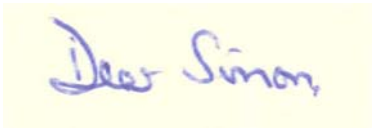
HOUSE OF LORDS
European Union Committee

House of Lords
London
SW1A 0PW

Tel: 020 7219 7291
Fax: 020 7219 6715
euclords@parliament.uk
www.parliament.uk/lords

Simon Hughes MP
Minister of State for Justice
Ministry of Justice
102 Petty France
London SW1H 9AJ

7 May 2014



EM 17067/13: Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows

EM 17069/13: Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU

Thank you for your Explanatory Memorandum of 20 December 2013 and for giving oral evidence to the Sub-Committee on Home Affairs, Health and Education on 9 April 2014. As you know, we considered the above Communications to be of sufficient importance for us to conduct enhanced scrutiny of them. We have no doubt that we will need to continue to consider many of these issues in greater depth over the period ahead. For the benefit of those readers who may not be so familiar with the provisions of safe harbour we have set out the background to our work in an Annex to this letter. We have written also to Commissioner Johannes Hahn, who has taken interim responsibility for the justice portfolio in the European Commission.

Value of safe harbour

We considered the relative strengths and weaknesses of the safe harbour scheme. Safe harbour "bridge[s] the gap" between the EU and US regulatory requirements when it comes to allowing transfer of personal data.[1] Our witnesses generally recognised it as useful, although all agreed on the need for its improvement. Chris Connolly, Management Consultant, Galexia, and Phil Lee, Partner, Privacy and Information Law Group, Field Fisher Waterhouse LLP, said that safe harbour was the most practical mechanism for a lot of organisations to do transatlantic business.[2] It involved less red tape than other provisions, such as data export contracts and binding corporate rules (BCRs), and so a company could comply, register and operate in the EU market relatively quickly.[3] This should be particularly attractive to smaller businesses which

[1] Q 36
[2] Q 3
[3] *Ibid.*

might not have the resources to put in place BCRs. Chris Connolly suggested that multinational corporations with complex business structures, such as Mastercard, would find it very difficult to have individual contractual clauses with all of their customers, so safe harbour was a "neat way" of enabling data transfer whilst complying with the European requirement for adequacy.[4]

David Smith, Deputy Commissioner at the UK Information Commissioner's Office (ICO), suggested that the principles-based approach of safe harbour had led to improvements in privacy practices in US, and that it was a better approach than trying to agree everything in legal documents, which do not necessarily effectively embed privacy practice in a business. He recognised, however, that such improvement was not universal.[5] The Government argued that safe harbour itself was an important means of giving protection for EU citizens' data when sent outside the EU to the US.[6] It had allowed the EU to safeguard principles of data protection in the US for EU citizens engaging with safe harbour compliant companies, and enjoyed significant confidence from many business sectors.[7] **We recognise that, despite some weaknesses, the safe harbour arrangements offer clear benefits to citizens and businesses on both sides of the Atlantic.**

Areas for improvement

The Commission Communications set out 13 recommendations on how to improve safe harbour under four broad headings: transparency; redress; enforcement; and access by US authorities. These recommendations are currently being considered by the US authorities, who have undertaken to bring back a package of commitments to bolster safe harbour in response by summer 2014.[8] We consider each group of recommendations in turn.

Transparency

The Commission recommended that:

- Self-certified companies should publicly disclose their privacy policies;
- Privacy policies of self-certified companies' websites should always include a link to the US Department of Commerce safe harbour website which lists all the 'current' members of the scheme;
- Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services; and
- Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.

There is insufficient awareness of safe harbour and the rights it affords EU citizens. Phil Lee said "outside perhaps very specialist audiences such as us, very few people understand that safe harbour exists, what it is and what rights it affords them".[9] He, along with the ICO, Peter Hustinx, the EU Data Protection Supervisor, the European Commission and Government agreed that more needed to be done to increase public awareness of the provisions of safe

[4] Q 3
[5] Q 22
[6] Q 37
[7] Q 36
[8] Q 16
[9] Q 3

harbour and how best to make use of them.[10] The low levels of complaints (which we consider in greater detail below), when considered alongside the significant concerns surrounding safe harbour, suggest that awareness must be improved.

