations which collect and process data across many Member States. Harmonisation reduced compliance costs. They believed this is particularly relevant to small IT start-ups whose target market extended beyond the UK.

2.109 The Federation of Small Businesses suggested that the suitability of harmonisation, and the level where action is taken, may depend on the particular aspect of data protection.[101] It listed cloud computing as an area where harmonisation of rules on the EU level was beneficial.

2.110 GeneWatch UK also emphasised the increased flow of personal data across the EU, in particular health data for European research projects.[102] They argued that the EU needs to have competence so that individuals can trust in their patient confidentiality being respected across all Member States. An extreme consequence of the EU not having this competence might be that people would avoid seeking medical care out of fear that their health or genetic data could be exploited.

---

97 British Naturism, *submission of evidence*, p2.

98 Idem, p5

99 The Law Society of England and Wales and the Law Society of Scotland, *submission of evidence*, response to Q7.

100 Digital Policy Alliance, *submission of evidence,* p5.

101 The Federation of Small Businesses, *submission of evidence,* p5.

102 GeneWatch UK, *submission of evidence*, response to Q1.

Need for Flexibility

2.111 Other stakeholders agreed action should be taken at the EU level but were cautious about excessive harmonisation. While some participants at the Edinburgh stakeholder workshop emphasised the benefits of consistency at EU level, others stressed the need to consider 28 different privacy, legal, and administrative cultures. The Nottingham University Business School also argued that EU level is needed for harmonisation, 'but nation level flexibility must be preserved'.[103]

2.112 The law firm Hunton and Williams also cautioned about harmonisation in the form of prescriptivism and the need to have consensus across the EU.[104] However, they suggested that attitudes to data protection were more uniform across the EU than attitudes to the issue of access to information. This may indicate that agreements such as the Convention 108 and OECD guidelines have had an effect on individuals' and organisations' attitudes to personal data.

2.113 The Law Society suggested that action at the EU level, or in a regional model, may be a solution that could strike a balance between flexibility and harmonisation.[105] Many respondents concluded that the Data Protection Directive found such a balance due to the form of instrument. Many other respondents acknowledged that action was best at the EU level but disagreed with how future harmonisation should proceed. These views will be discussed in the next chapter.

Influence of the EU

2.114 The EU's greater ability to promote data protection principles throughout the world is another factor to consider. As the Internet Advertising Bureau stated: 'Endeavours to harmonise data protection regimes at global level are sensible, and the EU is a unique position to make significant contributions to these efforts'.[106]

2.115 The Law Society highlighted the potential importance of framing regional agreements such as one between the EU and the US.[107] While stakeholders at the London workshop believed that a global regime was impossible to enforce, they advocated cooperation between different regions.[108] The EU may be better placed to bring this about than individual Member States. The British Bankers' Association also stated it was in businesses' interests for the EU to cooperate with other regional regimes to develop global codes of practice.[109] Both businesses and individuals would benefit from this consistency. Nottingham University Business School also stressed the need for systems that could work with different cultures and different needs, ranging from the differences between Member States to the differences between the EU and countries such as the US and China.[110]

---

[103] Nottingham University Business School, *submission of evidence,* response to Q7.

[104] Hunton and Williams, *submission of evidence,* p2.

[105] The Law Society of England and Wales and the Law Society of Scotland, *submission of evidence*, response to Q7.

[106] Internet Advertising Bureau, *submission of evidence,* p3.

[107] The Law Society of England and Wales and the Law Society of Scotland, *submission of evidence*, response to Q7.

[108] *Record of 29 April 2014 stakeholder event,* London.

[109] British Bankers' Association, *submission of evidence,* p3.

[110] Nottingham University Business School, *submission of evidence,* response to Q7.

2.116 Some participants at the Edinburgh workshop said it was important to recognise that the EU was not the only influence on major issues such as data protection.[111] Other regimes such as the Asia Pacific Economic Cooperation (APEC) also had an important role to play. However, participants concluded that the EU was likely to make more of an impact on international issues if it acted as one, rather than if Member States acted on their own.

2.117 The Digital Policy Alliance noted that the EU was already taking action to promote its standards through negotiations on free trade agreements.[112] The ICO echoed the call for regional regimes to be able to work better together.[113] One example of this is the cooperation between the EU and APEC on rules for international data transfers.

Access to Information

2.118 Two areas of debate were identified by respondents in their evidence. The first choice explored was whether the EU should extend its competence and develop an EU-wide Freedom of Information regime that was binding to Member States. The second choice identified was whether EU competence in promoting access to environmental information should be developed, reduced, or remain the same. Many respondents concluded that there was no need either to extend or reduce EU competence in this area. Little evidence was received for whether action should be taken internationally.

Arguments for Maintaining EU Competence

2.119 Among those who concluded that the balance of competence for access to information should remain as it is, the arguments focused on there being no discernible benefits to the UK, and the importance of cultural differences.

2.120 The National Farmers Union argued that it should be up to Member States to determine the extent of rights to access official information.[114] They concluded that extending EU competence would not offer any benefits to the UK.

2.121 The Law Society concluded that the current Freedom of Information regime, and the Environmental Information Directive implemented through the Environmental Information Regulation 2004 (EIRs), complement each other, and that there is no requirement for the EU to develop further competence in this area.[115]

2.122 The British Computer Society also found that the UK's competence in this area was sufficient, as currently exercised by the FOIA and FOISA. It observed that the ICO and UK legal system can already act to balance the right to access information with data protection rights. It concluded that this shows that Member States can act sufficiently in this domain, and therefore that there was no additional need for the EU to extend competence.[116]

---

[111] *Record of 28 May 2014 stakeholder event,* Edinburgh.

[112] Digital Policy Alliance, *submission of evidence,* p5.

[113] Information Commissioner's Office, *submission of evidence,* response to Q7.

[114] National Farmers Union, *submission of evidence,* p2.

[115] The Law Society of England and Wales; and the Law Society of Scotland, *submission of evidence,* response to Q6.

[116] British Computer Society, *submission of evidence,* response to Q6.

2.123 Several participants at the Edinburgh workshop agreed, arguing that access to information was an area that would not benefit from any greater EU-wide harmonisation of standards. Instead, a 'culturally-oriented' approach, which allowed Member States to legislate according to their own circumstances and practices, was more appropriate.[117]

2.124 Others focused their evidence on ways to improve the implementation of the existing Access to Document Regulation, and these suggestions will be set out in the next chapter.

Arguments for Reducing EU Competence

2.125 There was little evidence received on what the balance of competence should be for the Environmental Information Directive. The Scottish Government suggested that it would be beneficial to reduce EU competence by allowing Member States to opt out of the Environmental Information Directive if they already had domestic information rights legislation.[118] They argued this would avoid the confusion of having two different but parallel information rights regimes.

2.126 Reducing EU competence in this area would also allow Member States to tailor domestic legislation for their specific circumstances. For example, both of the domestic FOI and FOIS Acts have exemptions for royal material, but there is no specific exemption of this kind under the Environmental Information Directive. In addition the Environmental Information Directive does not allow that some exemptions are 'absolute', unlike domestic legislation.

2.127 In its evidence to the Environment and Climate Change Report, the law firm DLA Piper queried the necessity for EU legislation, given that Member States have ratified the United Nations' Aarhus Convention, granting individuals the right to access environmental information from public authorities.[119]

Arguments for Extending EU Competence

2.128 Overall, there was a split between the respondents. Some concluded that it may be beneficial to extend EU competence, for example by legislating to harmonise access to official information of Member States across the EU. Some advocated this as an opportunity for the UK to influence the culture of access to information across the EU and promote its own high Freedom of Information standards. Others were more critical of the UK's standards, arguing that exemptions for disclosure are overused. They argued that future EU legislation in this area may reduce this perceived problem.

2.129 Some participants at the Edinburgh workshop gave evidence stating that many Member States were impressed by the UK Freedom of Information regime and its default assumption that information should flow to the public.[120] They suggested there may be an opportunity for the UK to influence European standards and push also for action on the international level.

---

[117] *Record of 28 May 2014 stakeholder event,* Edinburgh.

[118] Scottish Government, *submission of evidence,* para 23.

[119] HMG, *Review of the Balance of Competences between the United Kingdom and the European Union: Environment and Climate Change* (2013), p56.

[120] *Record of 28 May 2014 stakeholder event,* Edinburgh.

2.130 The legal firm Hunton and Williams noted that the UK Freedom of Information regime 'appears to set a higher standard of openness and transparency for the public sector' than the EU Access to Documents Regulation does.[121] They observed that the UK would only benefit from EU action to harmonise standards of access to official information across Member States if these standards were raised to the level of those in the UK. If the EU were to legislate lower standards, this would be, in their view, undesirable for the UK.

2.131 Some respondents took a different view about why EU action would be beneficial to the UK. Caspar Bowden argued that the UK's Freedom of Information regime has too many exemptions compared to other countries, and that EU legislation that raised standards would be beneficial. [122] British Naturism also challenged how much information is released and observed that the EU could play a role in making sure that Member State public authorities are held accountable.[123] The ICO noted that EU action could help stabilise the UK's Freedom of Information regime.[124]

[121] Hunton and Williams, *submission of evidence,* p9.

