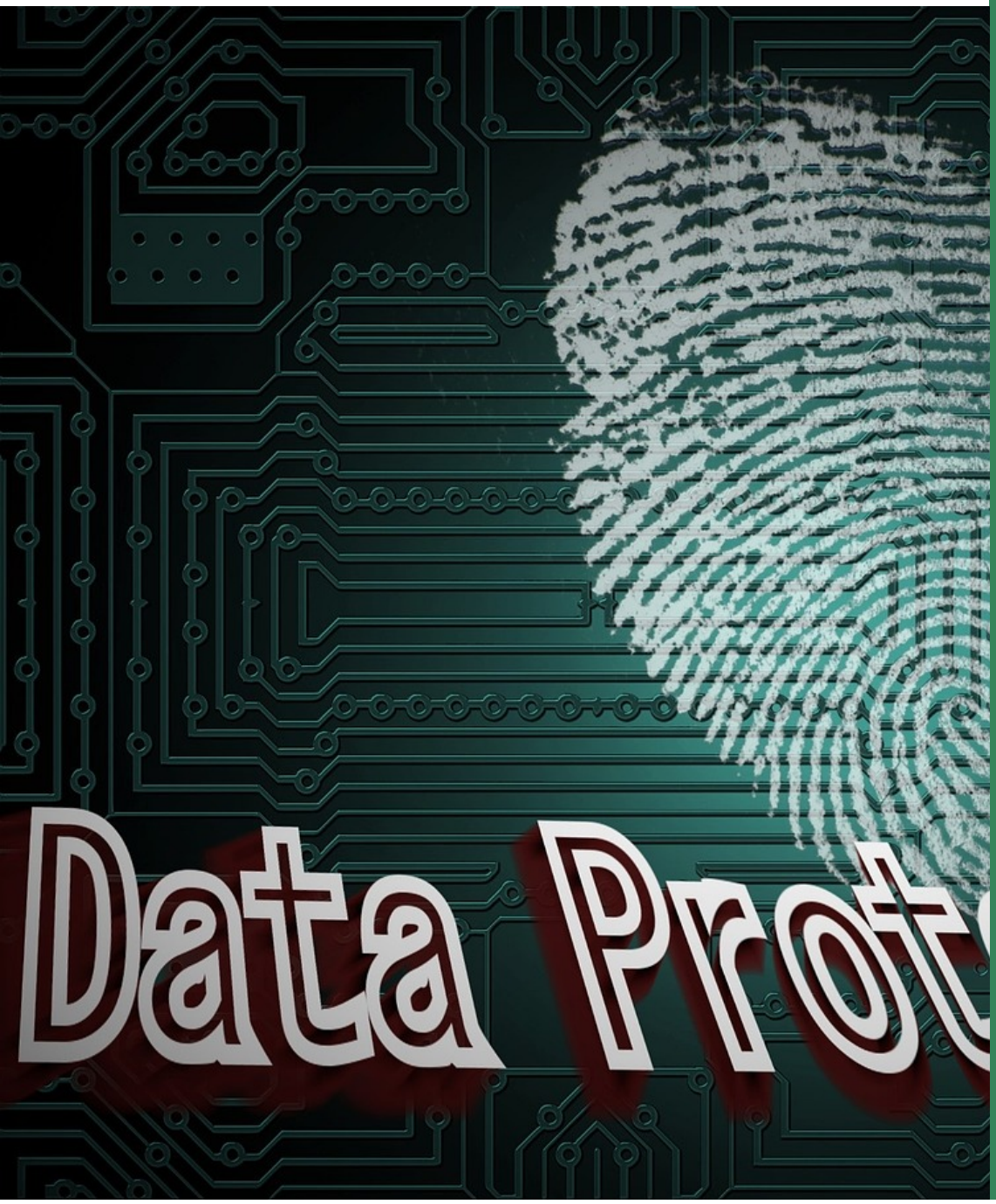
HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 8251, 13 April 2018

Data Protection Bill [HL] 2017-19: Committee Stage Report

By John Woodhouse



Contents:

Contents

Summary

The *Data Protection Bill [HL] 2017-19* has a number of purposes:

- it sets out how the UK would apply the derogations available under the General Data Protection Regulation (GDPR) – the GDPR will apply in the UK from 25 May 2018
- it would bring the Law Enforcement Directive (LED) into UK law – the LED will apply from 6 May 2018
- it would update the laws governing the processing of personal data by the intelligence services
- it aims to ensure that the UK would be able to freely exchange data with the European Union post-Brexit
- it would repeal the *Data Protection Act 1998*.

