House of Commons

Justice Committee

The Committee's opinion on the European Union Data Protection framework proposals

Third Report of Session 2012–13

Volume I

Volume I: Report, together with formal minutes, oral and written evidence

Additional written evidence is contained in Volume II, available on the Committee website at www.parliament.uk/justicecom

Ordered by the House of Commons to be printed 24 October 2012

HC 572
Published on 1 November 2012
by authority of the House of Commons
London: The Stationery Office Limited
£15.50

The Justice Committee

The Justice Committee is appointed by the House of Commons to examine the expenditure, administration and policy of the Ministry of Justice and its associated public bodies (including the work of staff provided for the administrative work of courts and tribunals, but excluding consideration of individual cases and appointments, and excluding the work of the Scotland and Wales Offices and of the Advocate General for Scotland); and administration and expenditure of the Attorney General's Office, the Treasury Solicitor's Department, the Crown Prosecution Service and the Serious Fraud Office (but excluding individual cases and appointments and advice given within government by Law Officers).

Current membership

Rt Hon Sir Alan Beith (*Liberal Democrat, Berwick-upon-Tweed*) (Chair)
Steve Brine *(Conservative, Winchester)*
Mr Robert Buckland (*Conservative, South Swindon*)
Jeremy Corbyn (*Labour, Islington North*)
Nick de Bois (*Conservative, Enfield North)*
Christopher Evans (*Labour/Co-operative, Islwyn*)
Ben Gummer (*Conservative, Ipswich*)
Rt Hon Elfyn Llwyd (*Plaid Cymru, Dwyfor Meirionnydd*)
Seema Malhotra (*Labour/Co-operative, Feltham and Heston)*
Yasmin Qureshi (*Labour, Bolton South East*)
Elizabeth Truss (*Conservative, South West Norfolk*)
Karl Turner (*Labour, Kingston upon Hull East*)

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publication

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the internet at www.parliament.uk/justicecttee. A list of Reports of the Committee in the present Parliament is at the back of this volume.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some or all written evidence are available in a printed volume. Additional written evidence may be published on the internet only.

Committee staff

The current staff of the Committee are Nick Walker (Clerk), Sarah Petit (Second Clerk), Gemma Buckland (Senior Committee Specialist), Helen Kinghorn (Committee Legal Specialist), John-Paul Flaherty (Committee Specialist), Ana Ferreira (Senior Committee Assistant), Miguel Boo Fraga (Committee Assistant), Greta Piacquadio (Committee Support Assistant), George Margereson (Sandwich student), and Nick Davies (Committee Media Officer).

Contacts

Correspondence should be addressed to the Clerk of the Justice Committee, House of Commons, 7 Millbank, London SW1P 3JA. The telephone number for general enquiries is 020 7219 8196 and the email address is justicecom@parliament.uk

Contents

Report

Summary

When EU legislation for general and commercial data protection purposes was last agreed in 1995, the digital economy was in its infancy and the boom in social media had not begun. As a result, 17 years on the current EU Directive has been described as an analogue regime for a digital world. Additionally, EU citizens have new rights and freedoms to protect their data and privacy as contained within the Charter of Fundamental Rights of the European Union and the Lisbon Treaty.

In January 2012, the European Commission published detailed legislative proposals for European reform of data protection. These take the form of both a draft Regulation and a draft Directive. We agree that the draft Regulation is necessary, first to update the 1995 Directive and take into account past and future technological change; and secondly to confer on individuals their new rights and freedoms. We can see why the Commission also wish to update data protection for the purpose of law enforcement as part of an overall package, but we are concerned that the twin-track approach being taken will cause confusion for data subjects and in particular for organisations within the criminal justice system. We are also concerned that the data protection provisions contained in the draft Directive are weaker than in the draft Regulation, and agree with the UK Information Commissioner that data protection principles should be consistent across both instruments. This must be at a high level.

The draft Regulation, through harmonising data protection laws across the 27 Member States, has the potential to make data protection compliance easier, in particular for small business who wish to trade across the European Union. We can understand why the European Commission decided that a Regulation was the correct instrument to achieve harmonisation, but by also setting out prescriptive rules there is no flexibility to adjust to individual circumstances. We believe that the Regulation should focus on stipulating those elements that it is essential to harmonise to achieve the Commission's objective, and that Member States' data protection authorities should be entrusted to handle factors associated with compliance. We are also concerned that the impact assessment has been heavily criticised, and believe that further work, with the input of all stakeholders, is required to produce a full assessment of the impact of the proposals. The UK Information Commissioner has asserted that the system set out in this Regulation "cannot work" and is "a regime which no-one will pay for". We regard this as authoritative, and believe that the Commission needs to go back to the drawing board and devise a regime which is much less prescriptive, particularly in the processes and procedures it specifies.

We understand that the draft Directive does not apply to domestic processing by law enforcement agencies within the UK, and it should be placed beyond doubt that this is the case. Additionally, we believe it needs to be made clear that the Directive must not impact on the ability of the police to use common law powers to pass on information in the interests of crime prevention and public protection. Member States need to have the flexibility to implement the Directive in ways which achieve its purposes through processes which are appropriate and proportionate in the national context.

However, we take some comfort from the fact that both the Government and the

Information Commissioner believe that the necessary changes in the Regulation and the Directive can be agreed through negotiation, and we support them in their efforts to achieve this.

1 Introduction

1. In late January this year, the European Commission published new legislative proposals for data protection.[1] The proposed data protection legislative framework consists of two EU documents: a draft Regulation (directly applicable) legislating for general data protection across the EU;[2] and a draft Directive (binding as to the result to be achieved, but leaving to national authorities the choice of form and method) with the specific aim of protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities.[3]

2. The right to the protection of personal data is explicitly recognised by Article 8 of the Charter of Fundamental Rights of the European Union. In addition, Article 16 of the Treaty on the Functioning of the European Union (TFEU) provides a legal basis for rules on data protection for all activities within the scope of EU law. The proposals would bring EU data protection up-to-date, and satisfy the obligations set out in the Treaties. The draft Regulation would repeal and replace the 1995 Data Protection Directive, which is implemented into UK law by the Data Protection Act 1998. The draft Directive would repeal and replace the existing Data Protection Framework Decision, which was negotiated in 2008, and implemented in the UK through the issuing of an administrative circular.[4]

3. On 13 February, the Ministry of Justice (MoJ) submitted Explanatory Memoranda to the European Scrutiny Committee, which gave its initial view on both documents. The Memoranda explained that the MoJ had begun a one month consultation on the proposals between February and March. On 14 March the European Scrutiny Committee reported on the proposals. Chapter 7 of the Report, *General Data Protection Regulation*, states in paragraph 7.55:

> [W]e consider that the proposed reforms to EU data protection rules are not only legally and politically significant, but also complex, with broad ramifications for individuals, businesses and national authorities. It is not possible for the European Scrutiny Committee to inquire into these matters in sufficient depth, because of the number of EU documents it has to review on a weekly basis. Pursuant to paragraph 11 of Standing Order (No.) 143, we therefore ask the Justice Committee to give its Opinion on this draft Regulation, together with the draft Directive reported in the following chapter of this week's Report. That Opinion should assess whether the proposed legislation strikes the right balance between the need, on the one hand, for

1 "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", European Commission press release, 25 January 2012

2 5853/12, Draft 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)

3 5833/12, Proposal for a directive of the European Parliament and of the Council 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

4 5834/12, Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, para 2.1.1, and Circular 2011/01, Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters 2008/977/JHA, Ministry of Justice

> a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them.[5]

In addition, Chapter 8 of the Report, *Data processing in the framework of police and criminal cooperation*, set out in similar terms the request for a opinion on the draft Directive in paragraph 8.38.[6] This Report sets out our opinion on both documents in response to the European Scrutiny Committee's request.

4. Following the publication of the MoJ's *Summary of Responses*[7] to its consultation on 28 June 2012, we launched an inquiry on 12 July, calling for written evidence by 20 August.[8] We received 54 written submissions from a wide variety of witnesses, and held oral evidence sessions with 6 panels of witnesses. These are listed at the end of this Report. We are extremely grateful to our witnesses for submitting written evidence within the short timeframe, and for making themselves available to give oral evidence, especially those who travelled to Westminster from Brussels.

The basis for reforming the current data protection framework

5. When the proposals were published, the European Commission set out the aims of the reforms, stating:

> Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.

Additionally, the European Justice Commissioner Viviane Reding, Commission Vice-President said:

> 17 years ago less than 1% of Europeans used the internet. Today, vast amounts of personal data are transferred and exchanged, across continents and around the globe in fractions of seconds. The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights and in more control of their information. The reform will accomplish this while making life easier and less costly for businesses. A strong,

5 European Scrutiny Committee, Fifty-ninth Report of Session 2010–12, *Documents considered by the Committee on 14 March 2012*, HC 428-liv, para 7.55

6 European Scrutiny Committee, *Documents considered by the Committee on 14 March 2012*, para 8.38

7 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012

8 "New Inquiry: European Union Data Protection Framework Proposals", Justice Select Committee, 12 July 2012

> clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation.[9]

6. As referred to in paragraph 2 above, the draft Regulation would repeal and replace the Data Protection Directive 1995. The MoJ's *Summary of Responses*, stated:

> The proposals for a new Regulation in the area of data protection came about as the 1995 Data Protection Directive is widely perceived to be out of date. Since 1995, there have been numerous technological developments, notably the increased use of computers, the expansion of the internet and the emergence of social media networks which have seen changes to the ways that personal data are handled and processed.[10]

7. The draft Directive would repeal and replace the existing Data Protection Framework Decision 2008, which entered into force on the 19 January 2009, with Member States having to implement its provisions by 27 November 2010. It applies to public bodies authorised by national law to detect, prevent, investigate or prosecute offences or criminal activities. The Commission has provided an assessment on the current state of the Decision's implementation and functioning across the EU, and concluded that the difficulties encountered by a number of Member States could be solved through a new Directive.[11] The MoJ stated that the argument for the replacement of the Framework Decision was not as clear as for the general Data Protection Directive 1995, as the Framework Decision was only adopted four years ago.[12]

The approach to reforming the current data protection framework

8. The European Commission's decision to introduce both a Regulation and a Directive will significantly alter UK law in the area of data protection. The Regulation will be directly applicable, whilst the Government will have to take separate steps in order to implement the Directive. Data subjects and organisations within the criminal justice system in particular, will have to refer to different pieces of legislation in different circumstances. This will be a departure from the current system, whereby the Data Protection Act has broad application.

9. Christopher Graham, Information Commissioner, told us in oral evidence that "[The] Office is deeply sceptical of this proposal to split the current Directive between a Regulation and a Directive. All sorts of mischief follows from that decision".[13]

Additionally, David Smith, Deputy Commissioner and Director of Data Protection, Information Commissioner's Office stated:

---

9 "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses", European Commission press release, 25 January 2012

10 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 3

11 European Scrutiny Committee, *Documents considered by the Committee on 14 March 2012*, paras 8.1–8.5

12 Ev 53

13 Q 32

> From our point of view, we are proponents of good regulation. Good regulation means consistent law that is clear and easy to understand and easy to apply. Once we start to diverge and we have a Regulation for the commercial sector and a different legal instrument for police and justice, you start to move away from that and you cause particular problems in areas like local authorities, perhaps, which have functions that will come under the Regulation and others that will come under the Directive.[14]

He contended that this was a difficult area because there was a political element to the UK's position in relation to the European Union and, particularly, measures in the police and justice areas.

10. We asked Françoise Le Bail, Director-General, Directorate-General Justice, European Commission, whether the two instruments would lead to an inconsistent approach. She replied:

> [A]s you may imagine, we have discussed this internally a great deal and also with stakeholders before taking the decision to bring forward two different proposals. In fact these proposals have quite a lot in common. [...] The same principles of data protection apply at the core of the Regulation, but I think the new element is that they are at the core also of the Directive, which was not necessarily the case to start with. [...]
>
> [W]e have applied, first of all, the obligation we have under Article 16 of the Lisbon Treaty, but we have also applied declaration 21, which is annexed to the Lisbon Treaty, which says that for this particular field, which is police and judicial co-operation in criminal matters, of course specific provision should be taken.

She argued that the Directive gave Member States the flexibility to take into consideration their particular culture and type of legislation, such as common law in the case of the UK, and added:

> [The instruments] are part of the same exercise, which is to reinforce the rights of individuals in terms of data protection. This is also part of the exercise of stopping the fragmentation in the legislation, both in Regulation matters where we have 27 different types of legislation but also in what is the framework decision area now, where, first of all, there is a very different way of implementing these framework decisions and a very different degree of application of the framework decisions. We believe that, by presenting two types of legislation at the same time, we will fight against this fragmentation but we can also give the necessary flexibility.[15]

11. The MoJ's written evidence explained that in the UK, the Data Protection Act 1998 (DPA) implemented the Data Protection Directive 1995, and included in its scope police and law enforcement processing. This meant that the DPA applied to the processing of all personal data, including that covered by the Data Protection Framework Decision 2008. It

14 Q 32

15 Q 71

concluded that "it is likely that the DPA will need to be amended or repealed and replaced in order to implement the new EU legislation once it comes into force".[16]

12. This is an issue that was raised by some of our witnesses. Privacy International, a campaign group for privacy issues, argued that the data processing principles contained in the draft Directive were less ambitious and more ambiguous than those in the draft Regulation, and that this could be problematic for the UK because the Data Protection Act applied across the board.[17] Intellect, the UK trade association for the IT, telecoms, and electronics industries, told us it "could imagine seven pieces of separate legislation on data protection that organisations would need to consult – as the Government could choose to implement [aspects of the Regulation] separately", and argued that the ideal situation would be for one piece of legislation.[18]

13. **We are concerned that the approach taken by the European Commission, introducing two instruments, will lead to a division of the UK law, set out in the Data Protection Act. We believe that this could cause confusion, both for data subjects, and for organisations within the criminal justice system in particular, as they will have to consider which law applies in their given circumstance. We are also concerned that this twin-track approach might also lead to inconsistencies in application, both due to differing provisions in the instruments and over time, due to court decisions under each instrument. If this is still to be the approach, we recommend that there is consistency between the two instruments from the outset, to mitigate the future divergence in their application. Furthermore, the UK Government and the Information Commissioner's Office will be required to work effectively together in order to produce and disseminate effective guidance so that data subjects know their rights and organisations know their responsibilities under each law.**

The negotiation process

14. Both documents are subject to the Ordinary Legislative Procedure. This is a process which requires the European Council and the European Parliament to agree on a proposal for legislation before it can come into effect.

15. With regard to the draft Directive, on 24 April the then Parliamentary Under-Secretary of State, Ministry of Justice, Mr Crispin Blunt MP, informed the House that the Government's view was that the draft Directive could be classified as a Schengen building measure. Therefore, under protocol 19 of the TFEU, which governs how the Schengen acquis is integrated into the UK framework, the UK had the option of opting-out of the Directive. The then Minister argued that not exercising the opt-out would enable the UK to improve the draft text during negotiations, and concluded "our national interests are best served by participating in this directive".[19]

16 Ev 53

17 Ev 50

18 "Ev w76 *[Note: references to 'Ev wXX' are references to written evidence in the volume of additional written evidence published on the Committee's website]"*

19 HC Deb, 24 April 2012, col 885–886

16. The *Summary of Responses* states "[t]he negotiations in the Council of the EU and in the European Parliament are ongoing and are likely to last until 2014".[20] In addition, Lord McNally, Minister of State, Ministry of Justice, told us:

> The Commission have a very ambitious time scale. They want to see substantial progress during the Cypriot Presidency, which is on now, and conclusion during the Irish Presidency, which is the first six months of next year. To be fair, the Cypriots have given priority to these negotiations and devoted the time to it, and as far as we understand, the Irish are taking a similar approach, but whether they will be successful or not, I don't know. We are negotiating to get results, not to fit into a timetable. We are certainly not on a go-slow or anything else. We simply want to get the best practical result from the negotiations.[21]

20 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 35

21 Q 139

2 The draft Regulation

The basis for, and aims of, reforming the Data Protection Directive 1995

17. The draft Regulation would repeal and replace the existing Data Protection Directive 1995.

The Government's Explanatory Memorandum states:

> The objective of the 1995 data protection Directive, to ensure the effective protection of the fundamental rights and freedoms of individuals within a functioning Single Market, remains valid. However when the 1995 Directive was adopted the internet was in its infancy. The Commission believes that a new, stronger and more coherent data protection framework is necessary because rapid technological and business developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. The Commission also considers that existing rules provide neither the degree of harmonisation required, nor the necessary efficiency to ensure the right to personal data protection. The Commission therefore wants greater consistency in the way data protection is implemented across the Union by introducing a single set of harmonised core rules, whilst still ensuring the free flow of personal data within the internal market.[22]

18. Privacy International's written evidence stated:

> The fundamental rights to protection of personal data and privacy are specifically mentioned in EU charters and conventions, and have to be complied with by EU member countries signatories of the Lisbon Treaty. Under current legislation these rights are not respected.[23]

The obligations under EU treaties were also commented on by the Information Commissioner in oral evidence, when he said:

> the challenges of data protection for citizens and consumers, not just in Europe but across the world, are really significant challenges of the 21st century. [...] unless we get data protection right—and it is a fundamental right under the Charter of Fundamental Rights of the European Union—we are all in trouble.[24]

When giving oral evidence to the Committee, Lord McNally, Minister of State, Ministry of Justice, also highlighted how data protection concerns had changed with developments in technology:

22 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 3

23 Ev 50

24 Q 36

> In the two years that I have been in this job I have become aware that we are really at the dawn of a new era in terms of just how much information is in the hands of various organisations, and the possibility and capability of its misuse. [...] The capacity to acquire information about the citizen and to cross-reference it is quite serious. All I can say is that we are alert to that and want to build it into both our domestic and EU legislation because that threat does exist. [...] In the new digital age it is the downside to what is also a very exciting opportunity in terms of exchanging information for the benefit of the citizen.[25]

19. Most of the written evidence we received agreed that new EU legislation for data protection was required, and welcomed the aims of the draft Regulation. For example, the NHS European Office said it "welcome[d] the European Commission's revision of the existing EU Data protection laws, particularly in light of technological developments since the last Directive was implemented",[26] whilst the Association for Financial Markets in Europe stated, "[o]ur members welcome the aims of the Regulation to improve legal certainty through harmonisation, to reduce the administrative burden on companies and to provide effective rights to individuals".[27]

20. One of the key aims of the draft Regulation is to provide harmonisation and clarity of data protection laws across the European Union. David Smith from the Information Commissioner's Office explained how current approaches to data protection regulation differed among Member States:

> We have traditionally taken what we would see as a good UK regulatory approach. [...] People don't come to us as an authority to get approval for what they do in advance; they take their business decisions and we step in if things go wrong. We have some strong powers [...] to impose penalties if businesses do get things wrong. But [...] you trust them to get it right and you step in if they abuse that trust [...] whereas some other data protection authorities have to check things in advance and prior approve things. This is particularly true in international transfers. [...] As we try and come together to one harmonised instrument, you see those sorts of tensions emerging. We are critical of this instrument because it will require us to prior approve international transfers, but I have to say that some of our colleague authorities are equally critical of it from the opposite direction because it will allow international transfers through, in some cases without their approval, where they have to give their approval under the current regime.[28]

21. Françoise Le Bail explained why harmonisation would be particularly beneficial for small and medium sized enterprises (SMEs):

> The first thing that the SMEs told us was, "What is a problem for us is fragmentation. If I am an SME and I have to deal with 27 different legislations in terms of data protection, it is awful. [...] I cannot cope with it because I don't have a legal service.

25 Q 111

26 Ev w25

27 Ev w63

28 Q 38

> [...]" The first thing we are doing for SMEs is to stop this fragmentation. We will stop this fragmentation by one single law. This is a huge benefit for an SME because, for a big company, in a way they can cope; they have legal services.[29]

We heard similar views from other witnesses:

- The Federation of Small Businesses told us, "there are benefits [to updating the legislation] because data is free flowing [...] so you need harmonised rules on that. [M]ore of our small businesses will use the European market to find new customers. So harmonisation is important".[30]

- Privacy International stated, "harmonisation and legal certainty would encourage more SMEs to expand their businesses in other EU countries because they would not need to engage expensive lawyers.[31]

However, Business Software Alliance believed that prescriptive elements of the draft Regulation, such as the imposition of large fines, "could be extremely detrimental to the launch or survival of start up companies and innovative SMEs". They argued "[s]uch a regime would significantly raise the cost and associated risk of introducing new products and services into the market while neither reducing the risks to data being processed nor providing added protection for consumers".[32]

22. Which? believed that a sound framework for data protection could help boost consumer confidence, especially with more business and public services moving online. It argued that whilst growth of the digital economy was important to both the UK and wider EU, a lack of trust and concerns over data protection presented a significant barrier to this growth. A recent Eurobarometer showed that 43% of British consumers were concerned about someone taking/misusing their personal data when shopping or banking online.[33] Georgina Nelson, Lawyer, Information Policy, Which?, highlighted an Office of Fair Trading study that showed 6.27% of UK consumers had never provided their personal financial details online because of privacy and security concerns, which was an estimated loss for e-commerce business of £2.48 billion.[34] Additionally, Privacy International, contended that the lost opportunities due to a lack of consumer confidence online equated to 1.7% of EU GDP.[35]

23. The draft Regulation sets out:

- principles governing personal data processing;

- rights of individuals to access their personal data, to have it rectified or erased, to object to processing and not to be subject to profiling;

---

29 Q 78

30 Q 15

31 Ev 51

32 Ev w54

33 Ev 47

34 Q 61

35 Q 57

- the obligations of data controllers and data processors to provide information to individuals, to report on breaches of data security and to put in place technical and organisational measures;
- rules on transfer of personal data to countries outside the European Economic Area (EEA) and to international organisations;
- rules relating to national regulators ("supervisory authorities"), and how they will co-operate with each other and the European Commission; and
- remedies available to data subjects and the administrative sanctions available to supervisory authorities.[36]

24. Some of the key changes that the Regulation introduces are as follows:

- a new definition of consent that requires that consent to the processing of personal data be given explicitly;
- new definitions of key terms, and introduction of new terms such as "online identifier", "location data", and "genetic data";
- the mandatory appointment of data protection officers for organisations in the public sector and some parts of the private sector;
- greater levels of protection for children (defined as those under 18 years of age);
- a right for data subjects to be "forgotten", including the right to obtain erasure of personal data available publicly online;
- new obligations on data controllers and processors, including mandatory security obligations, an obligation to maintain documentation of their processing operations and an obligation to notify supervisory authorities of data breaches without undue delay and where feasible within 24 hours;
- updated rules on transfer of data to countries outside the European Economic Area and to international organisations, including the need for data controllers to obtain prior approval from supervisory authorities in some circumstances;
- changes to cooperation and consistency between supervisory authorities, and the establishment of a new regulatory body, the European Data Protection Board; and
- a requirement for supervisory authorities to impose prescribed fines of up to 2% of an enterprise's worldwide turnover where there has been a breach of certain requirements of the Regulation.[37]

36 European Scrutiny Committee, *Documents considered by the Committee on 14 March 2012*, para 7.6

37 *Ibid,* para 7.8

Arguments for and against a Regulation

25. We received a mixed response to the Commission's decision to use a Regulation as the instrument to update the 1995 Directive. The Newspaper Society said "[t]hat the proposals are put forward by way of a proposed Regulation is itself a major disadvantage. This deprives the UK Government of any flexibility in implementation or enforcement".[38] However, RSA Insurance Group stated, "We support the new proposals being in the form of a Regulation rather than a Directive. As a multinational insurance group we welcome the European Commission's aim of creating a level playing field".[39]

26. In oral evidence to the Committee, the Federation of Small Businesses argued, "you need some form of prescription if you want to harmonise" and therefore they were happy with a Regulation instead of a Directive.[40] Microsoft added, "[w]hat is very good with this reform is that it is supposed to bring the maximum of harmonisation, which is really key. [...] Today I think we all agree that 27 different regimes is 27 risks, 27 good reasons not to make business".[41]

27. This view was not shared by the Information Commissioner's Office, and David Smith told us that it would have been easier to achieve an outcome driven approach, favoured by the UK, through a Directive. However, he acknowledged:

> that wouldn't meet the Commission's desire for harmonisation or would put that at risk. The Commission are very much, we think, driven [...] by the likes of Microsoft, the big multinational internet businesses, who say, "Above all else, we want the same rules throughout Europe so that we know what the rules are for Europe." There is an element that the Commission see that as necessary for economic progress and making Europe a good place to do business, and clearly there is some merit in that. But driving this harmonisation does lead to these detailed prescriptive rules that everybody has to follow, which are not necessarily good for, say, the people that the Federation of Small Businesses represent, who don't necessarily need the same regime in every country in Europe. What they just need is a sensible regime, from their point of view, in the UK. If the price of that is extra detail and extra prescription, because that is what you have to have to reach agreement among all 27 member states, maybe that is too high a price to pay.

He concluded, "[i]t does not matter too much whether it is a Regulation or a Directive, but we would favour lightening up on the detail".[42]

28. Which? believed that a certain level of prescription was required,[43] and told us that if the Regulation was to focus on outcomes, "[t]here needs to be clear steps about how those outcomes would be achieved. Just to focus purely on outcomes without that guidance

38 Ev w66

39 Ev w6

40 Q 18

41 *Ibid.*

42 Q 40

43 Q 54

would mean that it would be left up to the different Member States to provide that guidance, and that is when you would get differences in interpretation and fluctuation".[44]

29. When Lord McNally appeared before us, he set out the Government's view, and described the impression garnered from the early negotiations:

> We think the Regulation is too heavy-handed and prescriptive in an approach to something that would be much better dealt with by a Directive that leaves a great deal more flexibility to domestic implementation. [...] From what I understand, the balance of the discussions so far has been much more about what's in the Regulation and whether it could be better handled in a Directive.[45]

30. **Bringing EU data protection legislation up-to-date is necessary and could provide benefits to both individuals and businesses. Many of these benefits are only attainable if there is effective harmonisation of laws across Member States, and therefore we can understand why the European Commission decided that a Regulation was the correct instrument to achieve their objective. However, by setting out prescriptive rules there is no flexibility to adjust to individual circumstances. We believe that the Regulation should focus on stipulating those elements that it is essential to harmonise to achieve the Commission's objective, such as the consistency mechanism and the establishment of the European Data Protection Board. Member States' data protection authorities should be entrusted to handle factors associated with compliance, such as the level of fees or when it should be informed about a data protection impact assessment, whilst also being a source of guidance. Consistency of approach should then be delegated to the European Data Protection Board.**

Impact assessment

31. The Commission's impact assessment explains that whilst strengthened data protection rules are expected to give rise to some additional compliance costs for organisations, it could also offer a competitive advantage for the EU economy, as the higher level of protection and expected reduced number of data protection incidents and breaches may increase consumer confidence. Requiring companies to adopt high standards of data protection could also lead to long-term improvements for European businesses, which could become world leaders in privacy-enhancing technology or privacy-by-design solutions, drawing business, jobs and capital to the European Union.[46] When, for example, we asked Microsoft what weight was given to data protection legislation when the company was making investment decisions, Jean Gonié, Director of Privacy EU Affairs, told us, "I would say that this is in between the top and bottom in the list because, as you can imagine, we also have other incentives like tax regimes, skills employability and so on to determine investment. But, definitely, if we have coherent clarity in a data protection regime, this will really help".[47]

44 Q 55

45 Q 109

46 European Scrutiny Committee, *Documents considered by the Committee on 14 March 2012*, para 7.32

47 Q 19

32. The Commission also considers that the enhanced harmonisation will make the cross-border processing of personal data simpler and cheaper. This is expected to provide considerable incentives for businesses to expand across borders and reap the benefits of the internal market, with beneficial effects both for consumers and the European economy as a whole.[48] The Commission claims that the reforms are expected to achieve benefits and savings of about €2.3 billion in administrative burden per annum.[49]

33. The Commission's opinion was not shared by the MoJ. Its *Summary of Responses* contains its own *Regulation – Checklist for analysis on EU proposals*, which states:

> The overall impact is likely to be substantially negative. Though it is difficult to place a figure on the scale of net costs, the positive benefit to individuals of strengthened data rights are judged to be likely to be outweighed by negative impacts on small businesses, third sector, the ICO and wider justice system.[50]

We address some of the aspects of the Regulation that have raised concerns that burdens will be imposed later in this Report.

34. In its written evidence, the MoJ stated:

> Our initial assessment suggests that the Commission's impact assessment does not provide a credible foundation to underpin the proposals. We have noted three issues in particular.
>
> - the quantified impacts have not been thoroughly investigated. In particular, there are significant weaknesses with the widely publicised €3bn benefit from reducing "legal complexity";[51]
>
> - the impact assessment has focused on quantifying benefits without corresponding assessment of costs;
>
> - the impact assessment exhibits many issues in relation to the method used to compile the analysis, for example: lack of a clear baseline; failure to consider impacts over time; absence of sensitivity testing to account for uncertainty; lack of Member State level analysis; multiple statistical errors; and no explicit consideration of winners and losers.[52]

Furthermore, in oral evidence, Glenn Preston, Deputy Director for Information and Devolution, Ministry of Justice, explained:

---

48 European Scrutiny Committee, *Documents considered by the Committee on 14 March 2012*, para 7.33

49 5853/12 ADD 2, Executive summary of the impact assessment accompanying the document, European Commission, para 7

50 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 45

51 "The costs of current legal fragmentation for economic operators only in terms of administrative burden are estimated to amount to more than €2.9 billion in total per annum. The expected net savings for economic operators would be around €2.3 billion per annum, arising from the elimination of legal fragmentation and the simplification of notifications". 5853/12 ADD 1, Impact Assessment accompanying the document, European Commission, para 6.1.2(c)

52 Ev 55

> We are committed to doing our own impact assessment of the Commission's proposals. The aim is for us to make that publicly available [...] before the end of this calendar year. That is proving challenging, partly because we are trying to get information out of the Commission on the basis of the methodology that was used for their own impact assessment, which is taking slightly longer than we hoped it would. [...] The purpose of producing that is to have a public discussion [...] about a proper analysis of the costs and the benefits, which we think was slightly lacking in the impact assessment provided by the Commission.[53]

35. Microsoft agreed that the draft Regulation would be more burdensome than the Commission estimated, and said, "[w]ith this figure of €2.3 billion we have difficulties, to be candid, because we have no real details regarding the impact assessment. We have just a few pages at the end of the text. We would like to have more information to understand better what these €2.3 billion savings really represent".[54]

36. More positively, Glenn Preston, Ministry of Justice, explained that as the UK Government sought to change the content of the Regulation substantially, the Ministry would look at the different options that may exist, and added "[w]e would expect the final instrument, whether it is a Regulation or a Directive, to be considerably different and to be less burdensome and prescriptive. Therefore, it could well have a more beneficial impact if that is the case".[55]

37. **We call on the European Commission to work with the UK Government, the governments of other Member States, and other stakeholders, and to pool resources, expertise and information, so that a full assessment of the impact of the proposals can be produced.**

Impact on the Information Commissioner's Office

Resources

38. Respondents to the MoJ's *Summary of Responses* questioned whether the Information Commissioner's Office (ICO) would be able to meet the Regulation's requirements given the breadth of the processing activities that the Regulation applies to. The general perception was that the ICO would be unable to keep up with the demand to respond to requirements such as receiving breach notifications, approving international transfers of personal data and reviewing the results of data protection impact assessments. The ICO confirmed that the Regulation would have considerable resource implications for all supervisory authorities, and that Member States would be committed to the adequate funding of these.[56]

39. Françoise Le Bail, explained:

---

53 Q 112

54 Q 13

55 Qq 113–114

56 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 28

> In the EU Regulation we ask the Member States to make sure that their data protection authorities are staffed with the right amount of people and also have the necessary financial backing. The picture we have around the EU is of course very different. [...] Therefore [...] in the Regulation [...] is an obligation to make sure they have both the necessary finance and staff. The reason for this is that the data protection authorities will have to continue the work they are doing now, but they will also have to participate in the consistency mechanism [the European Data Protection Board].[57]

She added that data protection authorities would also be relieved of a number of duties. The Commission had requested from all data protection authorities a cost estimate, but she believed the main issue was with new Member States.

40. In oral evidence, Christopher Graham, Information Commissioner, shared with us his office's assessment of the impact the draft Regulation would have on resources:

> I accept [it] may change, but it raises the question of whether any of this is actually doable, because, if we were to do the least that we can identify as being down to the ICO under these proposals, our funding would have to increase from the current £15 million for data protection—from the notification fee, which itself is under a question mark—by a further £8.4 million: that is a 56% increase.
>
> It isn't going to happen, Chairman. But if we were to do what is frankly the more realistic role of what we think we ought to be doing, given the legislation that is set out, the figure is even more scary and, frankly, unbelievable. It is £15 million at the moment; we would need a further £28 million. Is anyone going to vote an additional 187% to the ICO, excellent though it is? No, they are not.
>
> So you then have to say, "This system cannot work." They are certainly not going to vote 56% either. This system cannot work because you are describing a regime that nobody will pay for. We are about the best funded of the data protection authorities within the European Union. If we can't do it, and we particularly can't do it when the notification fee on which our funding is based is abolished, how is anyone going to be able to do it?[58]

41. We put these figures to Françoise Le Bail, who responded:

> First of all, we don't know these figures yet. [...] My first reaction is that it seems a huge amount. Certainly, in the reflection we have had, we never envisaged that it would be as much as that. So we need to have a look at these figures in detail. My guess is that it will be much less.
>
> Secondly, when he says, for example, that he will need to look at details, dealing with every single complaint that the Regulations, they believe, oblige them to do, this is a subject of discussion among Member States. This is also the subject of discussion with the data protection authorities. [...] They say there are too many cases to deal

57 Q 96

58 Q 48

> with [...] and we cannot, as we do now, concentrate on the main cases. This we are discussing and we are confident we will find a solution for this. [...] [W]e are engaged in this process with Member States, DPAs and national Parliaments, and we are gathering all information that we have. But, coming back to the figures, they seem a lot.[59]

42. Lord McNally, Ministry of Justice, emphasised that this was not a problem for the UK alone, stating:

> Our Information Commission Office is well resourced compared with other parts of Europe. [...] [T]hat is why one of the things we will be pointing out in the nicest possible way to the Commission is that having a wish list of extra responsibilities and tasks for the Information Commissioners across Europe is going to be genuinely wishful thinking because the resources simply won't be there in the present circumstances to fulfil this wish list.[60]

43. **We regard as authoritative the UK Information Commissioner's assertion that the system set out in this draft Regulation "cannot work" and is "a regime which no-one will pay for", and we believe that the Commission needs to go back to the drawing board and devise a regime which is much less prescriptive, particularly in the processes and procedures it specifies.**

Relationship with data controllers

44. The Association of Chief Police Officers' written evidence stated that the current healthy relationship between data controllers and the Information Commissioner's Office would not be able to continue under the draft Regulation. It argued that the "possessively descriptive approach" the EU Commission takes will result in Information Commissioners identifying failure and imposing fines, rather than being a source of advice and guidance, and a promoter of good practice.[61]

45. The Information Commissioner's Office were sympathetic to this assessment, and David Smith, Deputy Commissioner and Director of Data Protection, told us:

> If we lose discretion, all we will be able to do is punish and not advise and assist. We believe very strongly that advising and assisting people to get it right, as well as punishing those who fail in their responsibilities, is the duty of a rounded, proper, effective regulator. [62]

Christopher Graham, Information Commissioner, added:

> I want discretion, and in the negotiations [...] a very important victory would be to change that bit that has all the lists of what the data protection authority "shall" do and amend that to "shall be empowered to" or "may do" so that we have the

59 Q 99

60 Q 116

61 Ev 58

62 Q 48

> discretion to go after the bad guys, understand where things may have gone wrong and where there are mitigating circumstances.[63]

European Union Data Protection Board

46. The Government's Explanatory Memorandum on the draft Regulation commented on the establishment of a new regulatory body, the European Data Protection Board. It stated "In general, the Government supports cooperation between supervisory authorities but wants to take care to ensure the continued independence of the Information Commissioner and flexibility of national supervisory authorities".[64]

47. Christopher Graham, Information Commissioner, told us that increasingly the data protection authorities within the European Union were cooperating, partly due to pressure from the big international companies who want greater consistency in the application of the current Directive. The Article 29 Working Party was the mechanism for this work, which under the new proposals would be formalised as the European Data Protection Board. He added that the trend towards greater consistency among Member States would continue because it was clearly demanded, and said, "[t]hat makes me wonder whether we need to impose all these restrictions, particularly on the smaller players, in the name of achieving something that the dynamic of the marketplace and good sense is achieving anyway".[65]

48. We asked Françoise Le Bail, European Commission, if there was a danger that the Data Protection Authorities of some Member States could be weaker than others. She replied:

> Let's imagine, for example, that there is a huge problem in a particular member state. The other data protection authorities can raise it in the framework of the European data protection board [...] and there can be a co-operation that can be put in place between the strong data protection authorities and the weaker data protection authorities.

Her colleague, Marie-Hélène Boulanger, Head of the Data Protection Unit, added:

> If you look at the text in detail, you will see that there are a lot of [...] safety measures in the provisions [...] to avoid that risk. [For example as] the data protection authority of one member state, if you feel that [another] authority in charge does not have enough staff to deal with the specific case, you have the possibility to send your own staff in support and the competent data protection authority for the specific case cannot refuse the support. [...] That is one of the mechanisms. [...] There are many possibilities to ensure that there are no discrepancies between data protection authorities. In addition, the European Commission always has the possibility to intervene in such cases.[66]

63 Q 44

64 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 35

65 Q 40

66 Q 97

General comments on the draft Regulation

49. As has been alluded to already in this Report, the vast majority of the written evidence we received argued that the draft Regulation is over prescriptive, and imposes unnecessary administrative burdens. During our oral evidence sessions, the Federation of Small Businesses told us:

> We think the rules are too prescriptive indeed. [...] [W]e think you can also make legislation on the basis of principles instead of prescription, because prescriptive rules also prevent innovation. If you prescribe in too much detail, you don't leave room for industry to develop their own standards or find their own solutions. In that sense, prescription goes against harmonisation because you stifle growth and trade in Europe.[67]

Microsoft told us they were very happy to see a proposal that gave maximum protection to the data subject. However, from an industry perspective they were very surprised to find that a lot of new burdens were imposed on them, without receiving any new rights and new incentives. They concluded that because they were very much in favour of harmonisation, they were expected to take on these new burdens.[68]

50. When the proposed Regulation was published, the Information Commissioner described it as "unnecessarily and unhelpfully over prescriptive" in a number of areas.[69] During oral evidence he expanded on this, stating:

> [T]he proposed legislation, in the name of consistency across the European Union, [is] very specific about processes, whereas our approach has been much more to focus on outcomes and to go for the better regulatory approach of risk-based proportionate intervention. We are really quite worried that it will be very difficult to operate this regime. It will turn the ICO from, on a good day, a Better Regulation regulator into a vast administrative machine processing a lot of forms, permissions and ticking boxes.[70] [...]
>
> [W]e believe that [an] overall obligation to comply, in general, doesn't then need to be broken down by, "This happens to you if you do this; this happens to you if you don't do that; and that happens if you don't do the other." Quite apart from the fact that it is going to tie the data protection authority up in knots, it would be much better to have a general obligation to comply rather than specific steps which have been derived from what has been developed as good practice.[71]

David Smith, Deputy Commissioner and Director of Data Protection, said that the level of prescription was a factor of the attempt to achieve harmonisation, "[b]ut that just gets you to undesirable, unintended consequences and unmanageable regulation". He continued:

---

67 Q 16

68 Q 17

69 "Initial response from the ICO on the European Commission's proposal for a new general Data Protection Regulation", Information Commissioner's Office press release, 25 January 2012

70 Q 35

71 Q 43

> In our view, you have to lighten up. You have to take the risk that there won't be complete harmonisation. It doesn't actually matter whether the fine is exactly the same or not, and we do have the European Data Protection Board, which is there to try and ensure consistency. Equivalence as an approach is much better than harmonisation, in our view.[72]

51. Privacy International's written evidence was more positive towards the draft Regulation. It contended that the Regulation did achieve the right balance between the rights of individuals and the obligations of controllers and administrations, and that considerations of possible burdens to businesses had to be counterbalanced by growth opportunities provided by furthering consumer trust.[73] It stated that the proposed Regulation, "on the whole, goes some way towards [...] [making] data protection law fit for the 21st century".[74] It also argued that the draft Regulation redressed current imbalances, such as extensive data mining and profiling (use of algorithms or other techniques that allow the discovery of patterns or correlations in large quantities of data) without individuals' awareness; difficulties for people to stay in control; different rights in different EU countries; authorities without clout and weak enforcement; and difficulties in getting redress.[75] It stated:

> Claims of stifling burdens, possibly affecting economic growth and innovation are not justified in this case. It is important to ensure that individuals are adequately and effectively protected: as […] lack of trust and concerns over data protection are significant barriers to the growth of the digital economy.[76]

52. In oral evidence, Anna Fielder, Trustee and Company Secretary, Privacy International explained how the Regulation provided balance between burdens and rights:

> [T]he bulk of these administrative burdens [are] particularly in the sections that concern data subject rights. [...] [T]he reason they have been put in there is because, precisely, the current legislation does not respect those rights and it was felt that you need a bigger degree of prescription and administration in order to ensure that that happens.

In addition, she argued that technological solutions and off-the-shelf e-commerce packages would greatly alleviate administrative burdens imposed on businesses. However, she did conclude, "there are some provisions in the Regulation that could be streamlined and reduced. We are not saying everything is perfect, but what we are saying is don't throw the baby out with the bath water".[77]

53. Georgina Nelson, Lawyer, Information Policy, Which?, told us "there should [not] be any fettering [...] of [data subject] rights due to administrative burdens. It is getting that balance right, and obviously any administrative burden which is superfluous to those rights

72 Q 45

73 Ev 49

74 *Ibid.*

75 Ev 50

76 *Ibid.*

77 Q 61

should be lightened". She added that the debate on the proposals had focussed on short-term administrative burdens, whilst the legislation would be in place for a generation. Furthermore, she emphasised the opportunities that the reforms would bring, stating:

> The Regulation is trying to open up this very competitive market of personal data so that it is not sat on by the few big players but it can be utilised by everyone for the greater good, whether that is business or consumers. That is really important to bring into the economic analysis; it is that future scope.
>
> Also, with regard to SMEs, the evidence previously was that at the moment cross-border trade is not something that they engage in, but obviously this is because it is hugely complicated. They probably can't afford the legal advice and the benefits don't justify the pain in getting there. But, if we do move towards this harmonisation, they will then hopefully have the confidence and it will be a far easier procedure to open up a whole new market for them, and then again you would seek to reap the benefits.[78]

54. Lord McNally, Minister of State, Ministry of Justice, stated that the Government intended that the draft Regulation which eventually emerged from the legislative process would have an entirely beneficial effect. He explained how the Government would negotiate for this result:

> Just as the single market gives us access to a market of 500 million, so legislation that will give some kind of harmony to the workings of this sector of the economy could and should be entirely beneficial. Why we are being, for want of a better term, awkward in these negotiations is that we do see that there are real threats to business if we allow the Regulations to emerge in such a way as to put an extra burden on business.
>
> We are also very aware that small businesses could be particularly affected by some of the suggestions. [...] We are trying to get a proportionality into the structure of the Regulations that we don't feel is there at the moment in what the Commission are putting forward.[79] [...]
>
> We are not negotiating for failure. We believe that we have allies. [...] The Commission come up with ideas and proposals and then others say, "No, thank you." Although the negotiations have been slow, we are not in a position where we feel that we can't achieve our objectives. [...] We want something that is proportionate, flexible and that doesn't impede entrepreneurship by either large or small companies but does get the balance right in protecting the privacy of the citizen.[80]

The Information Commissioner told us that there was scope for changes to the proposals, stating:

78 Q 61

79 Q 108

80 Q 110

> I suspect there is a lot about this draft Regulation and Directive which can be easily changed with an appropriate negotiating stance from the UK and others. The big mistake we make is to say, "We hate this; we hate this; we hate this—we're not going to play", whereas, with a little bit of diplomacy, we could achieve a much better result.[81]

55. **We note that both the Government and the Information Commissioner believe that the necessary changes in the Regulation and the Directive can be agreed through negotiation, and we support them in their efforts to achieve this.**

Specific aspects of the draft Regulation

56. We highlight here some specific aspects of the Regulation as it is currently drafted that witnesses have particularly commented on.