[122] Caspar Bowden, *submission of evidence,* response to Q6.

[123] British Naturism, *submission of evidence,* p1.

[124] The Information Commissioner's Office, *submission of evidence,* response to Q6.

Chapter 3: Future Challenges and Options

Summary

A number of challenges and opportunities were identified by respondents in their evidence. Key challenges were the rise of Big Data, Cloud Computing, and the Internet of Things. While these offered opportunities for economic growth, efficiency, advancement in knowledge, and other benefits valued by society, their unpredictable development poses a challenge for policy-makers. Developments such as these are already challenging traditional data protection terminology and concepts, making it all the more important to find a balance between protecting personal data and facilitating its use and flow.

The draft data protection Regulation proposed by the Commission was highlighted by all respondents. Most saw it as an opportunity to update data protection law to reflect these new concepts and developments. However, on the whole, respondents concluded it was too process-driven and prescriptive to succeed in this goal. Above all, respondents emphasised the need to have legislation that is future-proof, principle-based, and flexible enough to cover diverse and unpredictable uses of data in the future.

The potential future clash of access to official information and data protection principles was a concern for some. Suggestions were also made to improve the existing legislation on the access to official documents.

Introduction

3.1 In 2016, the 'zettabyte' is expected to be born. Equal almost to 1.1 trillion gigabytes, this is a revealing example of how quickly the world of data changes and develops. Respondents to the Call for Evidence were asked to consider what challenges the future might pose for information rights. The four most significant challenges respondents identified were:

- The rise of Big Data;
- The rise of Cloud Computing;
- The Internet of Things; and
- The proposed General Data Protection Regulation.

3.2 Central to all these issues is the question of how to protect privacy in the face of the rapidly increasing importance of information flows to our economy and society.

Big Data

3.3 A number of respondents listed Big Data as both a challenge and an opportunity. Big Data is a concept that often eludes a definition through its very nature. It consists often of very large datasets from a variety of sources, gathered and analysed sometime at a very fast pace. Accordingly, it is often characterised by the three V's: volume, variety, and velocity. The ICO adds further attributes that are characteristic of Big Data, such as frequent use of algorithms for analysis, and changing purposes. The International Data Corporation (IDC) offered another definition:

> The intelligent economy produces a constant stream of data that is being monitored and analysed. IDC estimates that in 2011, the amount of information created and replicated surpassed 1.8ZB (1.6 trillion gigabytes). Social interactions, mobile devices, facilities, equipment, R&D, simulations, and physical infrastructure all contribute to the flow. In aggregate, this is what is called Big Data.[1]

Benefits of Big Data

3.4 The Big Data market is predicted to grow globally at a compound annual rate of 39.4%.[2] For the UK, there are many gains to be had in terms of efficiency, employment, and prospects for small businesses. A report by the Centre for Economics and Business Research (CEBR) predicts that Big Data could bring the UK £216bn between 2012 and 2017.[3] Gains in efficiency will make up £149bn of this total and the potential creation of small businesses £42bn.

Big Data Case Study[4]

In the United States, Vree Health uses analytics to reduce hospital re-admission rates for patients hospitalised for heart attack, heart failure or pneumonia. They use data collected throughout the hospital stay (this can amount to 12m pieces of data each day) and combine it with data from follow-up visits by their representatives, patient interactions with their internet and phone-based help systems and third party data. Analysing all of this data enables them to spot characteristics or behaviours associated with readmission, and if a particular patient exhibits these they can put support in place.

3.5 An e-skills UK report commissioned by SAS Institute UK found that vacancies in the Big Data sector have risen by 912% between 2008 and 2012. The report predicts a further 132,000 jobs to be created by 2017.[5]

3.6 In its response to the Call for Evidence, Nottingham University Business School argued that UK firms and the public sector were only 'scratching the surface of what can be done with their data'.[6] The firms which were most advanced in this area were still only beginning to learn how they could fully use Big Data, and consequently the ways it would develop cannot be predicted.

---

1 International Data Corporation, *Worldwide Big Data Technology and Services 2012-2015 Forecast* (2012).

2 Idem.

3 The Centre for Economics and Business Research, *Data Equity: Unlocking the Value of Big Data* (2012).

4 Information Commissioner's Office, *Big-Data-and-Data-Protection* (2014).

5 e-skills UK, the Sector Skills Council for Business and Information Technology, and SAS, *Big Data Analytics: An Assessment of Demand for Labour and Skills, 2012-2017* (2013).

6 Nottingham University Business School, *submission of evidence*, response to question 3.

3.7 Big Data brings wider societal benefits other than economic growth. In its July 2014 paper *Towards a Data-Driven Economy*, the European Commission identified a wide variety of ways in which society could benefit from Big Data. Amongst its examples, it considered the efficiency which Big Data can bring to the health sector. Greater access to data helps doctors with diagnoses, and researchers testing new drugs for illnesses.[7] In its response to our Call for Evidence, the Research Councils UK (RCUK)[8] echoed this and emphasised the advantages which research brought in showing links between health and various socioeconomic factors.

3.8 The European Commission gave further examples of the diverse advantages Big Data can bring to society, from managing traffic flows and congestion to predicting weather conditions to help farmers and giving policy-makers more information to make evidence-based decisions. Big Data also can help companies personalise their products and services when they know what their customers are looking for.

Concerns

3.9 Much Big Data may contain personal data, and there are concerns from privacy groups and others about how it may be used and the risk it poses to anonymity and privacy. In its evidence to this Review, the Cookie Collective expressed its concern that anonymised or pseudonymised personal data were less safe in the face of aggregated Big Data.[9] The Digital Policy Alliance also echoed this concern.[10] There is a high risk posed by the emergence of new technology and software that can make deductions from Big Data and potentially re-identify even if it has been encrypted or had its identifiers removed. In a piece written as evidence for the *Podesta Review*, the Electronic Privacy Information Centre highlighted recent large data breaches associated with Big Data and the risks these pose for individuals.[11]

3.10 A related concern is how algorithms make deductions from a massive range of datasets. Electronic Privacy Information Centre (EPIC) warned against algorithms being used to draw conclusions about people, revealing personal data that was never disclosed by the individual. It gave the example of one company which used Big Data, including online browsing activity, and analytical algorithms to predict which of its customers were pregnant.[12] The *Podesta Review* also highlighted the risk of this type of analysis being used to discriminate against certain types of individual.[13]

Looking Ahead

3.11 Big Data is important to the UK. The Government has chosen Big Data as one of Eight Great Technologies in which Britain can be a global leader, and £189m has been allocated for spending on Big Data and energy efficient computing.

> The UK has the potential to lead one of the defining developments of the 21st century: the data revolution.[14]

---

7 European Commission, *Towards a Thriving Data-Driven Economy* (2014).

8 Research Councils UK, *submission of evidence,* p4.

9 Cookie Collective, *submission of evidence,* response to question 4.

10 Digital Policy Alliance, *submission of evidence,* p4.

11 Electronic Privacy Information Centre, *Request for Information: Big Data and the Future of Privacy* (2014).

12 Idem.

13 J.Podesta,et al., *Big Data: Seizing Opportunities, Preserving Values* (2014).

14 Department of Business, Innovation, & Skills, *Seizing the Data Opportunity: A Strategy for UK Data Capability* (2013).

3.12 In the Budget 2014 Statement, the Chancellor of the Exchequer, George Osborne announced the creation of the Alan Turing Institute for Data Science[15] This will strengthen the UK's aim to be a world leader in the analysis and application of Big Data.

> We will keep building towards effective personalised 21st century democracy, with transparency informing better choice over more modern and effective public services, and open data as a key driver of innovation and growth. The future is open and Britain is leading the way.[16]

3.13 The UK is not alone in this aim. In 2012, the United States announced a $200m investment into Big Data. Furthermore, the European Council Conclusions of October 2013 called on the EU to 'provide the right framework conditions for a single market for Big Data and Cloud computing […]'.[17] In July 2014, the European Commission published its strategy for Big Data. As part of this strategy, the EU intends to:

- Support lighthouse data initiatives capable of improving competitiveness, quality of public service and citizen's lives;
- Extensively share, use, and develop its public data resources;
- Develop enabling technologies, underlying infrastructures, and skills, particularly to the benefit of SMEs, and
- Make sure that the relevant legal framework and policies are data-friendly.