The Bill was originally introduced in the House of Lords on 13 September 2017 where it was broadly welcomed by the opposition parties. However, at Report stage, the Government was defeated on amendments relating to press regulation – i.e. on commencing part 2 of the Leveson inquiry and bringing section 40 of the *Crime and Courts Act 2013* into force.

The Bill [Number 153] was introduced in the House of Commons on 18 January 2018. Much of the second reading debate on 5 March 2018 was taken up with the Lords amendments on press regulation.

The Bill had eight sittings in Public Bill Committee between 13 March and 22 March 2018. The Lords amendments on press regulation were overturned in Committee. Labour has said that it will try and put these back into the Bill at Report stage. The Bill's provisions on immigration control have proved controversial but are still in the Bill after Labour and the SNP failed to get them removed. This Paper looks at these issues in further detail. It also looks at some of the other subjects on which the Committee divided or where there was lengthy debate. These included:

- The representation of data subjects
- Obtaining an adequacy decision from the European Commission to enable the free flow of data between the UK and the European Union after Brexit
- Automated decision making
- Data sharing by the intelligence services
- Exemptions to the applied GDPR scheme

The Bill [Number 190], as amended in Committee, has been published. A date for Report stage has yet to be announced.

Related Library Briefing: *The Data Protection Bill [HL] 2017-19* (CBP 8214, 1 March 2018).

1. Second reading

The Bill had its second reading in the House of Commons on 5 March 2018.[1]

Tom Watson, the Shadow Secretary of State, said that Labour welcomed "improvements" made to the Bill in the House of Lords but said that further changes were needed to, among other things:

- ensure the continuous flow of data with the EU after Brexit[2]
- incorporate article 8 of the EU Charter of Fundamental Rights into the Bill[3]
- allow civil society and other bodies to act on behalf of data subjects[4]

He also said that Labour would seek to retain the Lords amendments on press regulation i.e. on section 40 of the *Crime and Courts Act 2013* and on part 2 of the Leveson inquiry.[5]

Liam Byrne, Shadow Minister for the Digital Economy, said that Labour would attempt to "delete" the Bill's measures on immigration control.[6] He also raised concerns about the Bill having "insufficient safeguards" relating to algorithmic decision-making.

Brendan O'Hara, the SNP Spokesperson for Culture and Media, said that his party would challenge the Bill's provisions on immigration control.[7] He also raised concerns about obtaining an adequacy decision from the European Commission, automated decision making, and the Lords amendments on press regulation.

Sir Edward Davey, the Liberal Democrat Spokesperson on Home Affairs, referred to the potential loss of UK influence in the data protection field after Brexit. He said that the GDPR was a "perfect example of why Brexit is a bad idea for the UK".[8] Sir Edward also spoke against the Bill's provisions on immigration control.[9]

Although Joanna Cherry, the SNP's spokesperson on Justice and Home Affairs, said that Leveson related issues should not dominate debate on the Bill,[10] much of the second reading was taken up with the Lords amendments. However, other issues that were raised included:

- The potential impact of the GDPR on small businesses[11]

1 HC Deb 5 March 2018 cc75-132
2 HC Deb 5 March 2018 c83
3 HC Deb 5 March 2018 c84
4 HC Deb 5 March 2018 cc84-5
5 HC Deb 5 March 2018 cc85-7
6 HC Deb 5 March 2018 c128
7 HC Deb 5 March 2018 c89
8 HC Deb 5 March 2018 c122
9 HC Deb 5 March 2018 cc122-4
10 HC Deb 5 March 2018 c108
11 See James Cartlidge at HC Deb 5 March 2018 c79, Rebecca Pow c81, Stephen Timms c102