Similarly, more could be done to improve understanding in the corporate world. David Smith suggested simplifying the guidance and explanations offered by the Department of Commerce.[11] The Government agreed that more needed to be done to ensure the business world was aware of the safe harbour principles.[12] **We recommend that the Government scrutinise the package submitted in due course by the US to see whether it addresses the need for clarity for business; and if it does not they should make representations to the European Commission for it to consider this issue in its planned "stock-take" which will follow the US response.**

The Commission was open to greater involvement of national Data Protection Authorities (DPAs) and the safe harbour panel in "reinforcing" citizen's awareness of safe harbour.[13] Professor Charles Raab, University of Edinburgh, judged that national DPAs could be "much more proactive in making safe harbour redress mechanisms, such as they are, better known than they are at the moment".[14] The ICO was open to providing more information about safe harbour and redress mechanisms than it currently did on its website.[15]

We recommend that the ICO update its website and literature with comprehensive and comprehensible information on safe harbour, and in particular on redress provisions. Furthermore, we recommend that the Government make representations to the Commission that the profile of the EU safe harbour panel be raised and that work be done to ensure that citizens understand their rights (including to redress) under safe harbour.

The Department of Commerce has worked extensively with US companies in the last year to add safe harbour notices to privacy policies (where they were missing) and links to its website (which contains a definitive list of certified compliant companies).[16] **The Commission recognised the value of this work in its Communication and insisted that it be completed by March 2014. We ask the Commission to confirm whether the US Department of Commerce has met this deadline.**

Witnesses also welcomed efforts by the Department of Commerce to highlight on its website companies whose safe harbour registration was not up-to-date in red.[17] It would appear that political attention on safe harbour has already led to some improvement in its administration over the last year.

---

[10] Q 6, Q 17, Q 26, Q 36, European Data Protection Supervisor: *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on "Rebuilding Trust in EU-US Data Flows" and on the Communication from the Commission to the European Parliament and the Council on "the Functioning of the Safe Harbour from the Perspective of EU citizens and Companies Established in the EU"*, 2014

[11] Q 26

[12] Q 45

[13] Q 15

[14] Q 8, supplementary written evidence from the Information Commissioner's Office (ICO)

[15] Q 25

[16] Q 6

[17] *Ibid.*

Finally, witnesses pointed to the need for privacy policies to be intelligible if they were to be of value. The Commission has asked for the privacy policies to be in clear language.[18] **We recommend that the Government take steps to ensure that this work is carried out effectively.**

Redress

The Commission recommended that:

- The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel;
- ADR should be readily available and affordable; and
- The US Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

In addition to institutional efforts to improve understanding of rights to redress under safe harbour, it is clear that more must also be done by companies. The Department of Commerce writing to 600 organisations last year saying information about ADR must be available on their websites was welcome[19] but long overdue. The EU Data Protection panel investigates breaches concerning human resources data, and acts as an ADR for companies who select it as their provider.[20] Caspar Bowden, an independent privacy expert and former Chief Privacy Adviser for Microsoft Europe, said that the panel had only received seven complaints since its establishment.[21] Phil Lee suggested that companies should submit themselves to the jurisdiction of national DPAs as this would be the natural place for a consumer to turn to complain.[22] **We invite the Commission to consider whether it should be possible for all disputes over safe harbour to be brought to the EU safe harbour panel in future.**

The European Data Protection Supervisor said that "DPAs have the potential to stop [data] flows [under safe harbour] in concrete cases as a remedy" under Article 3 of the Commission decision on safe harbour. He continued "simply put, data protection authorities have a sanction in concrete cases to intervene and stop data flows, provided that a number of conditions are fulfilled. They are quite demanding, but if they have tried and there is no prospect of things going better, then suspension is an appropriate sanction".[23] The UK ICO said: "essentially we are not able to do that. Safe Harbour is a European Commission finding of adequacy. We have to respect that. So long as businesses comply with Safe Harbour, we cannot stop them transferring data. In that process, it is not for us to judge whether Safe Harbour is adequate or not. If they are not respecting Safe Harbour rules, we can step in and take action against them".[24] The DPAs in Ireland, Luxembourg and Germany have paid considerable attention to this question (and there are court cases pending relating to it).[25] **We recommend that the ICO, perhaps in the context of the Article 29 Working Party, considers further what actions the safe harbour Decision empowers national DPAs to take.**