Delegated acts

57. The draft Regulation includes 26 provisions conferring power on the Commission to adopt delegated acts. Françoise Le Bail, explained how these could help keep the legislation up-to-date with technology:

> [O]ne thing we wanted to do when designing this Regulation was to make sure it will be technology-proof, [and] this Regulation [...] leaves flexibility in the form of delegated Acts. It is not that all Member States see with great enthusiasm delegated Acts for the Commission, but we leave this possibility to adjust to future developments. [...] Leaving it to secondary law, it is not that we are doing this without any control. For secondary law, we do that under the supervision of both the Council and Parliament. So it is not that the Commission itself is going to decide what is going to happen on these matters. [...] [T]he choice was either to put everything in great detail in the Regulation or to leave flexibility. We chose to leave flexibility.[82]

58. The extent and scope of the provision for delegated acts attracted significant criticism in written evidence. The Information Commissioner's Office has called on the Commission to provide a schedule of all the opportunities for delegated acts and their intentions in respect of each of them.[83] Microsoft argued that the provision for delegated acts should be significantly reduced because many of them dealt with essential elements of the law, and should be addressed in the Regulation itself. Additionally, other delegated act provisions gave the Commission power to prescribe technical formats, standards and solutions, which threatened to replace industry innovation with regulatory intervention.[84] In oral evidence, Jean Gonié, Director of Privacy EU Affairs, explained that some Articles

81 Q 45

82 Qq 91, 93

83 Information Commissioner's Office, *Initial analysis of the European Commission's proposals for a revised data protection legislative framework*, 27 February 2012, page 26

84 Ev 39

of the draft Regulation threatened technology neutrality and said, "[i]t is very important to have text that is future-proof and goes with no specific standard or format".[85]

The "right to be forgotten"

59. Article 17 of the proposed Regulation gives individuals the right to request that organisations delete their personal data in certain circumstances. Where an individual makes such a request and the personal data has been made public, data controllers are responsible for taking all reasonable steps to inform any third parties that process that personal data that the individual wishes them to erase that data and any subsequent links to the data.[86] Concerns regarding this aspect of the draft Regulation were expressed by almost all those who submitted written evidence.

60. The Information Commissioner's initial analysis paper stated:

> This is one of the more interesting parts of the Regulation. […] However, given [the] derogations, the various qualifications to the right and the technical difficulties surrounding online deletion, we are unclear how the right to be forgotten will be delivered. […] There is a risk that if individuals are led to believe they have a 'right to be forgotten' they will be disillusioned if they find that the right is strictly limited in practice. It might be preferable if this right was presented in less ambitious terms.[87]

During oral evidence, the Information Commissioner explained that whilst there had been a lot of attention on the "right to be forgotten", the Justice Commissioner Viviane Reding had said that it was more of a political slogan:

> I was sitting next to her when she said it. This was at a European Parliament briefing attended by many witnesses. Rather to my surprise, about six months after she had said this was the big idea, she said she couldn't understand why everyone was getting so excited about the right to be forgotten because it wasn't anything we didn't have already, and so everybody should relax. Because there are so many exclusions and derogations, we don't see it as very much of a threat because we don't see it as very much of a right either. You can't put the genie back in the bottle.

David Smith, Deputy Commissioner and Director of Data Protection, added:

> There was always going to be something in here that was called the right to be forgotten because of political statements that have been made and pressure, particularly from the French, to introduce this sort of approach. When you unpick it, much of what is there of the right to be forgotten is just a restatement of existing provisions—data shan't be kept for longer than is necessary; if it has been processed in breach of the legal requirements it should be deleted, which goes without saying.

85 Q 23

86 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 17

87 Information Commissioner's Office, *Initial analysis of the European Commission's proposals for a revised data protection legislative framework*, 27 February 2012, page 13

> What is [...] important is the new Article 19, and it is the right to object. [...] [The] balance of proof has changed in these new proposals. I can go along to any data controller and say, "I want you to delete my data", and they have to come up with the compelling legitimate grounds for keeping that data. Of course in many cases they are able to do that, but shifting the balance of power in the relationship a bit towards the individual seems to us to be important.[88]

61. When addressing the right to be forgotten in their written evidence, Privacy International said "[p]erhaps the title is a misnomer, but clearly an effective advertising tool",[89] and "we are not married to the name but we are married to the extra provisions".[90] Which? agreed, saying "[w]e realise that the term is a bit misleading"[91] and "our general position is that, if we can find something that wouldn't lead to that sort of consumer expectation of a wholesale full right, then that would be great". [92]

62. The MoJ's written evidence stated:

> the "right to be forgotten" should be resisted on the basis that it would raise expectations amongst individuals whose data is being processed that would be very difficult to fulfil in practice—in many cases it will prove impossible to delete data which has been disseminated across global networks.[93]

Lord McNally told us that the use of slogans such as "right to be forgotten" created a danger that expectations would be unduly raised. He said:

> That is why, even from the very early stages of this, we have suggested that "right to be forgotten"—which is a great headline and a good soundbite—is not practical. Anyone who knows how information goes round the world in this technology knows that. What we are hoping to do, again, is to make it clear that the individual citizen does have rights to get data expunged or changed, but what we don't want is to give particularly young people the idea that they can put things on social networks and that somehow they can recall it at will because they can't.
>
> There are a number of problems with the provision. For example, it creates a somewhat misleading right that may encourage reckless posting of information in the mistaken belief that it can be recalled. The UK supports strong deletion rights, but the term "right to be forgotten" is unhelpful given the details of the provision. We might suggest a change in the name in order that it better reflects the rights that are actually given.[94]

63. **The right of citizens to secure the erasure of data about them which is wrongly or inappropriately held is very important, but it is misleading to refer to this as a "right to**

88 Q 41
89 Ev 51
90 Q 67
91 Ev 48
92 Q 66
93 Ev 54
94 Q 120

be forgotten", and the use of such terminology could create unrealistic expectations, for example in relation to search engines and social media.

Notifying third parties

64. A further issue of concern arising from the "right to be forgotten" is that the draft Regulation would oblige data controllers to notify third parties of any requests from a data subject that they wished their data to be erased. Georgina Nelson, Lawyer, Information Policy, Which?, emphasised the benefits to online consumers that the changes would bring. Investigations by Which? found that some consumers who accepted third party marketing found that their details had been passed on to up to 2,000 different companies. Currently, if a consumer wanted to contact them, they would first contact that original company and ask for a list of the other companies that data had been passed on to. They would then have to contact each individual company.

65. Many organisations who responded to our call for evidence expressed concern that data controllers were responsible for informing third parties The Federation of Small Businesses' written evidence stated:

> This article is the crux of the whole data protection framework. […] We have no problem notifying third parties we have given data to, but a business' responsibility should stop there as they would be unable to ascertain that the party in question really deleted the data. Businesses need protections in circumstances when they may have taken 'all reasonable steps' to erase data but cannot be aware of any additional copies with third parties that they were not informed about. We would also like to see a general provision in the Regulation that people should be mindful of what personal data they put online themselves.[95]

Additionally, Microsoft told us that it welcomed the "right to be forgotten", and would comply with it as they currently do with the right to erase data, contained in the 1995 Directive. However, Jean Gonié, Director of Privacy EU Affairs, raised the problem that "[i]t is totally possible to retrieve any kind of data where, as a data controller, you have control of the data. [...] The problem is that it is not possible to retrieve all kinds of data because of the openness of the internet and the worldwide architecture of the web".[96]

66. David Smith, from the Information Commissioner's Office, agreed that it was unclear how informing third parties to delete data from the internet could work in practice. He said:

> Where information has been passed on directly to a third party, then we would expect a business to have a record of that and be able to inform them that that information should be deleted. If they have allowed or can find links into their sites, they should be able to trace that. But, if information has gone out on the internet, it

95 Ev 42

96 Q 22

> has been accessed from their site, taken and posted elsewhere, it is very hard to see what can be done.[97]

67. Anna Fielder, Trustee and Company Secretary, Privacy International, told us that in her assessment of the "right to be forgotten" there was a provision of endeavour on the part of the data controller to inform third parties about erasing data. She said:

> It tells them to try. What they have to prove is that they make a good stab at it—not that they actually did it. [...] [I]f you look for example at social networking sites like Facebook, they have contractual agreements with app providers, and these contractual agreements include privacy provisions. If they have contractual provisions with all these companies, they can easily [...] notify them of the need to erase.[98]

68. Georgina Nelson, Which?, agreed that contracts could aid in the retrieval of data from the internet:

> We obviously understand the limitations [...] and we are not saying that we should expect 100% erasure. [...] But, [...] on a website you are going to have terms of service with your users. If you are a social networking site, you also have terms of service with your account holders. It should not be too much of a jump to say in those terms of service you have, if there is a notification on this website that someone has [...] exercised their right to be forgotten, then you need to do the following steps and we expect that of you. I would hope that the big noise about the impossibility and the costs could be possibly broken down into easy, possibly legal solutions through those contracts. [...] The focus needs to be on efforts rather than the results. There needs to be some elaboration on the right as it currently stands so that people clearly understand their obligations and guidance is provided on what they would expect in those scenarios.

69. We asked Françoise Le Bail, what could be considered 'reasonable steps' to inform third parties of a request to delete data. She answered:

> They have to inform, for example, the search engines and all this to a possible, reasonable extent so that this is deleted. They must prove that they are making a real effort, but we are not asking them something that is impossible to realise. [...] There is no guarantee of this and this is why we said "all reasonable steps". The message we want to pass to these big companies that are running these social networks and search engines is that they need to demonstrate that they are making a real effort. We cannot exclude it resurfacing at some stage, but we would not like them to say, "Not for us. This is nothing to do with us".
>
> The final solution is that they have to participate [...] in creating trust in the internet. Creating trust means that you can have an influence on it—an influence which is not rewriting your life but an influence on these things that are on the net that you have not posted yourselves or you have posted at an age when you were not conscious of

97 Q 42

98 Qq 62–63

> the damage it can do and you want to see it disappear. It is a very important element for trusting the internet.[99]

70. However, David Smith, Information Commissioner's Office, questioned how the "right to be forgotten" could apply to search engines:

> To put it simply, if there is information about me on a website that has been published that I do not like, and maybe I have even obtained an injunction to stop that information being published but it is in a foreign country and I can't do that, can I go to Google—as an example of search engines people usually use—and say, "Google, stop returning that information in a search"?
>
> It is unclear how or if this Article would apply to that, and clarification on that would be welcome.[100]

Subject access requests

71. The proposed Regulation would make subject access requests free of charge. Françoise Le Bail, explained:

> [T]he right of access is a fundamental right; it is part of the fundamental rights that should exist. We have looked at what exists in the Member States and again it is a very varied picture. In some Member States it is free; in other Member States it is not. We believe that for simple access it should be free. At the same time we say in this Regulation that, if the demands are excessive or repetitive, you can put a fee on this. You will have seen also that we say that, if necessary, there will be a delegated Act from the Commission in order to make sure that the conditions are not too different from one member state to the other.[101]

72. Currently in the UK, data controllers may charge a fee of up to £10 when a subject access request is made. The majority of written evidence submissions which addressed this point wished to retain a fee for subject access requests. The Federation of Small Businesses told us:

> Previous feedback from FSB members indicated that the Subject Access Request (SAR) fee, although in some senses only a token fee of £10 given the amount of time and resources taken to follow up such requests, was actually quite helpful for businesses in a) preventing time wasters and b) actually recouping some costs. We would prefer that this fee, albeit token, is reinstated. […] Abolishing the fee for a subject access request will in fact mean a net burden increase for small businesses. Also, people could misuse this right by massively asking for their data in the same way cyber attacks are carried out. This could lock up business systems and overload businesses.[102]

99 Qq 82–84

100 Q 41

101 Q 85

102 Ev 41–42

73. The MoJ's *Summary of Responses* states:

> [B]usinesses and other organisations have not welcomed the removal of the ability to charge a fee. These groups have predicted an increase in the volume of subject access requests they receive if the fee is abolished, which would have detrimental effects on resource capabilities and budgets. Public sector organisations in particular have commented that they currently feel under strain with the amount of subject access requests they receive. They suggest that the proposal to abolish the fee will leave them stretched and possibly prioritising subject access requests over other similarly important pieces of work, so as to avoid the substantial administrative penalties. [...] Many of the responses which covered Article 12 asked the European Commission to clarify the term 'manifestly excessive' and 'repetitive character' in this context.

The MoJ have set out their negotiating position on subject access requests:

> [The UK Government will] support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge.[103]

74. Which? are strongly opposed to the Government's position to "resist that subject access rights be exercisable free of charge". They argue consumers have a right to know what data an organisation holds about them and should not have to pay to access their data. They state:

> We fully understand the need to protect companies from vexatious requests, but such safeguards already exist in the proposal which states that "where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested". […] A £10 fee is likely to deter consumers, especially vulnerable consumers, from obtaining this information. We also think such a fee goes completely against the spirit of the Government's midata programme which aims to give consumers access to their personal data in a portable, electronic format.[104]

Georgina Nelson, Lawyer, Information Policy, Which?, questioned whether the removal of a fee would have any impact on organisations stating:

> From *Which?*'s own experience, when I first arrived, [a fee] system in place as standard and we removed it. We didn't suddenly see a flood of subject access requests hit us. I would question this call from business that, "We are going to be inundated. These are the costs that we're going to experience." I would actually question that. When we have done a recent poll on this area, only half of people knew that they had the right; only 7% had ever exercised it, but 76% thought it was completely unacceptable for a company to charge them for their information. [...] It

103 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 34

104 Ev 48

> is a barrier, effectively, which companies want, and that barrier will be provided by the exemptions within the Regulation around "manifestly excessive", so they will still have that caveat and get-out. For the majority, it should be free.[105]

75. Anna Fielder, Trustee and Company Secretary, Privacy International, described her husband's experience of identity theft. A bank account was opened in his name and goods were ordered from various catalogues. It took over six months, and subject access fees of approximately £200, to access all the companies that had wrong records. She added, "Imagine an elderly vulnerable person who doesn't know the law, having to do that individually with every company. It just wouldn't be possible and it would be excessive as well in terms of charges. There are concrete examples [...] where we need specific, good measures to make sure that people can access their records and correct them".[106]

76. We raised this issue with Lord McNally, Ministry of Justice, who said "the Government currently set a £10 fee for access. It is important to note that many organisations do not charge this fee; instead it serves as a useful filter to deter more speculative requests if those are problematic for the data controller".[107] When we directly asked the Minister 'why should I have to pay to have access to know what information about me is being held?', he responded "That is a very powerful argument". He went on to concede there was an element of unfairness in seeking to charge people to find out what organisations held information about them, and stated, "[t]he concept of 'This is my data' is very fundamental".[108]

77. **An individual's right of access to their own personal data is a fundamental right; and individuals should not be required to pay a fee to make a subject access request. We urge the Government to change its negotiating position to one which accepts that subject access rights should be exercisable free of charge.**

Obligation to appoint Data Protection Officers

78. Another issue that has been subject to a large number of comments in written evidence is the requirement placed on organisations to appoint a data protection officer (DPO). Françoise Le Bail, European Commission, explained how the Commission decided which organisations were mandated to employ a DPO:

> We say, if you are a big company with more than 250 employees, then you need a data protection officer. But, if you are a small company, unless you specialise in dealing with very sensitive data, you do not need one. I can tell you that I dealt with that one personally. If you take Germany, for example, if you are a company with 10 employees, you need a data protection officer. Of course we discussed this question very openly. Should we say above 10 employees that you need a data protection

105 Q 70

106 *Ibid.*

107 Q 122

108 Qq 122–124

> officer? We took the right decision, which is to avoid the obligation of having a data protection officer if you have less than 250 employees.[109]

We asked her if it would be more effective to look at the sensitivity of the data that the organisation was handling, rather than the number of employees, to which she replied:

> It is a possibility. [...] We chose the European definition of an SME, which is 250, for simplicity. Everybody knows the definition; either you are above or below. It was for reasons of simplicity. But, again, if there are better ideas to reduce the burden for SMEs, we will look at them, because one of the essential elements of this Regulation was to take into consideration the admin burden. So we are prepared to look at it; if there is a better idea, if it is as simple, why not?[110]

Additionally, we asked if, for example, it might be better for a company to have heads of departments with data protection responsibilities on a scale dependent on how much data their section handled. She answered:

> We specify data protection officers again for big companies because, from the consultation we had, we gathered that most big companies already have a data protection officer. The only difference is that, sometimes, somebody is only doing that and sometimes it is a member of the legal service doing something else. This is the information we collected. It seems to us that, to have one point of reference dealing with data protection for the company, wherever they are organised, means they can liaise and co-ordinate all the services, and all this is up to them, not to us. But to have one point of reference—one person who can be the contact point, for example, of the data protection authority and the Information Officer in the UK—would be a simple solution. This is why.[111]

79. The Federation of Small Businesses told us:

> We think that a data protection officer should not be mandatory at all for SMEs. Of course we are happy with the exemptions. It should be assessed by the business itself if you need a data protection officer because it is very expensive to have one. We would advocate it for businesses that are data-centric and monitor data on a daily basis. We think it is a matter of assessing yourself, based on the risk you run.[112]

80. Lord McNally agreed with this view, and stated:

> We are also very aware that small businesses could be particularly affected by some of the suggestions, such as an absolute commitment to appoint a data protection officer [...] which might be easily absorbed by one of the data giants but which a small enterprise would find difficult. However, we don't want to do it by a simple cut-off. It may be a relatively small business that is dealing with very highly sensitive data and we wouldn't want them just to escape their responsibility simply by size. We

109 Q 78

110 Q 79

111 Q 80

112 Q 31

> are trying to get a proportionality into the structure of the Regulations that we don't feel is there at the moment in what the Commission are putting forward.[113]

81. **We believe that if the requirement to employ a Data Protection Officer is retained it should be based on the type of business and the sensitivity of data that is handled, rather than the number of employees.**

Breach notifications

82. The Government's Explanatory Memorandum on the draft Regulation supported the principle of notification of data breaches to the supervisory authority, but questioned the general requirement for notification within 24 hours where feasible, stating that this could delay necessary work to mitigate or remove the data breach and ensure the data was protected again as quickly as possible. The Government suggested the revised E-privacy Directive 2002/58 could provide a useful precedent for consideration. This Directive sets out that, when a personal data breach occurs, the provider has to report this to a specific national authority *without undue delay*.[114] The majority of written evidence we received concurred with this position.

83. Which? told us there was also an obligation to notify data subjects of a breach without undue delay. They argued:

> Last year there were a vast number of high street breaches that hit the press. Consumers often didn't hear about it from the high street themselves; they heard about it through social networking sites or through the media, and that again really shook trust. What the Regulation is proposing to do is put an obligation on data controllers so that, if they do suffer a breach that adversely affects consumers, then they have to notify them. [T]hat would really build trust.[115]

However, some respondents to our call for evidence raised the issue of 'notification fatigue'. The Direct Marketing Association (UK) Limited explained:

> If every data breach has to be reported, regardless of its nature or importance, there is a strong possibility of "notification fatigue" setting in – there is evidence of this effect in the USA where most states have this obligation. There is then a risk that consumers may ignore the notification of a serious breach, where they need to take action in order to prevent identify theft.[116]

Sanctions

84. Article 79 of the draft Regulation introduces the power for supervisory authorities to impose fines of up to €1m, or in the case of an enterprise up to 2% of its annual worldwide

113 Q 108

114 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 33

115 Q 56

116 Ev w78

turnover.[117] In the UK the Information Commissioner currently has the ability to impose a Civil Monetary Penalty of up to £500,000 for the most serious breaches of the principles set out in the Data Protection Act where there is likely to be harm to an individual. The Government's Explanatory Memorandum states "the proposed provisions in the Regulation appear to be very prescriptive, leaving little flexibility for supervisory authorities".[118]

85. Microsoft commented in their written evidence, "the Regulation takes a 'one-size-fits-all' approach, [applying] the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental. [...] To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for truly bad actors".[119]

86. The Information Commissioner told us he wanted the discretion to use the experience and judgment of his team to judge behaviour, judge the circumstances and consider mitigating actions, which is what happened currently with civil monetary penalties. He added that he did not favour a one-size-fits-all approach, whereby sanctions were imposed on every occasion and a fine for a particular sum of money was imposed, as he thought this would have no impact on compliance.[120]

87. Françoise Le Bail, European Commission, explained the rationale for the sanctions, stating, "for the first time we are proposing fines that matter, which make you think twice. [...] That was very important because the fines that exist now currently in Member States are minimal and you can ignore the Directive [...] or the national law that implemented it; it doesn't matter".

In addition, she explained that there was a staggered approach to the level of sanctions:

> You will also see that in the fines we are proposing there are steps to be taken. If you forgot about it, you didn't remember the provision and didn't do it intentionally, you get a warning, if I remember correctly. Then, if it is a repetitive pattern where it starts to become obvious that you intentionally don't respect the Regulation, these fines are implemented to the full.

Her colleague, Marie-Hélène Boulanger, Head of the Data Protection Unit, added:

> If you look at the provision purely from a legal point of view, you will see that [...] there is a clear requirement to take into account the nature, the gravity, the duration of the breach, the intention and the negligent character of the infringement and so on. [...] Then, if we go to the other paragraph, it is a maximum. It is "up to". So there is a margin for discretion in the way you apply the fines.[121]

117 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 31

118 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 36

119 Ev 39

120 Q 44

121 Qq 88–90

88. **We believe that data protection authorities should have more discretion as to the sanctions that they can impose in order to effectively punish the worst behaviour. We are aware that this could result in different approaches being taken in each Member States, and therefore recommend that, where there is evidence that such differences are having a deleterious effect on compliance, the European Data Protection Board be entrusted to provide guidelines on the type of sanction that may be appropriate in given situations.**

Exemptions for small and medium sized enterprises

89. The Government's Explanatory Memorandum on the draft Regulation commented that the proposal was one of several where the scope for a lighter regime for SMEs would be considered in the Commission Communication, *Minimizing regulatory burden for SMEs*.[122] The Federation for Small Businesses' written evidence noted a number of areas where small businesses will be exempted such as: Article 14 – Information Duties; Article 28 – Keeping Documentation; and, Article 35 – Data Protection Officer. However, it also noted that many of the exemptions for small businesses are only included in delegated acts, rather than on the face of the Regulation.

Concerns raised by specific groups

90. During this inquiry we received a large number of written submissions which raised concerns specific to a particular industry or activity. We highlight some of them here.

Credit Reference

91. Equifax believed that in their current form, there was a significant risk the proposals could restrict the ability of credit reference agencies to provide critical services to the financial services sector, consumers and Government. They argued that the proposals overlooked an important distinction between 'citizen data'—information necessary to make business, Government and the economy work—and 'consumer data' such as a Facebook profile, twitter account or internet history.[123]

92. We raised this with Christopher Graham, Information Commissioner, who said:

> I [...] think that all the benefits that come from the online world are benefits for consumers as consumers but also consumers as citizens. [...] But we do need a very strong data protection framework for us to be able to get all the benefits of online without the risks. I don't see any merit in splitting one's persona between, "I am a citizen at the moment, but at the next minute I am a consumer and I therefore deserve less protection".

David Smith, Deputy Commissioner and Director of Data Protection, Information Commissioner's Office, added:

122 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 39

123 Ev w9

> The same arguments are being made about the definition of personal data—that this is cast too wide and it captures things like IP addresses on the internet. But having a rigid definition which captures the right things and doesn't catch the wrong things in a changing technological age [...] is very difficult. It is right that a wide range of information—anything that can be potentially used to affect you in anyway—is caught by the legislation. What we then need to do, whether it is consumer data or citizen data, is to ensure that the provisions apply in a sensible proportionate way, given how that data is being used.[124]

Social Media

93. The Brussels European Employee Relations Group argued that the draft Regulation was overly centred on issues relating to social media business and not the vast number of other types of business. They stated, "It is inequitable and impracticable to lump together the concerns relating to data privacy and new social media with the data processing that every business must do on the employment relationship: hiring people, managing them and dealing with their departure".[125]

94. Lord McNally agreed that some of the proposals seemed to be over-concerned with social media, and said, "what we are really looking for is a coherent set of rules that will apply for all data controllers, which is simple and clear to understand and apply".[126]

Freedom of speech

95. The Newspaper Society highlighted the potential detrimental effect upon freedom of expression which could be wrought by the application of a "right to be forgotten" They quoted the former Justice Secretary, Rt Hon Kenneth Clarke MP, as saying "Other voices than mine have raised concerns over [the right to be forgotten's] ability to impinge on free speech, and to censor information which has been legitimately circulated in the public domain".[127]

96. Lord McNally told us:

> On the freedom of speech issue, Article 8 states very clearly that the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression should be open to exemptions or derogations.

Glenn Preston, Deputy Director for Information and Devolution, Ministry of Justice, added:

> It pretty much replicates what was already there in the existing Directive. There has not been a great call for us to change or amend that. Certainly we don't have any

124 Q 47

125 Ev w1

126 Q 136

127 Ev w67

> expectations that that is high on the list of things that people have been concerned about.[128]

Health

97. The British Medical Association (BMA) had serious concerns that Article 83 of the draft Regulation appeared to permit the processing of health data, in identifiable form, for research purposes without any reference to consent. Their written evidence explained the only safeguards which appeared in the clause seemed to be that identifiable data had to be kept separate and researchers would use identifiable data only if research could not be fulfilled by using non-identifiable data. The BMA argued that this seemed to significantly lower the existing standard for protection of health data.[129]

98. When we put this to the MoJ, they stated:

> We are aware that the individual citizen is very concerned that their medical records are not able to be disseminated in an improper way. Our conclusions are that, with the way the proposals are put, there are sufficient protections for medical records, but it is something that we will keep closely in view. [...] We do think the provisions in the Regulation are relatively strong on this particular point.[130]

99. Lord McNally wrote to us on 27 September, and stated:

> I can confirm that the Government did not receive a submission from the BMA [...] during our Call for Evidence. The evidence session was therefore the first time that these issues had been brought to my attention, for which I am grateful to the Committee. Fortunately, MoJ officials are attending a roundtable event on these proposals with the BMA in October. We will use this opportunity to listen to their concerns and factor them into our policy positions and negotiations in the Council.[131]

Fraud detection

100. A number of organisations expressed extreme concern that changes to the EU data protection legislative framework might impact on the ability of organisations to share information to aid fraud detection. The Association of British Insurers stated:

> Given the importance of fraud prevention and its benefit to consumers, it should not be left ambiguous or vulnerable to interpretation. It is therefore important that efforts to combat fraud are supported and explicitly recognised in the Regulation. Whilst we believe that Article 6, Clause 1(f) for non-sensitive data, encompasses data sharing for fraud purposes, it is not clear whether there is sufficient flexibility in the Regulation for sensitive data to be shared for these purposes. Of particular concern is

128 Q 134

129 Ev w92

130 Q 128

131 Ev 62

the restriction in the use of criminal conviction data, which can be an important component for insurance fraud detection or prevention.[132]

101. **The Government have told us that some organisations who submitted written evidence to us have not shared their concerns with them. We call on the Government to consider the points raised in paragraphs 90 to 100, and in more detail in written evidence, and inform us as to how, where necessary, they will be addressed in negotiations.**

The Committee's opinion

102. **The Regulation is necessary, first to update the 1995 Directive and take into account past and future technological change; and secondly to confer on individuals' rights that are necessary to protect their data and privacy as stipulated in the Lisbon Treaty and the EU Charter of Fundamental Rights.**

103. **However, the Regulation as drafted is over-prescriptive as to how businesses and public authorities should comply to ensure these rights are upheld. We have been told that the Information Commissioner's Office will require substantial extra resources, and businesses have argued that many administrative burdens will be imposed on them.**

104. **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.**

105. **To answer the European Scrutiny Committee's specific question to us:**

As currently drafted, the Regulation does give data subjects essential rights that must not be compromised during negotiations, and it has the potential to make data protection compliance easier for businesses, especially small businesses, which trade across the European Union. However, we do not believe that in its present form it will produce a proportionate, practicable, affordable or effective system of data protection in the EU.

132 Ev w30

3 The draft Directive

106. The overwhelming majority of the written evidence submissions we received focused solely on the draft Regulation, as was the case during the Government's consultation.[133] However, we were able to question several of our witnesses about the draft Directive during our evidence sessions.

The basis for, and aims of, reforming the Data Protection Framework Decision 2008

107. The draft Directive would repeal and replace the existing Data Protection Framework Decision, which was negotiated in 2008, entered into force on 19 January 2009, and had to be implemented by 27 November 2010.

108. The Government's Explanatory Memorandum states:

> The Commission believes that new rules governing the processing of personal data for the purpose of law enforcement and judicial co-operation are needed given the unprecedented growth of new and emerging technologies and the parallel increase in flows of information within and across national borders. The Commission also wants to provide greater consistency across Member States in the interpretation and implementation of rules governing data protection rights and contends that a harmonised set of rules will provide both greater certainty for individuals in understanding their rights and greater efficiencies in law enforcement co-operation.[134]

109. The Association of Chief Police Officers (ACPO) told us it was "rather surprised that the [Framework Decision] is going to be changed so soon after implementation", that it provided for the essential exchange of criminal conviction data with colleagues across Europe, and that the processes worked relatively well.[135]

Lord McNally, agreed with this assessment, and told us:

> [W]e do think it is a bit soon after the last tweak to this in 2008 to be looking at it again. It is a matter of balance whether you say that, since you are looking at the Regulation, which is much older, you might as well take another look at the police and law enforcement Directive at the same time. It is an argument for starting from square one again with that. From what I understand, the balance of the discussions so far has been much more about what's in the Regulation [...] rather than going back to square one with the police and law enforcement Directive.[136]

133 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 8

134 Ministry of Justice, *Explanatory Memorandum – Directive 5833/12*, para 4

135 Q 1

136 Q 109

110. The EU Commission's belief that a new Directive is required is based on a Commission Report which assessed the implementation and functioning of the Framework Decision.[137] Twenty Member States did not report any particular problems with the Framework Decision, whilst six Member States made comments on issues of concern to them. The Commission concluded that a new Directive could solve the practical difficulties encountered by a number of Member States in distinguishing between rules for domestic and cross-border data processing, clarify the scope and possible exemptions concerning data subjects' right to information, and strengthen data subjects' right of access through clarification and minimum harmonised criteria, while also providing exemptions to allow the police and justice authorities to properly perform their tasks. In addition, the Commission stated:

> [...] under Article 16 TFEU, which enshrines the right to the protection of personal data in the EU Treaties, there is now the possibility of establishing a comprehensive data protection framework ensuring both a high level of protection of individuals' data in the area of police and judicial cooperation in criminal matters and a smoother exchange of personal data between Member States' police and judicial authorities, fully respecting the principle of subsidiarity.[138]

111. The Commission argue that the Framework Decision has a limited scope of application, since it only applies to cross-border data processing, and this can create difficulties for authorities because they are not always able to easily distinguish between purely domestic and cross-border processing. Additionally, because of its nature and content, the Framework Decision leaves a lot of room for manoeuvre to Member States' national laws in implementing its provisions, and it does not contain any mechanism to support the common interpretation of its provisions, or enable the Commission to ensure a common approach in its implementation.[139]

112. Françoise Le Bail told us that the European Commission thought it was right to have an overall framework for data protection, and because the draft Directive would enable increased harmonisation and more consistent implementation across Member States it was an important element of the overall package of reforms. She commented that the Framework Decision imposed administrative burdens as it was difficult for authorities to make a distinction between data that are domestically processed and data that are not. Furthermore, including domestic processing in the draft Directive brought consistency to the overall regime, as the current general Directive applied to domestic and cross-border processing in non-criminal matters. She also explained that the draft Directive would make data protection a reality, because if the Member States did not apply the Directive, or did not apply it in the right way, the Commission could intervene.[140]

137 5834/12, Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions based on Article 29 (2) of the Council Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

138 *Ibid,* page 8

139 5833/12, page 2

140 Q 76

113. The Commission contend that a Directive is the best instrument to ensure harmonisation at EU level, whilst also leaving the necessary flexibility so that Member States can implement the principles, the rules and their exemptions at national level,[141] and the Government supports this view.[142]

114. **We are not convinced that there is a pressing need to alter EU law in this area, given that the Framework Decision 2008 was only recently implemented. However, it is arguable that since the general 1995 Directive requires updating, the corresponding legislation which deals with criminal matters should also be updated so that the principles in each instrument are consistent.**

115. The draft Directive sets out (for the purposes of police and judicial cooperation in criminal matters):

- principles governing personal data processing;
- rights of individuals to access their personal data, to have it rectified or erased, to object to processing and not to be subject to profiling;
- the obligations of data controllers and data processors to provide information to individuals, to report on breaches of data security and to put in place technical and organisational measures;
- rules on transfer of personal data to countries outside the European Economic Area (EEA) and to international organisations;
- rules relating to national regulators ("supervisory authorities"), and how they will cooperate with each other and the European Commission;
- remedies available to data subjects and the obligation for Member States to lay down rules on penalties, to sanction infringements, and to ensure their implementation.[143]

116. Some of the key changes that the Directive introduces as compared to the existing regime are as follows:

- an extension to the scope of data processing to include domestic processing for the purpose of policing and judicial cooperation;
- new definitions of key terms such as a "data subject", which includes identification of the individual by "online identifiers" and "genetic" identity;
- new rights of access and information for data subjects, such as the identity of the data controller, the purpose of the data processing and the period for which the data will be stored;
- an obligation for data controllers to implement "appropriate technical and organisational measures" to ensure an appropriate level of security;

141 Ministry of Justice, *Explanatory Memorandum* – 5833/12, page 6

142 *Ibid*, para 21

143 *Ibid*, para 5

- a right for data subjects to directly demand the erasure of their personal data by the data controller;
- an obligation on data controllers to inform supervisory authorities and data subjects of data breaches, informing the former within 24 hours of discovery and the latter "without undue delay"; and
- an obligation for data controllers or processors to appoint data protection officers.[144]

Perceived weakness in comparison to the draft Regulation

117. On the face of it, the scope of the draft Directive is similar to the draft Regulation, but there are important differences and various witnesses drew attention to the relative weakness of the Directive's provisions for the protection of personal data. For example, when the legislative framework was presented, Peter Hustinx, European Data Protection Supervisor, welcomed the new steps towards data protection in Europe but criticised the rules for the police and justice area as "inadequate", and stated:

> The Commission has not lived up to its promises to ensure a robust system for police and justice. These are areas where the use of personal information inevitably has an enormous impact on the lives of private individuals. It is difficult to understand why the Commission has excluded this area from what it intended to do, namely proposing a comprehensive legislative framework.[145]

118. The Information Commissioner's written evidence stated:

> [D]ue to the removal or adaptation of certain provisions, we are concerned that the Directive is now weaker than the Regulation. For example, the recitals of the Directive do not include important provisions relating to the retention of personal data, and its transparency provisions are weaker than those in the Regulation.[146]

Additionally, the Information Commissioner's initial analysis paper stated:

> [...] we would expect the principles to be consistent across both instruments. However, this is not the case and the recitals of the Directive fail to include important elements regarding the retention of personal data, transparency towards individuals, keeping personal data up to date, and ensuring it is adequate, relevant and not excessive. Accountability provisions requiring the data controller to demonstrate compliance are also missing. The December 2011 version also included provisions limiting access to data to duly authorised staff in competent authorities who need them for the performance of their tasks. This should be reintroduced.[147]

119. Privacy International told us:

144 Ministry of Justice, *Explanatory Memorandum – Directive 5833*/12, para 6

145 "EDPS welcomes a 'huge step forward for data protection in Europe', but regrets inadequate rules for the police and justice area", European Data Protection Supervisor press release, 25 January 2012

146 Ev 46

147 Information Commissioner's Office, *Initial analysis of the European Commission's proposals for a revised data protection legislative framework*, 27 February 2012, page 30

> As far as the proposed Directive is concerned [...] [w]e consider that the EU Commission drafters have failed in their duty to ensure a high level of data protection for citizens across the board. [...] Police and judicial cooperation in the context of law enforcement is an area where sensitive personal data is likely to be involved, and therefore citizens may be put at particular risk. We agree with the views of the UK Information Commissioner and the European Data Protection Supervisor in this respect.[148]

We asked Privacy International to expand on why they thought the draft Directive had a weaker level of protection in comparison to the draft Regulation, to which they answered:

> [...] it seems the rationale is one of ratcheting up the existing Framework Decision 2008/977/JHA and including data processing activities by the police and judiciary on the domestic levels, as agreed in the Lisbon Treaty, but at the same time playing to various member countries' political sensibilities and current situations. The result is not satisfactory in our view. In the explanatory memorandum to the Directive the Commission emphasises the need for a more comprehensive approach to data protection in the EU and seems to conclude that this will be achieved to a certain degree by this proposed Directive as it follows the same broad principles to the Regulation. But it doesn't and in our view it will create further confusion and grey areas.[149]

120. We also asked Françoise Le Bail, European Commission, why the draft Directive was perceived as weaker than the draft Regulation. She said the level of protection was not less, but was made differently because it applied to the area of cooperation in criminal matters. She argued that the data protection authorities might have wished for one single instrument for data protection, which would have been simpler, but this would not have been the ideal solution for police cooperation.[150]

121. **We agree with the Information Commissioner that data protection principles should be consistent across both the draft Regulation and the draft Directive. We recommend that during the negotiations on the legislation, the Government seek to amend the draft Directive so that this consistency is achieved.**

Impact assessment

122. The European Commission's impact assessment, which covers both the draft Regulation and the draft Directive, has been received with a high degree of scepticism. Table 5 of that impact assessment provides an overview of how the envisaged changes to the current regulatory framework will contribute to overall simplification. It states that the Directive will have "no impact on administrative burden[s]".[151]

123. The MoJ's *Summary of Responses* contains its own assessment of the draft Directive in a "Checklist for analysis on EU proposals". It states:

148 Ev 50

149 Ev 55

150 Q 72

151 5833/12 ADD 1. Impact Assessment accompanying the document, European Commission, page 95

> The overall impact is likely to be substantially negative, though it is difficult to place a number on it. The proposals are likely to impose new costs on criminal justice system agencies and the ICO. Though some measures are designed to aid good practice, many of the new obligations appear disproportionate and unnecessary leading to an overall negative outcome.[152]

These issues are explored in more detail in the accompanying Annex, *Assessment of impacts*, in particular identifying the groups likely to be affected.

> The proposal will impact on public authorities ("competent authorities") that processes personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. [...] Competent authorities include all Criminal Justice System (CJS) agencies, including the Police, Crown Prosecution Service, HMCTS, Probation, Youth Offending Services, Prisons, agencies with powers of prosecution and the judiciary.
>
> It is likely to affect the Police and other law enforcement authorities with regard to the processing of personal data. In particular, the scope of the legislation is being extended to include internal/domestic processing: all data transfers between domestic UK police forces (for example, data sent from the Metropolitan Police to South Yorkshire Police). This was previously not covered by the 2008 DPFD.
>
> Suspects, defendants, victims, witnesses will also be affected by the proposals by continuing to have their personal data protected by the law, with recourse to either a supervisory authority or the courts when their rights are infringed. This proposal therefore impacts on the civil liberties of citizens in general.
>
> The Information Commissioner's Office (ICO), the UK's supervisory authority that regulates inter alia data protection policy, will also be affected. There is a widening of the powers of the ICO and more areas where it will need to regulate and therefore both its scope and resource requirements will be increased.[153]

124. In paragraphs 31–37, we considered the impact assessments of both the Commission and the UK Government in relation to the draft Regulation. We repeat our recommendation here in relation to the draft Directive:

> We call on the European Commission to work with the UK Government, the governments of other Member States, and other stakeholders, and to pool resources, expertise and information, so that a full assessment of the impact of the proposals can be produced.