- The potential impact of the GDPR on universities and the research sector[12]
- The need to protect children and young people online[13]

At the end of the debate Margot James, Minister of State at the Department for Digital, Culture, Media and Sport (DCMS), tried to reassure the House on the immigration exemption.[14] She also said that the Government would "attempt to defeat" the Lords amendments on press regulation.[15]

12 See Daniel Zeichner at HC Deb 5 March 2018 cc97-8
13 See Christine Jardine at HC Deb 5 March 2018 c115, Eddie Hughes cc116-7
14 HC Deb 5 March 2018 cc130-1
15 HC Deb 5 March 2018 c131

2. Public Bill Committee

The Bill had eight sittings in Public Bill Committee between 15 March and 22 March 2018. The following sections of this Paper look at the issues on which the Committee divided as well as some of the areas that prompted lengthy debate. It is not intended to cover everything that was discussed in Committee.

Written evidence submitted to the Committee is available from the parliamentary website.

The Bill [190], as amended in Committee, has been published. A date for the Bill's Report stage has yet to be announced.

2.1 The protection of personal data

When clause 2 (the protection of personal data) was considered, Liam Byrne moved **new clause 12**:

> "(1) A person ("P") has the right to protection of personal data concerning him or her.
>
> (2) Personal data must be processed fairly for specified purposes as set out in the GDPR, and in accordance with the provisions, exceptions and derogations of this Act; and on the basis of the consent of P or some other legitimate basis.
>
> (3) The Information Commissioner shall be responsible for ensuring compliance with the rights contained within this section."

The purpose of the new clause would be to incorporate Article 8 (the right to the protection of personal data) of the Charter of Fundamental Rights of the European Union into the Bill.

When introducing the new clause, Mr Byrne spoke of the need to obtain an adequacy agreement to ensure friction-free trade with the EU after Brexit:

> (…) When we leave the European Union, we will need to agree with it an adequacy agreement by which it recognises the data protection regime in this country as adequate and therefore indicates that it is permissible for us to share data across the continental borders. The question, therefore, is how do we put that adequacy agreement beyond any doubt, not just for the immediate years after Brexit but for the decades to come? We know that trade will be fundamental to the health and wellbeing of our economy over many, many years. Let us put the data sharing regime between us and the European Union beyond doubt, not just for the short term but for the long term. Failure to get an adequacy agreement could arguably be fatal to the British economy. We simply cannot consider a shred of risk to that adequacy agreement….
>
> (…) A British tradition helped shape the EU charter of fundamental rights…In killing off the whole thing, and in particular article 8—the fundamental foundational right to privacy—we create a new risk to keeping in lockstep the data protection regime in this country and the data protection regime in the European Union…[16]

[16] Public Bill Committee 13 March 2018 c6

Brendan O'Hara supported the new clause. He said that it was needed for two reasons:

> (…) With the Bill as it stands, we see an erosion of the rights of UK citizens in a range of areas. This is particularly important because, as drafted, the EU (Withdrawal) Bill, eliminates important rights that are protected by article 8 which would otherwise constrain Ministers' ability to erode the fundamental data protection rights that we currently enjoy.
>
> On top of that, it is essential that, post-Brexit, the United Kingdom has an adequacy agreement with the rest of the European Union…[17]

For the Government, Margot James agreed that an adequacy agreement was "absolutely essential"[18] for the free flow of data after Brexit. However, she said that the new clause was unnecessary and would cause confusion:

> (…) There is no doubt in our minds that we have fully implemented the right to data protection in our law and gone further. Clause 2 is designed to provide additional reassurance. Not only will that be clear in the substance of the legislation, but it is on the face of the Bill. The Bill exists to protect individuals with regard to the processing of all personal data…
>
> New clause 12 creates a new and free-standing right, which is the source of our concern. Subsection (1) is not framed in the context of the Bill. It is a wider right, not constrained by the context of EU law. However, the main problem is that it is not necessary. It is not that we disagree with the thinking behind it, but it is not necessary and might have unforeseen consequences, which I will come to.
>
> Article 6 of the treaty on European Union makes it clear that due regard must be had to the explanations of the charter when interpreting and applying the European charter of fundamental rights. The explanations to article 8 of the charter confirm that the right to data protection is based on the right to respect for private life in article 8 of the ECHR. The European Court of Human Rights has confirmed that article 8 of the ECHR encompasses personal data protection. The Government have absolutely no plans to withdraw from the European Court of Human Rights.
>
> The new right in new clause 12 would create confusion if it had to be interpreted by a court. For rights set out in the Human Rights Act, there is a framework within which to operate. The Human Rights Act sets out the effect of a finding incompatible with rights. However, new clause 12 says nothing about the consequences of potential incompatibility with this new right to the protection of personal data.[19]

Margot James also said that the EU Charter of Fundamental Rights "merely catalogues rights that already exist in EU law":

> (…) The rights, including to data protection…arise from treaties, EU legislation and case law. They do not arise from the European charter of fundamental rights, so we argue that the new clause is completely unnecessary.[20]

---

17 Public Bill Committee 13 March 2018 c7
18 Public Bill Committee 13 March 2018 c9
19 Public Bill Committee 13 March 2018 c10
20 Public Bill Committee 13 March 2018 c11

Darren Jones (Labour) disagreed:

> The right exists in its own right in the European charter of fundamental rights. That is why European Courts refer to it when making decisions. If the Courts did not think that it was an established right in itself, they would refer to the other sources of legislation that the Minister mentioned. It therefore must, as a matter of logic, be a legal right that is fundamental; otherwise, the Courts would not refer to it.[21]

Liam Byre said that the Minister's argument against the new clause was "very weak":

> (…) First, there can be no risk of confusion because this is not a new right. It is a right we already enjoy today, and our courts are well practised in balancing it with the other rights we enjoy. We are simply seeking to roll over the status quo into the future to put beyond doubt an adequacy agreement not just in the immediate years after we leave the European Union but in the decades that will follow.
>
> Secondly, the Minister sought to persuade us that the new clause was not needed…she said that the source of our new protections would be the incorporation of EU case law and legislation as enshrined by the European Union (Withdrawal) Bill. Of course, that is simply not applicable to this case, because the one significant part of European legislation that the withdrawal Bill explicitly does not incorporate is the European charter of fundamental rights. The Minister slightly gave the game away when she read out the line in her briefing note that said that the rights we currently have in EU law would be enshrined and protected "so far as it is possible to do so." That is exactly the kind of risk we are seeking to guard against.
>
> As noble peers argued in the other place, the challenge with incorporating the GDPR into British law is that this is a piece of regulation and legislation that reflects the world of technology as it is today. It is not the first bit of data protection legislation and it will not be the last. At some point in the years to come, there will be a successor piece of legislation to this Bill and the courts' challenge will be to make judgments that interpret an increasingly outmoded and outdated piece of legislation. We have to ensure that judgments made in the British courts and in the European courts remain in lockstep. If we lose that lockstep, we will jeopardise the future of an adequacy agreement…[22]

Liam Byrne said that he would put the new clause to a vote, but hoped that the Government would "see sense" before then.[23]

The Chair of the Committee said that a vote on new clause 12 would take place at a later date.[24]

2.2 Lawfulness of processing

The GDPR

Article 6 of the GDPR sets out the circumstances when data processing is lawful. Under Article 6(1)(e), data processing is lawful where it "is necessary

---

21 Public Bill Committee 13 March 2018 c11
22 Public Bill Committee 13 March 2018 c13
23 Public Bill Committee 13 March 2018 c14
24 Public Bill Committee 13 March 2018 c14

for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". Article 6(2) allows Member States to be more specific about how this will apply.

The Bill

Under **clause 8** of the Bill, processing under Article 6(1)(e) would include processing for:

- the administration of justice
- the exercise of a function of either House of Parliament
- the exercise of a function conferred on a person by an enactment
- the exercise of a function of the Crown, a Minister of the Crown or a government department.