---

[18] Q 37
[19] Q 7
[20] ICO
[21] Q 27
[22] Q 8
[23] Q 23
[24] *Ibid.*
[25] Q 14

Although the Federal Trade Commission (FTC) has worked to reduce to two the number of ADRs charging a fee,[26] access to redress should never be prevented or inhibited by cost. We are pleased that Mrs Brill, the FTC Commissioner, has called for an end to fees.[27] Paul Nemitz, Director of Fundamental Rights and Citizenship at the Directorate-General for Justice, European Commission, told us that the Commission supports this objective.[28] **We recommend that these initiatives be pursued vigorously by both the Commission and the Government**

Several witnesses suggested that EU citizens should be able to pursue class actions against safe-harbour compliant companies in the US courts.[29] This highlights to us the importance of redress mechanisms being seen as "having teeth". **Efforts to strengthen redress mechanisms are crucial to the success or failure of the current negotiations over bolstering safe harbour.**

Enforcement

The Commission recommended that:

- Following the certification or recertification of companies under the safe harbour, a certain percentage of these companies should be subject to *ex officio* investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements);
- Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after one year;
- In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority; and
- False claims of safe harbour adherence should continue to be investigated.

427 false claims of safe harbour compliance were said to have been made last year, which means that around one of every seven claims of safe harbour compliance is false.[30] This is an unacceptable situation and we are pleased that the Commission has recognised this. The FTC has brought cases against 10 companies in the period 2009-2013, and 13 more were brought in January 20114.[31] It has also brought seven enforcement actions over false claims (all since 2010).[32] **We welcome the FTC's actions in recent years against companies making false claims or otherwise failing to comply with the safe harbour scheme, but the scale of the problem means further action must be taken.**

We are pleased that the Commission, Department of Commerce and the FTC are having constructive talks on how to intensify the *ex officio* validation of

---

[26] Q 8, Federal Trade Commission (FTC): *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the US-EU Safe Harbor Framework*, November 2013 available from: http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf
[27] Q 8
[28] Q 19
[29] Q 8
[30] Q 2
[31] FTC: *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the US-EU Safe Harbor Framework*, *Op. Cit.*
[32] *Ibid.*

compliance.[33] This must be a key part of any package of reforms to safe harbour. Paul Nemitz suggested that the US authorities did not seem terribly open to committing to a percentage of applications that they would investigate in detail.[34] **We believe that the Commission should aim to ensure that investigating false claims of adherence is a priority for the FTC. Such a commitment would be strengthened if there were audits and frequent checks of companies, and these checks were not entirely driven by complaints.**

The FTC was open to increased reporting of enforcement issues from national DPAs.[35] **We invite the ICO to tell us what efforts it makes to ensure US companies operating in the UK claiming adherence to safe harbour do in fact comply with the scheme, and to consider whether this work could be strengthened.**

Concerns about self-certification as the model for safe harbour have been raised by national DPAs since the concept of the scheme was first introduced.[36] Phil Lee suggested that regulators did not have the resources for direct regulation and a full system of audit.[37] He suggested self-regulation "with teeth" in the event of breach was more realistic.[38] Paul Nemitz suggested that "stepping up of *ex officio* checks and controls on companies to supply good papers, and not only to the Department of Commerce, about their self-certification—in the same way in which the tax authorities from time to time go on location and check that the papers comply with reality—will, we believe, provide higher certainty that the safe harbour principles will be complied with in future", and did not consider a change of system away from self-certification likely.[39]

Peter Hustinx argued that the system should be more than complaints-driven.[40] The Government agreed that random checks would be desirable.[41] The ICO said consideration should be given to greater use of third party assessors and auditors if a self-certification system continued.[42] **It is clear that a more credible compliance and audit regime, not simply driven by complaints, needs to be established. We recommend that the Commission and the Government take further steps to achieve this.**

Given the many concerns surrounding the safe harbour scheme, the absence of a published Commission evaluation report between 2004 and 2013, and the continued growth in transfers of personal data due to increasing use of e-commerce facilities, we recommend that the Commission and US authorities commit to producing a regular evaluation of the implementation of the safe harbour Decision, similar to the reports produced concerning transfer of Passenger Name Records and the Terrorist Finance Tracking Programme.