Application to the United Kingdom

125. The Government's position is that, as the proposals stand, they only apply to the UK in the limited circumstances where data sharing is done under Title V measures in the area

152 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, 28 June 2012, page 66: Directive – Checklist for analysis on EU proposals

153 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, Directive – Checklist for analysis on EU proposals – ANNEX A: ASSESSMENT OF IMPACTS, paras 4–7, 28 June 2012

of police and judicial cooperation in criminal matters that bind the UK.[154] The Government's Explanatory Memorandum states:

> It is important to note, however, that Article 6a of the UK and Ireland's Title V Protocol (Protocol 21 TFEU) is likely to mean that there is a limited application of the Directive to the UK (and Ireland). Although no final position has been agreed with the Commission, current UK legal opinion of Article 6a of the Protocol means that the Directive will only apply in instances where data processing is being carried out pursuant to an EU measure that binds the UK. This necessarily excludes internal processing from applying to the UK if this legal opinion is accepted. It also means that any rights exercised in regards to internally-processed data, such as rights of access to Police data, will not apply to the UK.[155]

The then Minister, Mr Crispin Blunt MP, told the House on 24 April "We believe that the limiting effect of Article 6a on the aspects of the directive that relate to data exchanges within the United Kingdom means that we should be content to be part of it, which will of course substantially reduce the costs identified in the impact assessment".[156] Mr Blunt told the European Scrutiny Committee:

> we believe our understanding to be shared by the Commission. In order to try and reinforce our belief and what we understand to be the Commission's belief as to the correct interpretation of Article 6(a), we want to get that written on to the face of the Directive in the negotiations that are ongoing. [...] There is obviously a very small risk that if we did not get it written on to the face of the Directive, we could then find ourselves with different parts of European institutions [...] attempting to apply it.[157]

126. The Annex assesses the impact of the Directive on the basis that the UK will be subject to the domestic processing provisions, and as such has reached the conclusion that the overall impact will be substantially negative.[158]

127. The Association of Chief Police Officers (ACPO) told us "[w]hat has yet to be made clear is whether the Directive will apply only to the UK in circumstances where data is being shared for the purposes of an EU instrument and not when we are sharing information purely for domestic reasons. Clearly, if this were to impact on day to day exchange of information between forces, the ramifications would be significant and come at a high cost".[159] However, they go on to say, "we believe that providing the Directive does not impact upon domestic processing, that the impact will not be severe".[160]

154 Ministry of Justice, *Explanatory Memorandum – Directive 5833*/12, paras 10–12

155 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, Directive – Checklist for analysis on EU proposals – ANNEX A: ASSESSMENT OF IMPACTS, para 15, 28 June 2012

156 HC Deb, 24 April 2012, col 890

157 Oral evidence taken before the European Scrutiny Committee on 11 July 2012, HC (2012–13) 528-i, Q 30 [Mr Blunt]

158 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, Directive - Checklist for analysis on EU proposals – ANNEX A: ASSESSMENT OF IMPACTS

159 Ev 36

160 Ev 38

128. **It needs to be clear beyond doubt that exchange of information between UK law enforcement agencies is not covered by the Directive, and the Government's negotiating stance should seek to ensure that the exemption of the UK from provisions relating to domestic processing is written into the Directive. In order to clarify the position, the Ministry of Justice should provide an impact assessment of the draft Directive on the basis that domestic processing does not apply to the UK.**

Practical impact on competent authorities

129. Ian Readhead, Director of Information, Association of Chief Police Officers, said in oral evidence, "in relation to the exchange of European conviction data, I want to impress upon you first how important that is and the kind of work we are undertaking at present". He continued by explaining how records of previous convictions in other Member States could be produced in UK courts, to aid a prosecution in this country. UK police forces could also track offenders across Europe, so that if an individual was arrested and returned to a Member State on a European Arrest Warrant, the case would be followed. If the individual was convicted of a serious offence, the police would notify the UK Border Agency who would be able to prevent the individual's re-entry to the UK. In a similar way the police were able to track sex offenders across Europe. He said "[t]hrough all of these processes [...] we try proactively to put in place schemes to try and monitor offending behaviour on a European level to protect local communities".[161]

130. However, Mr Readhead expressed concern about how the draft Directive could change current practices. He stated:

> The Directive uses four principles in relation to how we can use data: it talks about the execution of criminal penalties, investigation, detection and the prosecution of criminal offenders. It doesn't talk about common law. If we had a paedophile offender released from prison who goes to live on a caravan park, we go to the caravan park; we talk to the local families who are in caravans; we tell them, "There is a paedophile here." We do that unashamedly because we have to protect communities and protect vulnerable persons and children. This Directive, written in the way it currently is, in our view would prevent us from doing that. [...]
>
> It prevents us [from making that kind of disclosure] because of the prescriptive nature of the Directive. As we read this, those areas do not permit us to use our common law powers anymore, because, effectively, the argument would be that we are no longer processing data in accordance with either this Directive or the Regulation. That is a real concern to us because there is huge value in exchanging information with other agencies.[162]

131. Françoise Le Bail, European Commission, told us the Commission believed that the draft Directive would reinforce and greatly simplify the operations of law enforcement agencies, reiterating that the data protection principles would remain the same and there

161 Q 7

162 Qq 8–9

would still be distinctions in how Member States transposed the draft Directive.[163] Her colleague, Marie-Hélène Boulanger, Head of the Data Protection Unit, added:

> We believe that having more common grounds among Member States and more common understanding about which data protection requirement conditions will apply to the law enforcement authorities, especially in the framework of the law enforcement co-operation, will simplify co-operation between law enforcement authorities, will foster this co-operation and will also have an important impact on the efficiency of law enforcement co-operation.[164]

132. During oral evidence, the Information Commissioner's Office stated:

> [W]hen whatever comes from Brussels is applied in the UK, the Government do have a choice as to what rules they apply to policing domestically. Even if we are not part of the Directive for policing domestically, we will still have data protection law in the UK for domestic policing, just as we do at the moment. Our position will be that that should be closely aligned to the Brussels regime, even if it is not mandatory on the UK to follow that approach, because that makes it easier for individuals and for us as the regulator. [...]
>
> I think you can align the principles and the basic operation. I do not think any of the witnesses so far have really questioned any of the basics. It is the administrative burdens that go with it that are the problems. I do think we could [...] take a proportionate approach to how that is applied in the UK so that the principles are there. It doesn't stop the exchange of data with Europe because we have different rules, but we don't necessarily apply all the detailed prescription that has caused so much concern. [...]
>
> Of course the police have concerns about whether they are going to be able to do their job across borders, capturing criminals and so on. There are also very basic questions about protection for the citizen in their dealings with the police that arise from data protection law.[165]

133. **We understand that the Directive does not apply to domestic processing by law enforcement agencies within the UK, and it should be placed beyond doubt that this is the case. We have noted the evidence of the Association of Chief Police Officers, that the Directive might nevertheless impact on the ability of the police to use common law powers to pass on information in the interests of crime prevention and public protection, and we believe that it needs to be made clear beyond doubt that it must not have this effect. We also agree with ACPO that the Directive, like the Regulation, is unnecessarily prescriptive about the structures and processes for securing data protection compliance.**

163 Q 73

164 Q 74

165 Qq 32–33

General comments on the draft Directive

134. The MoJ told us it has concerns with the draft Directive as it was "presently too long and prescriptive, which we believe will represent a burdensome cost on data controllers and processors. It may not, therefore, be considered proportionate or practicable". It would therefore negotiate to remove or modify the most disproportionate and prescriptive aspects of the proposal, whilst ensuring that there was always adequate and effective protection for data subjects.[166]

ACPO told us that due to the burdens contained within the draft Directive "[t]here is a risk that such an approach may create barriers which hinder the ability to conduct effective intelligence analysis or to create excessive burdens on law enforcement agencies. [...] Affordability should be a feature of proposals being promulgated against the backdrop of austerity measures within the public sector".[167] Ian Readhead, Director of Information, Association of Chief Police Officers, expanded on this when he appeared before us:

> [W]e need to be very clear that the prescriptive nature of this Directive is, in our view, excessive and is totally alien to the way in which we provide compliance with the [Data Protection] Act. [...] The Commission should not be saying, "You've got to have a data protection officer and this is the role and function of that data protection officer." What they should be saying is, "Against the backdrop of the Directive you should have compliance." How we provide compliance is a matter for us, because [...] chief constables have looked very carefully at their structures and we don't have data protection officers anymore; we have information managers who cover a whole raft of compliance areas. [...] It is compliance that is critical, not a bureaucratic process that seeks to say, "These are your structures."

In addition he said that some of the business processes stipulated by the Directive would involve significant costs at a time when public services were seeking to reduce their costs.[168]

135. However, Privacy International considered that the fundamental rights of individuals to privacy and data protection had to be taken into account alongside considerations of burdens to business and administrations. They argued that, in terms of the Directive, the Commission drafters had failed in their duty to ensure a high level of data protection for citizens across the board, and that it required radical improvement.[169] In addition they argued that the draft Directive would not achieve its aims, stating:

> The rights of the individual are weaker in the case of the proposed Directive than in the case of the proposed Regulation and inevitably the transposition of the Directive in the different nations will result in the very fragmentation that the new Framework aims to avoid. In addition, these weak provisions in the case of the Directive have the potential to also undermine individual rights under the Regulation, in cases where law enforcement authorities have access to data from private entities. [...] As the result of these two differing 'legal instruments', the new Data Protection Framework

166 Ev 52

167 Ev 37

168 Q 3

169 Ev 49

> suffers as a whole, because the original aim of achieving harmonised and comprehensive data protection rules is not achieved.[170]

In addition, Privacy International raised concerns that the Directive was not addressed in the 'next steps' section of the *Summary of Responses*, despite it requiring "major surgery in order not to undermine the whole Framework".[171] Anna Fielder, Trustee and Company Secretary, Privacy International, told us:

> You could align the provisions in the Directive much more with the provisions in the Regulations. Indeed, in our analysis of the Directive, we have proposed concrete amendments for this to happen, and we would very much urge the UK, in the Council of [Ministers], to lobby and ensure that that happens. We know also that quite a lot of other Member States are not happy about the situation because it weakens their domestic Regulations as well, so I think it is still not too late to achieve some consistency.[172]

136. Françoise Le Bail, European Commission, told us that the two instruments had the same data protection principles in common, but whilst the Regulation would be directly applicable, the Directive gave Member States the flexibility to take into consideration their particular culture and type of legislation, such as the common law in the UK. She stated:

> This is the reason why, although there is a huge amount of commonality, there are also a number of elements that are different because the field itself is different. But they are part of the same exercise, which is to reinforce the rights of individuals in terms of data protection. [...] We believe that, by presenting two types of legislation at the same time, we will fight against this fragmentation but we can also give the necessary flexibility.[173]

Specific aspects of the draft Directive

137. We highlight here some specific aspects of the Directive as it is currently drafted that witnesses have particularly commented on. A number of issues are broadly covered by similar aspects of the draft Regulation, which we comment on in chapter 2 of this Report.

Domestic processing

138. The draft Directive extends the scope of EU law to cover domestic processing — processing purely between domestic authorities with no cross-border element, for example between the Metropolitan Police and West Midlands Police. The MoJ's written evidence stated:

> Consultation with key stakeholders in the field of law enforcement and judicial cooperation has uncovered no evidence that the current lack of EU rules in this area has obstructed co-operation between Member States; or had detrimental impacts on

170 Ev 51

171 *Ibid.*

172 Q 52

173 Q 71

> [...] the protection of individuals. Indeed, we think that introducing prescriptive requirements for domestic processing may instead have a detrimental effect on law enforcement operations, placing onerous burdens on data controllers and huge costs on public authorities — without delivering better data protection for individuals.[174]

139. However, as explained in paragraphs 124–126, the Government are confident that domestic processing will only apply to the UK in the limited circumstances where processing is being carried out pursuant to an EU measure which binds the UK. The Government have explained it will seek to negotiate to remove domestic processing from the Directive for all Member States as a matter of policy,[175] because it does not consider domestic processing to be an area that should be regulated at the EU level.[176]

140. David Smith, Deputy Commissioner and Director of Data Protection, Information Commissioner's Office told us:

> Even if we are not part of the Directive for policing domestically, we will still have data protection law in the UK for domestic policing, just as we do at the moment. Our position will be that that should be closely aligned to the Brussels regime, even if it is not mandatory on the UK to follow that approach, because that makes it easier for individuals and for us as the regulator.[177]

141. In oral evidence the European Commission explained why it believed it was now appropriate to include domestic processing under EU legislation. Françoise Le Bail told us:

> [...] the framework decision doesn't cover domestic processes. From all the contacts we had, having consulted very widely for two years before putting forward these proposals, we realised from all the stakeholders we were in touch with that it is increasingly difficult to make a distinction between the data that is domestically processed and the data that is not. For the enforcement authorities themselves, this has become a great difficulty and, paradoxically, it has become an admin burden to make this distinction. We thought, having consulted widely, that this was the time to include domestic processing in it, again to create consistency in the overall regime in the same way it is done for the Regulation and, for that matter, for the current Directive.[178]

Her colleague, Marie-Hélène Boulanger, Head of the Data Protection Unit, European Commission, explained why domestic processing was not included in the Framework Decision 2008:

> the framework decision is [...] a pre-Lisbon instrument, which means that the way it was adopted [differed from the proposed] Directive. [...] [I]n order to get the consensus of all Member States at that time, it was necessary to exclude domestic

174 Ev 53

175 *Ibid.*

176 Ev 52

177 Q 32

178 Q 76

> processing. What I have been told by my colleagues who were there is that it was not a majority that was against it; it was the way to get a consensus on this text.[179]

142. However, Lord McNally maintained that the position of the UK – shared with allies among other Member States – was that the draft Directive should not apply to domestic processing and the Government would be negotiating for its removal in order to achieve "the best outcome for the Directive as a whole". He added, "[i]t is almost a belt-and-braces approach. We are securing our own position but we want to argue the case for keeping these matters to domestic control across the Community or the Union".[180]

143. **The Government argues that the current lack of EU legislation on domestic processing has not obstructed cooperation between Member States, but the European Commission argues that it does cause difficulties for a number of Member States. We call on the Government to explain further why they are opposed to domestic processing for other Member States, given the current position that it will not apply to the UK, and to clarify what impact the changes would have on cooperation with the UK.**

Right to erasure

144. The draft Directive differs from the draft Regulation in that it does not include the "right to be forgotten". It does contain a right for data subjects to directly demand the erasure of their personal data by the data controller if it does not conform with the data protection principles, and they will now be able to make this demand directly to the data controller.[181]

Obligation to appoint Data Protection Officers

145. Article 30 of the draft Directive states that data controllers will be obligated to designate data protection officers (DPOs), all of whom must have "professional qualities" and "expert knowledge of data protection law and practices". The proposed Directive prescribes a list of eight tasks that the DPO will have to fulfil, including the monitoring of documentation kept by processors and controllers, to monitor the implementation of data protection policies and to consult with the supervisory authority.[182]

146. The Association of Chief Police Officers' written evidence stated:

> The prescriptive nature of [...] the [...] Directive is evidenced again with regard to the proposals concerning the designation of Data Protection Officers. As a matter of principle, the focus should be upon compliance not how an organisation structures itself in order to deliver compliance. At present appointed Data Protection Officers are not consistent with information management regimes contained within the Police Service. As part of the austerity programme, roles have been converged which often cover a range of portfolio responsibilities focused upon Freedom of

179 Q 77

180 Qq 103–104

181 Ministry of Justice, *Explanatory Memorandum – Regulation 5853*/12, para 29

182 Ministry of Justice, *Summary of Responses: Call for Evidence on Proposed EU Data Protection Legislative Framework*, Directive– Checklist for analysis on EU proposals – ANNEX A: ASSESSMENT OF IMPACTS, para 53, 28 June 2012

> Information, Data Protection and security. This does not mean that we have lost our focus upon adhering to the legislation but we have made management decisions on how best to deliver our compliance strategy.[183]

Ian Readhead, ACPO's Director of Information expanded on this point when he gave oral evidence to the Committee. He highlighted that administrative burdens such as these would be disproportionately heavy on smaller forces "because those smaller forces are the ones that have recruited one person to undertake a number of [...] roles. The concept that you wind the clock back to having a data protection officer is just inconsistent with the way in which you provide compliance with the legislation".[184] His ACPO colleague, Merilyne Knox, Head of Public Access Office, Metropolitan Police, explained:

> One facet of my role is as a data protection officer. I take on multiple portfolios with regard to information management, and it is important that is maintained because, in order to come to an informed judgment regarding how the police force should manage its information, it should have due regard to all the information management legislation, codes of practice and so on.[185]

Bi-lateral and multi-lateral agreements

147. The MoJ's written evidence sets out its policy position, that bi-lateral and multi-lateral agreements existing at the time the Directive is adopted should not be subject to renegotiation under the Directive. It argued that there are numerous international data sharing agreements in place which would require renegotiation under the provisions of the Directive.[186]

148. We asked the Information Commissioner's Office what they thought the impact of renegotiating these agreements might be. David Smith, Deputy Commissioner, answered:

> Those bilateral treaties have, presumably for the most part, been entered into under our current data protection regime and should respect the requirements under that regime. As we said, the principles under the new regime are very similar so, if those bilateral agreements meet the current requirements, they won't necessarily fail to meet the new requirements. A process of review is required, but our understanding is that there are very many of these bilateral agreements. We believe that the Ministry of Justice have developed a catalogue of these; so they may be able to advise in more detail. But, clearly, those sorts of agreements should be consistent with whatever the new legal regime is and so a review at the very least would be needed.[187]

183 Ev 36

184 Q 4

185 Q 5

186 Ev 54

187 Q 34

The Committee's opinion

149. **From the point of view of the data subject, the draft Directive provides a weaker level of data protection in comparison to the draft Regulation. We recognise the significant differences in the handling of sensitive personal data by law enforcement authorities, but in a number of respects this lower level of protection does not appear justifiable. During negotiations, the Government should seek to amend the draft Directive so that data protection principles are as consistent as possible across both EU instruments. This will additionally ensure that the rights set out in the Lisbon Treaty are upheld.**

150. **The Government's position is that the Directive will have limited application to the UK, due to Article 6a of Protocol 21 of the Treaty on the Functioning of the European Union. If this is the case, we believe it will be beneficial to the UK as law enforcement authorities will not be bound by over-prescriptive measures contained within the Directive. This would also mean that EU law will not apply to the domestic processing of data, such as between police forces. Domestic processing for criminal justice matters will continue to be covered by the Data Protection Act 1998.**

151. **To answer the European Scrutiny Committee's specific question to us:**

As currently drafted, the Directive does not sufficiently protect personal data. In particular, the level of data protection is not to the same standard as that contained in the draft Regulation which covers general data protection matters. We are concerned that it should be clear that domestic processing of data within the UK by law enforcement agencies will not be covered or restricted by the Directive, and it should also be clear that Member States have the flexibility to implement the Directive in ways which achieve its purposes through processes which are appropriate and proportionate in the national context.

Conclusions and recommendations

The approach to reforming the current data protection framework

1. We are concerned that the approach taken by the European Commission, introducing two instruments, will lead to a division of the UK law, set out in the Data Protection Act. We believe that this could cause confusion, both for data subjects, and for organisations within the criminal justice system in particular, as they will have to consider which law applies in their given circumstance. We are also concerned that this twin-track approach might also lead to inconsistencies in application, both due to differing provisions in the instruments and over time, due to court decisions under each instrument. If this is still to be the approach, we recommend that there is consistency between the two instruments from the outset, to mitigate the future divergence in their application. Furthermore, the UK Government and the Information Commissioner's Office will be required to work effectively together in order to produce and disseminate effective guidance so that data subjects know their rights and organisations know their responsibilities under each law. (Paragraph 13)

The draft Regulation

Arguments for and against a Regulation

2. Bringing EU data protection legislation up-to-date is necessary and could provide benefits to both individuals and businesses. Many of these benefits are only attainable if there is effective harmonisation of laws across Member States, and therefore we can understand why the European Commission decided that a Regulation was the correct instrument to achieve their objective. However, by setting out prescriptive rules there is no flexibility to adjust to individual circumstances. We believe that the Regulation should focus on stipulating those elements that it is essential to harmonise to achieve the Commission's objective, such as the consistency mechanism and the establishment of the European Data Protection Board. Member States' data protection authorities should be entrusted to handle factors associated with compliance, such as the level of fees or when it should be informed about a data protection impact assessment, whilst also being a source of guidance. Consistency of approach should then be delegated to the European Data Protection Board. (Paragraph 30)

Impact assessment

3. We call on the European Commission to work with the UK Government, the governments of other Member States, and other stakeholders, and to pool resources, expertise and information, so that a full assessment of the impact of the proposals can be produced. (Paragraph 37)

Impact on the information Commissioner's Office

4. We regard as authoritative the UK Information Commissioner's assertion that the system set out in this draft Regulation "cannot work" and is "a regime which no-one will pay for", and we believe that the Commission needs to go back to the drawing board and devise a regime which is much less prescriptive, particularly in the processes and procedures it specifies. (Paragraph 43)

General comments on the draft Regulation

5. We note that both the Government and the Information Commissioner believe that the necessary changes in the Regulation and the Directive can be agreed through negotiation, and we support them in their efforts to achieve this. (Paragraph 55)

The "right to be forgotten"

6. The right of citizens to secure the erasure of data about them which is wrongly or inappropriately held is very important, but it is misleading to refer to this as a "right to be forgotten", and the use of such terminology could create unrealistic expectations, for example in relation to search engines and social media. (Paragraph 63)

Subject access rights

7. An individual's right of access to their own personal data is a fundamental right; and individuals should not be required to pay a fee to make a subject access request. We urge the Government to change its negotiating position to one which accepts that subject access rights should be exercisable free of charge. (Paragraph 77)

Obligation to appoint Data Protection Officers

8. We believe that if the requirement to employ a Data Protection Officer is retained it should be based on the type of business and the sensitivity of data that is handled, rather than the number of employees. (Paragraph 81)

Sanctions

9. We believe that data protection authorities should have more discretion as to the sanctions that they can impose in order to effectively punish the worst behaviour. We are aware that this could result in different approaches being taken in each Member States, and therefore recommend that, where there is evidence that such differences are having a deleterious effect on compliance, the European Data Protection Board be entrusted to provide guidelines on the type of sanction that may be appropriate in given situations. (Paragraph 88)

Concerns raised by specific groups

10. The Government have told us that some organisations who submitted written evidence to us have not shared their concerns with them. We call on the

Government to consider the points raised in paragraphs 90 to 100, and in more detail in written evidence, and inform us as to how, where necessary, they will be addressed in negotiations. (Paragraph 101)

The Committee's opinion

11. The Regulation is necessary, first to update the 1995 Directive and take into account past and future technological change; and secondly to confer on individuals' rights that are necessary to protect their data and privacy as stipulated in the Lisbon Treaty and the EU Charter of Fundamental Rights. (Paragraph 102)

12. However, the Regulation as drafted is over-prescriptive as to how businesses and public authorities should comply to ensure these rights are upheld. We have been told that the Information Commissioner's Office will require substantial extra resources, and businesses have argued that many administrative burdens will be imposed on them. (Paragraph 103)

13. 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. (Paragraph 104)

14. To answer the European Scrutiny Committee's specific question to us:

As currently drafted, the Regulation does give data subjects essential rights that must not be compromised during negotiations, and it has the potential to make data protection compliance easier for businesses, especially small businesses, which trade across the European Union. However, we do not believe that in its present form it will produce a proportionate, practicable, affordable or effective system of data protection in the EU. (Paragraph 105)

The draft Directive

The basis for, and aims of, reforming the Data Protection Framework Decision 2008

15. We are not convinced that there is a pressing need to alter EU law in this area, given that the Framework Decision 2008 was only recently implemented. However, it is arguable that since the general 1995 Directive requires updating, the corresponding legislation which deals with criminal matters should also be updated so that the principles in each instrument are consistent. (Paragraph 114)

Perceived weakness in comparison to the draft Regulation

16. We agree with the Information Commissioner that data protection principles should be consistent across both the draft Regulation and the draft Directive. We recommend that during the negotiations on the legislation, the Government seek to amend the draft Directive so that this consistency is achieved. (Paragraph 121)

Application to the United Kingdom

17. It needs to be clear beyond doubt that exchange of information between UK law enforcement agencies is not covered by the Directive, and the Government's negotiating stance should seek to ensure that the exemption of the UK from provisions relating to domestic processing is written into the Directive. In order to clarify the position, the Ministry of Justice should provide an impact assessment of the draft Directive on the basis that domestic processing does not apply to the UK. (Paragraph 128)

Practical impact on competent authorities

18. We understand that the Directive does not apply to domestic processing by law enforcement agencies within the UK, and it should be placed beyond doubt that this is the case. We have noted the evidence of the Association of Chief Police Officers, that the Directive might nevertheless impact on the ability of the police to use common law powers to pass on information in the interests of crime prevention and public protection, and we believe that it needs to be made clear beyond doubt that it must not have this effect. We also agree with ACPO that the Directive, like the Regulation, is unnecessarily prescriptive about the structures and processes for securing data protection compliance. (Paragraph 133)

Domestic processing

19. The Government argues that the current lack of EU legislation on domestic processing has not obstructed cooperation between Member States, but the European Commission argues that it does cause difficulties for a number of Member States. We call on the Government to explain further why they are opposed to domestic processing for other Member States, given the current position that it will not apply to the UK, and to clarify what impact the changes would have on cooperation with the UK. (Paragraph 143)

The Committee's opinion

20. From the point of view of the data subject, the draft Directive provides a weaker level of data protection in comparison to the draft Regulation. We recognise the significant differences in the handling of sensitive personal data by law enforcement authorities, but in a number of respects this lower level of protection does not appear justifiable. During negotiations, the Government should seek to amend the draft Directive so that data protection principles are as consistent as possible across both

EU instruments. This will additionally ensure that the rights set out in the Lisbon Treaty are upheld. (Paragraph 149)

21. The Government's position is that the Directive will have limited application to the UK, due to Article 6a of Protocol 21 of the Treaty on the Functioning of the European Union. If this is the case, we believe it will be beneficial to the UK as law enforcement authorities will not be bound by over-prescriptive measures contained within the Directive. This would also mean that EU law will not apply to the domestic processing of data, such as between police forces. Domestic processing for criminal justice matters will continue to be covered by the Data Protection Act 1998. (Paragraph 150)

22. To answer the European Scrutiny Committee's specific question to us:

As currently drafted, the Directive does not sufficiently protect personal data. In particular, the level of data protection is not to the same standard as that contained in the draft Regulation which covers general data protection matters. We are concerned that it should be clear that domestic processing of data within the UK by law enforcement agencies will not be covered or restricted by the Directive, and it should also be clear that Member States have the flexibility to implement the Directive in ways which achieve its purposes through processes which are appropriate and proportionate in the national context. (Paragraph 151)

Formal Minutes

Wednesday 24 October 2012

Members present:

Sir Alan Beith, in the Chair

Steve Brine	Nick de Bois
Mr Robert Buckland	Seema Malhotra
Jeremy Corbyn	Yasmin Qureshi

Draft Report (*The Committee's opinion on the European Union's Data Protection framework proposals*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 151 read and agreed to.

Summary agreed to.

Resolved, That the Report be the Third Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

Written evidence was ordered to be reported to the House for printing with the Report, together with written evidence reported and ordered to be published on 4 and 17 September 2012.

Written evidence was ordered to be reported to the House for placing in the Library and Parliamentary Archives.

[Adjourned till Tuesday 30 October at 9.15am.

Witnesses

List of printed written evidence

List of additional written evidence

(published in Volume II on the Committee's website www.parliament.uk/justicecom)

List of unprinted evidence

The following written evidence has been reported to the House, but to save printing costs has not been printed and copies have been placed in the House of Commons Library, where they may be inspected by Members. Other copies are in the Parliamentary Archives (www.parliament.uk/archives), and are available to the public for inspection. Requests for inspection should be addressed to The Parliamentary Archives, Houses of Parliament, London SW1A 0PW (tel. 020 7219 3074; email archives@parliament.uk). Opening hours are from 9.30 am to 5.00 pm on Mondays to Fridays.

Hargreaves Lansdown

List of Reports from the Committee during the current Parliament

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2010–12

First Report	Revised Sentencing Guideline: Assault	HC 637
Second Report	Appointment of the Chair of the Judicial Appointments Commission	HC 770
Third Report	Government's proposed reform of legal aid	HC 681–I (Cm 8111)
Fourth Report	Appointment of the Prisons and Probation Ombudsman for England and Wales	HC 1022
Fifth Report	Appointment of HM Chief Inspector of Probation	HC 1021
Sixth Report	Operation of the Family Courts	HC 518-I (Cm 8189)
Seventh Report	Draft sentencing guidelines: drugs and burglary	HC 1211
Eighth Report	The role of the Probation Service	HC 519–I (Cm 8176)
Ninth Report	Referral fees and the theft of personal data: evidence from the Information Commissioner	HC 1473(Cm 8240)
Tenth Report	The proposed abolition of the Youth Justice Board	HC 1547 (Cm 8257)
Eleventh Report	Joint Enterprise	HC 1597 (HC 1901)
Twelfth Report	Presumption of Death	HC 1663 (Cm 8377)
First Special Report	Joint Enterprise: Government Response to the Committee's Eleventh Report of Session 2010–12	HC 1901

Session 2012–13

First Report	Post-legislative scrutiny of the Freedom of Information Act 2000	HC 96–I
Second Report	The budget and structure of the Ministry of Justice	HC 97–I

Oral evidence

Taken before the Justice Committee

on Tuesday 4 September 2012

Members present:

Sir Alan Beith (Chair)

Mr Robert Buckland	Seema Malhotra
Jeremy Corbyn	Yasmin Qureshi
Mr Elfyn Llwyd	Elizabeth Truss

Examination of Witnesses

Witnesses: **Ian Readhead**, Director of Information, Association of Chief Police Officers, and **Merilyne Knox**, Head of Public Access Office, Metropolitan Police, gave evidence.

Q1 Chair: Ms Knox, Mr Readhead, welcome. We are very glad to have you helping us with our work on the EU Data Protection Framework Directive. Both of you have been involved in ACPO's work in this area. Although Ms Knox is from the Metropolitan Police, it is in the ACPO capacity, I think, that you are here with us today. The Framework Decision 2008 is what you have been working with for some years. Was there anything much wrong with it and couldn't we have carried on with that?

Ian Readhead: I think the answer to that is we are rather surprised that the Directive is going to be changed so soon after implementation. The Directive provided to the police service is the framework upon which we exchange criminal conviction data with our colleagues across Europe and I cannot underestimate how critical that is to the police service, against a backdrop that so many offenders who now come into our custody centres are not UK nationals. In the Metropolitan Police, for example, that level is nearly 40%, and so having a process whereby we can exchange conviction history is absolutely essential to good crime investigation and also to ensure that the courts obtain that information so that they can advise magistrates and judges about tariff and bail. We think those processes worked relatively well and we are surprised that we are now looking at a new Regulation and Directive.

Q2 Chair: In your communication with other countries and police forces in other countries are they similarly surprised, do you think, and happy with the arrangements?

Ian Readhead: There would be some countries who would say that their systems are well developed and perhaps there are others who still have some way to go to mature an approach to data protection. It is the concept that one hat fits all that worries us about the Directive. We think that compliance with the current Data Protection Act, although it perhaps is described as inelegant, with regard to proportionality, accuracy and retention periods, provides an excellent framework for exchange and also creates the right balance between the rights of the state and the police service in particular to hold personal data, against the rights of the individual as well for privacy.

Q3 Mr Llwyd: Good morning, Ms Knox and Mr Readhead. In your written evidence ACPO says "… we do not underestimate the new levels of bureaucracy and cost the Directive will cause to fall upon the police service". What is your assessment of the actual cost of this proposed Directive that is likely to fall upon the police service?

Ian Readhead: As you know, the Ministry of Justice at the moment are going through a costing exercise and we are unaware of any due diligence being carried out by the Commission with regard to these proposals. But we need to be very clear that the prescriptive nature of this Directive is, in our view, excessive and is totally alien to the way in which we provide compliance with the Act.

With the greatest respect to the Commission, the Commission should not be saying, "You've got to have a data protection officer and this is the role and function of that data protection officer." What they should be saying is, "Against the backdrop of the Directive you should have compliance." How we provide compliance is a matter for us, because, as in many other public services, chief constables have looked very carefully at their structures and we don't have data protection officers any more; we have information managers who cover a whole raft of compliance areas—be that freedom of information, subject access, data protection or vetting. It is compliance that is critical, not a bureaucratic process that seeks to say, "These are your structures."

I also have to say that some of the business processes within the Directive will involve us in significant cost—for example, the proactive method by which we would have to advise individuals potentially that we hold their data. The concept that you can hold data separately for victims, witnesses, suspects and offenders is, in our view, absurd because some individuals will be all of those. This kind of approach, in our view, is administratively cumbersome, would have significant costs for us in IT terms, would involve us recruiting more staff and comes at a time when public services are going the opposite way. We are actually trying to reduce our costs, whilst having compliance.

Q4 Mr Llwyd: The likelihood is that it would be disproportionately heavy on smaller forces.

Ian Readhead: I think that is right because those smaller forces are the ones that have recruited one person to undertake a number of those roles. The concept that you wind the clock back to having a data protection officer is just inconsistent with the way in which you provide compliance with the legislation.

Q5 Mr Llwyd: Ms Knox, do you wish to add anything to that?

Merilyne Knox: No. I would echo the views that Ian has put to you. One facet of my role is as a data protection officer. I take on multiple portfolios with regard to information management, and it is important that is maintained because, in order to come to an informed judgment regarding how the police force should manage its information, it should have due regard to all the information management legislation, codes of practice and so on.

Q6 Mr Llwyd: This is a question for either one or perhaps both of you. Where, in your opinion, should the balance lie between data protection rights and administrative burdens?

Ian Readhead: The role of the police service is to hold data differently from colleagues in the private sector. We run informants. Informants are very often criminals. How we manage that data, which is based on opinion rather than fact, is not the same as that envisaged by the Commission. It is not a factual process; it is an opinion process.

What we wholly accept, though, is that our accountability is to a number of structures. We account to the Information Commissioner, the Communications Commissioner, the Surveillance Commissioner and the courts. There are good examples of where the way in which we have held data historically has not found favour with the European Court of Justice and we have had to change that. Those are the checks and balances that exist for the police service. Inevitably, though, we will hold more information about individuals than will exist in the private sector and the balance is through those checks and balances that I have described.

Q7 Mr Buckland: In your written evidence, you make the proper point that it is unclear as to whether or not the new proposal would apply just for EU purposes or for domestic purposes. Have you had any guidance or assistance from the Ministry of Justice as to what their view is as to the applicability of the new proposal?

Ian Readhead: We have. We have worked very closely with the Ministry of Justice and also with the Home Office. We have been through the legislation with them and we have also had the benefit of Hansard, looking at the debate in the House. The current advice from the Ministry of Justice is that domestic processing is not covered by this Directive, and I have to say we are extremely pleased that that is the case; it would be absurd if 43 police forces now had to have information-sharing agreements with each other. It runs against the whole concept of sharing information and having a common approach to areas such as intelligence that came out of the Bichard Inquiry.

None the less, in relation to the exchange of European conviction data, I want to impress upon you first how important that is and the kind of work we are undertaking at present. For example, in regard to a German national who is arrested in this country, we would go to our colleagues in Germany to find out if he had any antecedent history. Those convictions, if he had them, would then be produced to the court in this country. If that German national were then convicted in this country, that record, including the conviction history from Germany, forms part of the PNC record. However, we would not share that information with an inquiry that may come from America about that German national. We have to be proportionate in the way in which we hold that data and we would direct the Americans back to Germany in order for them to disclose what information they wanted to with the American inquiry.

We also track offenders across Europe. This is another really important piece of work. A Polish national arrested in this country, who might be here legitimately with his wife and children, is arrested on a European arrest warrant and taken back to Poland. We now track that individual and we observe whether or not they are convicted, because, if they are convicted of a serious offence, we then notify the UK Border Agency because that has an impact on their ability to re-enter this country.

Through all of these processes, we work with our colleagues in both the Home Office and the Ministry of Justice and we try proactively to put in place schemes to try and monitor offending behaviour on a European level to protect local communities.

Q8 Mr Buckland: On that point, you raised some practical examples there. Another example would be the requirement of sex offenders to notify the authorities on their arrival or return to the UK. How is that system working in practice and would that be affected potentially by this proposal?

Ian Readhead: Yes. Again, we track sexual offenders across Europe. So, in regard to UK nationals who have gone to Spain potentially to gain access to young vulnerable females because the age of consent in Spain is lower than in this country, we would seek to obtain from Spanish colleagues details of that offence. We then impose all of the structures—the MAPPA processes—that are put in place when that sexual offender comes back and then tries to live in the community.

It is one of the things that concern us about the Directive. The Directive uses four principles in relation to how we can use data: it talks about the execution of criminal penalties, investigation, detection and the prosecution of criminal offenders. It doesn't talk about common law. If we had a paedophile offender released from prison who goes to live on a caravan park, we go to the caravan park; we talk to the local families who are in caravans; we tell them, "There is a paedophile here." We do that unashamedly because we have to protect communities and protect vulnerable persons and children. This Directive, written in the way it currently is, in our view would prevent us from doing that.

Q9 Chair: Can you explain how that would happen—why the Directive would prevent you from making that kind of disclosure for which we have statutory provision in this country?
Ian Readhead: Yes. It prevents us because of the prescriptive nature of the Directive. As we read this, those areas do not permit us to use our common law powers any more, because, effectively, the argument would be that we are no longer processing data in accordance with either this Directive or the Regulation. That is a real concern to us because there is huge value in exchanging information with other agencies. We do that in relation to problem families and courts exercising warrants; we do it across a whole range of areas.

Q10 Chair: Youth offender teams as well.
Ian Readhead: Absolutely. We have dedicated resources working with our partner agencies to create those safer communities on a local level, and this prescriptive Directive, in our view, goes backwards. It takes us away from being able to do all of those very useful activities that mean so much to our local communities.

Q11 Jeremy Corbyn: Thanks for your points, Mr Readhead. When you disclose information to other agencies or, indeed, in the case you mentioned, owners of caravan parks for example, do you only disclose information that is based on a court process—a judicial process—or do you disclose police suspicions and police reports?
Ian Readhead: A high degree of care has to be exercised in relation to the disclosing of intelligence. If we had very good intelligence about an individual that gave us suspicion that they were actively involved in, let's say, grooming children, we would, in certain circumstances, talk perhaps to the headmaster of a school or to partner agencies where we felt that local safety was being prejudiced. On the whole we try and use factual information. What is really critical in there is that, if we were tested in a court of law, we could produce sufficient evidence to warrant disclosure in that way. But we recognise that we have to be very careful in how such information is shared. Do you want to add anything to that?
Merilyne Knox: No; I absolutely agree with that. It has to go through a proportionality or pressing need test, which is based in case law anyway, on which we would make these disclosures. You would have to balance out what the impact would be in disclosure against the impact in not disclosing, and that is how we would make that decision.

Q12 Jeremy Corbyn: Is there not a danger that you would expose yourselves to a prosecution on the basis of defamation?
Merilyne Knox: Absolutely, very much so, but so far the disclosures we have made have been safe, and they have been upheld in court at JR level and above. Mr Readhead has made reference to that caravan example, which has been tested in court and was upheld.
Ian Readhead: So the whole essence of enhanced vetting, which is about employing persons who have unsupervised access to children and vulnerable persons, has at its heart disclosure of intelligence. It is not just about factual issues; it is about disclosing to employers in those circumstances intelligence which may shape the way in which they determine to let somebody have access.
If you go back to Ian Huntley, for example, remember Ian Huntley was never convicted of anything. What he had was a sequence of arrests where his modus operandi was to commit sexual offences against vulnerable young women whose evidence would never be trusted. That arrest history was critical to the way in which he was able to get access and employment. You know it is the failing of the police to make that available that enabled him then to commit the awful crimes that he did, so it is at the very heart of the way in which you protect local communities.
Chair: Thank you very much indeed. We are very grateful to you for the very frank and clear evidence that you have given. Does anyone have any more points anyone wanted to raise with these witnesses? If not, we can move on to our next group, but we very much appreciate your help this morning.

Examination of Witnesses

Witnesses: **Jean Gonié**, Director of Privacy EU Affairs, Microsoft, and **Sietske de Groot**, Senior EU and International Affairs Policy Adviser, Federation of Small Businesses, gave evidence.

Chair: Ms de Groot from the Federation of Small Businesses and Mr Gonié from Microsoft, both of you are looking after European issues for those respective organisations. We are grateful to you for assisting us today in our work on the proposed Directive and Regulation. I am going to ask Mr Buckland to start.

Q13 Mr Buckland: Thank you very much. We have been dealing with the Directive. We are now turning to the draft Regulation itself, and, in particular, the impact assessment made of that Regulation by the European Commission, which acknowledges that there are going to be some additional compliance costs. But it comes to the conclusion, in their view, that the reforms are expected to achieve benefits and savings of about €2.3 billion in administrative burden per annum. What assessments have you made of that predicted saving?
Sietske de Groot: We have no exact figures, but this €2.3 billion refers to the savings made mainly through harmonisation but also because the notification procedure has been abolished, so the last thing for our members is a true saving per year. However, up to one quarter of our members export in general and most of them within the European Economic Area. This is export in goods and services. Of that quarter, very few

will export data, so the savings from harmonisation are very small. Then the savings from notifications are considerable.

However, the rest of the Directive introduces provisions that are much more burdensome. I can go into detail on that if you wish. The net result is negative, in our view, even though we don't have exact figures, but if you look at the provisions they are very burdensome.

Jean Gonié: First, thank you very much, Mr Chairman, for inviting me. I am very pleased and honoured to speak on behalf of Microsoft. I totally concur with what you have said. With this figure of €2.3 billion we have difficulties, to be candid, because we have no real details regarding the impact assessment. We have just a few pages at the end of the text. We would like to have more information to understand better what these €2.3 billion savings really represent.

Q14 Mr Buckland: Are there any specific heads of information, do you think, that are absent at the moment that need to be looked at?

Jean Gonié: I think the economic impact and the business impact are not taken into account enough. We have some ideas, which are not difficult, about the appointment of a data protection officer and some savings that are linked to that. But, to be candid, the real impact for the industry, which is our impact, is difficult to represent maybe but doesn't exist today.

Q15 Mr Buckland: We have dealt with some of the negatives. Do you see any benefits to business of having a harmonised data protection regime?

Sietske de Groot: Yes, of course there are benefits because data is free flowing not only in the UK but in the rest of Europe and the rest of the world, so you need harmonised rules on that. We have a number of members who provide cloud computing services, and especially for them it is important that the rules are harmonised. I suspect that will be the case for more businesses in the future because more of our small businesses will export and more of our small businesses will use the European market to find new customers. So harmonisation is important.

Q16 Mr Buckland: But is it a question of striking the right balance? Harmonisation can mean different things to different people, can't it? Putting it bluntly, how prescriptive do you think moves to harmonisation should be? What do you think the balance should be between harmonisation and too much prescription when it comes to domestic arrangements?

Sietske de Groot: We think the rules are too prescriptive indeed. Of course we would like to have as much harmonisation as possible, but we think you can also make legislation on the basis of principles instead of prescription, because prescriptive rules also prevent innovation. If you prescribe in too much detail, you don't leave room for industry to develop their own standards or find their own solutions. In that sense, prescription goes against harmonisation because you stifle growth and trade in Europe.

Q17 Mr Buckland: There should be clear objectives.

Sietske de Groot: Yes.

Q18 Mr Buckland: First of all, presumably, the protection and integrity of data that is personal and private has to be at the top of the agenda, doesn't it? Sometimes people say, "Yes, that's a very good argument, but how do you achieve harmonisation without some prescription?" What do you say to that?

Sietske de Groot: That is a very good question. I can't answer on that because you need some form of prescription if you want to harmonise. We are very happy that it is a Regulation already that helps in harmonising things instead of being a Directive. At the same time, in this Regulation there is some room for manoeuvre for the Government to define rules on employee data, and we are very happy that that is left to the UK Government. But, yes, you have to strike the right balance, and, honestly, I couldn't say. That is also a philosophical discussion. Do we have prescription and harmonisation? How far do you go? It is very difficult. For us it is important that it is not stifling growth, innovation and burdening small businesses.

Jean Gonié: I completely agree with all that and I think I can speak on behalf of the US industry established in Europe, because, for your information, I am also Vice-Chair of AmCham EU, and I was a reporter for the data protection position from the American Chamber of Commerce in Europe, in Brussels.

Basically, we are very happy to have this reform of the 17-year-old data protection regime. What is very good with this reform is that it is supposed to bring the maximum of harmonisation, which is really key. But you are correct: the devil is in the detail and we really want to be sure that we achieve the goal that we want. Today I think we all agree that 27 different regimes is 27 risks, 27 good reasons not to make business. All of us agree, from SMEs to worldwide companies, that this is really key. That is the reason why we are very happy with this text. The problem here is that we would like to have real harmonisation. There are a lot of different subjects that, for example, are already "discutable", like the one-stop-shop approach. I am happy to talk about the main establishment notion later on if you want. We really have some concerns about that.