3.14 Big Data clearly represents a considerable opportunity for the UK and the EU. This opportunity is not only measured in terms of growth but also by its potential for innovation, advances in research, and evidence-based policy and decision-making. However, it is not without risks to individuals' data protection rights. As many respondents pointed out in our Call for Evidence, finding the balance between unlocking the full potential of Big Data and protecting personal data will be a challenge for policy-makers. What is most challenging about Big Data is perhaps its unpredictability. As the Nottingham University Business School stated 'it is impossible to forecast the ways that data will be used, because it can be shared and reused without wearing out'.[18]

3.15 There are many challenges around how to utilise the value of data whilst making it more accessible. In October 2013, the Government published a strategy for UK data capability entitled: *Seizing the Data Opportunity*, which considers how the UK can make sure that it is well-positioned to be at the forefront of extracting knowledge and value from data.[19]

3.16 As an example of the work being done in this field, the IPO makes IP data freely available through online journals and online registers. The sources of data provide detailed information on IP cases but they do not easily allow for mass analysis. In May 2014, the IPO published its first analysable IP dataset for patent data allowing statistical research to be carried out more easily. Equivalent datasets for trademarks and designs are due to be published during 2014-15.[20]

---

15 The Rt Hon George Osborne MP, Chancellor of the Exchequer, *Budget Speech* (2014).

16 The Rt Hon Francis Maude MP, *Speech at the Connect Conference* (2014). Available at: https://www.gov.uk/government/speeches/francis-maude-speech-at-the-connect-conference, accessed on 29 August 2014.

17 European Council, *Conclusions October 2013* (2013). Available at: https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139197.pdf, accessed on 25 November 2014.

18 Nottingham University Business School, *submission of evidence,* response to question 3.

19 HMG, *Seizing the Data Opportunity*.

20 HMG, *Big Open Data Strategy* (2014).

Value of Public Data

The Public Data Group (PDG) brings together four public sector bodies – Companies House, Land Registry, Met Office and Ordnance Survey which collect, refine, manage and distribute data on the nation's companies, property, weather and geography.

Many datasets are available for free but not all are, and the value of the data that is charged for is vast. Two examples include Ordnance Survey data which is widely used in the insurance sector and the billions of pounds saved by the use of Met Office data in the aviation industry. The value of the Open Data released by the Public Data Group is very significant and growing. The most recent estimate placed the value of Open Data released by PDG at over £900m annually.[21]

There are key challenges in making data available free, for which there is currently a charge.[22] There may be a direct cost to the taxpayer where public funds are required to replace commercial income streams; there may also be indirect costs for the organisations involved. The UK is managing the different factors involved by making all data which can be legally released available under one of four pricing categories. These range from Open Data: where data is released at no cost and where necessary under an Open Government Licence to Commercial Rates: where data is available at a price that covers the cost of its collection, distribution and any service element and makes a reasonable level of return.

Cloud Computing

3.17 Connected to Big Data is 'cloud computing'. Many respondents listed this as another opportunity and challenge for the EU and the UK. The ICO defines cloud computing broadly as: 'access to computing resources, on demand, via a network'.[23]

3.18 The National Institute of Standards and Technology (NIST), part of the US Department of Commerce, viewed 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. These can be rapidly provisioned and released with minimal management effort or service provider interaction.[24]

3.19 Storing documents and files online instead of purely on a computer is an example of when we often use the Cloud. Accessing web-based email from mobile WiFi is another example. Services also exist which allow multiple individuals to share and work on the same document online.

---

[21] Deloitte. *Market Assessment of Public Sector Information* (2013).

[22] HMG, *Public Data Group Open Data Statement* (2014).

[23] Information Commissioner's Office, *Guidance on the Use of Cloud Computing* (2012).

[24] National Institute of Standards and Technology, *The NIST Definition of Cloud Computing* (2011).

3.20 The European Commission believes that action taken to develop the Cloud could lead by 2020 to an annual increase of €160bn to EU GDP. In the UK Government's *Information Economy Strategy Call for Evidence*, published February 2013, the Government observed that the UK Cloud services market is expected to reach £3.9bn in 2015, according to a report by TechMarketView.[25]

Advantages

Cloud Computing Case Study

Love Clean Streets is a free online portal that helps people who live or work in London to upload photographs of community problems like graffiti and illegal dumping which require action by the local authority.

Love Clean Streets, *Love Clean Street* (2012).

3.21 SMEs are foremost among the beneficiaries of the Cloud. Data-driven SMEs, particularly micro businesses started by a few individuals, can struggle with barriers to entry such as the necessary hardware, software, and the need to hire IT professionals. The Cloud offers SMEs opportunities to store their data online and access it remotely. It may often be 'pay as you use', affording SMEs flexibility to scale their data use up or down and therefore better manage costs. According to a 2012 journal article, the removal of these barriers to entry may go some way to addressing the competitive balance between SMEs and large companies.[26]

3.22 A 2009 European Union Agency for Network and Information Security (ENISA) study provides evidence for these benefits to SMEs.[27] The study surveyed 74 SMEs across a variety of countries, with UK SMEs making up the largest proportion of businesses polled. SMEs were asked to give reasons for why they have used or would use a form of cloud computing. The most popular reason cited was 'avoiding capital expenditure in hardware, software, IT support', with 68.1% of SMEs indicating this as a factor.[28] The second most popular reason was 'Flexibility and scalability of IT resources' (63.9%).[29]

3.23 In its evidence to this Review, the Cookie Collective stated the Cloud offered 'enormous opportunities for economic efficiency, growth, and benefit to individuals in terms of new global services'.[30] However, it cautioned against regulatory barriers which may restrict these benefits.

[25] Business, Innovation, & Skills, *UK Government Information Economy Strategy: A Call for Evidence* (2013).

[26] J. Zabalza, R. Rio-Belver, E. Cilleruelo, G. Garechana, J. Gavilanes, *Benefits Related to Cloud Computing in the SMEs* (2012).

[27] ENISA, *An SME Perspective on Cloud Computing* (2009).

[28] Idem.

[29] idem.

[30] Cookie Collective, *submission of evidence,* response to question 3.

Concerns

3.24 While many respondents viewed the Cloud as an opportunity of which the EU must take advantage, concerns have also been expressed over the risks it poses to personal data and the way it relates to traditional data protection concepts.

3.25 Durham University observed that the Cloud is often characterised by a lack of control over the data.[31] This is echoed by the European Data Protection Supervisor, who noted that most cloud-clients do not know where physically in the Cloud the data for which they are responsible is located.[32] In addition to the problem this may pose for security of the data, this also challenges classical data protection terminology and the traditional distribution of responsibilities between Controller and Processor. In the previous chapter, evidence was discussed from stakeholders who felt the traditional terminology was not adapting to the new environment of Cloud Computing. Several participants in the Belfast workshop commented that it was leading to situations of data controllers without control.[33]

3.26 In his response to the Commission's paper on *Unleashing the Cloud*,[34] the European Data Protection Supervisor warned that there was already an imbalance between the relatively small number of Cloud providers and the far greater number of clients. This imbalance may affect the negotiations of contracts between clients and providers, giving providers the potential to limit their security obligations and liability. Coupled with the reduced ability of data controllers to control the data, this could undermine the security of personal data. Durham University also cautioned about the lack of transparency about the relationship of responsibilities and processes within the Cloud.[35]

3.27 The ability of data to move rapidly within the Cloud and the lack of transparency about its physical location pose another problem for policy-makers. The Cloud is often spoken of as borderless. In its evidence, the British Bankers' Association stated that the EU's focus on geographical restrictions to transfers was at odds with the nature of how information moves in the Cloud.[36]

3.28 In 2012, the Article 29 Working Party, the panel of European data protection authorities adopted an Opinion expressing its concerns.[37] It emphasised the uncertainty and lack of transparency about where the data were held, and what the consequence was for the individual who wanted to know how and where their data was being processed.

---

[31] Durham University, *submission of evidence*, p11.

[32] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the Potential of Cloud Computing in Europe'* (2012).

[33] *Record of 11 June 2014 stakeholder event,* Northern Ireland.

[34] European Commission, *Opinion of the European Data Protection Supervisor.*

[35] Durham University, *submission of evidence,* p11.

[36] British Bankers Association, *submission of evidence,* p6.

[37] Article 29 Working Party, *Opinion on Cloud Computing* (2012). Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, accessed on 10 September 2014.

3.29 As the Cloud develops, with more types of data being uploaded, these concerns become even more relevant. In its evidence to this Review, GeneWatch UK noted that recent research and technological developments have allowed the human genome to be sequenced and stored in the Cloud along with medical records.[38] It stressed the importance of data protection principles and their applicability to the Cloud in order to improve security and privacy.

Looking Ahead

3.30 The European Data Protection Supervisor observed that there was a danger of the already imbalanced Cloud market consolidating and leading to an even more limited number of service providers. A number of respondents to this Review stated that the market was dominated by a small number of providers primarily based in the US. Part of the Commission's strategy involves supporting the development of European cloud providers. Among its many goals, the Commission intends to:

- Cut through the jungle of technical standards;
- Support EU-wide certification schemes for trustworthy cloud providers;
- Develop model 'safe and fair' contract terms for cloud computing contracts, and
- Develop a European Cloud Partnership with Member States and industry to harness the public sector's buying power to shape the European cloud market, and boost the chances for European cloud providers to grow and become competitive.