---

[33] Q 17
[34] Q 19
[35] FTC: *Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the US-EU Safe Harbor Framework, Op. Cit.*
[36] ICO
[37] Q 9
[38] *Ibid*.
[39] Q 19
[40] Q 29
[41] Q 44
[42] ICO

Access by US authorities

The Commission recommended that:

- Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the safe harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements; and
- It is important that the national security exception foreseen by the safe harbour Decision is used only to an extent that is strictly necessary or proportionate.

Caspar Bowden said that President Obama's promises in January to reform NSA activities "offers very little comfort" that US surveillance practices would change, and that the national security exemption remains too broad to satisfy the Commission's concerns.[43] Paul Nemitz said that the exemption for national security must not be used as an excuse to routinely examine data which is supposed to be private.[44] He suggested that the US and the EU needed to come to some credible joint oversight and review mechanism for safe harbour, including the use of the national security clause.[45] Peter Hustinx said that if the US's assurances about accessing data only when necessary and in a proportionate manner remain as "general" as they currently are, it could have quite negative political consequences.[46]

David Smith said that the Snowden revelations about the scale of US surveillance of data related to EU nationals were "a bit of a red herring". He argued that the surveillance would have taken place in any case, and it is not exactly clear how much data accessed by US authorities was transferred under the safe harbour agreement.[47] At the same time, however, the problems over surveillance would not be solved by addressing safe harbour alone, and some sort of intergovernmental agreement was needed.[48]

The Commission's attempts to secure US agreement to an approach towards use of national security concerns as a reason to access data transferred under safe harbour based on necessity, proportionality and targeting seem reasonable. At the same time, however, we recognise that security concerns are part of a broader conversation between the EU and the US on data protection and the digital single market.

The Government were very clear that national security questions prompted by the revelations about US surveillance were not matters of EU competence, and that "national security matters are outwith these arrangements and are not intended to be encompassed by them".[49] The Government also said that current and proposed EU legislation on data protection identify different strands to national security, and that the EU does not have competence to act with regard to an activity which falls outside the scope of Community law.[50]

---

[43] Q 4
[44] Q 13
[45] Q 18
[46] Q 30
[47] Q 22
[48] Q 31
[49] Q 33
[50] Q 35

Simon Hughes MP said: "there have to be separate discussions and negotiations to see whether agreement could be arrived at at all on those issues [national security and privacy], but they must not be confused with this".[51] He continued: "what right the citizen has to prevent government interfering with that and taking data and finding information is a debate between citizen and state".[52] **We note and share the Government's view that national security remains a national responsibility and that European institutions have no competence in these areas. That said, there are many issues related to the need for a balance between privacy and security under negotiation at EU level. It would be in the UK's interests to conduct a dialogue on these issues with the European institutions, including the European Parliament, and other Member States to ensure that its position is understood. We do not consider that conducting such a dialogue would compromise the position over competence.**

The issue of suspension of safe harbour

Having considered the weaknesses of the current scheme and the Commission's list of desired improvements, we considered whether the safe harbour scheme should be suspended, as recommended by the European Parliament Committee for Civil Liberties, Justice and Home Affairs (LIBE).[53] The weight of evidence was that the safe harbour agreement should not be suspended at this time, although many felt that the option should remain on the table. Exceptionally, Caspar Bowden argued that there should be a "planned, strategic and phased shutdown of data flows".[54] Phil Lee, Professor Raab, the Government, the EU Data Protection Supervisor, the ICO and the Commission did not support suspension at this time because of the possible adverse effects on business, and said that time should be given to try and improve the arrangements as safe harbour had merits.[55] Professor Raab suggested that "the European Union probably could not realistically revoke" safe harbour "without some envisaged replacement for it, because it plays a big part in EU-US commerce".[56]

Phil Lee and the Government pointed to the adverse effects of uncertainty over safe harbour's future for businesses, which, they claimed, were nervous about committing to future investments that depended upon safe harbour.[57] Phil Lee said that "a number of cloud providers in the US that want to conclude deals with customers in Europe … are already refusing to acknowledge their ability to transfer data on the basis of safe harbour".[58]

Paul Nemitz explained that there would be a point in time when it could be sensible to reopen discussion of suspension: "there is a deadline, which is accepted by the United States, of summer 2014. We are awaiting new commitments from the United States, and then, on the basis of the new commitments, we will see whether they are sufficient to comply with our law".[59] **We are not persuaded of the case for suspension at the present time and endorse the Commission's decision not to give effect to the European Parliament's**

---

[51] Q 34
[52] *Ibid*.
[53] European Parliament: *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,* 2014
[54] Q 5
[55] Q 4, Q 14, QQ 22-3, Q 33
[56] Q 4
[57] Q 4, Q 14
[58] Q 4
[59] Q 13.

recommendation that safe harbour be immediately suspended. We also support the Commission's efforts to strengthen the provisions of safe harbour. The response from the US by summer 2014 about how to strengthen safe harbour seems the appropriate moment for the Commission, the Government and other Member States to consider next steps.