Another thing I think we all need to discuss is the notion of delegated Acts. A delegated Act is very good. We need to have delegated Acts if we want to have maximum harmonisation and reform of the Regulations, but we think that some of them are maybe not useful; some of them go against a very important principle, which is technology neutrality; and some of them also deal with essential elements of the law. We don't want a delegated Act that deals with essential elements of the law to be present in the text. I can develop that if you want, but it is really very important for us that the text shall not be too prescriptive.

If I may, I have one general comment on the text. We are all very happy to see a good reform that protects the data subject the maximum. I personally was a member of the French data protection authorities—

CNIL—10 years ago. This is very important for everybody; there is nothing to discuss.

On the other hand, as an industry, we are very surprised to see that we have a lot of new burdens but very new rights and very new incentives. We do not have a lot of incentives to develop all that we are supposed do. The data subject has a lot of new rights—the right to be forgotten, the right to data portability, the right to lodge a complaint, which is good. But we would like the industry also to have new rights to help us, for example, to develop data transfer and to have an appropriate mechanism to put in place. So we have a lot of new burdens because we are supposed to be happy with this harmonisation.

Q19 Mr Buckland: Specifically to you, Mr Gonié, in terms of the decision making and investment decisions made by companies, taking your company as an example, what sort of weight would you give to data protection legislation in a particular jurisdiction when making investment decisions? Is it of priority or is it some way down the list of priorities when it comes to making those sorts of judgments?

Jean Gonié: I would say that this is in between the top and bottom in the list because, as you can imagine, we also have other incentives like tax regimes, skills employability and so on to determine investment. But, definitely, if we have coherent clarity in a data protection regime, this will really help. Like we have the digital single market objective, if we can have the same like a data single market, it will be very helpful for all of us. It would be a very good signal from Europe to the rest of the world.

Q20 Seema Malhotra: I want to continue on the analysis of the proposed Regulation, looking at specific criticisms that have been made and, in particular, the discretion about the right of data subjects to be forgotten. Article 17 of the Regulation gives individuals the right to request that organisations delete their personal data in specific circumstances. How feasible is it to permanently delete data, particularly if published on the internet, in accordance with this right to be forgotten?

Sietske de Groot: We think that it is very difficult. You can notify the parties to whom you have given or sold the data, but how can you check that everything is deleted, especially at a time when everybody is on Facebook and posts messages on Facebook? We think that it is not feasible to do that. Also, I would like to take the opportunity to say that we have stricter rules for businesses to comply with data protection, and, as Jean Gonié was just saying, we don't have any rights that compensate that.

For example, you have to comply as a business with all these rules; it is very burdensome. But then one of your employees or one of your clients posts personal information on himself online. If that data gets compromised, who is responsible then? You can't point to the data subject in that case. We feel that the burden of compliance and the burden of proof is very heavy on business, and that is not right at a time when we have Facebook, LinkedIn and other social media, and where personal data is easily submitted to the internet.

Q21 Seema Malhotra: Just so that I understand, you think it is disproportionately heavy on business.

Sietske de Groot: Yes, especially if you see how easy it is to post your personal data online. If you put the same data online that you hold as a business and it then gets compromised, it is difficult to trace back when the source was. But as a business you are responsible by definition, so you have then to prove that you did comply with the rules. It is very difficult then to prove that the data was already there online and the source of it.

Q22 Seema Malhotra: I would be interested if you had any further comments on that and also what you might consider to be reasonable steps to inform third parties of a request that data is to be erased.

Jean Gonié: Yes. The phrase you used—"third parties"—is really key and essential in the text, but I would say more generally I think we all like this right to be forgotten. In Microsoft we have absolutely no concern in trying to do our best to comply with this right. Anyway, as you know, this right already exists. The right to erase data already exists in the 95/46 Directive.

It is good to have new rights, but the problem is that, if a new right is not workable, if as a company, as a data controller, you cannot test the feasibility of this right and you cannot erase the data, there is a huge problem. I think that this right to be forgotten idea is very good up to a certain limit. It is totally possible to retrieve any kind of data where, as a data controller, you have control of the data. This is totally possible. This is very important; it is key and essential. It is very important to do that. The problem is that it is not possible to retrieve all kinds of data because of the openness of the internet and the worldwide architecture of the web.

I suggest that perhaps you invite or discuss with a body called WCC, which is in charge of liberating the architecture of the internet, and you will certainly understand better, because this is a very tricky question and it is not easy to understand, that it is not possible to have access to data anywhere in the world for many reasons, such as sovereignty of state. So this is really the first problem; it is not possible to have access to data.

The second problem for us is as a data controller. When I say "for us", data controller is a large notion. It is not only us; it can be ISVs; it can be a lot of other actors. In fact, basically what is asked of them is to control or to monitor the internet. Once again, because of the freedom of the internet, because of the openness of the tool itself, it is not possible for them to do that, and it goes against an idea that is already established in the E-Commerce Directive, which is the idea that internet service providers shall not have the ability to monitor the internet.

We have a lot of different notions here, and once again I think everybody wants to comply with the text, but the problem is, first, the feasibility and, secondly, the theoretical debate that goes behind this very notion.

I would just finish on a very important point because the right to be forgotten, which is the same for other rights, is subject to a fine. If we don't comply with rights established in Article 17(1) and (2), we may be

subject to an administrative fine up to, I think, 1% or 2% of our worldwide turnover, which is of course a lot and which is a huge risk for all of us. If you want, I will maybe develop this administrative fine approach later on, but basically I think the problem is what we have already said about this harmonisation already.

The problem is that we don't want to be fined for something where we don't know the ins and outs; we don't have the rules and we don't know what is at stake and what is feasible. There is a huge risk because there is a kind of a third party role and other parties' role in Article 17(2), and, if we don't comply with the text that we don't understand or that we know it's not possible to comply with, we will be subject to a fine.

Once again, we are happy to be fined, but we need to know the rules. If you start a football match or any kind of game, you need to know the rules. Once you know the rules, you can start the game. The problem is that, with half of the text of the Regulation to date, we don't really know the rules. There is nothing to discuss. We are companies who just follow the law, nothing more, but we want the law to be clear for us to know what the future looks like. We just want and need predictability.

Q23 Elizabeth Truss: You mentioned earlier the whole issue about technology neutrality not being covered in the proposed Regulation. Could you just comment overall to what extent you think that existing technology is taken into account in the Regulation?

Sietske de Groot: I am not a technical expert in this, but what strikes me is that in the delegated Acts the Commission sometimes says that it will define the electronic format for the provision. It strikes me that, if you define that and the Regulation comes into effect later on, that electronic format is maybe not up to date any more. Maybe you want to say something, Jean.

Jean Gonié: This is totally correct. The problem with part of the text here is that a part of some Articles is a threat to what we call technology neutrality. It is very important to have text that is future-proof and goes with no specific standard or format.

I will just take three Articles as examples, if you want to have something concrete: Article 18 on data portability, Article 23 on privacy by design and by default, and Article 33 on privacy impact assessment. Those three Articles go with the possibility for the European Commission in the delegated Acts to specify a format.

For example, on data portability, the Articles go clearly with the fact that the Commission have the possibility to define electronic format. It is the same for privacy by design. The Commission nailed it down—technical standard. It is the same for privacy impact assessment. It may make sense; it is maybe a very good idea; it is maybe very important—but it is also a threat because we don't know what the technology will look like in two or three years. Remember, Facebook is a very new company—some years ago no one knew Facebook. It is the same for Google, for very large companies who are very new; it is the same for Twitter. We don't know what the technology will look like and this is something that is very important for us.

Q24 Elizabeth Truss: Can I ask how what the EU is doing compares with other regulatory regimes around the world? Do you think the EU approach is restricting growth in this market compared to other markets, and could you point to an authority that you think is getting the Regulations right?

Sietske de Groot: I have to say I know very little about this, but you are talking about the internet here and that is difficult to police. There is no authority that polices the internet.

Q25 Elizabeth Truss: My question was more towards Microsoft as a global company, because you must deal in all those markets.

Jean Gonié: Yes. That is a very good question. I gave one or two examples spontaneously, but, if you would like, I am happy to send you further explanation or details. As you know, in the US there is no one federal privacy law but some state laws, so some states in the US—for example, the State of California—advocate technology neutrality because they know that this is very important because we don't know what the future looks like.

I also think spontaneously that in Singapore, which has just adopted a privacy law, this is also the same idea. But, to be candid, I do not know for the rest of the world. As you know, it is only like 60 to 80 countries that have a privacy law in the world, so it is not that much. But it is an interesting question anyway because it is a very important point.

Q26 Elizabeth Truss: You have also commented on international data transfers in cloud computing. Can you elaborate a bit on that? Why do you think there need to be stronger safeguards there?

Jean Gonié: As a worldwide company, this is really the key question; this is the most important question. To be candid, we think that in the text today that stipulation is good but it needs to be improved. Today, when we speak about cloud, online, internet, social media and so on, all that is about data transfer. We think that today the text needs to be improved because the safeguards proposed are not robust enough. They are very good; they want to improve what we call the safe harbour, which is the agreement between—

Q27 Elizabeth Truss: Can you just clarify a bit more for us, because on the one hand you are saying it needs to be less specific so it needs to be technologically neutral, and on the other hand you are saying the safeguards aren't tight enough? Can you just outline how you would move that around to fulfil both of those?

Jean Gonié: Thank you for this question and it confirms what I have said. Let me use a word that is very important for a lot of US companies and it will be a connection to what I have just said on the incentives. Today we think that for international data transfer what is missing is, I would say, a recognised accountability approach. What is recognised accountability and accountability? This is really the link I wanted to make with the notion of incentive. We think that today a lot of companies develop certifications and codes of conduct. They try to do their best to do more than what is compulsory and

they have no incentives for that; they have no real recognition. Today Article 39 is not clear on that.
So we would like this to be developed for data transfer. It does not mean more prescriptive text. It means that the text takes into account what companies are doing for data transfer in the world.
Can I tell you precisely what the Article 29 Working Party, which is the 27 data protection authorities in Europe, have just proposed in their cloud computing opinion last July? They say that, in addition to any kind of data transfer that already exists, it is good if a company, based on its pragmatic experience, develops appropriate safeguards—of course with a lot of control. But this is something really very important and that will go with the fact that we think the text is prescriptive.

Q28 Elizabeth Truss: This is a slight diversion, but do you think part of the problem is the underlying market structure of the internet and the way that it was developed and so on means that consumers don't necessarily pay for data transfer in the way that they might do?
Jean Gonié: I do definitely. I definitely think that there is a gap between the text proposed today, which is a good text, and the reality of this online approach from the internet. If there is one word that is the key word for this Regulation for this text, it is trust or transparency—but really trust. The text needs to take into account this notion of trust. If we can reach this notion of trust, I think the data transfer issue, for example, will be achieved and will be solved. Typically, the reason why I use the certifications and the codes of conduct is because, thanks to them, you can introduce a certain level of trust in the data transfer fleet.

Q29 Seema Malhotra: This question is more about the impact on small businesses, so it is slightly more directed to you, Ms de Groot. The FSB have argued that the proposed Regulation will have a greater effect on small business that won't necessarily have the resources. I am quite interested to know how effective you think the proposed exemptions for small businesses might be in relieving them from burdens and also your view about subject access requests and fees and the potential for perhaps an increase in volume should fees be abolished.
Sietske de Groot: First, on the exemptions, there are three notable exemptions in the Regulation. One is the exemption for the data protection officer, which of course we welcome very much. Then you have Article 28 on documentation. This is a big thing. Yes, we are very happy that that happened because that would mean an enormous burden otherwise.
Then you have the exemption that is in the delegated Acts on the data impact assessment (article 33). On the last one, of course, it is not sure whether that is going to happen because it is in a delegated Act. That might happen later; it might not even happen. Again, I can come back on delegated Acts later. So we are very happy with the exemptions.
There are also other smaller exemptions announced in delegated Acts. Jean Gonié, you calculated how many delegated Acts there were, but approximately half of them announced that they would take into account micro, small and medium-sized businesses. Of course we welcome that; it is very good. But we would like to see those exemptions addressed in the Regulation itself because delegated Acts cause a lot of legal uncertainty. We don't know what is going to happen, when and what, if and how. If the Commissioner is now saying there are exemptions in those delegated Acts, we are happy with that but we don't know how happy we can be with that because we don't know if they are going to happen or not. The intention is good, of course, and we welcome that.
On subject access requests, we really are not happy with the fact that you can't charge a fee any longer, because the burdens of subject access requests have increased because the rights of the data subject have increased.

Q30 Seema Malhotra: What kind of proportion have they increased by?
Sietske de Groot: What proportion? I can go through a list of new things that small businesses have to do and it is all to do with the new rights of the data subjects. I can't give a proportion, but I can go through a list later on. The loss of the fee means a net burden increase because there is more obligation you have to comply with and you can't charge a fee.
Especially, this fee acts as a barrier—that is what our small businesses say—to people asking for their data, people who are not serious or who want to make frivolous or vexatious requests. That is a real clear barrier to those people and that protects our businesses. If you leave that open, you can even think of people who are disgruntled with their employer or with a business just doing that on purpose, making data access requests on purpose and bombarding them with that, like you have a cyber attack.

Q31 Seema Malhotra: I have a slightly wider question, which is the requirement to appoint a data protection officer. Should this be based on the number of staff or also, perhaps, on how much data a firm might process? That could be to either of you.
Sietske de Groot: We think that a data protection officer should not be mandatory at all for SMEs. Of course we are happy with the exemptions. It should be assessed by the business itself if you need a data protection officer because it is very expensive to have one. We would advocate it for businesses that are data-centric and monitor data on a daily basis. We think it is a matter of assessing yourself, based on the risk you run.
Chair: Thank you very much. We are grateful to both of you for your evidence this morning. It is clear that this has a lot of very serious implications for business both on a large scale and a smaller scale, which we will take into account in what we have to say. Thank you.

Examination of Witnesses

Witnesses: **Christopher Graham**, Information Commissioner, and **David Smith**, Deputy Commissioner and Director of Data Protection, Information Commissioner's Office, gave evidence.

Q32 Chair: Mr Graham, Mr Smith, welcome back to the Committee. You are regular visitors to us and we are glad to have you with us on this issue, which, as is apparent from the evidence we have been receiving this morning, very important in the areas which it will particularly affect. I will start, if I may, with the Directive.

The first evidence session we had this morning was about its impact on the police. The Government's view, as we understand it, is that domestic processing should not be included at all but would not apply anyway. In the UK, the domestic processing of the kind of data that the police hold would remain governed by our provisions and is not affected, but the Government are still, I think, nervous about all these provisions being in the Directive. Is that how you see it?

Christopher Graham: Mr Chairman, perhaps I could begin by saying that the Information Commissioner's Office is deeply sceptical of this proposal to split the current Directive between a Regulation and a Directive. All sorts of mischief follows from that decision. Unfortunately, I was let down by Virgin Trains so I did not hear Mr Readhead's evidence, but my colleague David Smith, who was listening intently, will be able to answer that question with more precision than I can.

David Smith: I think it is a difficult area because there is clearly an element of politics about the UK's position in relation to the European Union and, particularly, measures in the police and justice areas—the third pillar here. From our point of view, we are proponents of good regulation. Good regulation means consistent law that is clear and easy to understand and easy to apply. Once we start to diverge and we have a Regulation for the commercial sector and a different legal instrument for police and justice, you start to move away from that and you cause particular problems in areas like local authorities, perhaps, which have functions that will come under the Regulation and others that will come under the Directive.

In many ways, we want consistency. I suppose, at the end of the day, that consistency could be delivered by one instrument from Brussels, but I think, in reality, we are not going to get that. We are going to get at the very least these two instruments and these questions about whether the Directive applies to domestic processing. But, when whatever comes from Brussels is applied in the UK, the Government do have a choice as to what rules they apply to policing domestically. Even if we are not part of the Directive for policing domestically, we will still have data protection law in the UK for domestic policing, just as we do at the moment. Our position will be that that should be closely aligned to the Brussels regime, even if it is not mandatory on the UK to follow that approach, because that makes it easier for individuals and for us as the regulator.

Q33 Chair: Are you saying that it should be closely aligned to the Brussels regime even in those areas where our witnesses have told us that the proposal is potentially very unsatisfactory and would not allow or might not allow the police to use intelligence, for example, in the way that they currently do?

David Smith: I think you can align the principles and the basic operation. I do not think any of the witnesses so far have really questioned any of the basics. It is the administrative burdens that go with it that are the problems. I do think we could, yes, take a proportionate approach to how that is applied in the UK so that the principles are there. It doesn't stop the exchange of data with Europe because we have different rules, but we don't necessarily apply all the detailed prescription that has caused so much concern.

Christopher Graham: It is worth adding that we see it as a prime aim of modernisation of the data protection regime to achieve clarity. This is going in exactly the opposite direction. Of course the police have concerns about whether they are going to be able to do their job across borders, capturing criminals and so on. There are also very basic questions about protection for the citizen in their dealings with the police that arise from data protection law. One of our early civil monetary penalties, I am afraid, had to be visited on the Lancashire constabulary because of lax handling of very sensitive personal data, with something as simple as leaving a missing person trace record in a squad car that was passed on to another team and was found blowing down the street, and was handed in to the local newspaper by a man walking his dog.

Let's not forget the very basic disciplines of data protection, which are what this reform should be about. One of our concerns is that it is going to become so complicated that we won't see the wood for the trees. There are real concerns and citizens' rights that need to be protected and they are not necessarily going to be better protected by these two measures.

Q34 Chair: Is there an issue, as the Government have indicated, around having to renegotiate a lot of bilateral treaties and agreements in this area?

David Smith: There is certainly a question. I do not think it is one that is very easy for us to comment on because we are not involved in the negotiation of those bilateral treaties. So we can't really comment on how difficult that is or on how far it will be necessary. Those bilateral treaties have, presumably for the most part, been entered into under our current data protection regime and should respect the requirements under that regime. As we said, the principles under the new regime are very similar so, if those bilateral agreements meet the current requirements, they won't necessarily fail to meet the new requirements. A process of review is required, but our understanding is that there are very many of these bilateral agreements. We believe that the Ministry of Justice have developed a catalogue of these; so they may be able to advise in more detail. But, clearly, those sorts of agreements should be consistent with whatever the new legal regime is and so a review at the very least would be needed.

Q35 Jeremy Corbyn: Do you think that the proposed Regulations are over-prescriptive across Europe for what they are intended to achieve?

Christopher Graham: Yes, we do think that. I think our position is very clear. We want a modernised data protection regime. It is an analogue regime for a digital world. That is a cliché, I know, but in this case we have been calling at ICO for many years for updating of data protection legislation. It is a case of "Be careful what you wish for", because we now have a proposal that is welcome in many respects, but we need a package which is clear and effective, and which delivers real rights for citizens and consumers. You will find that the evidence you are getting from the various witnesses shows a very wide consensus in the UK about where the current proposals don't fit that bill.

You ask about it being overly-prescriptive. It is very largely about the proposed legislation, in the name of consistency across the European Union, being very specific about processes, whereas our approach has been much more to focus on outcomes and to go for the better regulatory approach of risk-based proportionate intervention. We are really quite worried that it will be very difficult to operate this regime. It will turn the ICO from, on a good day, a Better Regulation regulator into a vast administrative machine processing a lot of forms, permissions and ticking boxes.

We don't see where the resources are going to come from to do that, but that is for another day. But this approach rather misses the point. You need to place clear obligations on data controllers in terms of their overall responsibility and let them work out how they are going to comply, rather than saying, "You do this; you do this; you do this; you do this", which is almost a painting-by-numbers approach to data protection.

Q36 Jeremy Corbyn: Do you think there is a cultural heritage here in that Europe is made up of a whole load of different nations with very different histories? In Eastern Europe you have former highly centralised states until 1990. In Spain, Portugal and Greece in recent memory you had fascist regimes that centralised all information. Do you feel there is an issue in Europe that some people just feel obsessed with collecting information for the sake of it rather than the outcome-based approach that you advocate?

Christopher Graham: No. We have to recognise the different histories and cultural traditions of our partners in the European Union. If we are going to be able to negotiate a better outcome, we need to treat our partners with respect and understand why they feel the way they feel. But we would be kidding ourselves if we caricatured a situation of this happy breed this side of the channel and a lot of Euro colleagues who have suffered under the fascist boot and so on, because the challenges of data protection for citizens and consumers, not just in Europe but across the world, are really significant challenges of the 21st century.

Concerns about the surveillance society, never mind the surveillance state, are very widely held. You don't have to be a German, either an East German who has gone through the whole experience portrayed in "The Lives of Others" or a German either side of the former divide who has lived through the Third Reich, to be concerned about this sort of stuff, because, unless we get data protection right—and it is a fundamental right under the Charter of Fundamental Rights of the European Union—we are all in trouble.

Q37 Jeremy Corbyn: Do you feel these Regulations then are going too far in the sense that there is a lot of unnecessary information being collected and therefore the surveillance society, as you mentioned it, becomes stronger because there are many people who are very concerned about what they see as unnecessary surveillance and unnecessary keeping of information on themselves? This country tried to introduce identity cards, and that was defeated because basically there was opposition to it.

Christopher Graham: Yes. There is that sort of chicken and egg argument. Do we have the Regulation and Directive that is proposed because—

Q38 Jeremy Corbyn: No. The right to challenge information and the right to know what is kept on you surely is the key.

Christopher Graham: Yes, and I support those rights. Our objection is simply to the means that are proposed by Brussels for delivering that fundamental right, which we don't think will be effective because you are going to tie the various data protection authorities—many of whom are much less well resourced than we are in the UK—in knots doing the process, instead of keeping an eagle eye on what is going on and intervening where there appears to be a problem, and concentrating our resources where clearly the regulator ought to be intervening.

If we really have to give prior approval for risky processing on international transfers and if we really have to go around checking whether everyone of a particular size has a data protection officer or whether they have conducted a mandatory data protection privacy impact assessment, that is all we will do. It will be phenomenally expensive and rather less effective than the system we have at the moment.

David Smith: There are some differences in approaches to data protection Regulation. We have traditionally taken what we would see as a good UK regulatory approach. The market continues. People don't come to us as an authority to get approval for what they do in advance; they take their business decisions and we step in if things go wrong. We have some strong powers now in terms of penalties, to impose penalties if businesses do get things wrong. But, if you like, you trust them to get it right and you step in if they abuse that trust, and trust was referred to previously, whereas some other data protection authorities have to check things in advance and prior approve things. This is particularly true in international transfers.

Many of our colleague data protection authorities have a system where they routinely sign off international transfers before they are allowed to take place. That is not the approach in the UK. As we try and come together to one harmonised instrument, you see those sorts of tensions emerging. We are critical of this instrument because it will require us to prior approve

international transfers, but I have to say that some of our colleague authorities are equally critical of it from the opposite direction because it will allow international transfers through, in some cases without their approval, where they have to give their approval under the current regime.

Q39 Jeremy Corbyn: Lastly, doesn't the British approach, characterised by yourselves, have with it the necessity of having a well-resourced Information Commissioner, who can retrospectively check on transfers and things like that, whereas, if you don't have those resources, quite clearly a whole lot of data collection—data abuse quite possibly—can go ahead and you wouldn't have the resources to do anything about it?

Christopher Graham: It is not just resources. We are in the fortunate position of having a notification fee system at the moment, which raises £15 million a year for the Information Commissioner to do the data protection job. Unfortunately, the Regulation proposes to abolish notification, which raises a bit of a problem for us.

But it is not just resources and I am sure you are bored with hearing the Information Commissioner turning up and rattling the tin. It is also about powers. In many areas, one is stymied from doing the work that clearly needs to be done because one simply doesn't have the power to audit, for example, without consent or to intervene without a court order based on a reasonable belief. You can't do the sort of sample checking of, for example, international transfers under current powers. We would say we would certainly need greater powers. The resources question is something that I would certainly also like to address.

Q40 Chair: Wouldn't the approach that you favour—the traditional British approach—be easier to achieve if the whole thing was done by a Directive and not by a Regulation?

David Smith: That must be true. It would be easier to do it, if you like, in the British way, with the freedom that a Directive would give, but that wouldn't meet the Commission's desire for harmonisation or would put that at risk. The Commission are very much, we think, driven—I think Microsoft's evidence was very helpful—by the likes of Microsoft, the big multinational internet businesses, who say, "Above all else, we want the same rules throughout Europe so that we know what the rules are for Europe."

There is an element that the Commission see that as necessary for economic progress and making Europe a good place to do business, and clearly there is some merit in that. But driving this harmonisation does lead to these detailed prescriptive rules that everybody has to follow, which are not necessarily good for, say, the people that the Federation of Small Businesses represent, who don't necessarily need the same regime in every country in Europe. What they just need is a sensible regime, from their point of view, in the UK. If the price of that is extra detail and extra prescription, because that is what you have to have to reach agreement among all 27 member states, maybe that is too high a price to pay.

It does not matter too much whether it is a Regulation or a Directive, but we would favour lightening up on the detail. Rather than saying that you must appoint a data protection officer who must be independent with two years' qualifications and spelling out that you must keep these forms and this documentation, it should just say that every business—it does not matter on the size—must have appropriate documentation relevant to the size of the business, the nature of the data it processes, to ensure it is able to meet the requirements imposed by the Regulation, and it must have appropriate staff in place with the necessary qualifications and experience and authority again to ensure it meets the obligations.

That sort of lightening up—prescribing the results rather than the forms to fill in—would be a much more effective regime. I do think that we will move some way towards that because we are not the only voice who is saying that, but we are pushing in that direction very much.

Christopher Graham: It is also worth saying that, increasingly, the data protection authorities within the European Union are co-operating very effectively because we feel this pressure from the big international companies saying, "Come on, you said we could do it here but we can't do it there. What is going on?" Working in the Article 29 Working Party in Brussels, my colleague David Smith is very active in that. I more recently selected the Vice Chairman of the Article 29 Working Party. That is clearly where an awful lot of the work has to be done.

Under the new proposals with the European Data Protection Board, that would be formalised, but it is formalising something that is already happening. We are dividing up the big questions between the different data protection authorities. The Irish will take one, the Brits will take another and the French will take another, usually based on country of main establishment. But that is a trend that is bound to continue, and you will see greater consistency because greater consistency is clearly demanded. That makes me wonder whether we need to impose all these restrictions, particularly on the smaller players, in the name of achieving something that the dynamic of the marketplace and good sense is achieving anyway.

Q41 Mr Llwyd: We did question other witnesses about the right to be forgotten, as it is known. In your evidence to us you say that this is one of the more interesting parts of the Regulation, but you go on to say, "given [the] derogations, the various qualifications to the right and the technical difficulties surrounding the online deletion, we are unclear how the right to be forgotten will actually be delivered in practice". How feasible, in your view, is it to permanently delete data published on the internet in accordance with the so-called right to be forgotten?

David Smith: A lot of attention has been focused on this supposed right to be forgotten. It was the Justice Commissioner Viviane Reding who said to Christopher Graham that this is actually more of a political slogan.

Christopher Graham: She wasn't just saying it to me; I was sitting next to her when she said it. This was at a European Parliament briefing attended by many

witnesses. Rather to my surprise, about six months after she had said this was the big idea, she said she couldn't understand why everyone was getting so excited about the right to be forgotten because it wasn't anything we didn't have already, and so everybody should relax.

Because there are so many exclusions and derogations, we don't see it as very much of a threat because we don't see it as very much of a right either. You can't put the genie back in the bottle. A lot of the problem arises from information which people have posted anyway publicly and which then gets, as it were, re-tweeted. You can't recall that. Where you are dealing with information held on databases between different authorities, it is good data protection practice anyway for that to be tracked. You have rights at the moment to ask for that to be deleted.

David Smith: There was always going to be something in here that was called the right to be forgotten because of political statements that have been made and pressure, particularly from the French, to introduce this sort of approach. When you unpick it, much of what is there of the right to be forgotten is just a restatement of existing provisions—data shan't be kept for longer than is necessary; if it has been processed in breach of the legal requirements it should be deleted, which goes without saying.

What is, in our view, important is the new Article 19, and it is the right to object. It is part of the right to be forgotten. At the moment, under the current law, people have a right to object. I can approach any data controller and say, "I object to you processing my data. Please delete it." But the onus is on me to provide the compelling legitimate grounds as to why it should be deleted. I have to make the case and that right is quite limited. That sort of balance of proof has changed in these new proposals. I can go along to any data controller and say, "I want you to delete my data", and they have to come up with the compelling legitimate grounds for keeping that data. Of course in many cases they are able to do that, but shifting the balance of power in the relationship a bit towards the individual seems to us to be important.

The point has been made about whether this is directed to social networking. Yes, there is no doubt it is. How you take reasonable steps to track information on the internet is extremely difficult and I don't think we can answer that. If you have information on your site and someone has put a link to it, you can trace that link and so on. But, clearly, as Christopher said, you can't put the genie back in the bottle.

The big risk here that we see is that you say to the public, "You have a right to be forgotten", and when they try and exercise that right it is quite limited. So you have a lot of disappointed individuals who don't have the rights they think they have, who then complain to the regulator that they are not getting what they expect. It is not what the law says, so we disappoint them as well and we become the problem. Again, we would like this to be not strengthened but just made more specific and more realistic.

If I may, there is just one other point about it. One of the other things it has been directed at, which is not all that clear, is the responsibility of search engines in the right to be forgotten. To put it simply, if there is information about me on a website that has been published that I do not like, and maybe I have even obtained an injunction to stop that information being published but it is in a foreign country and I can't do that, can I go to Google—as an example of search engines people usually use—and say, "Google, stop returning that information in a search"?

It is unclear how or if this Article would apply to that, and clarification on that would be welcome. It is also the subject of some cases before the European Court of Justice at the moment, particularly from Spain. How those come out and the implications that they have on how this Article is interpreted is very important, because search engines are absolutely crucial here, but it is arguable whether they are a data controller or a processer or caught by the legal regime.

Q42 Mr Llwyd: Do you consider the current draft Regulation, in respect of steps to inform third parties of a proposed deletion, to be adequate?

David Smith: It is very unclear, as other witnesses have said, how that will work in practice. Where information has been passed on directly to a third party, then we would expect a business to have a record of that and be able to inform them that that information should be deleted. If they have allowed or can find links into their sites, they should be able to trace that. But, if information has gone out on the internet, it has been accessed from their site, taken and posted elsewhere, it is very hard to see what can be done.

That does take you then into this question of what the responsibilities are of search engines and so on in returning this information. Is that where you can be effective? You can stop search engines returning it more easily than you can wiping it from the record, which may have implications as well for the historical record, freedom of expression and so forth.

Q43 Mr Llwyd: It is clear that the proposed Regulation will impose a number of new obligations on data controllers. Why is it your belief that a focus on outcomes would be beneficial?

Christopher Graham: Why do I believe that a focus on outcomes will be beneficial?

Mr Llwyd: Yes.

Christopher Graham: I think that the Better Regulation approach has been tried and tested. It is a bit retro for Brussels to be quite so specific about all the detail that 'shall' happen, when it is more sensible to intervene either to deal with problems as they arise or to audit compliance with good practice, rather than to have a whole series of very costly obligations imposed on individual data controllers regardless of their circumstances.

You might have a very large enterprise that is doing almost no processing and a very small enterprise whose sole existence was rather buccaneering data processing. We think it is better to put the obligation and the responsibility clearly on the data controller. You are almost subcontracting the responsibility to a particular official. I can imagine that the data protection officer is not going to be part of the club and it will be like referring to the IT guy, "These are

issues that we leave for the data protection officer", when these ought to be a main board responsibility. This is what ought to be keeping the chief executive awake at night. Instead what is going to be keeping the chief executive awake at night is whether the data protection authority will decide to—sorry, there is no discretion about this—when the data protection authority will impose a fine of up to €1 million or 2% of global turnover because the company failed to carry out a privacy impact assessment in appropriate circumstances.

Those are pretty scary obligations, and we believe that the overall obligation to comply, in general, doesn't then need to be broken down by, "This happens to you if you do this; this happens to you if you don't do that; and that happens if you don't do the other." Quite apart from the fact that it is going to tie the data protection authority up in knots, it would be much better to have a general obligation to comply rather than specific steps which have been derived from what has been developed as good practice. It is almost as if the Commission has said, "That's a good idea; we'll have that. There's another one; we'll have that, and we will fine you"—what was it?—"up to €1 million if you don't do it."

Q44 Mr Llwyd: Microsoft told us, and I think quite reasonably, that in their view the one-size-fits-all approach to compliance is inappropriate. They do in fact say, for example: "To be balanced, the Regulation should ensure the most punitive sanctions are reserved for truly bad actors." What would you say about that?

Christopher Graham: I absolutely want the discretion, as Information Commissioner, to use the experience and judgment of my team to judge behaviour, judge the circumstances and consider mitigating actions, which is exactly what we do with civil monetary penalties now. If we were obliged to go blasting in on every occasion and fine a particular sum of money, we would be in no better place in terms of compliance, and probably a rather worse place, so I don't favour that one-size-fits-all approach at all.

I want discretion, and in the negotiations—and there do need to be real, hard negotiations within the European Union to improve this draft—a very important victory would be to change that bit that has all the lists of what the data protection authority "shall" do and amend that to "shall be empowered to" or "may do" so that we have the discretion to go after the bad guys, understand where things may have gone wrong and where there are mitigating circumstances, and not—

Q45 Mr Llwyd: "May" could be the right word, couldn't it?

Christopher Graham: When I raised this point with a very senior figure within the European Commission and I said, "'Shall' is a real problem", he said, "'Shall'—you can easily change that to 'shall be empowered to'". I suspect there is a lot about this draft Regulation and Directive which can be easily changed with an appropriate negotiating stance from the UK and others. The big mistake we make is to say, "We hate this; we hate this; we hate this—we're not going to play", whereas, with a little bit of diplomacy, we could achieve a much better result.

David Smith: That is entirely right. What it does do is to illustrate some of these problems of harmonisation. You really want harmonisation. If you have a data protection officer without the right qualifications, you should face exactly the same fine whether you are in the UK, Poland, France or wherever, which gets you to, "There must be a fine and it must be a certain amount." But that just gets you to undesirable, unintended consequences and unmanageable regulation.

In our view, you have to lighten up. You have to take the risk that there won't be complete harmonisation. It doesn't actually matter whether the fine is exactly the same or not, and we do have the European Data Protection Board, which is there to try and ensure consistency. Equivalence as an approach is much better than harmonisation, in our view.

Q46 Chair: Your belief that diplomacy can sort a lot of these things out might be particularly welcome to the many industries and organisations who have given written evidence to us about particular difficulties they think that the Regulation presents, whether it is credit reference agencies, newspapers, the BMA in respect of health data from research, or the insurance industry. A whole series of industries and activities have got quite worried about their returns.

Christopher Graham: We are worried too, but we are trying to do what we can, within the Article 29 Working Party, to influence discussion in a more pragmatic direction. We are very active on this issue. We did a briefing for members of the European Parliament very early on. We are doing another one in two weeks' time. As I said, we are very active within the Article 29 Working Party, and the Article 29 Working Party has considerable influence because of the expertise that exists there. I hope the Committee will not feel that the UK position is going unheard. But I would say that we are not going to get anywhere just by saying how awful everything is. We have to come up with ideas for making it better and we have to behave in a co-operative way that actually achieves results rather than just grandstanding.

Q47 Chair: Sometimes I get the rather odd feeling that there are people like us who worry a great deal about the protection of data and individual rights, and then there are a whole lot of other people who spend much of their time loading vast amounts of information about themselves on to the internet by means of social media and also by means of shop loyalty cards and other things, which they cheerfully use.

Some of the evidence to us has suggested that there is some sort of distinction that could be drawn between citizen data and consumer data, on the basis that there are things which are relevant to Government and there are other things which citizens generally don't have the same protective concerns about. Is there any basis for that kind of distinction?

Christopher Graham: When things go wrong you are concerned about it, whether it was the state that did it to you or, say, Sainsbury's. If the concern is that

people are putting lots of very personal information, in particular photographs taken late on a Saturday night in a bar, on Facebook, I am not terribly sympathetic when they ask for the record to be wiped clean, and I am not terribly sympathetic when people express surprise that employers might be quite interested in knowing a little bit more about their employees by accessing information that is publicly available.

But I also think that all the benefits that come from the online world are benefits for consumers as consumers but also consumers as citizens. There is easier access to services and, frankly, when we get this right, better service from public authorities and better service from companies able to deliver services with the efficiencies that online deliver and so on. But we do need a very strong data protection framework for us to be able to get all the benefits of online without the risks. I don't see any merit in splitting one's persona between, "I am a citizen at the moment, but at the next minute I am a consumer and I therefore deserve less protection." I don't know whether, David, you have any thoughts about that.

David Smith: Only that a lot of it does come down to this flexibility of application. The same arguments are being made about the definition of personal data—that this is cast too wide and it captures things like IP addresses on the internet. But having a rigid definition which captures the right things and doesn't catch the wrong things in a changing technological age—we wouldn't have been talking about IP addresses five or 10 years ago—is very difficult. It is right that a wide range of information—anything that can be potentially used to affect you in any way—is caught by the legislation. What we then need to do, whether it is consumer data or citizen data, is to ensure that the provisions apply in a sensible proportionate way, given how that data is being used.

It is quite different if, say, the police are using that data or if you are on Facebook using that data or it is on a credit reference file. It comes down to not trying to categorise data differently but giving more flexibility in what you mean by "accurate", "up to date", "not kept for longer than is necessary", depending on the nature of the data and the way in which it is being used.

Q48 Chair: Mr Smith and Mr Graham, thank you very much indeed. We are very grateful for your evidence today.

Christopher Graham: Would I be allowed to amplify one point or are you really up against the clock?

Chair: By all means.

Christopher Graham: A real concern for us, with the proposals, is the impact that it will have on data protection authorities having the resources to do the job necessary. I thought the Committee might be interested that we have run some sums to find out the impact on the ICO of implementing what is currently in the proposed legislation. I accept that may change, but it raises the question of whether any of this is actually doable, because, if we were to do the least that we can identify as being down to the ICO under these proposals, our funding would have to increase from the current £15 million for data protection—from the notification fee, which itself is under a question mark—by a further £8.4 million: that is a 56% increase.

It isn't going to happen, Chairman. But if we were to do what is frankly the more realistic role of what we think we ought to be doing, given the legislation that is set out, the figure is even more scary and, frankly, unbelievable. It is £15 million at the moment; we would need a further £28 million. Is anyone going to vote an additional 187% to the ICO, excellent though it is? No, they are not.

So you then have to say, "This system cannot work." They are certainly not going to vote 56% either. This system cannot work because you are describing a regime that nobody will pay for. We are about the best funded of the data protection authorities within the European Union. If we can't do it, and we particularly can't do it when the notification fee on which our funding is based is abolished, how is anyone going to be able to do it?

David Smith: If we lose discretion, all we will be able to do is punish and not advise and assist. We believe very strongly that advising and assisting people to get it right, as well as punishing those who fail in their responsibilities, is the duty of a rounded, proper, effective regulator.

Chair: You could not have been clearer. Thank you very much.

Tuesday 11 September 2012

Members present:

Sir Alan Beith (Chair)

Mr Robert Buckland	Christopher Evans
Jeremy Corbyn	Mr Elfyn Llwyd
Nick be Bois	Seema Malhotra

Examination of Witnesses

Witnesses: **Anna Fielder**, Trustee and Company Secretary, Privacy International, and **Georgina Nelson**, Lawyer, Information Policy, *Which?*, gave evidence.

Q49 Chair: Ms Nelson, Ms Fielder, welcome. We are very grateful to you for coming to help us with the work we are doing on the European Regulation and Directive. Ms Nelson, you are from *Which?*, and, Ms Fielder, you are from Privacy International.

We are confronted with both a proposed Directive and a proposed Regulation covering different fields, one covering police and law enforcement and the other is what one might call loosely the private sector. Is this structure appropriate and are changes of this scale necessary?

Anna Fielder: I will answer this, if I may. First of all, thank you very much for having me to give evidence. I am very honoured and proud to do so.

As we said in our submission, we do not think that this structure is necessary. It creates a two-speed protection for citizens and consumers and, in particular, we are concerned by the fact that the Directive is far, far weaker than the proposed Regulation.

From the point of view of legislation, the Lisbon Treaty mandates the EU and Member States to have Regulation on data protection in the domestic law enforcement sector. So, from that perspective, yes, we need to have Regulation, but at the moment our Data Protection Act covers all sectors. We don't see why this should not be the case also in regard to the Regulation covering all sectors, but having specific exemptions and provisions for the law enforcement sector, which obviously deals with some more delicate and important provisions.

Q50 Chair: Isn't the law enforcement agencies' case not just that there might be a need for specific exemptions but that the whole process should be one that allows us to operate in the ways we have traditionally done in this country, by domestic legislation, because, as you say, our existing domestic legislation covers both sectors? There is a difference between that and having both sectors dealt with at European level.

Anna Fielder: The domestic legislation at the moment is an adaptation of the EU Directive dating from 1995 and it applies to all the sectors. The UK signed the Lisbon Treaty, so it is obliged to apply EU-wide legislation, and also there are provisions in the treaties of fundamental rights and so on. We have an obligation to implement those provisions. The crucial question to consider is how we implement them. Do we create two-speed rights regimes?

We need to remember that the law enforcement agencies hold records about millions of citizens and consumers, and a lot of them are perfectly innocent people and victims. It is estimated that the Police National Database holds records of about 15 million people, and I have seen estimates that about six million of those are perfectly innocent citizens. Therefore, there needs to be some kind of consistency, like we have now in the UK, in the Regulations. What has happened is that the Regulation has been ratcheted up; it has more rights for the data subject. The Directive that has been introduced is very much like the old Directive, with a few extra bells and whistles—for example, separating victims from offenders on the Police National Computer. But, essentially, it is very similar to the old Directive provisions. The result is that you have two totally different pieces of legislation.

That has also impacted on the Regulation because a lot of the data collected for commercial purposes passes on to law enforcement agencies. One classic example is passenger name records that are collected by all the airlines. At the moment different countries have different rules about those and what needs to be collected and why. I have seen records from one airline saying almost for each European country that you need different records. Of course those pass on lock, stock and barrel to the enforcement agencies, and suddenly the provisions for data subjects become much weaker and it doesn't make any sense.

It is the same with financial records; a lot of financial records would be accessed for law enforcement reasons such as money laundering. You are left with a lot of grey areas and we are very concerned about this.

Q51 Chair: You talk about two-speed rights, but couldn't that objective be achieved if there was a greater reconciliation between the Directive and the Regulation?

Anna Fielder: Absolutely, yes.

Q52 Chair: Rather than it all being the Regulation—the outcomes specified could be reconciled more closely.

Anna Fielder: You could align the provisions in the Directive much more with the provisions in the Regulations. Indeed, in our analysis of the Directive, we have proposed concrete amendments for this to happen, and we would very much urge the UK, in the Council of Europe, to lobby and ensure that that happens. We know also that quite a lot of other

Member States are not happy about the situation because it weakens their domestic Regulations as well, so I think it is still not too late to achieve some consistency.

Q53 Chair: I think when you said "Council of Europe" you meant the European Council, didn't you—the Council of Ministers?
Anna Fielder: Yes, correct.
Chair: I just wanted to clarify that.