3.31 When the Commission unveiled its Cloud strategy paper, Vice-President Neelie Kroes stated:

> Cloud computing is a game-changer for our economy. Without EU action, we will stay stuck in national fortresses and miss out on billions in economic gains. We must achieve critical mass and a single set of rules across Europe. We must tackle the perceived risks of cloud computing head on.[39]

3.32 In its evidence, Durham University stressed the necessity of trust for the Cloud's future development.[40] Individuals or consumers must have the confidence that their personal data were secure if the industry is to grow. The Cookie Collective expressed the interaction of trust and growth in its evidence:

> Cloud computing – and the potential for better borderless delivery of services that it represents – is a huge opportunity for the UK and the global economy […]. We also need strong protections in order to give consumers confidence that their interests are protected in the global marketplace. This is what will see the true benefits of cloud computing released and shared amongst us all.[41]

3.33 As with Big Data, the Cloud's development may be unpredictable. Policy-makers are faced with several challenges: not only the challenges of making sure the Cloud's potential is tapped while protecting personal data within it, but also of future-proofing any legislation in an ever-changing environment.

---

[38] GeneWatch UK, *submission of evidence,* response to question 4.

[39] European Commission, *Digital Agenda: New Strategy to Drive European Business and Government Productivity via Cloud Computing* (2012).

[40] Durham University, *submission of evidence,* p11.

[41] Cookie Collective, *submission of evidence,* response to question 10.

The Internet of Things

3.34 The IoT was cited by a small number of respondents as a challenge for the future. In an article for the *Privacy & Data Protection Journal*, Treacy and Bapat gave the following definition:

> The Internet of Things refers to devices that are connected via the internet and communicate with each other, individuals, and enterprises. The Internet of Things encompasses virtually all products and services, including phones, medical devices, smart home appliances, wearable technologies, banking services, and cars […].[42]

3.35 The IoT can include devices which monitor your fitness level and blood pressure and then transmit the information to your computer or online account. Another example is a baby monitor with information about the child's movements and temperature. A report from Gartner predicted that there will be 26bn units as part of the IoTs in 2020, compared to a predicted 7.3bn of smartphones, tablets, and PCs.[43]

Internet of Things Case Studies

- Web-enabled lights can be used as an ambient data displays (glow red when my bus is 5 minutes away). These multi-functional lights can also help you to reduce electricity use (automatically turn off the lights when no one is in a room) or help to secure your home while you are away by turning your lights on and off.
- Glow Caps fit prescription bottles and via a wireless chip provide services that help people stick with their prescription regime; from reminder messages, all the way to refill and doctor coordination.
- Smart Belly rubbish bins use real-time data collection and alerts to let local authorities know when a bin needs to be emptied. This information can drastically reduce the number of pick-ups required, and translates into fuel and financial savings for local authorities.
- Smart thermostats like the Nest use sensors, real-time weather forecasts, and the actual activity in your home during the day to reduce your monthly energy usage by up to 30%, keeping you more comfortable, and offering to save you money on your utility bills.

Source: Internet of Things, *Internet of Things* (no date) available at: http://postscapes.com/internet-of-things-examples/, accessed on 25 November 2014.

3.36 The IoT shares many of its advantages and disadvantages with Big Data. Like Big Data, IoT devices can lead to more efficient outcomes by providing greater information. In March 2014, David Cameron announced the Government would be spending £45m on the development of technology for the IoT.

> I see the internet of things as a huge, transformative development – a way of boosting productivity, of keeping us healthier, making transport more efficient, reducing energy needs, tackling climate change.[44]

---

[42] B. Treacy, and A. Bapat, 'The 'Internet of Things' – already in a home near you?' *Privacy & Data Protection Journal.* Vol. 14 Issue 2 (2013), p11-13.

[43] Gartner, *Forecast: The Internet of Things, Worldwide* (2013).

[44] Rt. Hon. David Cameron, *CeBIT 2014 Speech* (2014). Available at: https://www.gov.uk/government/speeches/cebit-2014-david-camerons-speech, accessed on 24 November 2014.

3.37 Like Big Data, however, the IoT can also lead to concerns about privacy. A survey by the European Commission found that a majority of polled citizens and consumer organisations believed there needs to be a greater focus on data protection for the IoT.[45] In particular, they emphasised the importance of individuals' consent to becoming part of an IoT data system and consent to their data being used for purposes different from those they originally agreed to.

3.38 Treacy and Bapat observed that it is characteristic of the IoT to use and compare multiple data sets, and that care must be taken to limit data being processed for multiple purposes.[46] In the Commission's report, it noted that IoT devices often collect data as they move through environments, leading to data which possibly reveals individuals' activities and locations. Businesses responding to the Commission's report, however, worried that multiple requirements for explicit consent from individuals would limit the development of the IoT.

3.39 In its evidence, the Law Society expressed a concern that some IoT devices used by individuals may intrude on the privacy of others.[47] They suggested that in order to avoid the users of the device being deemed data controllers and regulated, policy-makers should investigate ways of regulating privacy into the design of these products.

3.40 This is another example of developments in technology challenging existing data protection concepts. As with Big Data and Cloud Computing, the challenge is to protect individual data protection rights while encouraging the industry's evolution.

The Proposed General Data Protection Regulation

3.41 Developments of new processing technologies and new trends of data-use formed part of the background to the European Commission's proposals for new data protection legislation. The perceived uneven implementation of the 1995 Directive across Member States also played a part.

3.42 While acknowledging that the 1995 Directive has performed well over the years, a Communication published in 2010 focused on the profound changes in the last 20 years and the need to meet new challenges.[48] In an age of automatic data collection, it has become increasingly difficult to determine when, how, and why personal data are being collected. Cloud computing and globalisation pose the question of where the personal data are being stored and by whom.

3.43 Moreover, a Euro-barometer Report found that 74% of Europeans surveyed considered that disclosing personal data was 'an increasing part of modern life'.[49] 79% felt it was most important to disclose their data for online shopping, and 61% mentioned the influence of social networks and sharing sites. In its Communication, the European Commission suggested individuals had experienced difficulties in retrieving or deleting their personal data from such sites.[50]

---

45 European Commission, *Conclusions of the Internet of Things Public Consultation* (2013).

46 Idem.

47 The Law Society of England and Wales, Law Society of Scotland, *submission of evidence*, p10.

48 European Commission, *A Comprehensive Approach on Personal Data Protection in the European Union* (2010).

49 Eurobarometer, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union* (2011). Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf, accessed on 29 August 2014.

50 Idem.

3.44 The Commission contended also that the 1995 Directive was implemented to differing degrees across Member States, leading to a fragmented European data protection framework. Many respondents to this Review observed that fragmentation can impose costs on businesses operating across borders.

3.45 With the aim of addressing these issues, the European Commission published new legislative proposals on 25 January 2012. The proposals contain both a Regulation (for general processing), and a Directive (for processing in police and judicial co-operation cases, even where there is no cross-border element).

Directive v Regulation

To increase harmonisation, the Commission has chosen a Regulation as the instrument to repeal and replace the Data Protection Directive.

Unlike a Directive, the provisions in a Regulation are directly applicable to all Member States. A Regulation can impose binding legal obligations and create enforceable rights for the individual without the need for primary national legislation.

3.46 While there was near consensus among respondents to this Review on the need to update the existing data protection framework, views were mixed on whether the Commission's proposed Regulation would strike the right balance between protecting personal data and facilitating its flows when necessary for societal and economic purposes. Some respondents welcomed the opportunity to strengthen individual rights.

3.47 However, respondents from a broad range of sectors questioned its 'one-size-fits-all' approach and its ability to meet the requirements which organisations and society have for data. Evidence from a variety of sectors, from medical research to fraud prevention services, revealed that data flows are not only necessary for economic growth alone. Data are vital for the purposes of life-saving medical research, for example.

UK Government Position

3.48 The UK's longstanding position has been a preference for a Directive over a Regulation. A Directive would allow for greater flexibility in the transposition of data protection rules into the domestic framework of Member States to take better account of national tradition and legal practice.

3.49 The evidence can be grouped into several key themes:

- Relation to individual rights;
- Importance of harmonisation;
- Challenges for research and archives;
- Challenges for fraud prevention and lending;
- Challenges for SMEs;
- Challenges for advertising and consent; and
- Importance of flexibility and proportionality.

Relation to Individual Rights

3.50 One of the Commission's aims in proposing the Regulation was to strengthen individuals' rights by increasing their awareness and control of how their data are used.

3.51 There were a number of respondents who identified opportunities in the draft Regulation to improve individuals' data protection rights. The British Computer Society observed that the proposed Regulation offered greater rights to individuals.[51] Similarly, the Law Society thought the Regulation would strengthen rights, with the possibility also of improving the security of personal data.[52] The Law Society viewed the draft Regulation as an opportunity to reinforce lawyer-client confidentiality.[53] The Open Rights Group argued that UK citizens benefit from less protection than individuals in other Member States, and that the draft Regulation would go some way to address this.[54]

3.52 Respondents cited a number of rights and provisions in the draft text to support these conclusions. Among these were the right to erasure and the right for a person to have their personal data transmitted in a portable format. In its evidence submitted to the Ministry of Justice's Consultation on the proposed Regulation, the Open Rights Group observed that the right to erasure could be useful for individuals wanting to remove their data from social networks.[55]

3.53 Krowdthink believed there was an opportunity to encourage awareness of the importance of trust for businesses. They gave the example of a person who withdraws money from a bank if he or she loses trust in the bank. This, they believed, should be possible with data and online service providers.[56] The Open Rights Group suggested the 'right to portability' could help promote both privacy and competition. However, it felt the right would need a greater interoperability between services than that which exists as present in order to be effective.[57]

3.54 The Open Rights Group welcomed other provisions such as the introduction of privacy by design and default, which would restrict data being used for further purposes. It observed that individuals often cannot predict how their data may be further combined and used by organisations.[58] Consumer Focus argued the proposed Regulation offers individuals greater control and transparency over how their data are used.[59] Both welcomed the right for individuals with complaints to be represented by consumer organisations.