The Explanatory Notes state that clause 8 gives a "non-exhaustive list of examples" and is similar to that contained in paragraph 5 of Schedule 2 to the 1998 Act.[25]

Debate in Public Bill Committee

Daniel Zeichner (Labour) moved **amendment 140** to ensure that university researchers and public bodies with a research function would be able to use the "task in the public interest" basis for the lawful processing of personal data where consent was not a viable basis.[26] He said that the Wellcome Trust and the Sanger Institute were worried that clause 8 had "narrowed the public interest terminology to a very narrow concept, which will be confined to public and judicial administration" and that this would have a negative impact on research:

> (…) One of our universities' main functions is to undertake research that will often involve processing personal data. In some cases, GDPR compliant consent, which may seem the obvious way of doing it, will not be the most appropriate lawful basis on which to process that data. It is therefore really important that an article 6 lawful basis for processing is available to university researchers with certainty and clarity.
>
> The Government have included reference to medical research purposes in the explanatory notes, but the worry is that that does not necessarily have weight in law and the reference excludes many other types of research that are rightly conducted by universities. This is not a satisfactory resolution to the problems that are faced.[27]

Margot James argued that the amendment was unnecessary:

> (…) Clause 8 helps to explain the meaning of "public interest tasks" by providing a list of processing activities that fall into that category. The list was always intended to be non-exhaustive, which is why we have used the word "includes". In law, that word is always assumed to introduce a non-exhaustive list, and we have tried to make that point as clear as possible in the explanatory notes.
>
> Additional phrasing in the Bill, such as that proposed in amendment 140, would add nothing to what is already in the clause's

25 Para 89 of the Explanatory Notes to Bill 153
26 Public Bill Committee 13 March 2018 cc17-19
27 Public Bill Committee 13 March 2018 c21

> interpretation under English law, and it would risk confusing the interpretation of the many other uses of that word elsewhere in the Bill. Given the non-exhaustive nature of the list, the fact that publicly funded research is not mentioned specifically does not mean that the research functions of public bodies will not be considered as "public interest tasks", thereby providing a legal basis for universities to process personal data.
>
> The Information Commissioner's Office said:
>
> "Universities are likely to be classified as public authorities, so the public task basis is likely to apply tomuch of their processing".
>
> Its guidance goes on to give "teaching and research purposes" as one such example. Hon. Members will appreciate that the list could become very long and still not be conclusive if we included everything that the Government and the Information Commissioner's Office consider amounts to a "public interest task"…[28]

The amendment was negatived on division by 10 votes to 8.[29]

Government amendment 9

Government **amendment 9** adds a reference to the processing of personal data that is necessary for "an activity that supports or promotes democratic engagement" to clause 8. Margot James explained:

> Since the Bill's introduction, it has been brought to our attention by a range of stakeholders from all sides of the political divide that there is concern about how processing for the purpose of democratic engagement should be treated for the purposes of the GDPR.
>
> Having considered the matter further since the debates in the other place, the Government have concluded that it would be prudent to include a provision in the Bill to provide greater clarity to those operating in the area of democratic engagement. Helpfully, clause 8 already provides high-level examples of processing activities that the Government consider could be undertaken on grounds of public interest if the data controller can demonstrate that the processing is necessary for the purposes of the processing activity. As a consequence of the importance that the Government attach to the matter, amendment 9 adds to that list
>
> "an activity that supports or promotes democratic engagement."
>
> That term has been deliberately chosen with the intention of covering a range of activities carried out with a view to encouraging the general public to get involved in the exercise of their democratic rights. We think that that could include communicating with electors, campaigning activities, supporting candidates and elected representatives, casework, surveys and opinion gathering and fundraising to support any of those activities. Any processing of personal data in connection with those activities would have to be necessary for their purpose and have a legal basis. We will ensure that the explanatory notes to the Bill include such examples, to assist the interpretation of what this provision might mean in practice.[30]