Q54 Mr Llwyd: May I ask you about the perceived benefits of the proposed Regulation? Do you believe that securing the fundamental rights and protection of personal data and privacy in fact requires the level of prescription in the current Regulation as drafted?
Georgina Nelson: Shall I take that one? We understand the benefits of principled Regulations: principle allows flexibility, future-proofing and can be technology-neutral. But, in our experience and especially in regard to the Regulation, we believe a certain level of prescription is required.
You can look at examples that we have in the Air Passenger Rights Directive and the Treating Customers Fairly initiative by the FSA, which were both outcomes-driven, principle- based pieces of legislation, which basically fell flat because the regulators did not know how to enforce them, companies did not know where the guidelines were, what was in and out of scope, and the consumers did not know what their rights were. In each case it ended up in the courts because interpretation fluctuated so widely that it was only left to a judge to decide. That is not the way we want to go down the path with the current Regulation.
If we look back on Microsoft's evidence of last week, it was clear that, while they were saying they wanted harmonisation, they also wanted clear rules, because when it comes to the heavy levy fines that are proposed they need to have assurance that what they are doing is within or out of scope and whether they are going to be fined or not. We do believe that a level of prescription will be required.
You can look at our current Data Protection Act as an example of where the lack of prescription has caused problems in interpretation. You have the interpretation of personal data when, internally, we have conflicts between what the ad agencies and networks believe, whereas IP addresses are not considered within the remit of personal data. Then you have the ICO's guidance, which is saying that maybe it should take a broad-brush approach, but there are clearly conflicts there and there is no harmonisation.
Then you can take a wider look at the whole of Europe and think about how different Member States deviate between enforcement of data protection authorities. It is huge when you look at the different fines between what our own ICO does and what Spain does, and that in turn breeds forum shopping and uncertainty and that doesn't breed consumer trust, which we want to see.
Anna Fielder: The point I would like to add, which is very vital, is that data nowadays doesn't stay within national borders. It is not just European; it is global. So you can't have consistency without some degree of prescription. I would fully support what Georgina said.

Q55 Mr Llwyd: By reference to the air passenger details, you may both answer but I think specifically this relates to what Ms Nelson was saying. Do I take it you believe that a focus on outcomes would not achieve the same result?
Georgina Nelson: There need to be clear steps about how those outcomes would be achieved. Just to focus purely on outcomes without that guidance would mean that it would be left up to the different Member States to provide that guidance, and that is when you would get differences in interpretation and fluctuation.
Anna Fielder: The current Directive is focused on outcomes. It has principles and results that Member States are expected to achieve, and you have a 27-track legislation. It doesn't work. In order to harmonise, you need to prescribe to some degree—not necessarily to a vast degree but at least to some degree.

Q56 Mr Llwyd: *Which?*, in particular, in evidence, has said that the lack of trust and concerns raised over data protection present a significant barrier to growth, referring to a lack of confidence in many consumers in the confidentiality of the whole thing. Do you think that updated legislation could change this perception that, indeed, data online is not secure?
Georgina Nelson: Yes, I do. Our recent research showed that 80% of consumers were concerned or very concerned about the use of their personal information online. The research that we have done, both qualitative and quantitative, has shown that there are usually four reasons why there is this lack of trust. First, it is the lack of transparency. It is the failure of the privacy policy to communicate to users how their information will be used. It has become a contract that companies use to protect their liability and it is written by lawyers in legalese. The result is that the vast majority of consumers don't even look at it. That means they feel that they are losing control and they don't understand how their information will be used. So the Regulation is brought to address that by pushing on transparency, by saying what information companies have to provide and by encouraging standardised formats.
Then you have breaches. Last year there were a vast number of high street breaches that hit the press. Consumers often didn't hear about it from the high street themselves; they heard about it through social networking sites or through the media, and that again really shook trust. What the Regulation is proposing to do is put an obligation on data controllers so that, if they do suffer a breach that adversely affects consumers, then they have to notify them. Again, that would really build trust.
Then you have the fact that there is patchy enforcement when it comes to companies who breach data protection and so consumers are not seeing wrists slapped; they are not seeing any action being taken. Again, that is something that the Regulation is trying to harmonise between Member States and trying to give DPAs further powers to take against those companies and higher fines to impose.

Then the final reason we believe is the lack of feasible redress mechanisms. At the moment you are quite powerless as a consumer. If Google, for example, breaches your personal data, if they suffer a breach, your route is to take Google to court. It is not feasible for an individual to take on Google's lawyers. Although we think there is still work to be done in this area, the Regulation is looking at easier routes for redress. Whether you do it via a consumer organisation representing you on your behalf or there are rights for compensation payments, we believe that these are all steps, hopefully, to build that consumer trust back up.

Q57 Mr Llwyd: Ms Fielder, do you want to add anything?

Anna Fielder: I totally support what Georgina said. I would say that we are not talking about some consumers. We are talking about the vast majority of consumers that are concerned, and all the surveys point to that.

The other economic issue worth bringing out here is having more confident consumers. I authored a study on e-commerce for the European Commission a while ago and we had an economic analysis of e-commerce in Europe, which shows that the opportunity lost for people not confident enough to go and shop online is about 1.7% of the EU GDP. Lack of confidence to engage has very serious implications for UK plc, basically.

Q58 Mr Llwyd: I can follow what both of you are saying, but how do you square that with the fact that the main four clearing banks would always say that online banking is increasing hugely year on year? How do you square that circle?

Georgina Nelson: Consumers are reassured by the levels of security that banks operate at. I don't think banks generally have been the ones highlighted in the data breaches. What we are looking at is when consumers are contacted by companies with whom they have never had a nexus of relationship because they may have ticked a box ages ago and they feel they don't know who their data is going to and what is happening to it.

Also, when you talk about privacy concerns for consumers, obviously the usual rebuttal is, do consumers really care because they are uploading their pictures on to Facebook? Are they just wanting their cake and eating it? What we need to remember is that there are these great short-term benefits online, but what you are seeing is this concern that consumers feel there is something in the wings, and, while they want the benefits, they are not sure about the long-term costs and they have a level of unease about it.

If you look at BIS's mydata strategy, on which I have been working with BIS, and think about what they are trying to implement there and how they are trying to take their personal data ecosystem forward, the huge barriers that they are facing are in consumer trust with the research that they have done. This is continually what we are going to find with the internet. Once we move to Digital by Default with the Cabinet Office and ID Assurance, unless we can build that consumer trust, these initiatives are going to have real problems getting off the ground.

Q59 Nick de Bois: I have a quick supplementary on that. I don't want to take away from what seems to be your enthusiasm for the proposals, but is it, in summary, realistic to think that this legislation will suddenly make consumer confidence no longer an issue in online transactions? If you ask 100 people in this room, if there were 100 people in this room, most of us who would use it would be worried about the possibility of fraud. Are you not raising expectations too much by putting emphasis on satisfying those objectives to this legislation?

Georgina Nelson: It is a really positive step in the right direction and I do believe the Commission have addressed the key concerns that we recognise with consumers. I am not saying it is a panacea, but I believe it is certainly a way forward.

Anna Fielder: Can I just add to this? Philosophically, legislation is always a first step. It doesn't solve anything in itself. There is plenty of legislation that is ineffective because it is not effectively enforced. So you need this first step; you need to create the basis, and then it is the work of the regulators, the consumer groups or the stakeholders to make sure that it works and it promotes the objectives that it needs to promote.

Q60 Nick de Bois: That leads us nicely on to the burden of business, if I may, Chairman. Bearing in mind what you have just said, I am trying to understand if either of you feels that the administrative burdens contained in the proposed Regulation are necessary to deliver this EU-wide harmonisation. I will put that in context, because clearly there is a difference of view between your two organisations and those of the Federation of Small Businesses and Microsoft, who do not take your position. Can you explain why you think it is necessary, and perhaps I will start with you, Ms Fielder?

Anna Fielder: Yes, with pleasure. I want to make two points and then Georgina can supplement me. If you read the Regulation, the bulk of these administrative burdens is particularly in the sections that concern data subject rights—in other words, consumer and citizen rights.

For example and concretely, you have an Article 12 that sets requirements for various procedures and mechanisms. You have an Article 14 that has a detailed list of all the information that has to be provided; Article 23 is on privacy by design and default. The bulk of those burdens are in the data subject rights, and the reason they have been put in there is because, precisely, the current legislation does not respect those rights and it was felt that you need a bigger degree of prescription and administration in order to ensure that that happens.

The second point I wanted to make is about technology. If you look at the amazing technological advances, you can do almost anything with algorithms and automated processing. Every time you go online, a cookie is placed in your computer so that there is knowledge on exactly which sites you visit and it can

profile you exactly on your tastes, how much money you have got and where you live, without necessarily knowing your name and address. If you can do all this technologically, why is it so difficult technologically to have a number of processes in place, which are good practice in any case, that when you put them in place they can stay there and be automatic? It is not such a burden and it is not expensive.

Q61 Nick de Bois: Is that realistic? I spent 25 years in business, and someone would come along and assure me that there was a program available and once it's in it wouldn't be a problem. I am constantly updating, I am constantly changing, and I saw an IT bill for a small business of about £20 million turnover go from £30,000 a year to about £200,000 a year. How confident are you that this will not become that sort of burden for the smaller businesses—I am more interested in the smaller businesses, as you can imagine—who will have to deal with this?

Anna Fielder: Absolutely, yes; smaller businesses are the bulk of UK business and it is very important. Even smaller businesses can buy off-the-shelf e-commerce packages at the moment. You probably know that if you have been in business. I have a friend who runs a photo gallery; she is a photographer but she is also a small business. She found that a combination of cloud computing and off-the-shelf packages, with the right IT provision and so on, provided her with about 80% of what she needed.

I just want to be clear. You have to have the right balance in order to enforce people's rights in having their data protected. You also have to have certain good practices that are in place there. If I go online, I want to know who I am dealing with and I want to have clear and very simple information. I don't know how many people read privacy notices now; very few do. Having said that, there are some provisions in the Regulation that could be streamlined and reduced. We are not saying everything is perfect, but what we are saying is don't throw the baby out with the bath water.

Georgina Nelson: Just to add to that, I believe Microsoft said that they fully support the data subject rights that are being provided for in the provision. I do not think there should be any fettering or mitigation of those rights due to administrative burdens. It is getting that balance right, and obviously any administrative burden which is superfluous to those rights should be lightened.

For me, from the MoJ consultation, there has been this focus on the short-term administrative burdens. I would just like to say a couple of things on that. First, what we are looking at is a piece of legislation that, like its predecessor, is probably going to be around for 20 to 30 years. I understand the economic climate of today, but how many economic cycles is this piece of legislation going to outlast? Indeed, by the time it is probably implemented, we will probably be out of the current one. I think perhaps we need to take a bit more of a long view.

Also, if we start thinking about technological changes as well, when this piece of legislation about the Data Protection Act that we have was drafted, Mark Zuckerberg was in primary school and Facebook hadn't even been thought of. If you think about how quickly processes have changed within five years, what we are putting in place is going to last decades, and who knows what technological and societal shifts will be in place by then? While there may be costs in terms of compliance because, yes, there are new rights and, yes, there are greater protections and the current businesses of today may have to pay to enforce those or to allow them, those short-term costs have to be looked at in a far bigger societal picture.

I would also like to say that, in regard to these burdens, if we can twist that around and think of the benefits to UK plc, if you look at BIS's mydata business proposal, you will see that they talk about a huge explosion of innovators and entrepreneurs—these companies who are going to learn how to guide consumer choice and behaviour on their data.

The Regulation is trying to open up this very competitive market of personal data so that it is not sat on by the few big players but it can be utilised by everyone for the greater good, whether that is business or consumers. That is really important to bring into the economic analysis; it is that future scope.

Also, with regard to SMEs, the evidence previously was that at the moment cross- border trade is not something that they engage in, but obviously this is because it is hugely complicated. They probably can't afford the legal advice and the benefits don't justify the pain in getting there. But, if we do move towards this harmonisation, they will then hopefully have the confidence and it will be a far easier procedure to open up a whole new market for them, and then again you would seek to reap the benefits.

Finally, just building on Anna's point about enhanced consumer trust, the OFT recently did a study where they asked consumers whether they engaged online. 6.27% said they didn't; they had never provided their personal financial details because of their privacy and security concerns. If you twist that on its head, that means 2.64 million of UK consumers don't engage online, and that is a loss for e-commerce business of £2.48 billion. Again, that is something we should look at in the long-term for this proposal.

Q62 Mr Buckland: Looking at the Regulation, in particular at Article 17, which is described in the headline as "the right to be forgotten and to erasure", it is interesting to note that in the body of the Regulation that phrase "right to be forgotten" is not used at all and we are back to the right to erasure, which is a pre-existing right under the old provisions. Do you think the "right to be forgotten" is a helpful term or do you think it is just a slogan?

Anna Fielder: I will start and Georgina will continue. If you look at Article 17 in detail, it is a bit more than just the right to erasure. It mentions the grounds on which permanent erasure is possible, including the right to object. It also has a provision of endeavour on the part of the data controller to inform third parties about erasing data. So it is a bit more than just the right to erase. Therefore, it needs to have an adequate title to denote that. It is aimed mainly at social networking and social sharing sites like photo sharing, video sharing and so on, and it is quite specifically aimed at that. The third party provision is one of endeavour. It tells them to try. What they have to

prove is that they make a good stab at it—not that they actually did it.

Q63 Mr Buckland: Yes. They have to "take all reasonable steps"; that is the phrase.
Anna Fielder: Yes, exactly. Also, I have just two more points to add. One is that, if you look for example at social networking sites like Facebook, they have contractual agreements with app providers, and these contractual agreements include privacy provisions. If they have contractual provisions with all these companies, they can easily notify them or try to notify them of the need to erase.
One caution I wanted to add in this is that we would be concerned about how this affects intermediaries like search engines, because there is other legislation—the E-Commerce Directive—which excludes them from liability when they are mere conduits of data. We would like that preserved; we would not want net neutrality affected at all.
Georgina Nelson: We support the move in regard to the "right to be forgotten" and its obligation on third parties. One problem that we see for consumers online is that, if they do tick that box, for example, to third party marketing, they find that their details have been passed, in some of our investigations, to up to 2,000 different companies. At the moment, if a consumer wanted to contact them, they would have to contact that original company and say, "I am making a subject 7 access request. Please tell me all the other companies you pass my data to." Then they would get the list back and they would have to go through each of those parties. This is proposing that the obligation is on that data controller to notify them, and we think reasonable effort is perfectly justifiable in that scenario.
Looking at public dissemination, I know there has been a lot of talk about how it is impossible on the internet because things are viral and things happen so quickly. We obviously understand the limitations of that and we are not saying that we should expect 100% erasure in those scenarios. But, likewise, on a website you are going to have terms of service with your users. If you are a social networking site, you also have terms of service with your account holders. It should not be too much of a jump to say in those terms of service you have, if there is a notification on this website that someone has—whatever it will be called in the future—exercised their right to be forgotten, then you need to do the following steps and we expect that of you. I would hope that the big noise about the impossibility and the costs could be possibly broken down into easy, possibly legal solutions through those contracts.

Q64 Mr Buckland: There is a danger, isn't there, that "all reasonable steps" could be interpreted in a restrictive way? Providers could say, "It is just not possible for technical reasons to do more than we are doing."
Georgina Nelson: Yes. The focus needs to be on efforts rather than the results. There needs to be some elaboration on the right as it currently stands so that people clearly understand their obligations and guidance is provided on what they would expect in those scenarios.

Q65 Mr Buckland: It is not an absolute right; it is a qualified right to be forgotten.
Georgina Nelson: Yes.

Q66 Mr Buckland: There are exemptions, as you say, set out in Article 17(A). Do you think the term is helpful or misleading?
Georgina Nelson: Our general position is that, if we can find something that wouldn't lead to that sort of consumer expectation of a wholesale full right, then that would be great. Maybe we can get our marketing team on it.

Q67 Mr Buckland: Putting aside the legal difficulty, there are technical difficulties, aren't there, in being completely forgotten by a data holder?
Anna Fielder: Just to sum up, we are not married to the name but we are married to the extra provisions. Yes, if the *Which?* marketing team devised a good name, that would be great.

Q68 Chair: But if you have a long record of defaulting on your credit that is not something that you are entitled to have forgotten, is it?
Georgina Nelson: I don't think that would be included in the exemptions.
Anna Fielder: Yes.

Q69 Mr Buckland: We have a number of exemptions: for example, public health, scientific and statistical and historical research purposes, and freedom of expression. They are quite wide derogations, aren't they, which can be interpreted widely, it seems to me, unless I am getting that wrong?
Anna Fielder: Yes. The focus of that Article is exactly as Georgina said—on certain circumstances—and all the derogations ensure that situations that need not be are not.

Q70 Mr Buckland: Can I just move on to another subject, which is the right of access to the data subject and how that is to be policed? There are issues, aren't there, about what would be regarded as vexatious or repetitive applications and the potential of, for example, a £10 charge being made? The Government seem to resist the idea that, no matter who the subject, there should be unrestricted access. What is your view as to the position of any charge in certain circumstances?
Georgina Nelson: A charge exists at the moment; a company can make the £10 charge for consumers. From *Which?*'s own experience, when I first arrived, that was the system in place as standard and we removed it. We didn't suddenly see a flood of subject access requests hit us. I would question this call from business that, "We are going to be inundated. These are the costs that we're going to experience." I would actually question that. When we have done a recent poll on this area, only half of people knew that they had the right; only 7% had ever exercised it, but 76% thought it was completely unacceptable for a company

to charge them for their information. It is showing, again, that times are changing and the days have gone of writing out a cheque and sending it in the post to a company to get a lever arch file of their photocopies of screenshots.

If you look at what mydata is trying to do, one of its big aims is moving subject access requests into the 21st century. The raison d'être of that is that they will be free, and so we have to move away from this. It is a barrier, effectively, which companies want, and that barrier will be provided by the exemptions within the Regulation around "manifestly excessive", so they will still have that caveat and get-out. For the majority, it should be free. Around "manifestly excessive", that is going to be decided in a delegated Act, and I guess from our perspective we would just be concerned that it wouldn't be a loophole for companies to refuse subject access requests. We just want a tightening up of what that actually means.

Anna Fielder: I had an example. My husband had his ID stolen. Somebody opened a bank account in his name and started ordering goods from various catalogues and so on. I know the law really well. It took me six months, and in subject access fees about £200, to access all the companies that had wrong records. Imagine an elderly vulnerable person who doesn't know the law, having to do that individually with every company. It just wouldn't be possible and it would be excessive as well in terms of charges. There are concrete examples—ID theft is a huge problem in this country as well—where we need specific, good measures to make sure that people can access their records and correct them.

Chair: Thank you very much indeed. You have both given us very interesting evidence this morning and we are very grateful. Thank you.

Examination of Witnesses

Witnesses: **Françoise Le Bail**, Director General, and **Marie-Hélène Boulanger**, Head of the Data Protection Union, Directorate-General JUSTICE, European Commission, gave evidence.

Q71 Chair: Madame Le Bail, Madame Boulanger, welcome to the Committee. We are very grateful to have your evidence today. As you will have seen from reading the previous evidence session, we are gathering evidence, ideas and thoughts about the proposed Regulation and Directive. That very sentence brings up the issue of there being both a Regulation and a Directive. Is there a risk of inconsistency between the Regulation and the Directive? One previous evidence session pointed to the fact that data is not necessarily confined to one or other sphere; it moves between both spheres.

Françoise Le Bail: Thank you very much, Chair. I would like, first of all, to thank you for leading this inquiry at this particular time, where we are trying to find the right balance for these proposals, which are very important—important for citizens but important also for business and for public powers. We very much welcome this inquiry.

To answer your question, on possible inconsistencies between the Regulation and the Directive, as you may imagine, we have discussed this internally a great deal and also with stakeholders before taking the decision to bring forward two different proposals. In fact these proposals have quite a lot in common. They have, first of all, the same principles in common. The same principles of data protection apply at the core of the Regulation, but I think the new element is that they are at the core also of the Directive, which was not necessarily the case to start with.

The second element, which is very important, is that the Directive covers domestic processing as well, which was not the case in the Framework Decision. The additional element is that the Directive, in the same way as the Regulation, is covered by the mechanism that allows data protection authorities and also the Commission to have a say if this is not respected.

In doing so, we have applied, first of all, the obligation we have under Article 16 of the Lisbon Treaty, but we have also applied declaration 21, which is annexed to the Lisbon Treaty, which says that for this particular field, which is police and judicial co-operation in criminal matters, of course specific provision should be taken. So, as I have said, there is a great deal of commonality between the two.

Secondly, in the Directive, we give to the Member States and law enforcement authorities the flexibilities that are required for exerting these powers in this very particular field. This is why you will find in the Directive a number of derogations that go with this particular field. This is also why the legislative instrument itself is different—a Regulation that does not need transposition—and the Directive leaves a bit of leeway to the Member States to take into consideration their particular culture and also the type of legislation; I am thinking about common law in the UK.

This is the reason why, although there is a huge amount of commonality, there are also a number of elements that are different because the field itself is different. But they are part of the same exercise, which is to reinforce the rights of individuals in terms of data protection. This is also part of the exercise of stopping the fragmentation in the legislation, both in Regulation matters where we have 27 different types of legislation but also in what is the framework decision area now, where, first of all, there is a very different way of implementing these framework decisions and a very different degree of application of the framework decisions. We believe that, by presenting two types of legislation at the same time, we will fight against this fragmentation but we can also give the necessary flexibility.

Q72 Chair: When the Directive was published, you had comments of both the European Data Protection

Supervisor and our own Information Commissioner, suggesting that it was a weaker position than was originally envisaged within the actual content of the Directive. How do you respond to that concern?

Françoise Le Bail: I do not think the protection is less. It is made differently and, again, it is proportionate, I would say, to this very particular field. I guess that, in the reflection of the comments you had from the data protection authority, they had expected to see one single instrument for data protection, whether for commercial data or police data, which of course would give a great degree of simplification. But, presumably, and this is a judgment we have passed ourselves, it would not have been the ideal solution for police co-operation.

Again, if you come back to the characteristic of the Directive, as I said earlier, the very principle of data protection applies through the Directive. It is the modalities that are going to be different and the derogations that are there are derogations which are of course limited but they are necessary for security and police matters, and for moving very quickly in the framework of a criminal inquiry. We felt that it was necessary for this particular field.

Q73 Mr Llwyd: What impact do you consider the proposed Directive will have on the operations of the law enforcement agencies?

Françoise Le Bail: We believe, first of all, that it will reinforce and simplify greatly the operation of the law enforcement agencies. Again, the principles will be the same, the parameters within which the Directive is implemented will be the same, and there will of course be distinctions in how it is transposed. But, again, by your position with what exists now, the principle will be the same and, again, the domestic processes will be covered, which is not the case in this current Regulation. These are, in my view, the two elements.

I will add another one, which is that, for the derogation, the Directive is planning criteria for defining this derogation. The situation you have now in the framework decision precisely is that there are no criteria for this derogation and therefore you have a very wide variety of derogations that are not based on the same principles.

Q74 Mr Llwyd: Do you wish to add anything?

Marie-Hélène Boulanger: I can just support what has been said. We believe that having more common grounds among Member States and more common understanding about which data protection requirement conditions will apply to the law enforcement authorities, especially in the framework of the law enforcement co-operation, will simplify co-operation between law enforcement authorities, will foster this co-operation and will also have an important impact on the efficiency of law enforcement co-operation.

Q75 Mr Llwyd: From evidence we have received there isn't quite as rosy a view of things as you actually state. Privacy International, for example, considers that, in the proposed Directive, data processing principles are less ambitious and more ambiguous than in the Regulation. The rights of the data subjects are weaker; for example, transfers rules are unclear and less restrictive, and supervisory authorities have fewer and weaker powers. The question I would ask you has been touched upon but I would ask you to restate your answer if you would. What is the rationale for the proposed Directive having a weaker level of data protection compared to the proposed Regulation?

Françoise Le Bail: As you have gathered from what I said earlier, I would question the fact that it has a weaker level. Again, by putting the same principles, we believe that it reinforces certainly the protection of individuals compared with the current situation. I would agree with you that there is a clear difference between the Regulation and the Directive in so far as the Regulation goes much further, it has of course less derogation, and it has an intervention by the DPAs and the consistency mechanism, which is much stronger than in the Directive.

Again, the reason for this is the very nature of the activities we are dealing with. We believe this is necessary for police co-operation and, as I said earlier, in order to move faster in an inquiry. By the very nature of this inquiry, for example, the rights of access of an individual are of course less wide than they are for the Regulation, and this is to protect the legitimate activities of the police. It is true that, in doing that, we had to balance the willingness we had to reinforce the right of the individual, but also we had to take a realistic view of what the activities of police and security were and, while preserving the right of individuals, we put a limitation by comparison with the Regulation.

Q76 Mr Llwyd: Apart from the issue of derogation, why does the Framework Decision 2008 need to be replaced so soon after being implemented?

Françoise Le Bail: There are a number of reasons for this. First of all, we thought it was the right thing to do to have an overall framework for data protection. You mentioned it yourself and you pointed to the difference. Yes, there are a number of differences, but there is also an overall framework. We wanted to make sure that citizens will be protected both for a transfer exchange of the commercial data but also in the framework of police activities.

It is up to the Member States to decide if they want to implement the framework decision or not. There is no intervention from, for example, the Commission to intervene if they don't want to do that. The report that we have issued at the time of issuing the proposal shows the discrepancies, the limits in the implementation and the variety of ways in which it is applied. We thought that it was necessary to have this overall framework.

The second element was that the framework decision doesn't cover domestic processes. From all the contacts we had, having consulted very widely for two years before putting forward these proposals, we realised from all the stakeholders we were in touch with that it is increasingly difficult to make a distinction between the data that is domestically processed and the data that is not. For the enforcement authorities themselves, this has become a great

difficulty and, paradoxically, it has become an admin burden to make this distinction. We thought, having consulted widely, that this was the time to include domestic processing in it, again to create consistency in the overall regime in the same way it is done for the Regulation and, for that matter, for the current Directive. This is the reason why we wanted to do that.

The third reason was to be able to make this protection of citizens—in the framework of their data—a reality, which means that, if it doesn't happen, there is a right of intervention by the Commission in the framework of its infringement powers to intervene if the Member States do not apply the Directive or do not apply it in the right way.

Q77 Mr Llwyd: Why was the domestic processes element not central to the 2008 decision? Why was it not considered? Why was it not realised then? It is a fast-moving area—I understand that—with new technology, but surely regard should have been had to these issues before 2008.

Françoise Le Bail: 2008—maybe you can answer.

Marie-Hélène Boulanger: I was not there either, but, regarding the domestic processing, the framework decision is also a pre-Lisbon instrument, which means that the way it was adopted to reflect the consensus of all Member States and the European Parliament was not involved as it would be for the Directive in the same way as the Council. I was not part of this negotiation, but, in order to get the consensus of all Member States at that time, it was necessary to exclude domestic processing. What I have been told by my colleagues who were there is that it was not a majority that was against it; it was the way to get a consensus on this text. But I cannot say more because I was not part of this negotiation.

Q78 Nick de Bois: Madame Le Bail, I was interested that you spent four years as the SME envoy, which I am sure is challenging. Bearing that role in mind, I am sure you perhaps understand some of the reservations of UK small business, the Federation of Small Businesses and indeed some of the larger businesses, about the perceived burden and cost as a result of the proposed Regulation. Is the prescriptive nature of the proposed Regulation entirely necessary to ensure the EU-wide harmonisation or could you not have done it as an updated general Directive as being a better approach, perhaps avoiding what many people feel would be an onerous burden?

Françoise Le Bail: As you said, for four years I was the SME envoy for the Union, which was a very interesting job and which gave me an insight and understanding of how a company works. It is true that, when preparing for this Regulation, we had extensive contact with the business community and, in particular, with the SME community.

The first thing that the SMEs told us was, "What is a problem for us is fragmentation. If I am an SME and I have to deal with 27 different legislations in terms of data protection, it is awful. It is simply awful. I cannot cope with it because I don't have a legal service, I don't have people who are able to follow this." The first thing we are doing for SMEs is to stop this fragmentation. We will stop this fragmentation by one single law. This is a huge benefit for an SME because, for a big company, in a way they can cope; they have legal services. But this is absolutely huge.

The second element for SMEs, which is very beneficial, is that they have to deal with one single data protection authority. They don't have to look at which data protection authority they should knock at the door of; they will have only one data protection authority to deal with. This is a huge benefit. We believe that, taken together, there will be a benefit of 2.3 billion in savings from having this harmonisation.

Of course the question is what are the obligations you put in this Regulation which are going to be detrimental to the SMEs? Believe me, we really worked on this question. I would like to point to a number of elements that are seen widely as administrative burdens for companies. The first one is the data protection officer. We say, if you are a big company with more than 250 employees, then you need a data protection officer. But, if you are a small company, unless you specialise in dealing with very sensitive data, you do not need one. I can tell you that I dealt with that one personally. If you take Germany, for example, if you are a company with 10 employees, you need a data protection officer. Of course we discussed this question very openly. Should we say above 10 employees that you need a data protection officer? We took the right decision, which is to avoid the obligation of having a data protection officer if you have less than 250 employees.

Q79 Nick de Bois: May I ask you a question on that point specifically? I initially think that it is a very welcome idea to limit it by the number of employees, but, if you dig deeper, wouldn't it perhaps be more effective to look at the sensitivity of the data that the organisation is handling, whether it is 10 employees or 1,000 employees?

Françoise Le Bail: It is a possibility. I will be very clear with you: it is a possibility. We chose the European definition of an SME, which is 250, for simplicity. Everybody knows the definition; either you are above or below. It was for reasons of simplicity. But, again, if there are better ideas to reduce the burden for SMEs, we will look at them, because one of the essential elements of this Regulation was to take into consideration the admin burden. So we are prepared to look at it; if there is a better idea, if it is as simple, why not?

Q80 Chair: Why should you specify that there needs to be a data protection officer if, for example, a company feels it is a much better system to have 10 heads of department, all with data protection responsibilities on a scale, depending on how much their section handles? Surely your interest ought to be in the outcome and not in the procedure or the structure.

Françoise Le Bail: We specify data protection officers again for big companies because, from the consultation we had, we gathered that most big companies already have a data protection officer. The only difference is that, sometimes, somebody is only doing that and sometimes it is a member of the legal

service doing something else. This is the information we collected. It seems to us that, to have one point of reference dealing with data protection for the company, wherever they are organised, means they can liaise and co-ordinate all the services, and all this is up to them, not to us. But to have one point of reference—one person who can be the contact point, for example, of the data protection authority and the Information Officer in the UK—would be a simple solution. This is why.

Q81 Nick de Bois: I have just one point on fragmentation, if I may. Because member Governments can deliver much of the detail through the Directive, do you not feel that your goal of the level playing field—which is the European dream, and I fear I am sceptical of its ability to deliver that—is a threat to achieving the fragmentation you are trying to avoid?

Françoise Le Bail: Certainly for trade data, the problem is all through Regulation. Again, it would have been much simpler to have a Regulation for the police data, but, because of the sensitivity and the particularities of this field, we took the view that it wouldn't have been efficient. We need to leave the flexibility to the Member States, which is within a framework, again, which has principles, which is a commonality of rules, which are criteria, which are much more precise than the framework decision. So we moved a step further and we reduced the fragmentation to a degree, less than in the trade field, but we did that because of the particularities of police data.

Q82 Mr Buckland: Can I turn to Article 17 of the proposed Regulation and the "right to be forgotten" issue, and in particular to Article 17(2) where it is enjoined that the data controller should take all reasonable steps, including technical measures in relation to data for which they are responsible, to inform third parties and so on? How would you regard that test of "all reasonable steps" to be met? In what ways do you think it can be met? In other words, what does "all reasonable steps" mean, in your view?

Françoise Le Bail: First of all, I want to point out that we chose to put that in Article 17, and we chose to do that because we did not want to make it an impossible task. This is very important to keep in mind. First of all, the right to be forgotten that we are proposing now is making something more precise that exists already in the current Directive, and it is also answering the claim of these citizens who have been vastly put at a disadvantage because of wrong information about them. It was very prejudicial. So we wanted to go a step further.

The second point I want to make is that this obligation is very different whether you are an individual or a controller. It is true that for the controller they have to go further. They have to inform, for example, the search engines and all this to a possible, reasonable extent so that this is deleted. They must prove that they are making a real effort, but we are not asking them something that is impossible to realise. That was also taking into account the current technology.

Q83 Mr Buckland: The burden will be on them to prove that they have taken all reasonable steps.

Françoise Le Bail: The reasonable steps.

Q84 Mr Buckland: Of course, putting aside the legalities, there are some technical issues, aren't there, about the right to be forgotten? How feasible do you think it is for this particular right to be applied to the extent that data can be permanently deleted from the internet?

Françoise Le Bail: There is no guarantee of this and this is why we said "all reasonable steps". The message we want to pass to these big companies that are running these social networks and search engines is that they need to demonstrate that they are making a real effort. We cannot exclude it resurfacing at some stage, but we would not like them to say, "Not for us. This is nothing to do with us".

The final solution is that they have to participate—this is an element I would also like to underline—in creating trust in the internet. Creating trust means that you can have an influence on it—an influence which is not rewriting your life but an influence on these things that are on the net that you have not posted yourselves or you have posted at an age when you were not conscious of the damage it can do and you want to see it disappear. It is a very important element for trusting the internet.

Q85 Mr Buckland: Can I move on to another subject that is somewhat related? It is the right of the data subject to access information. The proposed Regulation would make subject access requests free of charge. There are some issues, are there not, at the moment about whether or not the continuation of a fee should be applied by certain businesses or organisations? Taking as the principle that there should be free access, do you think there are circumstances in which requests could be refused and, if so, what do you think those circumstances should be?

Françoise Le Bail: First of all, the right of access is a fundamental right; it is a part of the fundamental rights that should exist. We have looked at what exists in the Member States and again it is a very varied picture. In some Member States it is free; in other Member States it is not. We believe that for simple access it should be free. At the same time we say in this Regulation that, if the demands are excessive or repetitive, you can put a fee on this. You will have seen also that we say that, if necessary, there will be a delegated Act from the Commission in order to make sure that the conditions are not too different from one member state to the other.

I would like to draw your attention also to Article 21. You see in Article 21 that the Member States, by law, can find conditions or limitations to all this. Article 17 is covered by this. I am saying that, but I am also saying that Article 21 doesn't allow you to do anything you want as a member state. Of course there are limitations, and the limitations we put, if I remember well, are the reasonable conditions of a democratic country. They have to be a necessary and proportionate measure in a democratic society, but there is a degree of flexibility there that can be

explored, and the question of a fee is also something that is discussed very much with Member States currently in the negotiations that will lead to the adoption of the Regulation.

Q86 Mr Buckland: Would I be right to draw the analogy between, let us say, the European Convention of Human Rights, where a general right should be interpreted widely, and derogations to those rights or qualifications, which should be interpreted more narrowly?
Françoise Le Bail: Exactly.

Q87 Mr Buckland: Would that be fair?
Françoise Le Bail: It's a fair description.

Q88 Mr Buckland: Finally, dealing with enforcement and fines, the proposal under Article 79 is, of course, to impose fines of up to €1 million or 2% of the annual worldwide turnover of an enterprise. Do you think there is enough room within the proposals to allow discretion and a differentiation to be made between, let's say, an accidental infringement and a deliberate infringement, because there is a difference, isn't there, between the two? Do you think there is enough discretion to allow an enforcer to make that differentiation?
Françoise Le Bail: First of all, for the first time we are proposing fines that matter, which make you think twice, because we deliberately decide not to respect the Regulation. That was very important because the fines that exist now currently in Member States are minimal and you can ignore the Directive—it doesn't matter—or the national law that implemented it; it doesn't matter.
You will also see that in the fines we are proposing there are steps to be taken. If you forgot about it, you didn't remember the provision and didn't do it intentionally, you get a warning, if I remember correctly. Then, if it is a repetitive pattern where it starts to become obvious that you intentionally don't respect the Regulation, these fines are implemented to the full. We realise that it may happen; by mistake or ignorance you don't respect the Regulation, but after a while it is a pattern and then we apply it.
Marie-Hélène Boulanger: May I add something to this point? If you look at the provision purely from a legal point of view, you will see that, with regard to your question, "Do we take into account the character of the breach?", there is a clear requirement to take into account the nature, the gravity, the duration of the breach, the intention and the negligent character of the infringement and so on. This is in paragraph 2 of Article 79.
Then you have paragraph 3, which Madame Le Bail just explained, where you have the situation of an actual person without commercial interest and also of a small and medium-sized enterprise. Then, if we go to the other paragraph, it is a maximum. It is "up to". So there is a margin for discretion in the way you apply the fines.

Q89 Mr Buckland: That is very helpful. I take that point; thank you.
Françoise Le Bail: Can I also say, if I may, that I sometimes see in the analyses which are made by the Member States that the amount of the fines is taken into account when analysing the admin burden? We take the view that the fine is not an admin burden because if you respect the law there will be no fine.

Q90 Mr Buckland: It is a penalty; it is a punishment.
Françoise Le Bail: It is a punishment; exactly. So it is not part of the admin burden.

Q91 Chris Evans: We have heard today about future technology and how rapidly technology is going. At the moment the Regulation is in place. However, we are living in a world that is moving ever forward, and we have already heard evidence that Facebook and Twitter were unheard of 10 years ago. Do you think the Regulation, as it stands at the moment, is in tune with the standard of technology we have?
Françoise Le Bail: First of all, one thing we wanted to do when designing this Regulation was to make sure it will be technology-proof, which means that the Regulation, as it is, can apply not only to the technology as it is now but will apply to new developments. We know the cloud; we don't know what will happen afterwards. It will happen and happen fast. We believe that the provision of this Regulation can apply to all these developments. One of the reasons why it applies to this, and it can apply to future developments, is that this Regulation, although some of you think it is very prescriptive, in fact leaves flexibility in the form of delegated Acts. We have two options: either we were describing it in great detail in the Regulation, including all the fields of technology we were putting in the Regulation, or we were giving the possibilities for adjusting to future developments. We have done so. The Regulation is technology-neutral and it leaves the possibility in a way that is being discussed with Member States. It is not that all Member States see with great enthusiasm delegated Acts for the Commission, but we leave this possibility to adjust to future developments.

Q92 Chris Evans: I find that very presumptive, to be honest with you. We don't know how technology is going to develop. At the moment the Regulation has 26 different provisions. Microsoft have come and seen us and told us they think that is just way too many. Having sat on other Bill Committees—for example, the Defamation Bill Committee—I find it difficult to understand how you can frame a Regulation which takes account of something you have no concept of at the moment, like people may have done 20 years ago. It seems to me absolutely impossible and it just seems a complete misnomer having 26 provisions. What are you actually trying to prepare for in the Regulation? I do not see the intention in that at the moment.
Françoise Le Bail: First of all, we had an intensive discussion with Microsoft. Let's be clear on that. Overall, Microsoft, to name it, are publicly very supportive of what we are doing. We are making their life much simpler by having only one Regulation by imposition with the 26—

Q93 Chris Evans: If I can stop you there, they have said that essential elements should be dealt with in the Regulations themselves and not with secondary law making conferring power on the Commission. What are your views on that?

Françoise Le Bail: If we fix everything in the Regulation, we then give a huge amount of rigidity to the Regulation and then there is a high risk that it will not be appropriate any longer for this future technology development, which can happen any time. So we choose to leave some flexibility there in order to be able to adjust. Leaving it to secondary law, it is not that we are doing this without any control. For secondary law, we do that under the supervision of both the Council and Parliament. So it is not that the Commission itself is going to decide what is going to happen on these matters. Secondary law as well will respect all the provisions of the Regulation. But the choice was either to put everything in great detail in the Regulation or to leave flexibility. We chose to leave flexibility.

Q94 Chris Evans: But my point is that you don't know how cloud computing is going to develop; you don't know how international data transfers are going to develop. What you have is a very complicated Regulation with 26 provisions conferring power on the Commission. It seems to me that, if you have a piece of technology that comes across that you have not accounted for, which we have seen developed in the last 10 years historically—and the pace of technology is only going to get faster in the future—you will have a Regulation that is quickly going to become out of date, you have 26 complicated provisions and you can't deal with them. You are going to be sitting here again in five years dealing with something you should be sorting out.

Françoise Le Bail: The best example to take is the cloud, which is now being developed and is the latest technology that we know of. In fact, this Regulation will apply to the cloud without change. It is cloud-compatible, and we believe that this Regulation is any- new-technology-compatible, because there are provisions, in spite of what you believe, which are not in that great detail because there are elements of flexibility. Doing the opposite will destroy this flexibility, but maybe, Marie-Hélène, you want to add something on this.

Marie-Hélène Boulanger: I want to go in the same direction exactly, just to say that this Regulation does not regulate technology as such. It establishes principles and safeguards conditions for fair processing. This is something that was already the case in the old Directive, but some elements became outdated. We have based this on new technologies and anticipate as much as we can new development, but it is still based on principle, responsibility, rights and so on. There is no Regulation as such of the cloud, for instance, but there are provisions on transborder data flows, requirements for processing of data, and making use of the processor to process personal data.

Q95 Chris Evans: That is not the point I am getting at. What I am getting at is that there has been technology developed in the last 10 years that has challenged the way the data is held at the moment. I can think of two examples straightaway: Facebook and Twitter. But what if you have technology that comes along which challenges how data is now held and the Regulation could quickly become out of date? That is what my fear is.

Marie-Hélène Boulanger: Exactly what has been explained. The basic principles are there: what you can do and how you can process personal data, based on key principles. Then you have a lot of mechanisms in this text that will support the fact that the text is future- proof. One element that provides legal certainty is that a delegated Act can be adopted. It is a way to supplement the text with non-essential elements and provide legal certainty.

But there are other mechanisms. There are a lot of other mechanisms, including the codes of conduct and the guidelines to be provided by data protection authorities all together at European level. These guidelines will help to provide guidance on how to apply principles to new technological development. There is no Regulation of the technology, so I don't really see the risk of having this text outdated very quickly. For instance, the right of access will remain valid even if there is a new technology. It will still make sense for the data subject to get access to his own personal data.

Chris Evans: I am sorry; I am just not convinced. I have no further questions.

Q96 Jeremy Corbyn: Thank you very much for coming to give evidence to us today. Are you confident that either the EU itself or Member States have sufficient resources to implement and monitor these proposed Regulations?

Françoise Le Bail: In the EU Regulation we ask the Member States to make sure that their data protection authorities are staffed with the right amount of people and also have the necessary financial backing. The picture we have around the EU is of course very different from Member States to Member States. You have a very strong data protection authority in the case in point certainly in the UK, and you have other Member States where it is much weaker. Therefore, we request Member States in the Regulation, and this is an obligation to make sure they have both the necessary finance and staff. The reason for this is that the data protection authorities will have to continue the work they are doing now, but they will also have to participate in the consistency mechanism, which is, in a way, finding a common definition or common position on an event that can take place or a new development that can take place. Google's review was a case in point, and so we have this consistency mechanism that we have to take part in.