3.55 In addition, one respondent observed that individuals could benefit from pseudonymous data being brought firmly into the scope of the Regulation.[60]

---

[51] British Computer Society, *submission of evidence,* p5.

[52] The Law Society of England and Wales, Law Society of Scotland, *submission of evidence,* p7.

[53] Idem.

[54] Open Rights Group, *submission of evidence,* p1.

[55] Open Rights Group, *Evidence to the Ministry of Justice Call for Evidence on the Regulation* (2012). Available at: https://www.openrightsgroup.org/ourwork/reports/moj-data-protection-call-for-evidence, accessed on 3 November 2014.

[56] Krowdthink, *submission of evidence,* p2.

[57] Open Rights Group, *Evidence to the Ministry of Justice Call for Evidence on the Regulation*.

[58] Idem.

[59] Consumer Focus, *Evidence to the Ministry of Justice Call for Evidence on the Regulation* (2012). Available at: http://www.consumerfocus.org.uk/files/2009/06/Consumer-Focus-response-to-Ministry-of-Justice-Call-for-Evidence-on-EU-Data-Protection-Proposals.pdf, accessed on 3 November 2014.

[60] Casper Bowden, *submission of evidence,* p3.

General Points on Harmonisation

3.56 Another of the Commission's aims in proposing this Regulation was to reduce national differences in the level of data protection across the EU. To increase harmonisation, the Commission has chosen a Regulation as the form of instrument to replace the 1995 Directive.

3.57 The Commission has argued that further harmonisation was necessary to help create a level playing field across Member States, and reduce legal uncertainty and administration costs for businesses.

3.58 Some respondents to this review identified opportunities for business in terms of greater harmonisation of data protection law through the Regulation. Durham University thought that reform of the current data protection framework would lead to greater harmonisation and the removal of administrative burdens for business.[61] BCS felt that the new proposals would benefit businesses as the same legal text would apply uniformly to all Member States.[62]

3.59 This assessment was echoed in several respondents' evidence. The Faculty of Advocates felt harmonisation would lead to fewer costs and risks when transferring personal data over borders.[63] Similarly, the Law Society believed harmonisation would help to offset implementation costs.[64] The concept of the One Stop Shop for investigation complaints was cited as an example by the Cookie Collective of how the text may benefit businesses who operate across the EU and would need to interact with up to twenty eight different regulators.[65]

3.60 Conversely, a large number of respondents were concerned that a lack of flexibility would be disadvantageous to organisations in diverse sectors. This evidence is explored further in the sections below.

Challenges for Research and Archives

3.61 There was a broad view among respondents that the draft Regulation may have a negative impact on research, particularly in the health sector. Access to personal data is a cornerstone of medical research. Patient data are used for researching diseases, conducting clinical trials, and testing treatments. In the view of the Breast Cancer Campaign and others 'patient data holds the key to medical progress'.[66]

3.62 Although respondents felt that the European Commission's original proposals struck a fair balance between promoting life-saving research and protecting patient data, concerns were expressed about the European Parliament's version of the text. This text will become particularly important during the 'trialogue' process when the Commission, the Council, and the Parliament negotiate a final version of the draft Regulation.

---

[61] Durham University, *submission of evidence,* p3.

[62] British Computer Society, The Chartered Institute for IT, *submission of evidence,* p5.

[63] Faculty of Advocates, *submission of evidence,* p3.

[64] The Law Society of England and Wales, the Law Society Scotland, *submission of evidence,* p3.

[65] The Cookie Collective, *submission of evidence,* p2.

[66] Breast Cancer Campaign, *submission of evidence,* p1.

3.63 Respondents including Eurocat, Medical Research Council UK, Breast Cancer Campaign, ARMC, NHS European Office, and Parkinson stated that the current European Parliament text would make 'much research involving personal data at worst illegal, and at best unworkable.[67] Requirements for consent were identified by all as a problem.

3.64 The Academy of Medical Sciences expressed a serious concern that the European Parliament has restricted the derogations which researchers can use regarding consent. They indicated that, while researchers seek consent whenever possible, a requirement for explicit consent is not feasible for certain types of studies. The Academy gave the example of cohort studies, bio banks, and disease registries as cases where data are frequently re-used, making obtaining explicit consent impractical. It was stressed by several respondents that strict safeguards for confidentiality and ethical approval always cover this type of research, and that much data is also anonymised to reduce the risk to patients' privacy.

3.65 Stakeholders from the research sector were unanimously clear that the retention of such restrictions in the final text would threaten the future of scientific research in the UK and EU. The Welsh Government warned that innovations in health technology were also at stake.[68]

3.66 The British Heart Foundation made the point that the final Regulation text 'must strike the right balance between protecting personal data whilst enabling life-saving research'.[69]

3.67 The National Archives provided evidence on the additional risk to archives. It warned that restrictions on archives could lead to higher costs for both public archives and private sector ones and challenge their financial viability. At worst, there was a risk that private sector archives' processing could be outlawed.[70]

Challenges for Fraud and Lending

3.68 The impact on the prevention of fraud and the provision of credit was identified as another concern. There was a widespread view amongst respondents from the financial, credit, insurance, and fraud-prevention sectors that both the Commission and Parliament texts posed problems.

3.69 The Finance and Leasing Association gave evidence highlighting the importance of data processing, profiling, and sharing for society. Credit reference agencies and lenders depend on the analysis of data to assess risks properly and make sustainable decisions about loans. The data are used to process applications for credit, provide the credit, and service the agreement.[71] Experian agreed and thought that restrictions on this processing could lead to poor decisions, increasing debt and financial exclusion.[72]

3.70 In addition, respondents identified a potential negative impact on fraud-prevention. CIFAS, the UK's non-profit fraud prevention service, was concerned that the draft Regulation would limit its ability to share data to prevent fraud.[73] Acromas also stressed the necessity of profiling for insurance providers in order to prevent fraud, restrictions on the ability

[67] British Heart Foundation, *submission of evidence,* p1.

[68] The Welsh Government, Department for Economy, Science, and Transport, *submission of evidence,* p.1

[69] British Heart Foundation, *submission of evidence,* p1.

[70] The National Archives, *submission of evidence,* p1.

[71] Finance and Leasing Association, *submission of evidence,* p1.

[72] Experian, *submission of evidence,* p8.

[73] CIFAS, *submission of evidence*, p2.

to profile, it considered, would lead to greater fraud and higher insurance premiums to cover it.[74] The British Bankers' Association also warned that the draft provisions could have the unintended consequence of limiting profiling to prevent money laundering and detecting terrorism.[75] The Wealth Management Association noted it has concerns about how the Regulation may affect obligations to prevent financial crime.[76]

3.71 Examples of problem areas include restrictions on processing, auto-processing and profiling. In addition, Experian and the Finance and Leasing Association expressed a worry about potential uses of the right to erasure. This may lead to the deletion of information vital for proper risk assessment and fraud prevention.[77] The Finance and Leasing Association also made the point that the principle of data minimisation is at odds with these purposes.[78]

Challenges for SMES

3.72 In general, respondents expressed concerns for the impact of the proposed Regulation on micro businesses or SMEs. The Department for Economy, Science and Transport in Wales felt it posed potential barriers for the development of SMEs, while the Federation of Small Businesses stated that the draft Regulation will increase costs and burdens on SMEs, sometimes unnecessarily. The Faculty of Advocates acknowledge that 'large economic operators may be able to absorb the costs associated with onerous and evolving data controlling obligations' but 'such costs may be unduly burdensome and even disproportionate' on smaller organisations.[79]

3.73 The Advertising Association identified several key areas of concern for SMEs, including requirements for explicit consent, complying with erasure requests, and possible restrictions or disincentives concerning the use of pseudonymous data.[80] A 2013 study by Christensen, Colciago, Etro, and Rafert examined the impact on SMEs and pointed out additional costs such as designing new systems to meet security requirements and to comply with individuals exercising their right to portability of their data.[81]

3.74 A requirement to appoint a Data Protection Officer, costing potentially £60,000 per annum, was also identified by several respondents as a potential problem. While not all SMEs may be affected by this requirement, the Federation of Small Businesses expressed particular concern about the European Parliament's use of the number of data subjects as a defining threshold. Which? thought the sensitivity of the data should be a factor.[82]

---

[74] Acromas Group, *submission of evidence*, p3.

[75] British Bankers Association, *submission of evidence,* p6.

[76] Wealth Management Association, *submission of evidence,* p1.

[77] Experian, *submission of evidence,* p8. and Finance and Leasing Association, *submission of evidence*, p3.