---

28 Public Bill Committee 13 March 2018 cc20-1
29 Public Bill Committee 13 March 2018 c21
30 Public Bill Committee 13 March 2018 c22

She confirmed that canvassing and collecting canvassing returns would be covered by the amendment.[31] The amendment was agreed without division.[32]

2.3 Special categories of personal data and criminal convictions etc data

The GDPR

Article 9(1) of the GDPR prohibits the processing of special categories of personal data (referred to as "sensitive personal data" in the 1998 Act) which "reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" and the processing of "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

Article 9(2) sets out when the prohibitions don't apply. Some of these have direct effect, others take the form of derogations requiring Union or Member State law in order to be relied on, subject to safeguards.

The Bill

Clause 10 makes provision for the processing of special categories of personal data for reasons of:

- Employment, social security and social protection
- Substantial public interest
- Health and social care
- Public health
- Archiving, research and statistics

Schedule 1 sets out a number of distinct areas in which the processing of the special categories of personal data would be permitted in the UK.

Clause 10 would allow the Secretary of State to make regulations that would:

- amend Schedule 1 by adding or varying conditions or safeguards, and
- omit conditions or safeguards added by regulations under the clause
- make consequential amendments to the clause

The regulations would be subject to the affirmative procedure.

The regulation making powers in clause 10 were debated and amended when the Bill was considered in the House of Lords. For discussion see pp24-5 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

31 Public Bill Committee 13 March 2018 c22
32 Public Bill Committee 13 March 2018 c23

Debate in Public Bill Committee

Stuart McDonald, the SNP Spokesperson on Immigration, Asylum and Border Control, moved **amendment 129**, together with amendments 132 and 134, to further remove the "Henry VIII powers" from clauses 10, 35 and 86 respectively.[33] He said:

> (…) There should always be a presumption against Henry VIII clauses, and that is definitely the case when we are talking about such sensitive information. There are fine balances to be struck between the right to privacy and the necessity of our law enforcement agencies, intelligence services and other bodies being able to process that information. The Bill seeks to strike that balance very finely.
>
> It would therefore be inappropriate to give the Government the power to hand out new powers to process sensitive data without proper scrutiny and the ability of parliamentarians in this place to amend such proposals. It would be completely inappropriate to do it by all or nothing, "accept or reject" statutory instrument procedures…[34]

The amendment was supported by Labour.[35]

Margot James resisted the amendment:

> (…) Amendment 129 would remove the ability to amend schedule 1 via secondary legislation. That would be particularly damaging because it would mean that primary legislation might be needed every time the need for a new processing activity involving special categories of data arose. The 1998 Act was itself amended several times through secondary legislation, and it is important that we retain the flexibility to respond to emerging technologies and the different ways in which data might be used in the future…[36]

The amendment was negatived on division by 10 votes to 9.[37]

Government amendments to Schedule 1

Government amendments were agreed to Schedule 1 to ensure that sensitive data would be able to "be processed without consent in certain circumstances for legitimate safeguarding activities that are in the substantial public interest".[38]

Victoria Atkins, Parliamentary Under-Secretary of State at the Home Office, noted that the amendments were a response to concerns raised in the House of Lords. She explained the purpose of amendment 85 with an example:

> (…) Amendment 85 permits the processing of sensitive personal data, which is necessary to safeguard children from physical, emotional, sexual and neglect-based abuse.
>
> (…) An example provided by a sports governing body is that a person may make an allegation or complaint about a volunteer that prompts an investigation. Such investigations can include witness statements,

33 Public Bill Committee 13 March 2018 cc25-7
34 Public Bill Committee 13 March 2018 c27
35 Public Bill Committee 13 March 2018 cc27-8
36 Public Bill Committee 13 March 2018 c29
37 Public Bill Committee 13 March 2018 c29
38 Public Bill Committee 13 March 2018 c38

> which reference sensitive personal data, including ethnicity, religious or philosophical beliefs, sexual orientation and health data.
>
> In some instances, the incident may not reach a criminal standard. In those cases, the sports body may have no legal basis for keeping the data. Keeping a record allows sports bodies to monitor any escalation in conduct and to respond appropriately. Forcing an organisation to delete this data from its records could allow individuals that we would expect to be kept away from children to remain under the radar and potentially leave children at risk.[39]