The second aspect of things is that, in a way, they are going to be relieved from a number of things they are doing now. I am thinking, for example, of notifications, which they will not have to issue at this particular stage. But, to be sure of this, we have launched our own inquiry and sent to all the data protection authorities a request for their own assessment of their situation, taking into consideration the implementation of the future Regulation and Directive and their assessment of the amount of

people they may need and necessary finance. I must say that the main problem there is of course in new Member States, which have not had data protection authorities in place for very long, by imposition with other Member States.

Q97 Jeremy Corbyn: Isn't there a danger that, since the internet is obviously universal, a member state with a very weak supervisory regime could become the centre of all kinds of intrusive abuses of data protection? What powers and particularly what resources do you have to ensure that there is some degree of uniformity across the whole of the EU, because without that uniformity the Regulations are pointless?

Françoise Le Bail: Absolutely. First of all, there is this obligation that these Member States have, and then, secondly, the co-operation that is going to take place between the data protection authorities. Let's imagine, for example, that there is a huge problem in a particular member state. The other data protection authorities can raise it in the framework of the European data protection board in the same way that the Commission can raise it, and there can be a co-operation that can be put in place between the strong data protection authorities and the weaker data protection authorities. But the objective is clearly to have a proportionate level. It has to be proportionate. Of course it is not going to be the same in Estonia as in the UK. It has to be proportionate, but there has to be the necessary level of staff and finance. That is the objective. Maybe you can add something.

Marie-Hélène Boulanger: If you look at the text in detail, you will see that there are a lot of what I would call safety measures in the provisions around Articles 15 and 16 to avoid that risk. In addition to what Madame Le Bail just explained, we also have the fact that there can, for instance be, joint French and German investigation teams. As the data protection authority of one Member State, if you feel that the authority in charge does not have enough staff to deal with the specific case, you have the possibility to send your own staff in support and the competent data protection authority for the specific case cannot refuse the support if there is cross-border effect. That is one of the mechanisms. There are many other mechanisms like that. A data protection authority can take urgent measures, with specific requirements and so forth. There are many possibilities to ensure that there are no discrepancies between data protection authorities. In addition, the European Commission always has the possibility to intervene in such cases.

Q98 Jeremy Corbyn: Two quick points from me before I finish. Does the Regulation affect the EU's own considerable storage of data on many issues, including individual information across the EU? Secondly, what consultation have you had with the European Court of Human Rights on the compatibility of the European Convention on Human Rights with these Regulations, particularly in relation to Article 8?

Françoise Le Bail: Let me start by dealing with the second question on the convention. We are of course in very close contact with the Council of Europe on this and we are in the process of requesting a mandate of negotiation from the Member States to take part as a Union, as must be the case now, in this negotiation. But we want to make sure of the compatibility of the new Convention 108 with our own development inside the EU. It doesn't mean that the convention will go into the same degree of detail, for example, than our own Regulation for obvious reasons, because there is a big variety of members of Convention 108 and it is a very different obligation from the Member States. But we want to make sure that there is no incompatibility. There are a number of questions we are currently discussing with them—for example, the notion of adequacy, which is a bit different, or at least the modality would be different. We are discussing that with them; I am sure we will sort out the problem, but very closely. What about the first question, Marie-Hélène?

Marie-Hélène Boulanger: On the first question, this package as such does not cover EU institutions and bodies, agencies, the European Commission, European Parliament, and Council. You have to see that in a broader perspective. Also, before this package was presented the year before, at the end of 2010, the Commission issued a communication where we made it clear that we would present the necessary instrument to have the complete set of rules. The idea was to start to discuss with the co-legislator to have the principles agreed, and, when there is a clear orientation the Commission should come with a new legislative proposal to complete the package and adopt the agreed principles to cover EU institutions and bodies. That is the logic.

Q99 Chair: Going back to the issue Mr Corbyn raised earlier, when we had our own Information Commissioner Chris Graham in front of us last week, he said that even minimal compliance or compliance with the minimum required would increase the costs of his office by 56%, and what he thought of as more satisfactory compliance could be as much as an 187% increase in his resources, which he confidently expected that the Government would not be providing him with. This is quite worrying, given that ours is one of the better funded information officer set-ups in the European Union.

I don't know whether you have seen that evidence or whether you will now be considering that the whole process is going to be too expensive, because along with that went his view that, if adjustments were not made, he would end up spending a lot of his resources on details of structural compliance rather than pursuing serious failure and giving appropriate advice.

Françoise Le Bail: First of all, we don't know these figures yet. I am sure he is going to transfer them to us and we will look at them, together with the assessment of the other data protection authorities as well. My first reaction is that it seems a huge amount. Certainly, in the reflection we have had, we never envisaged that it would be as much as that. So we need to have a look at these figures in detail. My guess is that it will be much less.

Secondly, when he says, for example, that he will need to look at details, dealing with every single complaint that the Regulations, they believe, oblige them to do, this is a subject of discussion among Member States.

This is also the subject of discussion with the data protection authorities because this is a remark they have made. They say there are too many cases to deal with; we will be submerged and we cannot, as we do now, concentrate on the main cases. This we are discussing and we are confident we will find a solution for this. So be aware that we are engaged in this process with Member States, DPAs and national Parliaments, and we are gathering all information that we have. But, coming back to the figures, they seem a lot.

Chair: Thank you very much indeed for your evidence; we appreciate it very much. We will in due course be reporting as part of the process by which the UK Parliament considers this matter. Many thanks.

Monday 17 September 2012

Members present:

Sir Alan Beith (Chair)

Steve Brine
Mr Robert Buckland
Jeremy Corbyn
Chris Evans
Mr Elfyn Llwyd

Examination of Witnesses

Witnesses: **Rt Hon Lord McNally**, Minister of State, **Glenn Preston**, Deputy Director for Information and Devolution, and **Tim Jewell**, Deputy Director, Legal Directorate, Ministry of Justice, gave evidence.

Q100 Chair: Lord McNally, Mr Jewell and Mr Preston, welcome. We are slightly depleted, not least because one of our members has been appointed as a Minister, another as a PPS and indeed half the Ministers in your Department at the Commons end of it are former members of this Committee.
I am not quite sure how the cards are being shuffled in terms of responsibilities of individual Ministers, but may we take it that as of now you are still responsible for the European Data Protection Directive and Regulation?
Lord McNally: Until midnight on Wednesday.

Q101 Chair: So it may change.
Lord McNally: It may change.

Q102 Chair: Is the policy likely to change?
Lord McNally: No.

Q103 Chair: We will rely on you for answers that will hold good for whoever takes over that responsibility. One of the issues that have been pursued in the UK Government's development of their position is that they do not want domestic processing to be covered by the Directive in the UK, but they don't believe that it is anyway. Why is it necessary to try to get it excluded if the legal position is secure and it can't apply to domestic processing?
Lord McNally: We believe, as you say, Mr Chairman, that the legal position is secure and that, whatever the final outcome of negotiations on the Directive, the British position is protected, but we believe that it is also important to have as good and as effective a Directive as possible with which we are going to have to work. Therefore, we have stayed in the broader negotiations even though, as I say, we are absolutely secure in our position that it will not apply to domestic transfers of information.

Q104 Chair: Isn't the practical conclusion of the British negotiating position that, if it was redrafted in the way we want it to be, it couldn't apply to domestic processing in other countries either?
Lord McNally: That is why we are staying in. We believe—and we believe we have allies among other countries in the negotiations—that that is precisely the best outcome for the Directive as a whole. It is almost a belt-and-braces approach. We are securing our own position but we want to argue the case for keeping these matters to domestic control across the Community or the Union.

Q105 Chair: You will have noted that, when we had law enforcement agencies in giving evidence, they were sceptical about the need for a new Directive and quite concerned about aspects that might affect their ability to carry on the job in the way they currently do, particularly information sharing in circumstances when it may be very important to the detection and prevention of serious crime. What is your take on that?
Lord McNally: We have taken very seriously the advice that we have received from our law enforcement agencies. They have been very clear to us that they do get a great deal of benefit from participation in exchange of data with other law enforcement agencies. Indeed, another common-sense reason for us to stay in the negotiations is to make sure that what has proved to be a very effective and beneficial exchange of information is secured following the outcome of these negotiations.
The case we made for opting in as far as these negotiations are concerned is that we believe there is real national interest in making sure that exchanges and co-operation already in existence remain secure and whatever governing instrument comes out of the negotiation is also compatible with our national interests.

Q106 Chair: Privacy International expressed the concern that in some respects citizens' rights were not as well protected under the Directive as, for example, they are under the Data Protection Act and that there was a mismatch between the across-the-board nature of the Data Protection Act and the more limited nature of the Directive. What is your reaction to that?
Lord McNally: I would be interested to see what their precise criticisms are on this. Of course, our citizens are protected by the Data Protection Act and that will continue. This carve-out for policing and security is to allow the specific needs of law enforcement authorities to be met, but I am not aware that in so doing we weaken the more general protections of the Data Protection Act.

Q107 Chair: One of the concerns is that there is now quite an extensive transfer of information between the law enforcement sector and the private sector. There are things like airline passenger information, to take just one example, where there will be one set of conditions in the private sector and a different set in the law enforcement sector.

Lord McNally: Yes. Where it crosses over I would hope that the protections will be as strong in the private sector. One of the dilemmas we face in these negotiations—and one that I am very aware of—is that, quite rightly, pressure groups like Privacy International are very keen to ensure that the legislation does protect the citizen. Looking across the piece, we are moving into an age where more information is held, available and transmitted. It is going to be a very difficult job to get the balance right between protecting the privacy and the rights of the individual citizen without building in so many safeguards, conditions and safety nets that the other benefit of the digital age is lost, which is the ability to exchange information freely.

I also sit on the Transparency Board chaired by Francis Maude. That is looking at the broader release of Government data. There is the same challenge there. How do you release as much data as possible to allow the entrepreneur to make good use of it in creating jobs and wealth without allowing practices to take place that genuinely would invade the privacy of the citizen? If you ask whether we have reached that state yet, I would say, no, that is why we are negotiating. We keep in mind both those objectives.

Q108 Steve Brine: It is nice to see you again at the Committee; thank you for coming. The Federation of Small Businesses has said in notes to us "that the Regulation as proposed will introduce"—in their view—"additional, and in some cases, unnecessary burdens on small businesses". Minister, I just wonder what your view would be of the impact that these data protection proposals would have on the growth of the digital economy in our country.

Lord McNally: Our intention is that it will have an entirely beneficial effect. Just as the single market gives us access to a market of 500 million, so legislation that will give some kind of harmony to the workings of this sector of the economy could and should be entirely beneficial. Why we are being, for want of a better term, awkward in these negotiations is that we do see that there are real threats to business if we allow the Regulations to emerge in such a way as to put an extra burden on business.

We are also very aware that small businesses could be particularly affected by some of the suggestions, such as an absolute commitment to appoint a data protection officer and some of the other regulations in the proposals, which might be easily absorbed by one of the data giants but which a small enterprise would find difficult. However, we don't want to do it by a simple cut-off. It may be a relatively small business that is dealing with very highly sensitive data and we wouldn't want them just to escape their responsibility simply by size. We are trying to get a proportionality into the structure of the Regulations that we don't feel is there at the moment in what the Commission are putting forward.

Q109 Steve Brine: What happens if we are not successful in introducing the proportionality? Microsoft, who are obviously not one of the little boys, have said that they support the FSB's views. You have the small and the large there saying that the Regulations should not be so prescriptive. I just wonder if the prescriptive nature of this Regulation is necessary to ensure the EU-wide harmonisation that the Commission are trying to get at. Wouldn't a general Directive be a better approach?

Lord McNally: Yes. That is exactly what we will continue to argue. We think the Regulation is too heavy-handed and prescriptive in an approach to something that would be much better dealt with by a Directive that leaves a great deal more flexibility to domestic implementation.

Just to go back to a point that the Chairman made on the Directive covering the police and law enforcement agencies, yes, we do think it is a bit soon after the last tweak to this in 2008 to be looking at it again. It is a matter of balance whether you say that, since you are looking at the Regulation, which is much older, you might as well take another look at the police and law enforcement Directive at the same time. It is an argument for starting from square one again with that. From what I understand, the balance of the discussions so far has been much more about what's in the Regulation and whether it could be better handled in a Directive rather than going back to square one with the police and law enforcement Directive.

Q110 Steve Brine: In conclusion, what I am trying to probe is the Government's resolve on this matter. You say it is heavy-handed and prescriptive. The EU has form in this area and in lots of areas. I just wonder how far the coalition Government is prepared to push it. If you don't feel that this is in the interests of our country, how far are you prepared to push it?

Lord McNally: We are not negotiating for failure. We believe that we have allies. As always with European Union negotiations, there is an element of the souk about the negotiations. The Commission come up with ideas and proposals and then others say, "No, thank you." Although the negotiations have been slow, we are not in a position where we feel that we can't achieve our objectives. I emphasise that our objectives are very close to what you have just outlined. We want something that is proportionate, flexible and that doesn't impede entrepreneurship by either large or small companies but does get the balance right in protecting the privacy of the citizen.

Q111 Jeremy Corbyn: I have a short supplementary question. You said you were worried about over-heavy regulation. Do you feel that the proposals or the outcome of all this discussion will be adequate protection against data mining and then profiling advertising to sometimes very vulnerable people?

Lord McNally: I hope so. In the two years that I have been in this job I have become aware that we are really at the dawn of a new era in terms of just how much information is in the hands of various organisations, and the possibility and capability of its misuse.

I will tell you a quick anecdote. It is no slur on Tesco but it is what was said to me. I went to see one of our organisations that was demonstrating to me their various capabilities. I said to the man who was doing it, "There are quite serious implications for civil

liberties in this." He said, "I wouldn't worry, sir. Tesco know much more about you than we do."
In a way it is true. The capacity to acquire information about the citizen and to cross-reference it is quite serious. All I can say is that we are alert to that and want to build it into both our domestic and EU legislation because that threat does exist. One can only say that I think parliamentarians and legislators at both European and national level have to be aware of that threat. In the new digital age it is the downside to what is also a very exciting opportunity in terms of exchanging information for the benefit of the citizen.
Chair: We will come in a later question to the issue of whether individuals can get out of all this. In the meantime, Mr Llwyd has a question.

Q112 Mr Llwyd: I am tempted to say that every little helps, but I won't. That would be plain silly.
On the issue of perceived costs and benefits, the impact assessment and the summary published by the Commission make certain presumptions and certain statements. They believe it is going to deliver substantial administrative savings. However, we believe that the initial assessment suggests that the Commission's thinking does not in fact provide a credible foundation underpinning the proposals that they have and the way in which they say it is going to save money and time.
I won't detail exactly what they are, but we have certain misgivings about the way in which the Commission believe these savings are to be made. My question to you and your colleagues, Lord McNally, is whether the Department has yet been able to use its improved modelling capacity to make an assessment of the costs and also benefits to the UK of the proposals.
Lord McNally: First of all, we share your concern. The other thing I have learned in the last two years is that both domestic and EU organisations that claim the benefits for any particular policy initiative invariably are optimistic when they present the savings and benefits that are likely to come from it. We are doubtful. I do know that the Department is planning to do its own exercise. I don't know if you would like to explain that, Glenn.
Glenn Preston: We are committed to doing our own impact assessment of the Commission's proposals. The aim is for us to make that publicly available—so available to this Committee and the European Scrutiny Committees—before the end of this calendar year. That is proving challenging, partly because we are trying to get information out of the Commission on the basis of the methodology that was used for their own impact assessment, which is taking slightly longer than we hoped it would. That remains the aim. The purpose of producing that is to have a public discussion domestically but also with our EU partners about a proper analysis of the costs and the benefits, which we think was slightly lacking in the impact assessment provided by the Commission.

Q113 Mr Llwyd: I accept what you say, Mr Preston. This may be an unfair question, but I ask it anyway. Do you believe at this stage that the Commission's estimate of €2.3 billion savings is reasonable and achievable?
Glenn Preston: No, we don't. We have already provided an impact checklist to the Scrutiny Committees where we said we didn't think that was an accurate reflection and that it was more likely to be a negative outcome on the basis of the Regulation as published in January. That is the analysis that we are doing. Obviously we would seek to change the content of that Regulation substantially. So part of what we will be doing is also looking at the different options that may exist if we end up with a very different instrument at the end of this, which is why it will take some time. We don't share the view at the moment that it has a €2.3 billion benefit to the EU economy.

Q114 Mr Llwyd: Taking Lord McNally's point, this €2.3 billion could be wildly optimistic.
Glenn Preston: It could be optimistic. I don't know if it is wildly optimistic, but it certainly looks initially like it is optimistic. It is important to stress the point about this being on the basis of the Regulation as published at the start of the year. We would expect the final instrument, whether it is a Regulation or a Directive, to be considerably different and to be less burdensome and prescriptive. Therefore, it could well have a more beneficial impact if that is the case.

Q115 Mr Llwyd: This leads me on to my next question. The Information Commissioner gave this Committee estimates of the impact on his office. He said that, if his office fulfilled the minimum duties required of them in the Regulation, they would in fact be seeking a 56% increase in funding amounting to £8.4 million. A more realistic estimate, given the new duties being imposed, could well turn out to be £28 million. The Commissioner said, memorably I think, "This system cannot work. Nobody will pay for it."
My question is: how will the Government fund the additional resources estimated at a minimum of £8.4 million that the Information Commissioner's Office will require?
Lord McNally: First of all, I would say that it is not only EU Commissioners that indulge in the politics of the souk; so do heads of Government organisations that want their organisation funding. I don't know whether those figures are absolutely accurate. There are problems about some of these proposals in that ending charges would take an income stream away from the Information Commissioner.
Of course, this would need discussions with the Treasury and the Government as a whole. The Information Commissioner is right. If we want him or his successors to do their job, we have to give them the resources to do it. There would have to be a proper negotiation about how to run an effective office if the present funding structure doesn't work. What I wouldn't like to see is a kind of salami slicing of responsibilities to save money so that they can struggle on. I do believe that, whatever comes out of this, we need an Information Commissioner to be able to carry out the necessary responsibilities, both under data protection and under freedom of information. As a country, we have to be willing to give him or his

successors the funding and the stability in order to do their job. In return, the Information Commissioner needs to run a tight ship and to run it efficiently and effectively.

Q116 Chair: I think what the Commissioner was saying was that in this country, where we have a relatively well-resourced Information Commissioner, it is inconceivable that so much more money could be spent. So what is it going to be like across the rest of Europe? In other words, he was drawing from the UK conclusion that the whole structure was unaffordable.
Lord McNally: I agree. Indeed, on Wednesday morning I will be in Brussels with our Information Commissioner talking to a panel of European parliamentarians and we will be making that very point. It is a point worth making. We often castigate ourselves on our record on these things. Our Information Commission Office is well resourced compared with other parts of Europe, although the Information Commissioner continually tells me how difficult it is to do his job on the budget he has. As I say, that is why one of the things we will be pointing out in the nicest possible way to the Commission is that having a wish list of extra responsibilities and tasks for the Information Commissioners across Europe is going to be genuinely wishful thinking because the resources simply won't be there in the present circumstances to fulfil this wish list.
As I said before, our starting point is that that wish list would end up with the worst of all worlds, which is an over-prescriptive, over-bureaucratic, costly and business-stifling regime that would not give protection anyway to the citizen.

Q117 Mr Llwyd: Thank you for that. It is what Mr Preston was saying earlier: there will be work now done to see what the estimate truly is. I am probably stating the obvious, but no doubt you will be in close liaison with the Information Commissioner's Office to see how they have come up with their figures.
Glenn Preston: Yes; that is absolutely right. We have already been working with them on the production of their estimates which they shared with this Committee. They have shared them with us too. We have to have that discussion in the context of the funding model for the Information Commissioner more generally.
We provide at the moment for grant in aid of about £4.5 million for all their freedom of information functions. We have this Select Committee's recommendations to consider in the context of post-legislative scrutiny of that Act and any potential impact on the funding of the Commissioner alongside the EU proposals, where the notification system, as Lord McNally has already said, is due to disappear—so a big funding stream disappears for them—and potentially some other functions that other Departments are interested in giving to the Commissioner too. We are talking with them now both about the impact of these specific proposals as a burden on the Commissioner's Office but looking more generally at how the Information Commissioner's Office is funded, with a view probably to having to find a different method of funding him and his office.

Q118 Chair: The other part of what the Commissioner was saying to us was that the nature of the work he was going to have to do was not particularly beneficial. It would be much more process-related and questioning of firms about their failure to make the appointment of a data controller or data protection officer, rather than going after egregious failings and carrying out advisory work to raise standards and achieve better outcomes. Not only would money be spent on a cumbersome process but it wouldn't achieve the outcomes which are desired.
Lord McNally: Indeed. I do think that we and the Commissioner are on the same page on this. The warnings that he has given from his vantage point are identical to the warnings that we have been giving to the Commission about the way they are going about it. There are just small things like wanting prescriptively to write in a specific 24-hour notice of a breach. That may be good guidance, but, if there has been a breach, it may be better to spend that first 24 hours trying to make sure that people are aware of it and that corrective actions are taken, rather than going through the tick-box of, "We have notified the Commissioner within 24 hours."
He has drawn attention to a range of practicalities for him that can be mirrored by the practicalities that will face companies in trying to match what we believe is an over-prescriptive regime. As I have said before, I am not pessimistic that we can't achieve success in getting this changed.

Q119 Mr Llwyd: I am pleased to hear that final remark. When one considers that we are dealing with a fairly well-resourced Information Commissioner's Office over here, how on earth is it expected that less well provided entities within the other European Union states are going to be able to comply? It is beyond belief really, isn't it? It is rather difficult to imagine how the thing is going to be workable without much simplification and amendment, which no doubt you are working hard on now.
Lord McNally: I don't think so. In a way, if they had the power—and they don't—to steamroll this through, it would prove a pyrrhic victory for the Commission because it wouldn't work. What we want is something that works.

Q120 Mr Buckland: I have this wonderful image in my head now, Lord McNally, of you haggling in the souk. Whether it is to buy a carpet or other item I don't know, but I have this great image. It is the right image, if I may say so. It is a very fair characterisation of the nature of negotiation. We shouldn't be shying away from the reality of it.
I want to look at some of the details of the proposed Regulation. I will start with Article 17, which is the so-called "right to be forgotten". It is a development on from the "right to erasure". It has been warmly welcomed and is seen as a step forward in terms of ordinary citizens being able to have their data removed from a database. Of course it is hedged with a number of qualifications, which again are entirely

understandable. Is there not a danger that expectations are being unduly raised by the use of such slogans as "right to be forgotten", whereas the reality is going to be somewhat different?

Lord McNally: Yes, is the short answer. That is why, even from the very early stages of this, we have suggested that "right to be forgotten"—which is a great headline and a good soundbite—is not practical. Anyone who knows how information goes round the world in this technology knows that. What we are hoping to do, again, is to make it clear that the individual citizen does have rights to get data expunged or changed, but what we don't want is to give particularly young people the idea that they can put things on social networks and that somehow they can recall it at will because they can't.

There are a number of problems with the provision. For example, it creates a somewhat misleading right that may encourage reckless posting of information in the mistaken belief that it can be recalled. The UK supports strong deletion rights, but the term "right to be forgotten" is unhelpful given the details of the provision. We might suggest a change in the name in order that it better reflects the rights that are actually given. The way you have presented it is the right approach. We will use the technology that does exist and the rights that we can build in to give people control over their information but remind them of the reality that this is a technology where a complete right to be forgotten is unattainable.

Q121 Mr Buckland: It may be best to keep it simple and just call it a "right to erasure"—just keep it as it is.

Lord McNally: Yes.

Q122 Mr Buckland: I turn to the question of the rights to access data of subjects—subject access rights—which is covered in general terms in Article 15. In particular, I want to look at the debate that is being held about the merits of charging—of organisations being able to charge people to access their own data. It happens already. A £10 fee is often levied. It is the Government's position that, unlike organisations such as *Which?*, the Government do not support access rights being universally exercisable free of charge.

At the same time the Government have their mydata programme, which aims to make it easier for consumers to have access to their data. How do the two positions sit with each other? Isn't there a contradiction between the Government's position on mydata and their attitude towards charging?

Lord McNally: There may be a slight rubbing up against the two objectives. As you have just said, the Government currently set a £10 fee for access. It is important to note that many organisations do not charge this fee; instead it serves as a useful filter to deter more speculative requests if those are problematic for the data controller. You had a similar discussion and debate when you came to freedom of information.

Chair: We came to a no-charging conclusion.

Lord McNally: This is a different issue from the mydata initiative. This would allow firms to sign up in order that data subjects can move their data around if they wish to. In each case we support the same principle of maintaining maximum flexibility for both the data subject and the data controller. Additionally, although there is a right to data portability in the proposed Regulation, we believe that this would be better suited to a consumer-focused internal market instrument.

I will be interested to see where we end up on this. As I say, the Information Commissioner does not want to lose an income stream. I don't know whether it is a filter and deterrent. As I say, you had the same argument with freedom of information.

Q123 Mr Buckland: It is slightly different. Let's take me. This is my data. It is my information. Why should I have to pay to have access to know what information about me is being held?

Lord McNally: That is a very powerful argument. I don't know whether either of my colleagues can comment.

Glenn Preston: The purposes are different. The subject access request as it is written into the current Directive and the Data Protection Act is about access to sensitive personal data. It is not usually for the purpose of changing your utilities provider, for example. The mydata initiative is focused more on that transactional level of data so that you can speak to your mobile phone company or gas company and say, "Give me this in a readable format that I can hand to somebody else who will give me a better deal." The purpose of that is quite a different thing from the vast majority of subject access requests that people are using for very different personal reasons. We can see differences between the two things that can justify the charging point that you make.

Tim Jewell: Similarly, there is the wider point. If one looks towards the front of the Regulation about the principles that inform the holding by other people of data about oneself in any event, they are relatively restrictive, aren't they? They are necessary for a specific purpose and only held in a proportionate way for as long as it is needed. Whilst it is quite right of course to say, "It is data about me", it is data which there was a valid purpose for that other person to hold for the duration that it is necessary for them to hold it for.

Q124 Mr Buckland: There is a worry amongst a lot of us that in various capacities we will have given personal data to organisations. Sometimes we tick boxes to make sure it is not shared; sometimes we don't—perhaps we are in a rush to do things. I know it is up to individuals to exercise a degree of responsibility, but it becomes difficult for the individual to know precisely where his or her personal data is being held, doesn't it? As Lord McNally properly concedes, there is a certain unfairness in seeking to charge people just to find out what should be their right to know about who or what organisation holds information about them.

Lord McNally: I think you are right. The concept of "This is my data" is very fundamental. As Mr Corbyn was saying, the bottom line with organisations that mine data and do profiling is that it is not their data;

it is the individual's. That has to be a very important principle in both drawing up the laws and in making sure that companies behave in a proper way.

Q125 Jeremy Corbyn: I would ask a short supplementary on that, and thank you for that point. If the EU draws up appropriate firewall regulations that prevent a supermarket chain or travel agent sharing information, what regulation could there be that somebody could base an internet provider outside the EU, collect information from commercial enterprises in the EU and then re-sell or re-advertise within the EU itself? Is there any way of preventing that?
Lord McNally: It is very interesting that you ask that question.

Q126 Jeremy Corbyn: Would you rather I didn't?
Lord McNally: No. What I would say to the Committee, quite seriously, is what I said at the beginning. We are at the dawn of a new age. We are going to find all kinds of problems that will be thrown up that will need fleetness of foot and flexibility to deal with. This goes back within the EU to how poorly-resourced regimes will handle this. What happens if some island in the Caribbean suddenly becomes a data centre, rather like some of them have become banking centres. Suppose you have companies that have data headquarters in regimes that can't possibly police them doing some of the things that you worry about.
My argument would be that that would strike me as a case for even greater international co-operation in dealing with some of these issues. I suspect they are issues that are coming down the track towards us in getting the balance right. That is why, in some ways, our argument for a slightly more flexible and lighter touch will allow us to be able to respond to some of these new challenges rather than having a rather sclerotic regulation that would be very difficult to change in response to new circumstances.

Q127 Jeremy Corbyn: The issue isn't just the big companies. In a sense, you regulate, and the big supermarket chains and so on would probably accept the Regulations; they would have to. It is not that difficult for an individual either to hack in and collect information on somebody's spending habits or use a rogue company to do it and access it via a Caribbean island or the Pacific or somewhere. Then they could set up a very attractive advertising opportunity to get through to a whole lot of individuals by e-mail, having illegally collected information on them. The individual receiving the advertising offers wouldn't even know where the information had come from in the first place.
Lord McNally: I think that is probably true. That is a gamble. We are really only at the beginning of being able to look at some of this properly. We can be absolutely sure that, just as we are working hard to set up a regime that will be beneficial to the citizen and to entrepreneurs to run honest companies in an honest way, there will be those who will be looking at how to abuse these systems and technologies. As I say, that is one of the challenges of twenty-first century Governments.

Q128 Chris Evans: We have heard from a number of industry groups who have been concerned about the Regulation. In particular, the BMA talked about concepts of patient confidentiality, while the Newspaper Society raised issues about freedom of speech. What are your views on this Regulation? Do they impinge on these key concepts?
Lord McNally: On patient confidentiality, again, there is a slight overlap with our own transparency agenda. It is something of which we are aware. We are aware that the individual citizen is very concerned that their medical records are not able to be disseminated in an improper way. Our conclusions are that, with the way the proposals are put, there are sufficient protections for medical records, but it is something that we will keep closely in view. Have the BMA given us similar concerns?
Glenn Preston: I don't think we have had them explicitly expressed to us directly. We do think the provisions in the Regulation are relatively strong on this particular point.

Q129 Chris Evans: Are you sure about that? In front of me I have something that says, "the BMA has serious concerns that Article 83 appears to permit the processing of health data, in identifiable form, for research purposes without any reference to consent."
Glenn Preston: That may have been in evidence to this Committee.

Q130 Chris Evans: Is that something they have said to you?
Glenn Preston: Not that I am aware of, but I don't want to say for definite that they haven't said it.
Chair: It is evidence to us, which we can certainly let you have.
Glenn Preston: It is evidence to the Justice Select Committee. That would be extremely helpful.

Q131 Chris Evans: Are they right to say that Article 83 appears to permit the processing of health data? If so, what protections are in place?
Glenn Preston: I think we should take this away from this session, but our take on the Regulation as it is drafted is that it already requires or has a classification for special category of personal data. There are specific measures in there that talk about how you safeguard that. There is also an exemption for the "right to be forgotten" for data concerning health, again subject to certain conditions and safeguards. It is quite well provided for in there. It sounds to me, on the basis of what you have just read out, Mr Evans, that we will need to have a specific discussion with the BMA to inform our negotiations in the working group in the Commission.

Q132 Chris Evans: I am quite concerned that the BMA have sent some evidence through to us but haven't sent that to you, and you will be framing the Regulation. Obviously medical records are extremely sensitive. What level of safeguards would you like to see in place before they were released to researchers?

Glenn Preston: We feel that the safeguards written into the Regulation at the moment are significant.

Q133 Chair: The key issue is whether there can be any use of identifiable information without consent. The principle we have had hitherto is that identifiable information requires patient consent. This seems unclear in the Regulation.

Tim Jewell: If it is of assistance, it may be worth simply pointing out, of course, that there are two Articles that are relevant to this question. The first is that which relates to health itself, which is Article 81. That is where the person-specific questions most generally would arise. There is a first level of protection in relation to data relating to health.

The Article that you mentioned is Article 83, which is processing for historical, statistical and scientific research purposes. There, too, there is a hierarchy of protections, which begin with consent, which you mentioned, and then there are some narrow exceptions. As Mr Preston suggested, one has to look at the two together. It is not a single layer of protection. One starts with a health protection, and then only if the additional protections in Article 83 kick in can you process for historical, statistical and scientific research purposes.

Q134 Chris Evans: But it is still identifiable, isn't it? The research is still identif—I am struggling here a bit with the word "identifiable". I didn't put my teeth in.

Tim Jewell: As I understand it, it would be very much the exception. I can't think of any instance of aggregated medical research of that sort, which is where the benefit is to be obtained, where an individual would be identifiable from the data itself. As I say, there is a consent requirement in Article 83 too where that would be requested, but it requires some more detailed consideration.

Lord McNally: It is a warning well taken because, as you rightly say, that is something where people are really very sensitive. I know that because the Transparency Board had a similar exercise when we were discussing releasing data from the national health service. Immediately there were stories in the newspaper that the Government were about to sell medical records and so on. There is a difference between data that is absolutely anonymised so that it can be used for proper research and assessment, but, even there, you have to be extremely careful that some of these clever chaps can't cross-reference various sources of information to identify individuals. It is an awareness of the threat. Certainly we will take extreme care to make sure that medical records are properly protected under any proposals.

On the freedom of speech issue, Article 8 states very clearly that the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression should be open to exemptions or derogations.

Again, I ask my colleagues who are dealing with this daily, have we had from the media specific concerns on these? It does seem to me that Article 8, chapter 1, is very specific on this.

Glenn Preston: It pretty much replicates what was already there in the existing Directive. There has not been a great call for us to change or amend that. Certainly we don't have any expectations that that is high on the list of things that people have been concerned about.

Chair: It is around the "right to be forgotten". One can imagine circumstances in which there would be a legitimate public interest in not allowing something to be forgotten.

Q135 Jeremy Corbyn: I want to raise a point on medical records. There have been reports recently of a number of hospitals outsourcing hospital letters to India. In the case of my local hospital, apparently 90,000 such letters have been drafted in India. They are e-mailed back to the UK, allegedly anonymised, and then the names are added in in the UK and the actual printed letter produced and sent out. Clearly, India is not within the EU restrictions and couldn't be, for obvious reasons.

Whilst I am not suggesting there is any foul play at the moment or anything has gone wrong, there is clearly a danger, with a huge amount of medical information of a very large number of people being held by internet providers in a completely different jurisdiction. It is not beyond the wit of somebody with a devious mind to try and get hold of the patient name information and then you have a ready-made source of pressure, advertising and all kinds of things. It could become extremely dangerous. I am not suggesting anything bad has happened, but I think it is something we need to be aware of.

Lord McNally: I can only say yes. We go back to this eternal vigilance. As you say, we are dealing with technologies that make things possible and it is very important that we are alert to possibilities.

Q136 Chris Evans: I want to probe a bit on social media. The world has gone mad for social media. There has been an argument by the Brussels European Employee Relations Group that says that this Regulation is too focused on social media and it is lumping in things that every business has to deal with in terms of processing—employment records and so on—with social media. Do you agree with that premise that this is too focused on social media?

Off the back of that, my second supplementary question is: do you think the Regulation in general will keep pace with future technology or will we be revisiting this in future?

Lord McNally: Yes. I met the head of one of the big Japanese technology companies. Trying to show my credentials and that my technology was up to speed, I said to him, "You know, sir, I suspect that a lot of what we are trying to deal with now will be out of date in 10 years." He said, "Three years." Future-proofing for domestic or international purposes in this area is an ambition that is beyond us all. We have to keep the flexibility within what we are doing to be able to adjust to new circumstances.

You are right that some of the proposals seem to be over-concerned with social media, and the "right to be

forgotten" slogan is part of that. Again, what we are really looking for is a coherent set of rules that will apply for all data controllers, which is simple and clear to understand and apply, but with a realisation that we are moving in an age of rapid change. I suspect that we will all be coming back to this as it develops.

Q137 Chair: One of the ways in which the Commission envisage that the change will be coped with is by delegated Acts. The Government and others have expressed some concern about the amount of delegation and therefore the departure from the decision-making processes that that Regulation requires and would involve.
Lord McNally: Yes. The House of Lords gets very excited about Henry VIII clauses in Bills. These look very much to us like Henry VIII clauses. We share the House of Lords' disapproval of Henry VIII clauses where they can be avoided. This should not be taken as a statement of Government policy about future legislation.

Q138 Chair: I would like to feel that it is a statement of Government policy.
Lord McNally: We have made it clear that we are not in the business of signing blank cheques for the Commission. We understand and appreciate that there is concern about mission creep by the Commission. Therefore we will resist such clauses in the Regulation.

Q139 Chair: What do you see as the time scale for negotiation and eventual decision making?
Lord McNally: The Commission have a very ambitious time scale. They want to see substantial progress during the Cypriot Presidency, which is on now, and conclusion during the Irish Presidency, which is the first six months of next year. To be fair, the Cypriots have given priority to these negotiations and devoted the time to it, and as far as we understand, the Irish are taking a similar approach, but whether they will be successful or not, I don't know. We are negotiating to get results, not to fit into a timetable. We are certainly not on a go-slow or anything else. We simply want to get the best practical result from the negotiations.

Q140 Chair: I suppose the worst outcome for business would be a bad result of negotiations. It is in businesses' interests to get things cleared up as soon as possible so that they know the position.
Lord McNally: Yes; this is always true. Obviously, because there is pressure to get this settled before the present European Parliament term ends in 2014, and because the negotiations have been going on a number of years now, there is a push to try and get a satisfactory outcome. But that always cuts two ways. If the Commission want an early result, then it may well be that they have to make substantial concessions to get the kind of outcome that we want.
As I say, what we want is a lighter-touch and more flexible system, which can give the benefits of harmonisation without the downside of over-bureaucratising and over-burdening business, yet keeping very much in mind the kind of things that Mr Corbyn has been talking about. There are real threats out there to the citizen that also have to have their proper place in this exercise in legislation.

Q141 Chair: We will be reporting on this matter very shortly. I anticipate it will be at the beginning of Parliament's return in October. We are very grateful to you, Lord McNally, to Mr Preston and Mr Jewell. We are also very intrigued to know to which of your ministerial colleagues you have passed this particular parcel.
Lord McNally: I was just going to say that it would be rude of me not to mention that I am going to Brussels tomorrow. One of the other points I should make is that this is a joint determination exercise with the European Parliament. That is why I am going to have these meetings with the MEPs. Therefore, at midnight on Wednesday I will be handing the torch over to Helen Grant, who I think is known to this Committee.
Chair: Indeed. She is a much respected former colleague. Perhaps the analogy of the torch is a more congenial one than that of the parcel. Thank you very much indeed.

Written evidence

Written evidence from the Association of Chief Police Officers

1. Introduction

1.1 This submission is from the Association of Chief Police Officers (ACPO) and has been discussed with the Serious Organised Crime Agency (SOCA). Both organisations have fully participated in the Ministry of Justice call for evidence on proposed EU Data Protection legislative framework and were included in the Government response. The summary of responses for the latter was published on 28 June 2012. Furthermore we have been working extensively with the Home Office and the Ministry of Justice assisting in the development of a high level government response with regard to the proposals within the Data Protection Regulation and Directive.

1.2 For the purposes of this submission, ACPO will retain a focus upon the strategic ramifications of the proposals and the impact that they may have upon the police service. We have the highest regard for the principles of Data Protection and the critical impact this has upon individual rights and protections. Clearly, the trust of citizens and the free flow of data are essential in order to sustain transparency and accountability. Of course this has to be seen against a backdrop that policing and law enforcement by its very nature has to maintain a degree of confidentiality in order to ensure the continuance of public safety, the arrest of offenders and the administration of justice. These proposals are made at a time when the movement of European Union nationals across borders within the European community has never been easier. There is no doubt that criminals are exploiting this situation in order to continue committing crime and to evade capture. Exchange of data between police and partner agencies has a clear relevance in both the prevention and detection of such criminal activities.

2. Key Questions

Q—*Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

2.1 In broad terms, we are supportive of the Regulation and recognise that it focuses on use of data by private sector and other organisations outside of law enforcement. The Data Protection Act, although described as inelegant legislation, still requires organisations to comply with relatively simple requirements to manage information in such a way so that it is accurate, relevant, proportionate and only shared with those who have a legal reason to hold it. Nonetheless we recognise that across Europe a similar position may not exist.

It is also fully understood that the technological advances that have been made over the last ten years, especially in areas such as biometric information have been immense. There is a clear need to ensure that Data Protection legislation is sufficiently broad to engage with these new capabilities, in such a way as to clearly inform Data Controllers and processors as to their responsibilities and liabilities. We are however concerned that in seeking to achieve the right balance, there is a risk that added bureaucracy may impinge the ability of the law enforcement agencies to fulfil relatively simple business processes which are aimed at protecting vulnerable persons. For example, a requirement to obtain explicit consent from a victim of crime concerning passing their details to Victim Support may lessen the opportunity to provide a critical service at a time when individuals are in need of care. We are further concerned about the recognition of common law systems, in particular the impact that this may have upon the lawfulness of processing. For example, information that is held on sex offenders and shared with other organisations and interested parties is achieved using our common law powers. It is not clear how the Regulation may impact upon this area. Whilst we understand that under the current Data Protection Act provision, the current charging regime of seeking up to ten pounds for a Subject Access request may be perceived as a financial impediment. In our opinion, it may prevent abuse of the process. The experience of the Police Service in this area is one of significant concern. Such requests are handled centrally by the Association of Chief Police Officers Criminal Records Office (ACRO) and at present they process in the region of about 60,000 applications per year. In their professional judgement, up to 90% of these applications are what are referred to as "enforced Subject Access" and represent pressure being applied by employers for individuals to undertake a Subject Access request concerning their criminal conviction history in order to secure a post. This process is clearly not undertaken in the spirit of the legislation and ACRO advise individuals that such a disclosure is excessive and that they should seek a basic disclosure which is available through Disclosure Scotland. ACRO are also aware that this abuse is promoted by some local authorities in order to potentially reduce their costs, for example when dealing with annual issue of taxi licences, removal of any fee as proposed within the Regulation may well lead to further abuse. It should be noted that Section 56 of the Data Protection Act 1998 provides for such actions to be prohibited but this Section has yet to be enacted.

2.2 The right to be forgotten should clearly sit within Data Protection principles concerning retention of information and excessiveness. We are of the view that there are some areas of our business including the retention of criminal records for up to 100 years which are critical in order to fulfil the responsibilities of the law enforcement agencies and the courts. This should not be confused with disclosure where there is full support for the rehabilitation of offenders and the opportunity for those who have committed crime to have a

fresh start. These principles were clearly articulated in the Chief Constable of Humberside and others vs. Information Commissioner (Case No: C1/2008/2124).

It remains a matter for a Judge to determine the relevance of such historical criminal convictions which often when added to other information may create a picture of an individual that may otherwise have not been so clear. Consideration will also have to be given to those areas where as a matter of government policy, more data is being provided into a public environment than may have been forthcoming in media coverage of court proceedings. For example, a number of police forces now proactively place details of offenders on public facing websites who have been convicted of serious crimes. Once these have entered an internet environment, it is unclear how they can be successfully redacted. We believe that these proposals have more to do with the potential exploitation of young persons using social media and essentially exposing more of their personal information than they would wish. It is known that these sites are now often searched by employers who are seeking to validate the behaviour of a potential employee. At the same time we are supportive of Data Protection by design, in particular to ensure that in the use of our technology we use capabilities sufficient to achieve our requirements without being overtly invasive. For example, we understand why the use of certain x-ray equipment in port areas which reveal the human form might in the future be replaced with screens that merely indicate that the individual requires a personal search because of material found within a certain area of the body.