[78] Finance and Leasing Association, *submission of evidence,* p3.

[79] Faculty of Advocates, *submission of evidence,* p2.

[80] Advertising Association, *submission of evidence,* p4.

[81] L. Christensen,A. Colciago, F. Etro and G. Rafert, *The Impact of the Data Protection Regulation in the EU* (2013).

[82] Which?, *Evidence for the Ministry of Justice Call for Evidence on the Proposed Regulation* (2012). Available at: https://consult.justice.gov.uk/digital-communications/data-protection-proposals-cfe/results/summary-responses-proposed-data-protection-legislation.pdf, accessed on 25 November 2014.

3.75 Even without a Data Protection Officer, SMEs may need to pay for guidance or legal advice to make sure they are compliant. One respondent pointed out that the complexity of the text, and its focus on processes rather than outcomes, would be particularly problematic for SMEs. Many may not have the necessary expertise and would struggle to understand the requirements for compliance. Similarly, the Federation for Small Businesses argued that many would not know how to apply the rules.

3.76 However, the proposed One Stop Shop was identified as a potential benefit to SMEs in the study by Christensen et al.[83] The One Stop Shop means that organisations operating in more than one Member State need only interact with a sole regulator in the country where their main establishment is based. The European Commission also emphasised that this would reduce costs for businesses, including SMEs. However, the extent of the benefits may be limited, depending on the number of SMEs which operate in several Member States. A survey of SMEs by the Department for Business, Innovation, and Skills found that only 19% of established SMEs in its sample exported products outside the UK.[84]

3.77 While the Federation for Small Businesses acknowledged that it was necessary to update data protection laws, overall it concluded that the proposed Regulation was 'overly prescriptive', and this imposed unnecessary costs and burdens on SMEs.[85] An Impact Assessment by the Government in 2012 estimated the effect the Commission's initial draft text would have on the UK's SME sector and considered it would cost between £80m and £290m per annum in 2012-2013 earning terms.[86] In its evidence, the Advertising Association warned of long-term consequences due to a decrease in innovation.[87] Further costs were predicted by Christensen et al in terms of unemployment and fewer start-ups.[88]

Challenges for Advertising and the Issue of Consent

3.78 The latest Council version of the proposed Regulation requires consent to be 'freely given, specific, and informed' if an organisation is to rely on it as a basis for processing. The original Commission text and the European Parliament text also require consent to be 'explicit'. Under the existing Directive, 'explicit' consent is required only for processing sensitive data which pose special risks.

3.79 Some respondents from the advertising sector and others thought the requirements for consent were particularly disproportionate. For example, the Advertising Association, the Direct Marketing Association, Acromas, and the British Bankers' Association argued explicit consent was unpractical and disproportionate. While the Advertising Association acknowledged sensitive data needed robust protection, a risk-based approach needed to be taken with other types of personal data. It warned that applying explicit consent to all personal data could lead to desensitisation for consumers.[89]

---

83 Christensen, L, A Colciago, F Etro and G Rafert, *The Impact of the Data Protection Regulation in the EU* (2013). Available at: http://www.intertic.org/Policy%20Papers/CCER.pdf, accessed on: 5th September 2014.

84 Business, Innovation, & Skills, *Small Business Survey 2012: Focus on New Businesses* (2013).

85 Federation of Small Businesses, *submission of evidence,* p5.

86 Ministry of Justice, *Impact Assessment: Proposal for an EU Data Protection Regulation* (2012).

87 Advertising Association, *submission of evidence,* p4.

88 Christensen, L, A Colciago, F Etro and G Rafert, *The Impact of the Data Protection Regulation in the EU.*

89 Advertising Association, *submission of evidence*, p4.

3.80 For example, consumers online would see constant pop up prompts demanding consent for every single ad which placed a cookie on their computer to track the ad's success. The British Bankers' Association agreed and felt this could lead to confusion and unnecessary worry for the consumer, particularly given the level of detail required for each notice. There was also the opposite risk according to the Advertising Association: consumers may become de-sensitised to these prompts and take them less seriously, undermining the meaningfulness of consent.

3.81 Acromas gave a further example of postal marketing, where a requirement for consent may lead to generic junk mail as opposed to marketing and discounts tailored to the recipient's interests.[90] The Advertising Association felt this served neither the interests of individuals nor organisations.[91]

3.82 In its evidence to the Ministry of Justice's consultation on the proposed Regulation, Which? questioned the effectiveness of privacy policies. It argued it was not feasible for many consumers to read their way through lengthy legal texts. This, it felt, was even less feasible to do on a mobile phone with a small screen.[92]

3.83 ARM Holdings considered that one future option to help minimise consent fatigue and complexity would be to create simplified sets of categories of data use.[93] This could be displayed in a prompt to the consumer and help them understand why the organisation wants their data. Which? recommended the development of accreditation schemes or kitemarks which would help the consumer better understand the choice they were making.[94]

3.84 No evidence was received on the impact of the draft Regulation on the Third Sector. However, in a briefing paper to its members in August 2014, the Institute of Fundraising (IoF) expressed concern that the European Commission's original proposals did not strike an appropriate balance between the rights of individuals and 'the fundamental need for charities to be able to fundraise'.[95] In particular, the IoF are concerned that the changes to the definition of consent contained in the draft Regulation would have a direct impact on those charities which use direct mail to fundraise. Under the proposed changes an individual would have to opt-in to receiving marketing material from organisations, including charities.

3.85 The IoF said that the proposal 'raised concerns that charities would be unable to target potential, current or past donors without having explicit consent'. The IoF believed the Regulation 'should include a clear statement clarifying that unsolicited marketing by post and telephone is considered to be a legitimate interest and therefore the existing opt-out regime remain in place for postal and telephone marketing'.[96]

---

[90] Acromas, *submission of evidence,* p3.

[91] Advertising Association *submission of evidence* p4.

[92] Which?, *Evidence to the Ministry of Justice Call for Evidence on the Proposed Regulation.*

[93] ARM Holdings and AMD, *submission of evidence,* p4.

[94] Which?, *Evidence to the Ministry of Justice Call for Evidence on the Proposed Regulation.*

[95] Institute of Fundraising, *EU Data Protection Proposals, Member Briefing* (2014).

[96] Idem.

Importance of Proportionality and Flexibility

3.86 The previous sections set out evidence from a wide range of sectors concerned with the impact on various organisations and industries in the UK and Europe. Two common factors in the evidence so far have been a perceived excess of detail and lack of flexibility in the Regulation, both of which may lead to disproportionate effects for organisations.

3.87 Several respondents thought that some of the proposals were excessively prescriptive and failed to take into account the different levels of risk associated with individual situations. RSA observed that a requirement to report even trivial breaches would become a considerable administrative burden. Excessive detail may lead to tick-box compliance instead of good practices. [97] Tick-box compliance was also a concern of Hunton and Williams, who argued that more emphasis should be given to principles over details.[98]

3.88 Some respondents raised concern about consequences for competition. The RSA made the point that disproportionate rules created burdens which acted as barriers to entry in markets and harmed competition. It argued that EU companies would be disadvantaged, while 'non EU businesses will be in a position to launch products and services far more expediently.'[99] In its response, the British Bankers' Association echoed this concern and stressed that limitations on international transfers were at odds with the reality of the global online economy.[100]

3.89 In its evidence to the Single Market report, British American Business emphasised the need to maintain the global competitiveness of the EU. Both it and the CBI expressed their concern that disproportionate, detailed rules may harm innovation.[101]

3.90 Such an approach may have implications for future-proofing. The British Bankers' Association suggested that a Regulation that is based on processes will be difficult to adapt and interpret in light of unpredictable technological changes. In its evidence, the British Bankers' Association, stated that the draft Regulation's detailed approach would soon lose its relevancy.[102]

> A principal concern is that the proposed Regulation goes well beyond the prescribing of what must be done by firms, to prescribing how they must achieve this, which removes technological neutrality.[103]

3.91 Flexibility was cited as an important requirement for data protection legislation. Respondents felt the approach of full harmonisation ignored the diverse ways in which data are required in many sectors. One respondent's evidence summarised the concerns of many: 'the EU looks to be running headlong towards enacting a Data Protection Regulation which does not address the different contexts in which data is processed, which sets rules that are in many contexts self-evidently unworkable, and does so against a background of large fines.'[104]

---

[97] RSA, *submission of evidence,* p4.

[98] Hunton and Williams, *submission of evidence,* p4.

[99] RSA, *submission of evidence,* p3.

[100] British Bankers' Association, *submission of evidence,* p1.

[101] HMG, *Review of the Balance of Competences: Single Market*.

[102] British Bankers' Association, *submission of evidence*, p3.

[103] Idem.

[104] Slober, *submission of evidence,* p1.

3.92 The British Bankers' Association agreed a one-size-fits-all approach was unworkable in the face of cultural differences and industry needs. A model based on risk assessment and principles was viewed as more appropriate by a number of respondents.

> The realities of business models needs to be reflected, making a one size fits all approach unworkable across the myriad of business models and realities, including cultural differences.[105]

3.93 Both the British Bankers' Association and Experian believed a flexible, principled approach was also vital for future-proofing.