We are copying this letter to William Cash MP, Chair of the House of Commons European Scrutiny Committee; Sir Malcolm Rifkind QC MP, Chair of the Intelligence and Security Committee of Parliament; Sarah Davies, Clerk to the House of Commons European Scrutiny Committee; Les Saunders, Cabinet Office; Patricia Zimmerman, Departmental Scrutiny Co-ordinator; all those who gave evidence; and will be published on our website.

Lord Boswell
Chairman of the European Union Committee

Annex A: Background

The Data Protection Directive and safe harbour

The European Commission's Directive on Data Protection came into effect in October 1998, and prohibited the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection.[60] The United States (US) takes a fairly different approach to privacy from that taken by the EU, predominantly based on self-regulation. In order to bridge the difference in approach and provide a streamlined means for US organisations to comply with the Directive, the US Department of Commerce, in consultation with the European Commission, developed the so-called "safe harbour" framework. This framework allows US companies to self-certify as compliant with 7 principles on the protection of personal data which satisfy the adequacy test of the Directive,[61] namely:

1. **Notice** - Individuals must be informed that their data is being collected and about how it will be used.

2. **Choice** - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.

3. **Onward Transfer** - Transfers of data to third parties may only occur to other organisations that follow adequate data protection principles.

4. **Security** - Reasonable efforts must be made to prevent loss of collected information.

5. **Data Integrity** - Data must be relevant and reliable for the purpose it was collected for.

6. **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.

7. **Enforcement** - There must be effective means of enforcing these rules.[62]

The safe harbour scheme is managed at the US end by the US Department of Commerce, to whom companies declare compliance, and there are currently 3246 certified companies. An organisation must re-certify every 12 months. It was developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. Telecommunications companies and financial institutions are not covered by safe harbour.

The US Department of Commerce maintains a website listing companies currently certified. Each company must have a Dispute Resolution Mechanism. Organisations assure customers that they are committed to resolving any privacy concerns that the customers may have. They should state clearly how customers who believe that their privacy has been violated in contravention of the safe harbour privacy principles should contact the organisation and what

[60] Article 25(1), Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data
[61] FTC: *Federal Trade Commission Enforcement of the US-EU and US-Swiss Safe Harbor Frameworks*, available from at: http://www.business.ftc.gov/documents/0494-federal-trade-commission-enforcement-us-eu-and-us-swiss-safe-harbor-frameworks
[62] *Ibid.*

steps the organisation will take to resolve such issues. Details of the mechanism should be published in an organisation's privacy policy.[63]

The Federal Trade Commission seeks to prevent business practices that are anticompetitive or deceptive or unfair to consumers; to enhance informed consumer choice and public understanding of the competitive process; and to accomplish this without unduly burdening legitimate business activity. It takes action against false statements of adherence and non-compliance.

Historic criticism

Safe harbour has been reviewed by the Commission in 2002 and 2004, and by the independent consultancy firm Galexia in 2008. All three reviews were critical. The 2002 review by the Commission found that although all the elements of the safe harbour framework were in place "a substantial number of organisations that have self-certified adherence to the safe harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard". That review was also critical of the available dispute resolution mechanisms.[64]

The 2004 review by the Commission examined 10% of safe harbour organisations in detail, and made a long list of criticisms, including concerns that a number of companies failed to identify an alternative dispute resolution body. It also raised concerns that "some alternative recourse mechanisms still fail to comply with applicable safe harbour requirements" and "less than half of organisations post privacy policies that reflect all seven safe harbour Principles".[65]

The 2008 review by Galexia raised concerns that many aspects of the Safe harbour Framework were not working. It found that the problems identified in previous reviews of the safe harbour have not been rectified, and that the number of false claims made by organisations represents a significant privacy risk to consumers. Galexia identified numerous problems with data accuracy and basic compliance with basic framework requirements.[66]

Recent criticism

In 2013, greater attention was paid to the arrangements given the revelations regarding the US mass data collection and surveillance program, PRISM.