2.3 The service seeks to hold personal data which is sufficient for us to progress our law enforcement responsibilities. We are concerned that requirements within the Regulation which introduce obligations for Data Controllers and Processors to maintain documentation of their processing operations will create a further level of bureaucracy which will be both complex and costly. Moreover, this appears to move away from current arrangements that have been put in place to ease the exchange of information between organisations or which allows a nominee to agree national sharing agreements on behalf of Data Controllers in Common. For example, the agreement for 10,000 police officers from across 43 different police forces to have their personal data collected by the Association of Chief Police Officers and then shared with LOCOG so that they could be accredited to enter Olympic venues only required three signatures.

2.4 The Police Service has already engaged the concept of Data Protection Impact Assessments and have undertaken these with regard to a number of national initiatives, for example the introduction of Crime Mapping. However we have learnt that it is critical to approach each national programme of work slightly differently. The concept that one hat will fit all which is a feature of both the Regulation and Directive again risks adding considerable cost and bureaucracy to a system that is relatively straight forward and simple to achieve.

2.5 A feature of the European proposals is the belief that Information Commissioners should fulfil a regulatory role which is divorced from any concept of providing guidance and best practice.

This structure is wholly alien to the system that has developed in the United Kingdom where the Commissioner has, over a number of years, produced excellent guidance material which has helped shape compliance and informed agencies on how to evidence their strategic information sharing obligations. The proposal that prior authorisation and consultation should be obtained from the supervisory authority before processing the personal data in our opinion would place an impossible burden upon the Information Commissioners Office, would clearly impact upon the ability to sustain the guidance element of his current activities and inevitably lead to a more remote oversight of Data Protection compliance. It is our opinion that this would seriously erode a process that works add huge costs to the Commissioners Office and impede the opportunity for organisations to freely seek advice. This could also have an impact upon the willingness of organisations to self report breaches and to act with transparency and accountability to his office. It seems inevitable that additional cost incurred by the Information Commissioner's Office will be passed on to organisations when they register on an annual basis with the ICO or will be recovered through the implementation of enhanced finds.

2.6 The prescriptive nature of both the Regulation and Directive is evidenced again with regard to the proposals concerning the designation of Data Protection Officers. As a matter of principle, the focus should be upon compliance not how an organisation structures itself in order to deliver compliance. At present appointed Data Protection Officers are not consistent with information management regimes contained within the Police Service. As part of the austerity programme, roles have been converged which often cover a range of portfolio responsibilities focused upon Freedom of Information, Data Protection and security. This does not mean that we have lost our focus upon adhering to the legislation but we have made management decisions on how best to deliver our compliance strategy.

Q—*Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

2.7 The proposed directive focuses on law enforcement and judicial authorities and our understanding is that it will replace the European Union Data Protection Framework Decision 2008. What has yet to be made clear is whether the Directive will apply only to the UK in circumstances where data is being shared for the purposes

of an EU instrument and not when we are sharing information purely for domestic reasons. Clearly, if this were to impact on day to day exchange of information between forces, the ramifications would be significant and come at a high cost. We would make the following observations with regard to the critical articles within the Directive that cause us most concern. For the purposes of this submission we would prefer to focus upon the specific articles so that we can adequately articulate the key issues. It can be assumed that we are supportive in all other areas.

— Article 3; we have concerns over the new definitions which are included in this article such as "genetic" and "location data". It is important to recognise that such information often applies to suspects and not necessarily individuals who have been indentified. We would argue that the focus of Data Protection should be upon single individuals and not broader information that may be less specific. We also feel there is a fine balance between localism and the provision of information on a geographic basis which allows local communities to be aware of crimes being committed in their area through crime mapping and more specific location data which might be attributable to the location of a mobile phone. We also note that Article 3(12) relates to data concerning health and it is our view that we need to ensure this does not constrain dissemination of information where an individual's state of mental health potentially raises issues about them being a danger to themselves or the public.

— Article 6; in a policing environment, there has to be explicit distinctions between intelligence, it's grading and targets who maybe identified as a result of this process. The article must not be too prescriptive and provide sufficient flexibility for processing data which may not be necessarily accurate and reliable.

— Article 7; with regard to the lawfulness of processing, the Police Service often relies on common law policing powers to process information, for example information regarding sex offenders. Moreover, we are concerned about the prescriptive nature of the words being used in the Directive, especially those associated with lawful processing. Policing in the UK uses broad terms such as protecting life and property and bringing offenders to justice. Sustaining common law principles will be a critical factor.

— Article 8; whilst a sensitive issue, it needs to be understood that investigations of criminality focusing on specific communities is sometimes necessary both for their safety and in order to identify offenders. For example, the recent cases of males of Pakistani descent recruiting vulnerable white juvenile females to become prostitutes.

— Article 17; we would want to be sure that such disclosure was in accordance with national rules. Moreover, it should not be used by individuals who have potential criminal proceedings pending against them as a method to obtain information on the current state of those investigations. This is currently an issue with areas where independent complaint processes are subject of deliberation.

— Article 10; The observations we have made about Subject Access with regard to the Regulation apply equally to the Directive.

— Article 18; we are very concerned that the intention of the Directive is to place very significant burdens upon Data Controllers. Moreover it is assumed that the content of the article assumes that "one size fits all". This is not consistent with the realities of cross border data processing or the management of criminal information.

There is a risk that such an approach may create barriers which hinder the ability to conduct effective intelligence analysis or to create excessive burdens on law enforcement agencies. Finally, we do not think that the current proposals have been through a process where costs have been correctly assessed. Affordability should be a feature of proposals being promulgated against the backdrop of austerity measures within the public sector.

— Article 19; we again believe that the measures in this article are to prescriptive and that compliance should be the aim and not the mechanism employed to achieve a lawful response.

— Article 26; Although this is focused upon the responsibility of the Information Commissioner, we believe that the requirement for consultation will lead to long delays and may well impact upon the delivery of policing.

— Article 30; this again demonstrates a possessively descriptive approach by the European Commission towards the delivery of compliance under the directive. It may also demonstrate a difference between mainland Europe thinking and that that exists in the UK. The Information Commissioner has always been a source of advice and guidance promoting best practice and ensuring a healthy relationship between Data Controllers and his office. This has significant benefits with regard to reporting of incidents and promotes confidence in the application of good governance. To specify that an organisation must have a Data Protection Officer and then to list the role and function of that individual is clearly not synonymous with the current approach. We believe that this is because in Europe, Commissioners act purely as Regulators leaving it to organisations to seek legal advice on how they should comply with the directives. If an organisation fails in this endeavour then the regulator is there to identify failure and impose a fine. We would strongly advise that this approach is not consistent with best practice and that if possible, an amendment to the article should be sought.

In summary, we believe that providing the Directive does not impact upon domestic processing, that the impact will not be severe. However, we do not underestimate the new levels of bureaucracy and cost which the Directive will cause to fall upon the police service. We also take the view that the changes which impact upon the Information Commissioner will change the governance procedures through his office causing it to be more remote, less able to provide guidance and impacting upon the continued development of good practice.

Q—*Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

2.8 We are supportive of the next steps being proposed by the UK Government. We recognise that these deliberations will take place over the next two years and believe it is essential that the proposed Regulation and Directive are implemented having had the benefit of a full cost assessment and ensuring that the correct balance has been struck between the rights of the individual and the needs of the law enforcement agencies.

2.9 We are pleased to be able to contribute to this debate and would be very happy to provide verbal evidence if so requested. The contacts in our organisations are as follows:

August 2012

Written evidence from Microsoft Ltd

1. *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

Microsoft welcomes efforts to strengthen and harmonise the EU's data protection regime. Our company's greatest asset is customer trust and our technologies are developed with data protection in mind. Our priority is to protect personal data in an age where we have ubiquitous connectivity, pervasive online business and social networking, and flows and storage of information all over the world on all kinds of computers and devices.

As we know from our direct experience, the challenge before us lies in protecting Europeans' privacy and at the same time enabling innovation. Achieving this requires that we strike a careful balance. On the one hand, companies that process data must be transparent about their processing practices and be responsible and accountable for applying high standards of data protection. But at the same time, the EU Regulation should not dictate in a highly prescriptive way how privacy protections are to be implemented, nor should it introduce new burdens on controllers and processors that ultimately do little to advance privacy.

Instead, organisations should be given flexibility to develop privacy protections that suit the circumstances involved, and should be given strong incentives to innovate to provide the strongest possible protections. And where organisations fail to adequately secure and protect the personal data in their care, they should face meaningful penalties.

The proposed Regulation takes important steps forward in this regard. For example, the proposal includes measures requiring that organisations design technologies with privacy in mind, are transparent about their processing activities, and remain responsible for how they use personal data. The proposal also helpfully addresses inconsistent rules and interpretations across the 27 EU Member States via, for example, the "one-stop-shop" approach.

However, other proposals need refining to ensure that the protections they offer are both strong *and* workable. For that reason, we think some amendments to the Regulation may be appropriate, among them in relation to:

- *International data transfers:* The Regulation introduces important new mechanisms to facilitate the secure flow of personal data, including in the cloud. These mechanisms include new rules on "standard" contractual clauses. We welcome these measures. But Microsoft also believes that cloud processors and others should be encouraged to go *beyond* the "baseline" safeguards set out in the Regulation in certain contexts. Where controllers and processors have practical experience that suggests that *additional* safeguards are appropriate to protect data, they should be incentivised to adopt these safeguards.
- *Processors and controllers:* Consistent with the existing EU framework, the proposed Regulation continues to allocate responsibilities between "data controllers" and "data processors." Because controllers and processors have different obligations and liabilities, it is *key* that organisations understand when they are a controller and when they are a processor. The proposed Regulation would distinguish between these roles by defining "controllers" as those who are responsible for determining the "*purposes, means and conditions*" of processing. But with the evolution of new computing models, processors are playing a greater role in determining the means and conditions of processing. As a result, the line between controllers and processors is blurring. We propose an amendment that we believe will help to clarify what role a given entity is playing depending on their involvement in the processing of personal data. Specifically, our amendment would make it clear that the controller is the one who determines the *purposes of processing*.
- *One-stop-shop:* Today, companies that operate across Europe are subject to multiple and divergent national data protection regimes. To address this problem, the Regulation introduces a "one-stop-shop," based on the location of an organisation's "main establishment". This approach offers a significant improvement over the existing, fragmented regime. Less helpfully, however, the Regulation applies *different* tests for controllers and processors in determining their country of main establishment. As with the rules defining the terms "controller" and "processor", the approach to "main establishment" does not reflect how many organisations currently operate. Today, in practice, many controllers also act as processors. Proposing a test for main establishment that subjects controllers and processors to *different* tests means that those controllers that also act as processors will be once again subject to multiple national authorities, and will find themselves unable to benefit from the one-stop-shop. We propose an amendment that would subject controllers to the *same* test as processors when they are playing both roles.
- *Delegated acts:* The Regulation includes 26 provisions conferring power on the Commission to adopt delegated acts. These provisions should be significantly reduced. For example, many of these provisions deal with essential elements of the law. These essential elements should be addressed in the Regulation itself, not left to secondary law-making by the Commission. Other delegated act provisions give the Commission power to prescribe technical formats, standards and solutions—threatening to replace industry innovation with regulatory intervention. Our proposed amendment would delete those provisions that relate to essential elements of the law and/or that are better addressed through innovation. Finally, as the Article 29 Working Party and the EU Data Protection Supervisor have noted, the delegated act provisions do not include a clear timetable for implementation. Our amendment would also introduce a deadline for the adoption of delegated acts.
- *Administrative fines/sanctions:* Data protection obligations are only effective to the extent they are enforced. Consistent with this view, the Regulation includes strong sanctions for violations. Less helpfully, however, the Regulation takes a "one-size-fits-all" approach, and could be read to apply the same sanctions to deliberate, flagrant violations of the rules as it does to violations that are merely accidental. This means that a company that inadvertently fails to use a specific electronic format when giving a customer access to his information could face the same penalty as a company that repeatedly and intentionally collects and processes data about individuals without informing those individuals about its activities. To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for truly bad actors.

2. *Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

Because the focus of the proposed Directive is on processing by law enforcement and judicial authorities, its rules generally do not apply to Microsoft's activities as a data controller. Importantly, however, the Directive includes several provisions relating to *processors* that would apply to Microsoft when providing cloud services to these authorities. Many of these provisions are similar to the processor-related provisions in the draft Regulation; for example: data breach, DPAs, impact assessments, judicial redress, processor contracts, documentation and record keeping.

As with the Regulation, the Directive gives the Commission broad authority to propose secondary legislation (generally subject to veto by the Parliament and Council) in a very wide range of areas. This mandate is intended to help to promote harmonization—but at the same time it may also result in greater and more detailed regulation and mandates.

Unlike the Regulation, which would apply directly in all 27 Member States, the Directive would have to be transposed into national law—creating the risk of divergent national implementations. Despite this risk, the Directive does not include rules specifying which Member State's law would apply to a given controller or processor's activities. Similarly, the Directive does not state that controllers and processors based in the EU would be subject to the authority of a single Member State DPA ("supervisory authority"). (*See* Article 47 (Competence)).

The impact of the lack of an applicable law rule in the Directive is unclear. On the one hand, the Regulation provides that processors are subject to a single supervisory authority in the country of main establishment—and it may well be that this rule applies even where a processor is processing data on behalf of law enforcement or the judiciary. But this is not clear from the Directive. If Microsoft processes relevant data and is subject to this Directive, it clearly would be preferable to have an explicit statement in the Directive that processors are subject to only one law and one supervisory authority. The current draft does not provide for this.

It is unclear how the provisions of the Directive regarding international transfers are intended to apply to processors, but they would appear to prevent a processor such as Microsoft from transferring relevant data outside of the EEA for operational or other technical/efficiency purposes. Similarly, it is unclear how Article 60 is intended to apply to processors, but it appears to create an unhelpful barrier to *intra-EU* transfers of data.

3. *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?*

We welcome the steps the UK Government proposes towards negotiating for an instrument that will offer an adequate level of protection, not overburden businesses, the public sector and other organisations, and that will encourage innovation and growth.

What is more, we would like to reinforce the need for negotiations towards achieving a proportionate and effective system of administrative penalties. Robust rules on the books are a key element of a strong data protection regime. But effective enforcement of those rules is equally important to ensure that companies take their responsibilities seriously. To be balanced and effective, the Regulation should ensure that the most punitive sanctions are reserved for *truly bad actors*. Furthermore, legal clarity is vital for ensuring that companies are able to comply, and consistent with this view, companies should not be subjected to fines that are subjected themselves to delegated acts.

August 2012

Written evidence from the Federation of Small Businesses

The Federation of Small Businesses (FSB) would like to take the opportunity to respond to the above-named inquiry.

The FSB is the UK's leading business organisation. It exists to protect and promote the interests of the self-employed and all those who run their own business. The FSB is non-party-political and, with around 200,000 members, it is also the largest organisation representing small and medium-sized businesses in the UK.

Small businesses make up 99.3% of all businesses in the UK, and make a huge contribution to the UK economy. They contribute up to 50% of GDP and employ over 59% of the private-sector workforce.

The FSB recognises that data protection rules need to be updated in an age of free flowing data through social media and ecommerce, both of which are increasingly used by small businesses to develop their business.

However, the Commission's new policy makes no distinction between normal business procedures and activities that carry more risk with regard to data handling. This means the cost of the new obligations would also need to be borne by low-risk businesses.

Therefore, the two main points that we would like to emphasis in our submission are:

- That the regulation as proposed will introduce additional, and in some cases, unnecessary burdens on small business at a time when they can least afford whilst trying to support economic growth and job creation and not necessarily result in better data protection outcomes; and
- That the Committee encourages the UK Government to ensure that the final Regulation is risk-based, low in administrative burden, and is geared towards the day-to-day practice of data handling.

We trust that you will find our comments helpful and that they will be taken into consideration.

1. Introduction

1.1 The most important aim of the EU Data Protection proposals in the current climate should be that they enhance, rather than hinder, economic growth. The FSB accepts that updating of existing legislation is necessary to allow for technological advances although we question whether the EU proposals achieve this. The FSB is concerned that the Regulation, as it is currently drafted, will place additional burdens on business. Considering the size of the small business community in the UK (4.5 million) any additional costs for individual businesses could result in significant increased costs for businesses more widely. That said, we do accept that protecting the rights of individuals with regard to the data held by businesses is an important aim. However, we are concerned that these additional burdens on business will outweigh any benefits to be gleaned by many members through the harmonisation of EU legislation in this area.

1.2 The FSB would echo the comments made by the UK Information Commissioner's Office in their initial analysis document (27 February 2012) that points to the fact that a detailed and prescriptive instrument does not necessarily bring about a better data protection regime.

2. Question 1

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

2.1 The FSB supports a balance between adequate data protection for individuals and the need for businesses to gather personal data and to handle them in the least burdensome way. However, the new rules place a greater focus on the data protection rights of individuals than before. This means there could be more burdens on businesses if individuals start exercising those rights.

2.2 The rights in Chapter Three (Rights of the Data Subject) could mean significant burden for small businesses. These rights are for example: the *right to be forgotten*, strengthened rights to access your personal data (*Subject Access Requests*), the right to transmit personal data in a structured electronic format (*data portability*), *data protection by design* and *by default*, and the burden of proof for a data subject's explicit consent to the processing of their personal data.

2.3 Below is an overview of the potential burdens for companies that handle any information relating to a data subject.[1]

Art. 4: Definitions

2.4 We have broad concerns that the new definitions of "personal data", "processing" and "controller" will increase the remit of data protection and take this too widely, risking capturing more businesses and more scenarios within the legislation and as a result, increasing burdens to their business process and procedures. It also appears currently that normal business processes would be affected, ie even businesses that do not handle data as an important part of that business.

Art. 7 and art. 4: Consent

2.5 The introduction of *explicit* consent could mean an extra burden for businesses. Ecommerce businesses will have to adapt their websites to ask for consent to gather data.

Art. 12(2): Period to reply to subject access requests

2.6 Under the new Regulation a business will have to reply to a subject access request within one month. This is now 40 calendar days.

Art. 14: Information duties

2.7 We are in principle happy that the Commission will take appropriate measures for MSMs (Micro, Small and Medium-sized businesses) with regard to some provisions of this article. However, we don't know when and how this will work out. This means that as long as the delegated acts haven't been agreed, small businesses will have to fully comply with art. 14 as currently drafted.

Art. 15: Abolishment of the fee for subject access requests

2.8 Previous feedback from FSB members indicated that the Subject Access Request (SAR) fee, although in some senses only a token fee of £10 given the amount of time and resources taken to follow up such requests, was actually quite helpful for businesses in a) preventing time wasters and b) actually recouping some costs. We would prefer that this fee, albeit token, is reinstated.

[1] We make the assumption that the majority of small businesses process personal data in some way or form, and that an increasing number of them are becoming data controllers as their businesses develop in a digital environment, where data is the new currency.

2.9 We are also concerned that the Commission will further specify criteria and requirements for the communication of the personal data to the data subject, because it is not clear what this would involve.

Art. 17: The right to be forgotten and to erasure

2.10 This article is the crux of the whole data protection framework. We acknowledge the right to have your data deleted as there are significant consequences if personal data fall in the wrong hands. A paper copy is easily shredded. However, due to the easy reproduction and migration of digital data, it will be difficult in practice to make sure all data has been truly deleted from all platforms. We have no problem notifying third parties we have given data to, but a business' responsibility should stop there as they would be unable to ascertain that the party in question really deleted the data Businesses need protections in circumstances when they may have taken "all reasonable steps" to erase data but cannot be aware of any additional copies with third parties that they were not informed about.

2.11 We would also like to see a general provision in the Regulation that people should be mindful of what personal data they put online themselves. Smart phones are now ubiquitous, and are rapidly multiplying data streams. Data could flow freely over the internet and their source can be difficult to establish.

2.12 Therefore, we call on the Commission to rethink article 17 in the light of the fact that data is a currency in an un-policed space, and that the question of responsibility cannot be laid just on businesses only.

2.13 The requirements in articles 14–17 mean another layer of bureaucracy for businesses. Therefore, consideration should be given to attaching costs to and reducing the business impact of some of these measures. Abolishing the fee for a subject access request will in fact mean a net burden increase for small businesses. Also, people could misuse this right by massively asking for their data in the same way cyber attacks are carried out. This could lock up business systems and overload businesses.

Art. 18: Data portability

2.14 This article could potentially be very burdensome for small businesses if lots of people exercise this right at the same time.

2.15 Furthermore we are concerned that businesses will be forced to change the electronic format they use for providing the data subject with their data when the Commission issues an implementing act with regard to article 18(1).

Art. 22: Responsibility of the controller

2.16 We are happy with the exemption for MSMs from art. 28 (keeping documentation) and from art. 35 (Data Protection Officer). We are also happy with the intention of the Commission to have special measures for MSMs with regard to security requirements (art. 30) and with regard to a data protection impact assessment (art. 33). However, we ask the Commission to involve businesses at an early stage when designing special measures.

2.17 For small businesses that do not fall under the exemptions or qualify for special measures, we would call for a common sense approach that placed the emphasis on appropriate compliance procedures for small businesses. This should not necessarily equate to elaborate and large quantities of paperwork and documentation.

Article 23: Data protection by design/default

2.18 The FSB supports the theory here, but would call for the proposals to be applied in a proportionate way to small businesses that is appropriate to the risks that they are working with in their business. It may not be appropriate for small businesses processing small amounts of data to buy in expensive software in this regard.

Art. 28: Documentation

2.19 We welcome the exemption from this article for businesses that process personal data only as an activity ancillary to its main activities. MSMs that process data as their core activity will need to adapt their systems and build in a documentation mechanism for all processing operations. This will mean high costs. We are therefore concerned by the implications for small businesses of this article and agree with the ICO's observations in that:

> *"Again, there is too much emphasis on mandating the bureaucracy of data protection when the objective of the Regulation is the protection of personal data in practice rather than the creation of paperwork".*

Art. 31: Notification of personal data breach

2.20 The new 24 hour notification period for data breaches (eg a business would have to inform every present and past customer) gives additional administrative burdens to businesses. The trigger point for such a notification should be the estimated impact a breach would have on the data subject(s). It is not in anyone's interest that unnecessary and inconsequential breaches are reported. A 24-hour time limit is completely inflexible and we would suggest alternative wording such as "without undue delay" to give businesses the flexibility need.

2.21 Furthermore, we regret that breaches of data that are professionally encrypted to a high standard also have to be notified. This is disproportionate and punishes businesses who take a sensible approach to data protection.

Art. 33: Data protection impact assessment

2.22 We are aware of good intentions here, particularly for businesses processing data in "risky" or sensitive scenarios, but we are concerned that this will be too onerous and costly for small businesses to implement. We note from the EU Commission impact assessment document that it is foreseen that small businesses are exempted from the relevant article (33) by Delegated Act. We think that this exemption should be cited in the proposal itself. This means that, as the proposal currently stands, small businesses face data protection impact assessments at a minimum cost of £12,000.[2]

2.23 We appreciate that there are small businesses that process large amounts of data and that an assessment may be useful. However, on the whole, we believe that greater thought should be given to how this measure will actually play out in practice in small businesses and whether it will actually achieve the desired results. We believe that this should be implemented in a light touch way if it is to go ahead. It will also depend on how "risky processing" is interpreted.

Art. 35: Data protection officer

2.24 We are pleased that common sense has prevailed and that the proposals state the requirement for an independent data protection officer will not apply to businesses with fewer than 250 employees. We think that this is a sensible decision. However, we are aware of debates around the proposals that point to the fact that size of businesses should not be the only factor in determining the application of the DPO. The FSB accepts that there are some businesses with small numbers of staff that process large amounts of data. However, for these types of businesses the DPO should not be mandatory and there should be sufficient flexibility for businesses processing large amounts of data to do their own risk assessments and decide themselves whether a DPO is appropriate or desirable in their business to comply with the aims of the directive.

2.25 We believe that small businesses that have to designate a data protection officer, as their core activities are based on processing personal data (eg financial and insurance companies) would be hard hit. The appointment of such an officer could costs around £30,000–£75,000 annually.[3] We believe that an amendment should be made to the text so that these "core activities" only relate to businesses processing a significant amount of data.

3. Question 2

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

3.1 The FSB agrees with the UK Government's approach but we think it can go further.

— The Government supports the provisions requiring transparency of processing, including the new transparency principle and the requirements for data controllers to provide accessible and easy-to-understand information about processing.

3.2 The FSB is not against transparency as a principle. However, every article that tries to achieve transparency of processing data should consider what it means for small businesses in terms of administrative burden and costs (eg changes in IT systems), and possible security risks (ie do you want the way you process data to be public knowledge?).

— The Government supports the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge.

3.4 As we understand it, the new requirements to provide information to a data subject will include an indication of the period of storage, an indication of the consequences of gathering personal data, and information on the right to lodge a complaint to the supervisory authority. This comes in addition to the existing requirements. These requirements add new burdens, and therefore we welcome the Government's intention to

[2] SEC(2012) 72 final. http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf
[3] CBI, March 2012.

resist the proposal that subject access rights be exercisable free of charge. If this fee is abolished, the existing and new information requirements would mean a net burden increase for small businesses.

— The Government will push for an overhaul of the proposed "right to be forgotten" given the practicalities and costs and the potential for confusion about its scope for both organisations and individuals; however, the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate.

3.5 We do not oppose the principle of the right to erasure of one's personal data. However, we would ask the Government to make sure the responsibilities for small businesses stop at notifying third parties to delete the personal data of their customer, and do not extend further.

— The Government will resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers.

3.6 The FSB fully agrees with the Government on this point.

— The Government supports the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement.

3.7 The FSB fully agrees with the Government on this point but we would like to ask the Government to look at breaches of encrypted data that are professionally encrypted to a high standard. We believe that they should not be notified.

— The Government reaffirms its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU, whilst allowing independent national authorities some flexibility in how they use their powers.

3.8 The FSB fully agrees, although "*allowing independent national authorities some flexibility in how they use their powers*" shouldn't result in (legal) fragmentation. For example, different rules and practices could hamper cloud providers to offer their services to the rest of the EU.

— The Government supports a system of administrative penalties for serious breaches of the Regulation's requirements, but push for a more proportionate level of maximum fines, which allows supervisory authorities greater discretion in applying the powers available to them.

3.9 The FSB agrees. However, the FSB is concerned that some of the fines envisaged in the proposal will be significant sums of money for a small business, forcing some to close. Therefore the fines should be applied in a proportionate way to small businesses and relate to the seriousness of the offence eg considering quantities of data handled and sensitivity of that data and the extent to which the organisation had effective procedures in place and that the event may have been a one-off. There should also be additional considerations for businesses that have a high turnover but small profits, compared with businesses with a low turnover but a high profit margin.

— The Government will push for the removal of many of the powers for the European Commission to make delegated and implementing acts, particularly where these have the potential to make a big difference to fundamental requirements and principles (for example, the legitimate interests upon which data controllers can rely to make their processing lawful or the safeguards that must be established to allow profiling to take place).

The FSB fully agrees with the Government on this point. We ask the Government to push the Commission for early consultation of businesses where the delegated acts remain.

August 2012

Letter dated 11 April 2012 from the Information Commissioner

I refer to your letter of 21 March 2012 following my appearance before the Justice Committee on 14 March and am happy to answer your additional questions relating to the European Commission's Data Protection proposals.

1. *When the EU Data Protection proposals were published, you said that in a number of areas they were unnecessarily and unhelpfully over prospective: Can you expand on this statement? Are there any positive elements to the proposals?*

An obvious feature of the proposed Regulation when compared to the current Directive (95/46/EC) is that it is far more detailed and prescriptive, particularly in respect of the measures it would require organisations to adopt to achieve and demonstrate compliance. Examples are the requirements relating to documentation

(Art. 28) and data protection officers (Arts. 35–37). In our view a more prescriptive approach will not necessarily bring about better data protection.

There is a risk that the implementation of rules that may be perceived as onerous or disproportionate could actually lead to more variable standards of compliance by reluctant data controllers. For data protection to be effective in practice we believe data controllers must be able to see a clear link between the measures they are required to take and the protection of privacy. Regardless of any penalties, if data protection is merely seen as legal "red tape" or form-filling, it will not be effective in practice.

A somewhat more flexible instrument, with rather less emphasis on ensuring all data controllers follow common processes, and rather more on ensuring they actually deliver equivalent standards of privacy protection across the EU, might well bring about a better standard of data protection in practice. We consider that it should be possible to achieve this without sacrificing the key enhancements of data protection that the Commission has included in its proposals.

For the most part these enhancements are welcome and necessary. Elements of the proposals that we are particularly pleased to see are:

- strengthening of provisions relating to consent so that when an individual's consent is relied on for processing personal data it is genuine consent;
- making the right to object meaningful by shifting the requirement from one where the individual has to demonstrate compelling legitimate grounds for deletion to one where the controller has to demonstrate compelling legitimate grounds for retention;
- introducing the right to data portability enabling individuals to obtain a copy of data held about them in a reusable, electronic format;
- placing important legal obligations directly on to processors;
- introducing a compulsory data breach notification duty that applies across all sectors (albeit that we consider this should be restricted to serious breaches only);
- giving legal recognition to the use of binding corporate rules to provide appropriate safeguards for international data transfers;
- encouraging incentives for Data Protection compliance in the form of certification mechanisms and Data Protection seals and marks; and
- strengthening the powers of Data Protection authorities including comprehensive investigative powers.

2. *How do you envisage the proposals, as published, differing from those agreed following the consultative and legislative process?*

You will be aware that the proposals will now be subject to the co-decision process in which the Council and the European Parliament have to agree on the Commission's proposals before they are formally adopted. It is almost certain that there will be changes agreed in this process, but it is difficult to speculate on just what these might be. It is also possible that at some point the Commission will revise its proposals and reissue them.

We are reasonably confident that some of the concerns that we have drawn attention to in our initial analysis of the Commission's proposals will be addressed. In particular we are hopeful that some of the over-prescription of obligations on data controllers and some of the unhelpful detail relating to administrative sanctions will be removed. We are less confident of positive changes in the provisions governing the processing of special categories of personal data and the transfer of personal data to third countries.

A copy of our initial analysis of the Commission's proposals is attached for your information (*not printed*).

3. *Are the public too complacent about the way in which they divulge personal data?*

Individuals differ in their attitudes to the privacy of their personal information. Some people are more concerned to protect their privacy than others. What is important is that data protection laws and the way they are applied accommodate these differing attitudes and that those who are concerned-to protect their privacy can, within reason, do so. This is why individual choice and the educational role of the ICO are so important.

One difficulty is when individuals divulge their personal data because they do not know or are misled as to how their data will be used. Data protection law addresses this through the transparency obligations it places on data controllers. These obligations are strengthened in the Commission's proposals and should be of benefit to individuals.

Another difficulty is when individuals divulge their personal data, whether knowing or oblivious to how it will be used, but then come to regret their actions. A typical example is a young person who posts images of himself "enjoying life to the full" openly on a social networking site and then finds that he has been denied a job by a potential employer who has accessed the images. In such cases there is not necessarily any breach of data protection obligations. It is in this context that the Commission's proposals incorporate a right to be forgotten. In practice the provisions do not amount to a true "right to be forgotten", but they do strengthen the

position of individuals in having some control over information that is posted about them on the Internet or otherwise processed by data controllers.

I hope these answers are of assistance to you and members of the Justice Committee. If it would be helpful at some point for the Committee to receive more detailed evidence on my office's view of the Commission's proposals and their likely impact I should be happy to provide this.

Written evidence from the Information Commissioner

Thank you for your invitation to submit evidence to your new inquiry into European Union Data Protection Framework Proposals.

The ICO issued a comprehensive initial analysis of the proposed new Regulation and Directive in February this year. This can be accessed at:

http://www.ico.gov.uk/news/~/media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx

A copy with numbered paragraphs (using the above link) is available as requested in your guidelines. This should provide you with all the background information you need.

Our analysis paper should also help to answer your specific questions concerning the proportionality of the proposals. In short, we are satisfied that current data protection law—the basic features of which are recognisable in the framework proposals—has generally provided a proportionate means of delivering information rights. In particular, the data protection principles constitute a well-established framework for delivering meaningful rights to individuals whilst setting standards that are reasonable and attainable for organisations.

There is no doubt that the data protection framework needs to be updated—this seems to be widely accepted. The current law was drafted in the mid-90s and it is definitely showing its age. I do want to see an improvement in the rights individuals have in respect of information about them. It seems anachronistic, for example, that individuals have to send in a letter and wait 40 days to obtain a copy of their personal information. I also think it should be easier for individuals to have information about them taken down from the internet—although I recognise the practical difficulties that can arise here.

The most obvious difference between current data protection legislation and the proposed framework is the level of detail the latter contains in terms of what organisations will be expected to do to demonstrate their compliance. For example, there are detailed provisions relating to the "paperwork" that organisations will be required to maintain in order to demonstrate that their processing of personal data is being performed in compliance with the Regulation. In general, there is too much emphasis on compliance mechanisms rather than outcomes, and too little scope for organisations to adopt their own ways of complying with the law based on their own circumstances.

In our view organisations of any size or complexity will need to have procedures in place to help them to comply with the law. However, as they stand, some parts of the Regulation are disproportionately prescriptive—not least those that relate to the duties of the regulator. We hope that the more burdensome parts of the Regulation will be lightened as the legislative process continues.

The proposed Directive contains less detail concerning compliance methods than the Regulation. Perhaps this is less of an issue anyway, given the sorts of bodies the Directive will apply to. Police forces, for example, can already be expected to have fairly robust procedures in place for demonstrating compliance with their various legal duties.

We are confident that the Directive has the features necessary to allow effective crime investigation to take place whilst safeguarding individuals' information rights. However, due to the removal or adaptation of certain provisions, we are concerned that the Directive is now weaker than the Regulation. For example, the recitals of the Directive do not include important provisions relating to the retention of personal data, and its transparency provisions are weaker than those in the Regulation. More detail concerning the differences between the Regulation and the Directive are contained in our analysis paper.

Finally, we are satisfied with the next steps that the UK government proposes to take during the negotiations of the new framework, and with its general approach. We have been working closely with the Ministry of Justice, particularly in terms of sharing our experience of regulating under the current law and our observations as to how the proposed framework is likely to work in practice. We are keen to capitalise on the emerging consensus between the ICO, the UK Government and UK business as to the changes that need to be made to the proposed framework so that it will deliver effective data protection in the coming decades.

August 2012

Written evidence from Which?

DATA PROTECTION REGULATION

Which? is a consumer champion. We work to make things better for consumers. Our advice helps them make informed decisions. Our campaigns make people's lives fairer, simpler and safer. Our services and products put consumers' needs first to bring them better value.

We welcome the opportunity to provide evidence to the members of the Justice Select Committee about the proposed Data Protection Regulation. Please note that Which? is only submitting answers to the questions about the proposed Regulation given that our expertise falls outside the scope of the proposed Directive which deals with areas of police and criminal justice.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

1. Which? supports the need to promote economic growth in the UK and is aware of the concerns that burdensome regulations may negatively impact innovation and growth. Consumer confidence is, however, equally central to economic recovery. A sound framework for data protection can help boost consumer confidence, especially in light of the fact more and more businesses and public authorities are moving online. Moreover, given the cyclical nature of economic conditions and the likely longevity of this piece of legislation (the existing Directive has lasted 17 years and counting) it would be short-sighted to consider the provisions within the light of the current economic climate alone.

2. Research from the Government[4] and the European Commission[5] shows the importance of the digital economy to overall economic growth. We know that lack of trust and concerns over data protection present a significant barrier to this growth. A recent Eurobarometer[6] shows that 43% of British consumers are concerned about someone taking/misusing their personal data when shopping or banking online (see further evidence from OFT[7] and the Commission[8]). The loss or misuse of personal data can result in significant harm to consumers in the form of damaged credit scores, time spent changing personal details, embarrassment or dealing with the ever-present threat of identity theft. As initiatives such as BIS's midata and the Cabinet Office's Digital By Default project grow, the volume of personal data exchanged, its sensitivity and depth will increase significantly and, in turn, so will the costs to consumers for its loss or misuse.

3. The proposed Regulation is a unique opportunity to address these concerns thereby unleashing the true potential of the digital economy in the UK and Europe. It is crucial that the final Regulation not only protects today's consumers, but also tomorrow's consumers who will undoubtedly see new technologies and ways of using, sharing and storing personal data emerge.

4. We are keen to see a wide definition of personal data in the Regulation to include location data and online identifiers as such information plays a key role in the identification, tracking and profiling of consumers online. We believe such data should be afforded the same protection as more traditional classes of personal data.

5. We find that the proposal strikes the right balance in the vast majority of areas. We especially support introducing consumer rights around breach notifications and data portability, strengthening the powers of data protection authorities and giving consumers easier means to obtain redress and compensation. The proposal does perhaps go too far in a few areas. We, for example, think that the obligation to have a data protection officer within an organisation should be based on the nature of the data being processed rather than the number of employees. We also think that the 24 hour deadline for breach notifications may be too tight and prevent a thorough assessment of breaches and their effects from taking place.

Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for evidence, the right approach?

6. We are pleased to see that the Government will "support the provisions requiring transparency of processing, including the new transparency principle and the requirements for data controllers to provide accessible and easy-to-understand information about processing". We consider this will enable consumers to make better choices about whom to hand over their data to. The key words are "accessible" and "easy-to-understand"—we need to move away from the current situation where such information is often written in legal language with a tiny font and tucked away on an obscure part of a website or in a long document. When information is presented to consumers in this fashion, companies should not be allowed to rely on the fact that they have given their "informed" consent to the manner in which their information was processed.

7. Which? sees accreditation schemes, which would allow consumers to easily identify companies with good data practices, as part of the solution. We are looking at the possibility of developing a privacy policy and seal

4 Contribution of the digital communications sector to economic growth and productivity in the UK, DCMS, September 2011
5 http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/571
6 http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_fact_uk_en.pdf
7 FDS International for the OFT. "Attitudes to Online Markets", 2010
8 Eurobarometer on Data Protection and Electronic identity, European Commission, 2011

which would be available to e-commerce websites. The policy would be presented in a standardised consumer-friendly format. Meanwhile, the seal would allow consumers to easily identify those companies, which comply with a set of criteria set by Which?. We believe this would help build consumer awareness of good practices in the online environment.

8. We strongly oppose the Government's position to "resist that subject access rights be exercisable free of charge". Consumers have a right to know what data a company or organisation holds about them and should not have to pay to access their personal data.

9. We fully understand the need to protect companies from vexatious requests, but such safeguards already exist in the proposal which states that "where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested".[9] We want to see is a clear explanation of what "manifestly excessive" means so businesses do not overly rely on this caveat to avoid their obligations to consumers.

10. A £10 fee is likely to deter consumers, especially vulnerable consumers, from obtaining this information. Moreover, it would quickly become expensive for victims of identity fraud to find out what has happened to their data and to rectify any false data. In a recent survey[10] commissioned by Which? 76% of consumers said that they found it unacceptable or completely unacceptable that companies can make a £10 charge to provide you with the information they hold about you.

11. We also think such a fee goes completely against the spirit of the Government's midata programme[11] which aims to give consumers access to their personal data in a portable, electronic format so that they can use this data to gain insights into their own behaviour, make more informed choices about products and services, and manage their lives more efficiently. We support this programme which we believe will help direct consumers towards the products and services best suited to their needs and empower them to make decisions about the use of their information.

12. Meanwhile we welcome that the Government will "support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests".

13. On the "right to be forgotten", we are pleased to see that the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate. The Government's position does, however, not address the additional consumer protection to the current "right to erasure" that the "right to be forgotten" should provide. We realise that the term is a bit misleading, and that deleting a consumer's data completely is easier said than done, but it is crucial that the proposal at least includes a requirement on businesses and organisations to take reasonable steps towards deleting a consumer's data at his/her request. This should include notifying third parties whom they have passed on a consumer's personal data to as it is the data controller who has these contacts, not the consumer.

14. We agree in principle with Government's plan to "resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals" though this must not be come at the expense of consumers. The Regulation should take a risk-based approach ie data protection requirements should be more stringent for companies and organisations handling sensitive personal data.

15. We welcome the Government's intention to "support the introduction of data breach notifications both to supervisory authorities and affected individuals, but only if the provisions reflect the timescales needed to properly investigate a breach and if a sensible and proportionate threshold is provided which excludes minor and trivial breaches from the scope of the requirement".

16. Research commissioned by Which? shows that 74%[12] of consumers would always wish to be notified of a data breach. However, we appreciate that a requirement to notify the data subject of all data breaches would be a burden on businesses, imposing significant cost for limited consumer benefit. We therefore support the proposed notification requirements in the Regulation calling for data subjects to be notified when the breach could adversely affect them. We would like a definition of "adversely affects" to include any moral and reputational damages, time spent in attempts to rectify the breach, distress and any financial costs.

17. We are pleased to see the Government "reaffirm its commitment to a strong and independent supervisory authority at national level and support the establishment of a consistency mechanism to ensure a degree of harmonisation in the application of data protection rules across the EU".

18. We are cautious about the Government's position of "allowing independent national authorities some flexibility in how they use their powers" as this could come at the cost of the benefits of harmonisation and potentially lead to forum-shopping ie companies operating from Member States with regulators known to impose low or no fines.

---

[9] See article 12(4) of the proposal: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[10] Which? commissioned an online survey of 1,005 adults between 3 & 5 August, 2012. The data was weighted by age, gender and region to be reflective of the GB population.

[11] http://www.bis.gov.uk/news/topstories/2011/nov/midata

[12] Which? commissioned an online survey of 1,336 adults in February 2011. The data was weighted by age, gender and region to be reflective of the GB population.

19. National regulators must be strong, open and proactive. They must have the resources to investigate companies and organisations thoroughly and do this in a proactive rather than reactive manner.

20. By being open, regulators can play a key role in enabling consumers to make informed decisions about the companies and organisations they share their data with. We would, for instance, like to see regulators regularly publish information about data breaches. In addition to empowering consumers, such "naming & shaming" would also incentivise companies and organisations to be more careful with the data they hold in order to avoid negative publicity.

21. On sanctions, these should be set at a level which will deter companies and authorities of any size and income from breaching the Regulation. The Regulation must, however, also ensure that consumers, who suffer as a result of a company breaching the Regulation, are able to obtain redress.

22. As such we welcome the provisions which allow consumers to seek compensation from data controllers. The Regulation should make it much clearer that the right to compensation can be exercised collectively. Individual damage will in most data breach cases amount to a small sum so individuals are highly unlikely to seek redress on their own yet the collective damage may amount to a substantial sum. Collective redress would not only provide an effective means for consumers to seek redress, but it would, together with sanctions, act as a further deterrent from breaking the rules. Businesses following the rules have nothing to fear from such an instrument; in fact, it can help ensure fair competition as no market player would be allowed to hold on to unlawful gains.

23. Finally, we share the Government's concern that too much detail is left to be decided through delegated acts. We are concerned that this will unnecessarily delay the establishment of a legal framework which is clear to all parties.