The UK's Position

3.94 The UK is negotiating for a sensible and proportionate data protection framework that will strengthen privacy rights while creating the right conditions for innovation and economic growth. We consider that these twin objectives can be achieved in tandem and not at the expense of one another. The original Commission proposals did not deliver against these aims, with an excessive focus on prescriptive requirements and process. In 2012, the UK carried out an impact assessment of the Commission's initial proposals which identified that the proposals, if implemented, could impose a net cost in the range of £100 – £360m to the UK economy alone.[106] The UK's impact assessment is currently being updated.

3.95 However, negotiations in the Council have led to a more risk-based approach being introduced into the text, so the obligations placed on data controllers and regulators are relative to the degree of harm involved in the processing of the personal data. While the UK consider that this approach should be further strengthened, the current working text has stripped out many of the more costly provisions which we were most concerned about and were identified through the evidence submitted to this report. It is important that no additional barriers are put in place that would undermine legitimate data processing that currently take place, which provides both business and wider societal benefits.

Cross-cutting Themes

3.96 Across these four challenges, and indeed this review, respondents identified potential weaknesses or opportunities in the area of information rights and suggested further action. Cross-cutting themes include:

- The relationship between access to information and data protection;
- The need for future-proofing;
- The need for a balance between harmonisation and flexibility; and
- The need for understanding and engagement.

[105] British Bankers' Association, *submission of evidence,* p3.

[106] Ministry of Justice, *Impact Assessment: Proposal for an EU Data Protection Regulation*.

The Need to be Aware of the Relationship between Access to Information and Data Protection

3.97 British Computer Society observed that Member States have differing views over what information should be made public and what should not. It highlighted the development of 'a line of jurisprudence and application that will over time create gaps between how publicly held data and personal data are understood to relate to each other across the EU'.[107]

3.98 One respondent warned that the development of data protection law may cause public bodies to be more risk-averse when deciding whether to grant access to official information. Another challenge identified was the increased volume of data in the future. The ICO felt there was an opportunity for a joined up approach with initiatives for the reuse of data and the EU's Open Data strategy. Big Data will indeed offer opportunities for individuals to access more information, but there is a concern this will put pressure on public bodies' resources. The ICO also warned that growing privatisation of public services could make it harder to access official information.

3.99 Several respondents identified ways in which the EU could improve the existing Access to Documents Regulation. Experian, the Advertising Association, and the Direct Marketing Association thought the EU could do more to facilitate access to documents concerning legislation in progress, although it was appreciated there may be a need for confidentiality. GeneWatch UK and some participants at the Edinburgh event suggested the Access to Documents Regulation should extend to official information, rather than documents. Other participants at the Edinburgh workshop called for better ways of challenging refusals to share documents.[108]

The Need for Future Proofing

3.100 Respondents were almost unanimous in believing the 1995 Data Protection Directive needed to be updated to take account of vast changes in how data are used and transferred. The rise of Big Data, Cloud Computing, and IoT have challenged the applicability of standard data protection terminologies and concepts to such developments and indeed to future, unpredictable ones. Several respondents and participants at the Brussels workshop felt a principled approach would allow flexibility to meet unforeseeable changes.[109]

> In the era of digitalisation and ubiquitous information, Big Data and the Internet of Things, data protection regulation needs to be supplemented by flexible tools and concepts, such as organisational accountability and risk-based approach to regulation, implementation, and enforcement.[110]

[107] British Computer Society, *submission of evidence,* p7.

[108] *Record of 28 May 2014 stakeholder event,* Edinburgh.

[109] *Record of 18 June 2014 stakeholder event,* Brussels.

[110] Hunton and Williams, *submission of evidence*, p5.

The Need for a Balance between Harmonisation and Flexibility

3.101 Flexibility therefore has a role to play in making sure legislation can cope with unpredictable developments in technology and data use. The evidence has also shown that it is not only a question of weighing up individual rights and economic growth: there are benefits which data processing brings to society beyond economic growth. These include research into life-saving treatments, ways to improve the efficiency of policy-making and guard against fraud and indebtedness. Action in the area of information rights must be able to strike a balance between protecting rights and increasing data flows which are important for society and progress. Different needs both across industry sectors and across Member States ought to be considered. While harmonisation of standards offers benefits to both individuals and organisations, legislation must also be flexible enough to cover a wide variety of processing sectors and sizes, from multinationals to micro start-ups across all Member States.

> The future data protection regime should be pitched at a level that reflects the diversity of uses for data and is able to adapt to sectoral circumstances rather than a blanket approach.[111]

3.102 The House of Commons Justice Select Committee set out the need for a balance between harmonisation and flexibility as follows:

> We believe that the European Commission has a choice: It can continue to pursue the objective of harmonisation through a Regulation by focusing on the elements that are essential to achieve consistency and cooperation across Member States, whilst entrusting the details on compliance to the discretion of data protection authorities and the European Data Protection Board; alternatively, it can use a Directive to set out what it wants to achieve in all the areas contained in the draft Regulation, but then leave implementation in the hands of Member States, and forgoing an element of harmonisation and consistency.[112]

The Need for Understanding and Engagement

3.103 A common theme throughout the evidence has been the complex nature of data uses, legislation to cover data uses, and the rapid advance of processing technologies.

3.104 In Chapter Two, the complexity of the 1995 Directive was evoked as problematic for both individuals and SMEs who may lack the expertise and resources to interpret it. Both individuals and data controllers must also cope with the increasing complexity of online developments and increasing diversity in how data is processed. It is also an obstacle for policy makers. The Internet Advertising Bureau identified a lack of digital expertise as a weakness for the EU.[113] Caspar Bowden also stressed the importance of all policy-makers to learn about the technical side of privacy measures.[114] The British Computer Society stated: 'those exercising competence to regulate need to understand these new technologies and enact proper legislation'.[115]

---

[111] Finance and Leasing Association, *submission of evidence*, p3.

[112] House of Commons Justice Select Committee, *The Committee's Opinion on the European Union Data Protection framework Proposals – Justice Committee* (2012). Available at: http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/57205.htm, accessed on 1 September 2014.

[113] The Internet Advertising Association, *submission of evidence,* p3.

[114] Casper Bowden, *submission of evidence,* p4.

[115] British Computer Society, *submission of evidence,* p6.

3.105 Other stakeholders highlighted the importance of consultation with a greater range of stakeholders. The Finance and Leasing Association expressed concern that data protection is the responsibility of the Directorate-General for Justice (DG JUST) and Ministries of Justice across many Member States. It felt more attention needs to be paid to the perspectives of organisations and businesses that are affected by legislation.[116] Respondents from the credit sector believed EU policy-makers had not intended adverse effects on the prevention of fraud but that their views should have been taken into account earlier. Experian suggested that a clear and sustained engagement with stakeholders would improve the effectiveness of future EU legislation.[117] Respondents also identified a need to be aware of existing EU legislation in other areas which could potentially overlap or conflict with proposals.

3.106 Several stakeholders also emphasised the need for the EU to take the initiative further and engage with organisations such APEC to promote global data protection principles. Many participants at the Edinburgh event indicated there was also a need for the EU to raise awareness amongst citizens of the right to access EU official documents.[118]

[116] Finance and Leasing Association, *submission of evidence,* p2.

[117] Experian, *submission of evidence,* p6.

[118] *Record of 28 May 2014 stakeholder event,* Edinburgh.

Annex A: Submissions Received to the Call for Evidence

Submissions were received through an online response form or by email. Some respondents requested that their evidence remain anonymous. Some submissions considered a broad range of topics within the scope of the review, while some individuals and organisations focused on issues about which they held a particular interest. Some submissions contained viewpoints on topics not within the scope of the review.

Responses to the Call for Evidence were received from the following individuals and organisations

Academics

Professor Louise Amoore and Dr Volha Piotukh, Durham University
Dr Duncan R Shaw, Nottingham University Business School

Lawyers

Rosemary Jay, Hunton & Williams
Steven Lorber, Lewis Silkin LLP

Legal organisations

Faculty of Advocates
Law Society of England & Wales
Law Society of Scotland

NGOs and Third Sector Organisations

Association of Medical Research Charities (AMRC)
Breast Cancer Campaign
British Heart Foundation
Cancer Research UK
British Naturism
Gene Watch UK
Open Rights Group
Parkinson's UK

Parliamentary and Governmental

Liberal Democrats' Home Affairs, Justice and Equalities Parliamentary Party Committee
Scottish Government
European Commission
Crown Dependencies
Department for Economy, Science and Transport – Welsh Government
Social & Employment (Semester 3 report)
The National Archives

Banking Finance, Insurance and Fraud Prevention

British Bankers' Association (BBA), Association for Financial Markets in Europe (AFME) and the International Regulatory Strategy Group (IRSG)
Acromas Holdings & Saga PLC
Experian
Finance and Leasing Association
Wealth Management Association
RSA Insurance Group
CIFAS

Tech Industry

British Computer Society (BCS)
ARM Holdings PLC
Cookie Collective
Krowd think Ltd

Medical and Research

Academy of Medical Sciences
Medical Research
NHS European Office
Wellcome Trust

Media and Advertising

Advertising Association
Direct Marketing Association (DMA)
Internet Advertising Bureau (IAB)
The Newspaper Society

Think Tanks and Regulators

Information Commissioner's Office (ICO)
Digital Policy Alliance
European Surveillance of Congenital Anomalies

Representative Bodies

Federation of Small Business (FSB)

National Farmers Union (NFU)

Individuals

One individual responded to the online platform dialogue, whilst Caspar Bowden emailed his Evidence.