The European Parliament Committee for Civil Liberties, Justice and Home Affairs (LIBE) has been at the forefront of the PRISM debate, investigating what these revelations mean for US-EU data protection agreements. It has gathered a range of experts including Members of the European Parliament (MEPs), Heads of EU Data Protection Authorities, the European Data Protection Supervisor and some members of industry to discuss, among other issues, the effectiveness of safe harbour. Some witnesses were relatively positive about the framework, such as the European Data Protection Supervisor, who considered that even though the

---

[63] The Commission Communications summarise the safe harbour provisions as does the list of Frequently Asked Questions published by the FTC available from its website: http://export.gov/safeharbor/eu/eg_main_018493.asp

[64] European Commission: *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, 2002

[65] European Commission: *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, 2004

[66] Galexia: *The US Safe Harbor – Fact or Fiction?*, 2008

framework is not perfect, it provides significant safeguards to enable DPAs to intervene if necessary, such as stopping data transfers. Others, particularly LIBE Committee MEPs, questioned safe harbour's effectiveness and even appropriateness. At the end of the hearing, some members of the LIBE Committee announced that it would call upon the European Commission to suspend the Safe harbour framework until a solution is found. The Committee's final report reflected that call for suspension.[67]

Our enhanced scrutiny

It was in the context of these reactions and ongoing consideration of the issues that we decided to conduct enhanced scrutiny on the two Commission Communications. We heard oral evidence from:

12 March 2014

- Phil Lee, Privacy and Information Law Group, Field Fisher Waterhouse LLP;
- Chris Connolly, Galexia;
- Caspar Bowden, an independent privacy expert and former Chief Privacy Adviser for Microsoft Europe; and
- Professor Charles Raab, University of Edinburgh.

2 April 2014

- Paul Nemitz, Director of Fundamental Rights and Citizenship at the Directorate-General for Justice, European Commission;
- David Smith, Deputy Commissioner at the Information Commissioner's Office; and
- Peter Hustinx, European Data Protection Supervisor.

9 April 2014

- Simon Hughes MP, Minister of State, Ministry of Justice (MoJ);
- Simon James, Deputy Director, Information Rights and Devolution, MoJ; and
- Tim Jewell, Deputy Director, Information and Human Rights Legal Directorate, MoJ.

We are grateful to all those who have assisted us in this work; the evidence taken is available on our website.[68]

[67] European Parliament: *Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs,* 2014.
[68] www.parliament.uk/hleuf

Appendix B: Membership and interests

Interests declared:

Lord Hannay of Chiswick (Chairman)

- Member, Advisory Board of the Centre for European Reform
- Member, the Future of Europe Forum, the proactive advisory board for the Centre for British Influence through Europe

Viscount Bridgeman

- Former Chairman (unpaid) of the Hospital of St John & St. Elizabeth
- Joint President, Reed's School

Lord Judd

- Emeritus Governor of the London School of Economics and Political Science
- Life Member of Court, Lancaster University
- Member of Court, Newcastle University
- President of the West Cumbria Hospice at Home
- Member of the All Party Parliamentary Group on Human Rights
- Member of the All Party Parliamentary Group on Penal Affairs
- Member of the All Party Parliamentary Group on Police
- Trustee, Saferworld

Baroness Prashar

- Member of the Committee appointed to consider UK's involvement in Iraq
- President, Royal Commonwealth Society
- Vice Chair, All-Party Parliamentary Group for the Commonwealth
- President, UK Council for International Student Affairs
- President, Community Foundation Network
- Trustee, Cumberland Lodge
- Governor and Member of Management Committee, Ditchley Foundation
- Patron, Runnymede Trust
- President, National Literacy Trust
- Deputy Chair, British Council

Lord Sharkey

- Governor, Institute for Government

Lord Wasserman

- Former Government adviser on policing and criminal justice matters

No interests declared:

Baroness Benjamin
Lord Blencathra
Lord Faulkner of Worcester
Lord Morris of Handsworth
The Earl of Stair
Lord Tomlinson