August 2012

Written evidence from Privacy International

SUMMARY

- Privacy International welcomes the Select Committee Inquiry. We approach the proposed EU Data Protection Framework from the perspective of individual citizens and consumers.
- We consider that this Inquiry and other consultations must take into account not just considerations of burdens to business and administrations, but also the fundamental rights of individuals to privacy and data protection that the UK has to comply with as a signatory to EU treaties and conventions.
- The proposed General Data Protection Regulation, on the whole, goes some way towards achieving harmonised rules across the EU and makes data protection law fit for 21st century. It contains a number of good improvements, particularly on the rights of the data subject, and also in terms of enforcement and redress. However, there are a number of weaknesses that can undermine these rights, so there is need for improvement.
- With regards to the proposed Data Protection Directive for the law enforcement sector, we consider that the Commission drafters have failed in their duty to ensure a high level of data protection for citizens across the board, as it is much weaker than the Regulation in many respects. The Directive needs radical improvement.
- In terms of specific questions asked by the Inquiry, we think that the Regulation does generally achieve the right balance between the rights of individuals and the obligations of controllers and administrations. Furthermore, considerations of possible burdens to businesses, etc have to be counterbalanced by growth opportunities provided by furthering consumer trust, reduction of costs due to more consistency in 27 countries' rules and potential increased engagement in cross-border trading by SMEs.
- The Directive on the other hand does not achieve the right balance, will result in 27 different regimes and has the potential to undermine individual rights under the Regulation.
- We agree with some, but not all the next steps proposed by the Government in its Summary of Responses to its Call for Evidence.

1. Privacy International (PI) is a registered charity, founded in 1990 and the first organisation to campaign on an international level on privacy issues. PI's mission is to defend the right to privacy and individual people's data protection across the world, and to fight unlawful surveillance and other intrusions into private life by governments and corporations.

2. We are therefore pleased to have the opportunity to provide our views on the European Union Data Protection Framework Proposals to the Justice Select Committee Inquiry, and address the specific questions asked by the Committee. We are fully engaged with the development of this framework legislation since it will have a long-lasting impact not just in the UK and Europe, but will influence data protection regimes for citizens and consumers across the world. The proposals have come not a moment too soon, as the current legislation is no longer fit for purpose. This is a fact that has been widely acknowledged, and does not need further elaboration.

3. However, as a general observation, we are concerned to see that this Inquiry and other home consultations have been framed primarily in the context of possible large extra burdens on businesses and administrations. The fundamental rights to protection of personal data and privacy are specifically mentioned in EU charters and conventions, and have to be complied with by EU member countries signatories of the Lisbon Treaty.[13] Under current legislation these rights are not respected. This is not to say that considerations of burdensome regulations and impacts on economic growth are not important, but that there is need for a more rounded analysis. We think the EU Commission has carried out such an analysis for the last three years,[14] including numerous consultations, commissioning several studies and surveys, and a detailed impact assessment.[15]

4. With regards to the proposed Regulation, we believe that on the whole it makes data protection law fit for the 21st century and goes some way towards achieving harmonisation of rules across the EU. We like the fact that it starts from the standards and principles set out in the current Directive (95/46/EC) and further enhances, elaborates and develops these. As a result it ensures more control on the part of the individual citizen/consumer for example with regards to access, correction and deletion and by attempting to ensure that these rights are meaningful in practice. It also attempts to ensure more effective enforcement by independent authorities with more teeth, as well as better possibilities for redress for individuals, including through the right for collective redress actions by for eg privacy rights and consumer groups. We also very much like the emphasis on responsibility and accountability of controllers for building privacy in their systems ("privacy by design"), and the requirement for breach notifications.

5. However, this is not to say that in our view the Regulation does not need improvement. It does have a number of weaknesses from the perspective of the data subject that have the potential to undermine the good points, and would need clarification or improvement. These include, for example, some of the fundamental definitions (eg personal data and data subject), aspects of lawful processing, enforcement and redress. (See also the answers to question 3, below).

6. As far as the proposed Directive is concerned, our view is very different. We consider that the EU Commission drafters have failed in their duty to ensure a high level of data protection for citizens across the board, both in the private and public sector (given the exceptions for law enforcement access in the Regulation). Police and judicial cooperation in the context of law enforcement is an area where sensitive personal data is likely to be involved, and therefore citizens may be put at particular risk. We agree with the views of the UK Information Commissioner and the European Data Protection Supervisor in this respect. We consider that in the proposed Directive: data processing principles are less ambitious and more ambiguous than those in the proposed Regulation; the rights of the data subjects are significantly weaker than in the proposed Regulation; controllers are subject to fewer, and vaguer obligations; transfers rules are unclear and less restrictive than they could be; and supervisory authorities have fewer and weaker powers. This is problematic also in the context of the UK where currently the Data Protection Act applies across the board.

7. Q: *Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?*

7.1 Yes, we think that the proposed Regulation does on the whole achieve this goal, and it goes a good way towards re-dressing the current imbalances, such as extensive data mining and profiling without individuals' awareness, difficulties for people to stay in control, different rights in different EU countries, authorities without clout and weak enforcement, difficulties in getting redress.[16]

7.2 Claims of stifling burdens, possibly affecting economic growth and innovation are not justified in this case. It is important to ensure that individuals are adequately and effectively protected: as behavioural studies have shown, people that feel in control are likely to share more, not less data,[17] while lack of trust and concerns over data protection is a significant barrier to the growth of the digital economy.

7.3 The EU Commission in its impact assessment[18] estimates that the current fragmentation of legal data protection regimes in the 27 member countries gives rise to an administrative burden costing businesses close to three billion Euros per year, over half of the total costs for administering the current Directive. Any increased administration under the proposed Regulation would be counter-balanced by the fact that firms won't have the burden to comply with the different regimes in the countries they operate (this was a major source of complaint).

[13] Specifically Art 8 of the European Convention on Human Rights and Art 16 of the Treaty on the Functioning of the European Union (TFEU)

[14] http://ec.europa.eu/justice/data-protection/index_en.htm

[15] SEC(2012) 72 final, Brussels, 25.1.2012, Commission Staff Working Paper, Impact Assessment

[16] For research evidence, see for e.g. inter alia section 3.3 of the Commission Impact Assessment (note 3); also results of ICO annual Track Surveys (2011)

[17] http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm; for brief overview see http://www.heinz.cmu.edu/~acquisti/papers/acquisti_privacy_behavioral_economics.pdf

[18] As note 3; Annex 9 has the cost impact assessment for the Regulation

7.4 Furthermore, harmonisation and legal certainty would encourage more SMEs to expand their businesses in other EU countries because they would not need to engage expensive lawyers to which currently only big businesses can afford. This is also shown by EU surveys of SMEs,[19] and would stimulate, not stifle, development. Finally, there are EU countries which currently have stronger and more prescriptive data protection legislation than the UK DPA, including with respect to powers of their Privacy Commissioners or obligations for business—this includes for eg Germany and the Netherlands, and there does not seem to be a stifling of their businesses or any direct correlation with their economic growth.

8. Q: *Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?*

8.1 No we do not believe it will, as stated in paragraph 6 above. The rights of the individual are weaker in the case of the proposed Directive than in the case of the proposed Regulation and inevitably the transposition of the Directive in the different nations will result in the very fragmentation that the new Framework aims to avoid. In addition, these weak provisions in the case of the Directive have the potential to also undermine individual rights under the Regulation, in cases where law enforcement authorities have access to data from private entities; for eg it remains unclear which of the two (Directive or Regulation) would apply in the case of Passenger Name Records being used for law enforcement purposes.

8.2 As the result of these two differing "legal instruments", the new Data Protection Framework suffers as a whole, because the original aim of achieving harmonised and comprehensive data protection rules is not achieved.

9. Q: *Are the next steps the UK Government proposes to take during the negotiations, set out in the Summary of responses to its Call for Evidence, the right approach?*

9.1 In our view, some of the proposed steps are the right approach and others are not.

9.2 Our concern is that the revision is not ultimately used as an opportunity to weaken fundamental principles of privacy and data protection, and result in the reduction of protections, in the name of economic growth, innovation and avoiding burdens. As stated above, while some improvements and tweaks would be necessary, we do not believe that on the whole the new Regulation will put a major extra burden on data controllers in comparison with the current regime. Furthermore, other potential benefits and growth opportunities resulting from the more harmonised rules have not been considered at all in the published Summary of Responses.

9.3 We are also concerned that the Directive is not addressed in the "next steps" section of the Summary of responses, while this really needs major surgery in order not to undermine the whole Framework in terms of the rights of the individuals.

10. Specific comments on some of the proposed next steps:

- "support the requirement for additional information to be provided to data subjects both proactively and in response to subject access requests (subject to consideration of the additional costs), but resist the proposal that subject access rights be exercisable free of charge"
  Comment: currently in the UK subject access charges (£10) can result in considerable costs for individuals who for eg have been victims of identity theft and have to repair a large number of records (sometimes 10 or more companies need to be approached); often the victims of id theft are vulnerable people that cannot afford such costs. In addition we note that in the BIS consultation on the proposed midata legislation, similar to the subject access provisions in the proposed Regulation, the government states a preference that the data (in readable electronic format) is supplied at no cost.[20]
- "push for an overhaul of the proposed 'right to be forgotten' given the practicalities and costs and the potential for confusion about its scope for both organisations and individuals; however, the Government reaffirms its commitment to the right for individuals to delete their personal data, where this is appropriate"
  Comment: Much ado has been made about art 17 in the Regulation, but in reality it is only just a little more than the right to erasure and the right to object. It states no more that the controller "shall take reasonable steps" to inform third parties in relation to data for the publication of which he is responsible. Perhaps the title is a misnomer, but clearly an effective advertising tool.

[19] As note 3; Annex 8, results of consultation with 383 SMEs
[20] http://www.bis.gov.uk/assets/biscore/consumer-issues/docs/m/12–943-midata-2012-review-and-consultation.pdf; para 1.19

— "resist new bureaucratic and potentially costly burdens on organisations which do not appear to offer greater protection for individuals; examples of this include mandatory data protection impact assessments, seeking prior authorisation from the supervisory authority for certain processing operations and the mandatory designation of independent data protection officers" *Comment*: Again, the provisions regarding privacy impact assessments (PIA, art 33) are much more nuanced in the Regulation than the above statement implies. In fact risk criteria set out in this article mean that PIAs will only be required when large-scale and/or sensitive data collection is taking place.

11. We hope also that the UK will strongly support the enhanced rights of the individual in the regulation and ensure there are no loopholes to weaken or undermine them. We will be pleased to share further with the Justice Select Committee our complete positions and more detailed suggested amendments, both for the Regulation and the Directive.

August 2012

Written evidence from the Ministry of Justice

Thank you for the invitation to respond to the questions the Select Committee has asked in relation to the European Commission's recent Data Protection Proposals.

The Committee asked three specific questions.

Will the proposed Regulation strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection in the EU, and on the other for business and public authorities not to be stifled by regulatory, financial and administrative burdens placed upon them?

As is stands, the Government has concerns with the proposed Regulation. It is presently too long and prescriptive, which we believe will represent a burdensome cost on data processors. It may not, therefore, be considered proportionate or practicable. The Government would prefer a data protection framework that is founded on the principles of necessity and proportionality, and which enables data controllers to protect personal data without prescribing the means by which such protection is achieved.

The Government's aim in negotiations in the Council of the European Union is therefore to lessen the regulatory, financial or administrative burdens which the proposal seeks to place on data controllers and processors. In many cases, we agree with the principle which the proposal sets down, but disagree with the level of detail which the instrument prescribes in order to achieve a particular outcome. We want to see EU data protection legislation that protects the civil liberties of individuals, while allowing for innovation and growth. These should be achieved in tandem, not at the expense of one or the other.

Will the proposed Directive strike the right balance between the need, on the one hand, for a proportionate, practicable but effective system of data protection for police and criminal cooperation in the EU, and on the other for law enforcement authorities to be able to investigate crime without disproportionate financial or administrative burden?

The Government also has concerns with the proposed Directive, as currently drafted. Again it is presently too long and prescriptive, which we believe will represent a burdensome cost on data controllers and processors. It may not, therefore, be considered proportionate or practicable. We also have a particular concern about the extension of the scope to cover personal data processed solely within the UK ("domestic processing"), which we do not consider to be an area that should properly be regulated at the EU level.

However, Article 6a of Protocol 21 has the effect of limiting the application of the Directive as far as the UK and Ireland are concerned. The. Directive will not apply to domestic processing which has no cross-border element. Rather, it will only apply where processing is being carried out pursuant to an EU measure which binds the UK. Further, the Government will seek to negotiate to remove domestic processing from the Directive for all Member States. In short, our approach to the Directive is the same as it is with the Regulation in that we will seek to remove or modify the most disproportionate and prescriptive aspects of the proposal, whilst ensuring that there is always adequate and effective protection for data subjects.

Are the next steps the UK Government proposes to take during the negotiations, set out in the summary of responses to its Call for Evidence, the right approach?

The Government has listened to the views of interested parties from a wide range of areas of society in order to inform its opinion. We remain committed to playing an active role in the negotiations in order that the resulting legislation protects the rights of data subjects whilst not representing a disproportionate burden for controllers. This is in line with the Government's existing commitments to both civil liberties and reducing regulation. To this end, we have adopted a position that maintains and enhances the rights of individuals, but which resists provisions that cannot be considered proportionate and which may not increase data protection rights.

I am enclosing further detail in a memorandum and I look forward to supplementing this with oral evidence to the Committee in September.

Executive Summary

1. New proposals from the European Commission for the protection of personal data were published on 25 January 2012 and negotiations commenced in February. These comprise, first, a Regulation on Data Protection, introducing a general framework that applies to businesses and the public sector. This replaces the existing Data Protection Directive from 1995 ("DPD"). The second measure is a Directive covering Data Protection in relation to police and law enforcement. This replaces the current rules, set out in the Data Protection Framework Decision (2008) ("DPFD").

2. In the UK, the Data Protection Act 1998 (DPA) implements the DPD. The DPA also includes in its scope police and law enforcement processing, as did the 1984 Data Protection Act. This means that the DPA applies to the processing of all personal data, including that covered by the DPFD. It is likely that the DPA will need to be amended or repealed and replaced in order to implement the new EU legislation once it comes into force.

3. The background to the legislation is the emergence of new information and communication. Technology and the unparalleled growth in data sharing between individuals and organisations, both of which have created concern in the Commission, shared by some businesses and campaigners, that the law needs to be modernised.

4. The Government welcomes the opportunity for a revision of the 1995 Directive, owing to the radical changes in data sharing practices since 1995, not least because of the growth of the Internet since then. We have concerns, however, with the length, complexity, prescriptiveness and the burdens on data controllers and processors that would be imposed by the proposed Regulation. The outcome we are aiming for in negotiations in the Council of the European Union is a data protection framework that protects data subjects' rights without causing disproportionate burdens on data controllers and processors.

5. The argument for the replacement of the DPFD is not as clear as for the DPD, as the DPFD was only adopted four years ago. Nonetheless, the Government recognises the need to protect individuals' personal data within the sphere of police and law enforcement. We have some concerns again with the length and prescriptiveness of the proposed Directive and in particular with the extension of its scope to cover domestic processing (processing purely between domestic authorities with no cross-border element, for example between the Metropolitan and West Midlands Police).

Specific Policy Positions

6. In terms of specific policy goals, the UK position is the following:

- domestic processing—processing purely between domestic bodies, should be excluded from the scope of the proposed Directive. Consultation with key stakeholders in the field of law enforcement and judicial cooperation has uncovered no evidence that the current lack of EU rules in this area has obstructed co-operation between Member States; or had detrimental impacts on the protection of individuals. Indeed, we think that introducing prescriptive requirements for domestic processing may instead have a detrimental effect on law enforcement operations, placing onerous burdens on data controllers and huge costs on public authorities—without delivering better data protection for individuals. It is important to be clear, that Government does not believe the provision relating to domestic processing will apply to the UK. The legal basis of the Directive is Article 16 of the Treaty on the Functioning of the European Union (TFEU), which is a new legal base specifically for data protection introduced by the Lisbon Treaty. Special rules in the UK's Justice and Home Affairs Protocol[21] (Protocol 21) mean that even with an Article 16 legal base the Directive will have limited application, as it will not apply to domestic processing. Instead, it will only apply to cross-border processing pursuant to EU measures that bind the UK. However, despite the view that domestic processing will not apply to the UK the Government will negotiate to remove domestic processing from the Directive for all Member States as a matter of policy;
- The Government is of the opinion that the proposed Regulation contains too many examples of powers being retained by the European Commission in the form of either delegated acts or implementing acts. Article 290 of the Treaty on the Functioning of the European Union says that delegated powers may only be conferred on the Commission when these powers give them: "...the power to adopt non-legislative acts of general application to supplement or amend certain non-essential of the legislative act." The Government believes that there are too many such acts in the proposals and considers that a significant number touch on essential areas of the proposals. Further, under Article 291 of the TFEU, the power to adopt an implementing act must only be conferred on the Commission where uniform conditions are needed to implement a legally binding act. In many instances in the Regulation where a power to adopt implementing acts is conferred, it is not clear that uniform conditions are needed;

[21] See Article 6a of Protocol 21 on the Position of the United Kingdom and Ireland in Respect of the Area of Freedom, Security and Justice, also known as the opt-in Protocol or the Title V Opt-in Protocol.

— The Government will therefore be negotiating to reduce the quantity and impact of delegated and implementing acts in the Regulation and (although it contains far fewer powers to make delegated and implementing acts) in the Directive, where appropriate;

— the "right to be forgotten" should be resisted on the basis that it would raise expectations amongst individuals whose data is being processed that would be very difficult to fulfill in practice—in many cases it will prove impossible to delete data which has been disseminated across global networks;

— prescriptive requirements contained in the body of the instruments should be resisted where they place unrealistic obligations on data controllers, particularly on SMEs and not-for-profit organisations—this includes requirements to notify the Information Commissioner's Office of a data breach without undue delay and where feasible not later than 24 hours after having become aware of it, to maintain documentation of all data processing operations and, if certain requirements are met, to designate data protection officers which could be costly and impractical for many business and organisations. Instead, the proposals should focus on the processing of data in accordance with data protection principles and less burdensome rules that focus on the outcome of providing proper data protection, rather than setting down processes which must be followed;

— the enforcement and sanctions regime must be proportionate to the risk and impact on individuals and the size and nature of the business or operation being regulated—a draconian system of fines is currently proposed which could be prove very costly for many businesses and in all but very limited exceptions the supervisory authority is obliged to sanction breaches of the Regulation even where they relate only to breaches of the Regulation's bureaucratic obligations;

— the Regulation or Directive should not preclude or inhibit data sharing between Government Departments—this could include but is not limited to case investigation, validation, fraud and error, and fine enforcement;

— provisions around the transparency of processing, including easy-to-understand information being available to the data subject and having clear information provided in response to subject access requests should be supported subject to these not representing a disproportionate burden on data controllers or processors;

— provisions for an independent supervisory authority at the national level, which can, via a consistency mechanism, provide a degree of harmonisation in the application and enforcement of data protection rights to data subjects across the EU should be supported;

— transfer of data to third countries outside the European Economic Area (EEA) should provide for proper levels of protection for cross-border data transfers, but neither international commerce nor law enforcement co-operation should be hampered by an overly complex system relying to a significant extent on prior authorisations by the Commission or supervisory authorities; and

— bi-lateral and multi-lateral agreements existing at the time the Directive is adopted should not be subject to renegotiation under the Directive—there are currently numerous international data sharing agreements in place which will require renegotiation under the provisions of the Directive. The US in particular has raised concerns about this.

Call for Evidence

7. The MoJ ran a Call for Evidence between 7 February and 6 March this year seeking views from stakeholders on the Commission's proposals and published a Summary of Responses on the 28 June. This builds on a previous Call for Evidence on the existing legal framework undertaken during 2010. The responses highlighted a number of issues, particularly around the practicability of the "right to be forgotten", the potential size of the fines available to the regulator and the financial impact of new obligations on data controllers and processors. This evidence has been used to help inform the UK's position in the ongoing negotiations.

8. Consumer and citizens' rights groups broadly welcomed the proposals, while many businesses expressed concern about the administrative burdens contained within the proposals. Some multi-national groups have expressed a preference for the proposed Regulation being a Regulation and not a Directive on the basis that they would gain benefits from having EU-wide harmonised rules.

Impact Assessment

9. The impact assessment and executive summary published by the Commission alongside the proposals make much of the possible savings to be made by minimising legal complexity and delivering administrative savings. We are in the process of conducting our own impact assessment to look at the precise costs and benefits of the proposals which will assist in our approach to negotiations in Council working groups. We will also engage with the Commission on their impact assessment and seek to highlight where improvements to the analysis can be made and offer to support them in this process.

10. However, our initial assessment suggests that the Commission's impact assessment does not provide a credible foundation to underpin the proposals. We have noted three issues in particular:

— the quantified impacts have not been thoroughly investigated. In particular, there are significant weaknesses with the widely publicised €3bn benefit from reducing "legal complexity";

— the impact assessment has focused on quantifying benefits without corresponding assessment of costs; and

— the impact assessment exhibits many issues in relation to the method used to compile the analysis, for example: lack of a clear baseline; failure to consider impacts over time; absence of sensitivity testing to account for uncertainty; lack of Member State level analysis; multiple statistical errors; and no explicit consideration of winners and losers.

11. The MoJ published impact assessment checklists on 28 March 2012, which gave a preliminary analysis of the areas in each instrument that were deemed to be of higher importance or impact as far as the UK is concerned. The summary of the documents stated that the proposals as they stand represent an increased burden on the UK overall. These checklists were included in the Government's Summary of Responses to the Call for Evidence.

July 2012

Supplementary written evidence from Microsoft Ltd

Thank you for the opportunity to give oral evidence to the Justice Select Committee on 4 September for Microsoft. There are two points I wanted to re-state for the purpose of absolute clarity on our position regarding the EU Data Protection proposals:

1. Microsoft is very much in favour of strong protection of personal data. We welcome the draft Regulation, which seeks to better harmonise the EU's data protection regime. Any responsible company has a role to play here. Our approach is based on Trust and Transparency.
2. Particularly for a company such as Microsoft operating in many jurisdictions, the harmonisation of data protection is highly desirable, providing a simplicity and confidence in approach across the EU.
3. There needs to be less specificity over the means to achieving data protection aims, allowing a greater level of flexibility in the technical requirements for compliance, such as the specific forms and format required. The draft should offer more incentives to trustworthy companies. It is key to motivate companies via the concept of recognised accountability (ie, to encourage good practices by rewarding organisations that demonstrate responsibility and adopt robust privacy programs including in relation to the transfer of data in the Cloud).
4. The concept of administrative fines is appropriate, but the "one-size-fits-all" approach that puts on the same level companies that intentionally cause harm and those that were negligent is disproportionate.
5. Finally, rules relating to international data transfers and the role of Processors/Controllers need to be adapted to the Cloud context.

September 2012

Supplementary evidence from Privacy International following the evidence session on 11 September 2012

DIRECTIVE

1. *What is the rationale of having a weaker level of protection in the Directive than in the Regulation?*

This is a question that for the Commission; it seems the rationale is one of ratcheting up the existing Framework Decision 2008/977/JHA and including data processing activities by the police and judiciary on the domestic levels, as agreed in the Lisbon Treaty, but at the same time playing to various member countries political sensibilities and current situations. The result is not satisfactory in our view. In the explanatory memorandum to the Directive the Commission emphasises the need for a more comprehensive approach to data protection in the EU and seems to conclude that this will be achieved to a certain degree by this proposed Directive as it follows the same broad principles to the Regulation. But it doesn't and in our view it will create further confusion and grey areas, for example when data collected for commercial purposes is used for law enforcement purposes. Also it does not clarify and ensure consistent application of rules in situations in which activities of the private sector and the law enforcement sector interact with each other and differences are blurred—eg PNR data, or financial transfers.

2. *Are delegated acts a suitable mechanism to make sure the Regulation keeps up to date with changes in technology?*

Delegated acts are good mechanisms for keeping the Regulation up-to-date with new developments and technologies without having to review the whole legislation too often. Specifically they are good for design specifications, and addressing standards for new technologies as well as sector guidelines. However there are too many of them currently in the draft, including a number that refer to essential definitions and clarifications that should be in the legislation itself to ensure certainty and in fact are not that time sensitive. Important examples of these last include Art 6.5 re clarification of the application of legitimate interests as ground for lawful processing; Art 12.4 re the definition of "excessive" for data subject access; Art 17.9 re the implementation of the right to be forgotten; Art 20.5 re defining safeguards for the data subject when profiling is allowed; and Art 31.5 re the threshold for data breach notification. It will take a few years to process all these delegated acts by the Commission, and in the meantime controllers and authorities will be left in the dark as to what exactly they are supposed to do.

3. *Where should the balance between data protection rights and administrative burdens lie?*

We answered this question to a large extent when addressing the previous question regarding administrative burdens**.** When considering such a balance, the burdens and benefits need to be assessed not just short term and in an economic crisis, but there needs to be a longer term view and weighing of costs versus benefits—what may seem an administrative burden now, compared to current business practices may become a routine process in two/three years time but pay dividends in increased confidence to transact from consumers, increased willingness to trade cross-border and innovation from SMEs (due for eg to increased data portability). In practical terms the extra duties entailed by increased data subject rights should not be in our view classified as administrative burdens but as necessary processes to fulfill those rights in practice. There may be on the other hand some administrative procedures contained in Chapters IV and VI that could be streamlined : in which case there should be an objective assessment of what exactly these burdens are, how much they would cost/ why they won't work, and what alternatives can be put in place that fulfill the same objectives.

4. *What assessment have you made of the Commission's estimated €2.3 billion savings in administrative burdens?*

In Annex 9 (pages 141 et ff) of its impact assessment the Commission gives a comprehensive account of the calculations, the methodologies and the data used and from what sources, including quantitative survey data. It gives an overall saving for the EU 27, if you remove legal fragmention, of 1.5 billion. I have not seen anywhere else an equally comprehensive calculation, with concrete figures, of possible impacts, and moreover giving an overview for the whole EU.

In addition and as answered elsewhere, a more long term view should be taken; there is research to show what are the missing potentials—for eg a recent study on e-commerce (2011) commissioned by DG Sanco found through economic analysis that the missing potential for e-commerce that would be provided by legal harmonisation and a single market in goods would be 1.7% of EU GDP (204.5 billion euro), four times higher than if the fragmented markets continue to exist. Of course data protection is only part of the "single market" feature, but even a fraction of this missing potential would outweigh any potential "burden costs".

5. *Are strong sanctions necessary to ensure compliance with the Regulation?*

Sanctions should be set at a level that deters companies and public authorities from not complying with the law. If the costs of non-compliance are lower than the costs of compliance, you have worthless regulation, with no teeth. Despite increased powers, the UK ICO's fines have been minimal in comparison to other EU regulators. According to its own data, 2010–11 there were five prosecutions and four fines totalling under £500,000, out of 603 breaches reported. Private sector companies account for very few undertakings despite the rise of breaches in the private sector according to the ICO himself. For eg in 2011 a legal firm (ACS Law) was fined for failing to keep sensitive personal information relating to 6,000 people secure. The fine was £1,000. Which? also has more figures on this resulting from a freedom of information request .

Therefore the prescription of sanctions according to the nature of the breach is the right approach in our view—it not only will harmonise the situation across the EU but it will also minimise the potential for forum shopping, as is currently the case.

September 2012

Supplementary evidence from the Information Commissioner following the evidence session on 4 September 2012

What assessment have you made of the EU Commission's estimate of €2.3 billion savings in administrative burdens?

We have not done our own research on this but we are rather sceptical of the claims to reduce burdens given the very prescriptive set of rules and the fact that the only reduced burden seems to be the removal of the current notification system. The removal of the notification requirement will probably be outweighed by all the costs emanating from the level of prescription in the Regulation. We are, however, also sceptical of some business estimates of the costs associated with the Regulation. The main problem in calculating the cost of data protection compliance is that even if there was no data protection law, organisations would still have to invest in keeping personal data secure, for example, so it is a bit unfair to see the costs of corporate information governance as being "additional data protection costs".

We are commissioning our own assessment of the impact on business. This assessment will help us to direct guidance to data controllers on areas where the regulation will have the most impact. We would be happy to send you a copy of this in due course.

Are there any industries or groups that will be particularly helped or hindered by the proposed Regulation?

For the most part we do not think so—the regulation will apply to all data controllers in the same way that current data protection law does—and our experience suggests that is it not possible to separate them into "winners" and "losers".

However, our understanding is that large multinational corporations particularly those that offer services online have been behind pressure on the European Commission to harmonise data protection law and its application across Europe. There is a strong focus on harmonisation in the Commission's proposals which will presumably assist such corporations.

Further, we are hopeful that the research mentioned above will cast some light on this. It does seem though that organisations with a sizable workforce but relatively low risk processing operations could be hit quite hard in terms of carrying out various compliance procedures. An obvious example might be an engineering company. It might have a large workforce, but its data processing operations might be straightforward and relatively low-risk—just routine record keeping about its employees and customers—yet it could be required to keep extensive documentation, for example.

On the other hand, organisations with a small workforce but very large amounts of personal data, such as some of the big electronic service providers eg social network site operators, could escape this.

It is also very important that whilst SMEs comply with the basic rules of data protection, they are allowed to do so in an administratively proportionate way.

Are concepts such as patient confidentiality and freedom of speech threatened by the proposed Regulation?

We do not think patient confidentiality is threatened as processing in the UK will still need to be lawful according to UK law—this includes the common law duty of confidentiality—which will still be in place post-Regulation. There will be some change in terms of the definition of "personal data concerning health" but this is a technical issue and it certainly will not lead to any erosion of a healthcare professional's duties in respect of patient data. If anything the stronger information protection provisions in the regulation will bolster this.

Any functioning data protection regime must accommodate freedom of the press and free speech more generally. The Regulation does open the way for national arrangements to ensure this and this is welcome. Article 80- freedom of expression allows for national arrangements to ensure exemptions (or derogations) for processing carried out solely for journalistic purposes. This is the same formulation as in the current directive.

We are concerned that there may be an intention on the part of the Commission to extend the full force of data protection law to individuals who post personal data on the internet for their own personal or domestic purposes but who make it available to all internet users. There is European case law that says—in a nutshell—that open online publication means the processing of personal data done in connection with this falls outside data protection law's "domestic purposes" exemption. However, that was a judge's interpretation of the current law and we need not be bound by it in framing the new regulation. I do not think any of us want to come to a state of affairs where everyone with an "open" social networking page—or who wants to publish their genealogical research findings on their webpage become a "data controller" subject to the full rigour of data protection law. This could clearly have implications for freedom of expression in a broad sense.

September 2012

Supplementary evidence from Which? following the evidence session on 11 September 2012

1. *Are delegated acts a suitable mechanism to make sure the Regulation keeps up to date with changes in technology?*

Delegated acts are needed to ensure the Regulation can be flexible, and adapt to new technologies and issues as and when they arise. However, there are a vast number in the proposed Regulation which raises a number of issues:

(a) It will be years before there will be any certainty—according to the estimated financial impact statement accompanying the Regulation proposal—only two delegated acts will be implemented per year. Therefore it will be at least 10 years before there is any legal certainty which could potentially undermine the objective of establishing a clear set of rules.

(b) It is thought that delegated acts have been used in key areas where they should actually be addressed in the body of the Regulation.

We believe that delegated acts should be limited to address non-essential issues—such as design requirements, criteria for technical measures etc.

The BEUC position paper on pages 37–39 provides examples of those delegated and implemented acts that should be maintained and those which need to be addressed in the body of the Regulation to provide legal certainty.

2. *Where should the balance between data protection rights and administrative burdens lie?*

Firstly, I think focusing on short term "administrative burdens" doesn't reflect the full picture of the proposed changes under the Regulation. Granted, yes—there are new rights and tighter protections for consumers and to be able to provide these may mean an initial cost—but the result of these changes won't just bring around benefits to consumers—business is also set to benefit—and UK Plc as a whole.

From our perspective we see some of the benefits as:

(1) *The value of data:* The value of data is just beginning to be realised—it is coined the new oil of the 21st century and consultancies like McKinsey are busy advising businesses and government of the huge costs savings and opportunities which can be made if it is utilised and understood. What the Regulation is going some way to do is opening up this new personal data ecosystem—making it a far more competitive market—so it is no longer sat on by a few of the large corporations but has the potential to be used by consumers and other service providers—as the business case for BIS's midata states—it is going to cause an innovation and entrepreneur explosion. As it is ultimately consumers data—it is only right that we should take a cut of that value and a piece of the pie too.

(2) *Enhanced consumer trust:* An OFT study reported that 6.27% of UK internet users said that they don't buy goods or services online because they are worried about providing their personal and financial details. This amounts to 2.64 million internet users and a potential loss of around £2.48 billion per annum to online businesses. If consumer trust can be built—and privacy concerns addressed—this is of huge benefit to e-commerce.

(3) *Cross-boarder trade:* While we have reports that the majority of our SMEs don't engage in cross boarder trade—this is presumably because they find the process too complex and it delivers too little rewards—they can't afford the legal advice. If this changes and markets open up there could be significant benefits for these businesses.

We are aware that there have been concerns from the MOJ that we want to refrain from burden on business when we are in a time of economic hardship—but I think we need to think about a longer term approach—this piece of legislation if anything like it's predecessor will last for over 20 years. This will outrun numerous economic cycles—indeed—by the time this is even implemented in four years or so from now—we will probably be out of the current one.

We also need to think about the pace of technological change. When the current data protection act was implemented—Mark Zuckerburg was in primary school. We have to make sure that the fundamental rights and protections are built in to protect consumers from the next huge technological advances and societal shifts—and who can imagine what those might be in the next 20 years or so—and if this means there's a short term cost for business to get there—I really believe that it's a cost worth taking.

Ultimately it has to be that the balance is struck when the consumer rights and protections are provided and can be enforced. Any administrative burdens which are superfluous to this goal, can presumably be lightened.

3. *What assessment have you made of the Commissioners' estimated $2.3billion saving in administrative burdens?*

We have not made a detailed assessment of this—however—we do think that it should not simply be about the analysis of the costs and savings of administrative burdens—but rather the long-term view of what the benefits will be to all players in the personal data space.

These benefits are: (List as above).

4. *Are strong sanctions necessary to ensure compliance with the proposed Regulation?*

Regulation generally is not worth paper written on if no one enforces it and there are no incentives to comply. We think that sanctions should be set at a level which will deter companies and authorities of any size and income from breaching the Regulation.

This is also key to ensuring a level playing field. If you don't penalise those firms which break the rules then you implicitly penalise those who play by the rules.

Previous fines in the UK have arguably been a drop in the ocean for the biggest players. A freedom of information request by Which? in 2011 revealed that of 1,400 cases where the ICO believed banks and lenders to have been in breach of the data protection legislation, they only took action in one.

The prescription of set sanctions in set circumstances and the use of the consistency mechanism in the Regulation is therefore welcomed as it should help to harmonise fining across the EU and reduce the potential for forum shopping, a practice that has serious impacts on consumer protection and confidence across the EU.

The Regulation must, however, also ensure that consumers, who suffer as a result of a company breaching the Regulation, are able to obtain redress, and this redress must be cost effective, quick and easy. We would ask the Commission for further clarification over the methods of redress currently proposed in the draft Regulation—what "compensation" would mean in practice—and how it could be claimed—and the scope of the collective redress mechanism currently proposed.
September 2012

Supplementary evidence from the European Commission following the evidence session on 11 September 2012

1. *Does the Commission wish to implement the documents as drafted, or are they an ambitious starting point which will be subject to compromise?*

The Commission has broadly consulted prior to the adoption of the reform package. The proposed texts provide ways forward in order to reply to a three-pronged objective, namely to strengthen the fundamental rights and freedoms of individuals with respect to processing of personal data, to enhance the Single Market dimension and embed trust in the digital environment and, finally, to ensure smoother and more effective cooperation between Member States' police and judicial authorities.

The Council and the European Parliament have already started analysing the proposals. The Commission is fully engaged in the legislative process with the co-legislators to make these proposals a reality for individuals, businesses, public administrations and law enforcement community.

2. *How confident are you that the proposals will achieve the level of savings set out in the impact assessment?*

The Commission is confident as regards the level of savings indicated in the impact assessment. One of the main objectives of the Regulation is to cut down existing red tape and administrative burden, and make it easier to transfer data within the EU internal market—and beyond. This is particularly important in today's digital and globalised environment.

The legal environment and the governance system (one single law and "one-stop-shop" for controllers) will be simplified and some of the existing obligations (eg, general notifications, authorisations for international transfers) will be removed or greatly reduced. Also the existing legal fragmentation will be remedied by putting forward one single law.

At the same time, we need to ensure that individuals have actual control over their personal data, particularly online and that strong accountability mechanisms are in place.

In the impact assessment the analysis focussed in particular on the costs incurred by the private sector in order to comply with information obligations contained in the data protection rules (so-called "administrative burden"). Nonetheless, other compliance costs have been estimated such as in the cases of Data Protection Officers and Data Protection Impact Assessments.

The general economic benefits, meaning the potential increase of business, the added growth in the EU and in the UK due to a better regulatory environment for the digital single market will also be significant.

The Commission remains open to consider any suggestion for further reducing administrative burden, while maintaining a high level of protection of fundamental rights as regards processing of data.

3. *Why would updated data protection laws draw businesses to invest in the EU rather than considerations such as taxation and skills?*

A combination of several factors accounts for attracting more and more businesses into the EU. The reform of the data protection framework is one of these elements.

Once the proposed Regulation will be in place it will bring about the necessary harmonisation, coherence, enhanced legal certainty and workable arrangements which are of key important for businesses.

For businesses having to comply with a myriad of data protection laws has a deterrent effect when considering intervening on the EU market.

This has been also acknowledged by some of the US interlocutors. For example, Mr Lamb-Hale, Assistant Secretary for Manufacturing and Services, International Trade Administration when testifying in front of the House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade in September 2011 has underlined that the differing EU Member State regulations create legal uncertainty which complicates US companies' efforts to plan for the future.

A high level of data protection can be a competitive advantage and an important element for growth in the EU. Additionally, the draft Regulation has been constructed with a view to greatly simplify the regulatory environment for businesses in Europe—and beyond.

Moreover, the draft Regulation is designed to increase trust and confidence in the digital marketplace and to restore consumer control over personal data. Trust is a key element for a company to be competitive on the global market.

4. *What impact might the requirements for International data transfers have on the development of cloud computing in the EU?*

The proposed regulation addresses the issues raised by the cloud. Centrally, it clarifies the important question of applicable law, by ensuring that a single set of rules would apply directly and uniformly across all 27 Member States. It will be good for business and individuals by bringing about a level playing field and reduced administrative burden and compliance costs throughout Europe for businesses, while ensuring a high level of protection for individuals and giving them more control over their data. Increased transparency of data processing will also help increase consumer trust. The proposal strengthens the role of the processor to take account of their increased responsibilities aspect which is very relevant for cloud computing. It also facilitates transfers of personal data to countries outside the EU and EEA while ensuring the continuity of protection of the concerned individuals. More specifically, it extends the scope and simplifies the procedures for tools such as "binding corporate rules"—codes of conduct allowing for intra-corporate transfers within companies with branches in the EU and outside and on binding standard contract clauses—which is essential to regulate issues such as cloud computing.

5. *Will the requirements for supervisory authorities prevent them from exercising discretion and providing guidance?*

The Regulation will further strengthen the status of supervisory authorities and harmonise their enforcement and sanction powers, so that also the same level of enforcement is guaranteed in all Member States. Their independence, which is enshrined in the Charter (Article 8) and in the Treaty on the Functioning of the EU (Article 16) is also strengthened in the proposal.

The proposed Regulation provides for rules for swift and efficient cooperation between DPAs such as mutual assistance and joint operations. It also sets up a consistency mechanism at EU level, to ensure that DPA decisions that have a wider European impact take account of the views of other DPAs concerned, and are taken in compliance with EU law.

6. *How will the new European Data Protection Board (EDPB) differ from the current Article 29 working group?*

The proposal establishes the European Data Protection Board (EDPB), consisting of the heads of the supervisory authority of each Member State and of the European Data Protection Supervisor. The EDPB replaces the Article 29 working group and strengthens its powers reflecting the increased scope of activities of the European Data Protection Board, within the Union and beyond.

The consistency mechanism will function in the framework of the EDPB which will contribute in an independent manner to the consistent application of the Regulation throughout the Union, issue opinions and guidelines.

The proposal clearly enshrines the independence of the EDPB in its activities. The Commission will not be a member of the EDPB, but will have the right to participate in its activities and be represented.

September 2012

Supplementary evidence from the Association of Chief Police Officers following the evidence session on 4 September 2012

1. *What is the rationale for the proposed Directive having a weaker level of data protection compared to the proposed Regulation? Will this inconsistent approach cause confusion for data subjects and data controllers?*

This would reflect the current position with regard to the exemptions that sit within the Data Protection Act. There has always been an appreciation that with crime investigation it is inevitable that certain legal rights that may apply elsewhere and which impact upon personal data may have to be infringed. For example, the holding of intelligence by the Police Service which is graded according to reflect its accuracy nonetheless is a depository of data some of which is unlikely to be accurate in content. This of course flows against the concept under the Data Protection Act that all data should be relevant and factual. The Association of Chief Police Officers therefore has no difficulty with this approach.

2. *If domestic processing does not apply to the UK, is there any value in the Government negotiating for its complete removal from the Directive?*

In our opinion, this is really a matter for government and has to be seen against the backdrop of not just the Directive but also the Regulation. We take the view that the UK government would need to look and consider all of these proposals taking cognisance of the power and role of the ICO, the rights of the individual and the need to protect local communities and national security. When this is done as a package, in our view the proposals are then inconsistent with the current regime that applies for the Data Protection Act. The cost of their implementation and the added bureaucracy will not equate to an added value that would support their implementation.

3. *Why do you think the relationship between data controllers and the Information Commissioner's Office will alter under the proposed Directive?*

The Police Service has an excellent professional relationship with the ICO which fully acknowledges his regulatory position but which at the same time continues to ensure that through debate, negotiation and on occasions litigation we have put in place policies and procedures which meet his expectation and those of the Police Service. This relationship means that forces voluntarily report breaches and evidence where necessary and that immediate action can take place to remedy defects in business processes. We accept that on occasions this will lead to fines but have always sought to learn and implement change where such actions have taken place. We believe these proposals will make the ICO office remote and that they will become a purely regulatory department who have little understanding of the policing world. Our charges for registration will rise and fine levels will be increased, not in furtherance of the application of regulatory process but in order to raise income to pay for a 24/7 operation which records every breach. We find such proposals excessive, very unlikely to work and the cost significantly out of place with the austerity that currently exists within the public sector.

4. *What impact would having to renegotiate bi-lateral data agreements have on policing?*

This really depends on what is meant by renegotiation. It is the opinion of the Association of Chief Police Officers that the current arrangements for European exchange of criminal data work best when all countries are doing the same. We are not confident that a process of trying to renegotiate bi-laterally will necessary be accepted by either the Commission or independent states.

September 2012

Observation from Privacy International following the evidence session with the Minister on 17 September 2012

Privacy International believes that the proposed Directive is weaker than the proposed Regulation, and as a result there will be a two speed regime. We do not believe the proposed Directive is weaker than the current UK Data Protection Act, and that it probably offers about the same level of data protection, but with added bells and whistles. We have not carried out a comparison of the two, since they will probably never operate in parallel.

September 2012

Printed in the United Kingdom by The Stationery Office Limited
10/2012 023539 19585

ISBN 978-0-215-04975-9

PEFC/16-33-622