The following interested parties also submitted existing material for consideration

European Commission submitted previously published documents and reports.

House of Lords European Union Committee submitted to the whole Balance of Competences Review.

EU Committee reports and scrutiny correspondence.

In addition to the formal submissions to the Information Rights Call for Evidence, the following responses to other reviews have been considered, as they provided evidence in scope of the Information Rights Call for Evidence:

HMG, *Review of the Balance of Competences between the United Kingdom and the European Union: Subsidiarity and Proportionality* (published in parallel).

HMG, *Review of the Balance of Competences between the United Kingdom and the European Union: Environment and Climate Change* (2013).

HM Government, *Review of the Balance of Competences between the United Kingdom and the European Union: Single Market* (2013).

Annex B: Engagement Events

To help inform the Information Rights Report a number of workshops were held with interested parties to explore the issues raised in the Call for Evidence document.

These workshops, held under Chatham House rule, included:

29 April 2014 – Balance of Competences Information Rights Review workshop, London

Attendees: Hunton & Williams; Internet Advertising Bureau (IAB); Credit Services Association; Market Research Society Policy Unit; University of London; Open Rights Group; Experian; The British Library; Information Commissioner's Office (ICO); Guardian Newspaper; University of Leeds; Royal Mail; Bank of England; Birmingham City Council; General Medical Council; Callcredit; ValueClick; IBM; DLA Piper UK LLP; The Law Society; British Medical Association; Nottingham University Business School; Lewissilkin; Association of Chief Police Officers (ACPO); Finance and Leasing Association (FLA); Cookielaw.org; Chartered Institute for IT- BCS; Yahoo!; News UK; The Direct Marketing Association; Symantec Corporation; NHS; GE Capita; The Newspaper Society PERA. (34)

28 May 2014 – Balance of Competences Information Rights Review workshop, Edinburgh, Scotland.

Attendees: The Law Society of Scotland; Dundas & Wilson CS LLP; Information Commissioner Scotland & Northern Ireland; Glasgow University; Common Sense Privacy Ltd; Durham University; University of Edinburgh; Computer Law Training Ltd; Scottish Information Commissioner; NHS National Services Scotland; The Scottish Government; PNN Police; Scottish Environment Protection Agency.(12)

11 June 2014 – Balance of Competences Information Rights Review workshop, Belfast, Northern Ireland.

Attendees: Department of Environment; Department for Social Development; Department of Justice; Department of Culture Arts and Leisure; Department of Enterprise Trade and Investment; Department of Health; Office of First Minister and Deputy First Minister; Department of Regional Development; Department of Finance and Personnel. (17)

18 June 2014 – Balance of Competences Information Rights Review workshop, Brussels, Belgium.

Attendees: Symantec Corporation; Channel Islands Brussels Office; Isle of Mann Brussels Office; Digital Policy Alliance; Office of the European Data Supervisor; The Law Society; Council of the European Union; Software Alliance; NHS European Office. (10)

Other events:

During the course of the Call for Evidence period the Balance of Competences Review was also discussed at events arranged by various organisations such as the Cambridge Privacy Laws & Business's 27th Annual International Conference (01 July), Hunton and Williams breakfast seminar on Safe Harbour (05 February), Amber Hawk data protection conference (12 May) and the MoJ Data Protection Advisory Panel (28 June). These events attracted a total audience of approximately 400 people from all different spectrums of the information rights world. Two separate meetings were also held where officials discussed the process and the Call for Evidence.

Annex C: Other Sources used for the Review

Domestic Sources

Caldicott, F. *Information: To Share or Not to Share? The Information Governance Review* (2013).

Department for Business, Innovation, & Skills. *Seizing the Data Opportunity: A Strategy for UK Data Capability* (2013).

Department for Business, Innovation, & Skills. *Small Business Survey 2012: Focus on New Businesses* (2013).

Department for Business, Innovation, & Skills. *UK Government Information Economy Strategy: A Call for Evidence* (2013).

Environmental Information Regulation 2004.

Environmental Information (Scotland) Regulation 2004.

e-skills UK, the Sector Skills Council for Business and Information Technology, and SAS. *Big Data Analytics: An Assessment of Demand for Labour and Skills, 2012-2017* (2013).

Consumer Focus, *Evidence to the Ministry for Justice Call for Evidence on the Regulation* (2012).

The Rt Hon Francis Maude MP, *Speech at the Connect Conference* (2014).

Open Rights Group, *Evidence to the Ministry for Justice Call for Evidence on the Regulation* (2012).

House of Commons Justice Select Committee, *The Committee's Opinion on the European Union Data Protection framework Proposals – Justice Committee* (2012).

INSPIRE Regulation 2009

Ministry of Justice, *Impact Assessment: Proposal for an EU Data Protection Regulation* (2012).

Office of Fair Trading, *OFT Response to the Call for Evidence on a Common European Sales Law for the European Union – A Proposal for a Regulation from the European Commission* (2012).

Research by Design, *FSB 'Voice of Small Business' Survey Panel* (2013).

The Centre for Economics and Business Research, *Data Equity: Unlocking the Value of Big Data* (2012).

Deloitte, *Market Assessment of Public Sector Information* (2013).

Public Data Group Open Data Statement.

The Data Protection Act 1998.

The Freedom of Information Act 2000.

The Freedom of Information (Scotland) Act 2002.

Rt. Hon. David Cameron, *CeBIT 2014 Speech* (2014).

EU sources

Article 29 Working Party, *Opinion 05/2012 on Cloud Computing* (2012).

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions* (2014).

Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995.

European Commission, *Digital Agenda: New Strategy to Drive European Business and Government Productivity via Cloud Computing* (2012).

Environmental Information Directive 2003/4/CE on public access to environmental information, 2003.

Eurobarometer. *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union* (2011).

European Commission, *A comprehensive approach on personal data protection in the European Union* (2010).

European Commission. *Conclusions of the Internet of Things Public Consultation* (2013).

European Commission, *Results of the Public Consultation of the Top 10 Most Burdensome Legislative Acts for SMEs* (2013).

European Commission. *Towards a Thriving Data-Driven Economy* (2014).

European Commission, *Unleashing the Potential of Cloud Computing in Europe* (2012).

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"* (2012).

International Data Corporation, *Worldwide Big Data Technology and Services 2012-2015 Forecast* (2012).

European Commission, *Towards a Thriving Data-Driven Economy* (2014).

INSPIRE Directive 2007/2/EC

Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data

Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

Regulation (EC) 1049/2001 regarding public access to European Parliament, Council and Commission documents ("Access to Documents Regulation")

Treaty on European Union (Maastricht text), July 29, 1992, Article F 1992 O.J. C 191/1.

ECJ cases

Yassin Abdullah Kadi, Al Barakaat International Foundation v Council of the European Union, Commission of the European Communities, United Kingdom of Great Britain and Northern Ireland Cases C-402/05 and C-415/05 [2008].

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) – Case C-131/12 [13 May 2014].

Digital Rights Ireland Ltd (C-293/12) v Minister for Communications – Case C-293/12 [8 April 2014].

Council of Europe

Agreement between the European Community and the Council of Europe on cooperation between the European Union Agency for Fundamental Rights and the Council of Europe (2008)

ECHR Cases

Osterreichischer Rundfunk [2003] ECR 1-000 and Lindqvist C-101/01.

International Sources

Electronic Privacy Information Center, *Request for Information: Big Data and the Future of Privacy* (2014).

Podesta, J et al. *Big Data: Seizing Opportunities, Preserving Values* (2014).

Publications or Academic Articles

Christensen, L., Colciago,A., Etro, F., and Rafert, G., *The Impact of the Data Protection Regulation in the EU* (2013).

ENISA, *An SME Perspective on Cloud Computing* (2009).

Gartner, *Forecast: The Internet of Things, Worldwide, 2013* (2013).

Hijmans, Hielke and Scirocco, Alfonso, 'Shortcomings in EU Data Protection in the Third and The Second Pillars. Can The Lisbon Treaty be Expected to Help?', *Common Market Law Review* Vol. 46 (2009).

Love Clean Streets, *Love Clean Streets* (no date).

National Institute of Standards and Technology. *The NIST Definition of Cloud Computing* (2011).

Polcak, R. Aims, 'Methods and Achievements in European Data Protection', *International Review of Law, Computers, & Technology*, 23 (3) (2009).

Treacy, B and Bapat, A. 'The "Internet of Things" – Already in a Home Near You?', *Privacy & Data Protection Journal* Vol.14 (2) (2013).

Zabalza, Rio-Belver, Cilleruelo, Garechana, Gavilanes, *Benefits Related to Cloud Computing in the SMEs* (2012).