She also explained amendment 86 with an example:

> Amendment 86 deals with a related issue where processing health data is necessary to protect an individual's economic wellbeing, where that individual has been identified as an individual at economic risk. UK banks have a number of regulatory obligations and expectations which are set out in the Financial Conduct Authority's rules and guidance. In order to meet best practice standards in relation to safeguarding vulnerable customers, banks occasionally need to record health data without the consent of the data subject.
>
> An example was given of a bank which was contacted by a family member who was alerting the bank to an elderly customer suffering from mental health problems who was drawing large sums of money each day from their bank account and giving it away to a young drug addict whom they had befriended. The bank blocked the account while the family sought power of attorney.
>
> Again, the amendment seeks to clarify the position and give legal certainty to banks and other organisations where that sort of scenario arises or where, for example, someone suffers from dementia and family members ask banks to take steps to protect that person's financial wellbeing.
>
> The unfortunate reality is that there still exists a great deal of uncertainty under current law about what personal data can be processed for safeguarding purposes…These amendments are aimed at tackling these issues. We want to stop the practice whereby some organisations have withheld information from the police and other law enforcement agencies for fear of breaching data protection law and other organisations have been unclear as to whether consent to processing personal data is required in circumstances where consent would not be reasonable or appropriate. The amendments intend to address the uncertainty by providing relevant organisations with a specific processing condition for processing sensitive personal data for safeguarding purposes.[40]

The amendments were agreed without division.[41]

2.4 Automated decision making

The GDPR

Article 22 of the GDPR states that data subjects have the right "not to be subject to a decision based solely on automated processing, including

39 Public Bill Committee 13 March 2018 c39
40 Public Bill Committee 13 March 2018 c40
41 Public Bill Committee 13 March 2018 cc40-1

profiling, which produces legal effects concerning him or her or similarly significantly affects him or her" unless it is:

- necessary for the creation and performance of a contract between a data subject and data controller
- authorised by law to which the data controller is subject and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or
- based on the data subject's explicit consent

Automated decision-making is not defined in the GDPR. However, the Article 29 Data Protection Working Party[42] guidelines[43] on automated decision-making suggest that a decision will be "based solely on automated processing" unless the level of human intervention "is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision".[44]

The Bill

Clause 14 relates to Article 22 and would provide additional safeguards where automated decision making is authorised by law to which the data controller is subject.

At Committee stage in the Lords, Liberal Democrat and Labour amendments explored, among other things, the impact of algorithmic decision-making, Artificial Intelligence, and the meaning of decisions taken solely on the basis of automatic processing.[45] For further detail, see pp26-8 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Debate in Public Bill Committee

Liam Byrne moved **amendment 153.**[46] He explained its purpose:

> Clauses 14 and 15 allow automated processes where they are authorised by law. That creates the obligation of giving notice and what is, in effect, an ex post facto right of appeal. The Opposition's argument is somewhat different: it is better not to take decisions on the basis of automatic processing of data where those decisions affect our human rights.
>
> (…) The great risk with automatic processing of data and the use of algorithms, whether in the public or private sector, where there is an ex post facto right of review, is that our surgeries end up as the final court of appeal. It will then fall to us to intervene…We think it would be better if we stopped the potential for that snowballing of problems in future by stopping the ability of algorithms to take decisions where human rights are engaged.
>
> The Minister may say that there are lots of nice safeguards in the Bill, such as that it is permitted only where it is authorised by law.

---

42 The Article 29 Data Protection Working Party is composed of "a representative of the supervisory authority (ies) designated by each EU country; a representative of the authority (ies) established for the EU institutions and bodies; a representative of the European Commission"

43 Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, October 2017

44 Paras 208 and 116 of the Explanatory Notes to Bill 153

45 Public Bill Committee 13 November 2017 cc1862-7

46 Public Bill Committee 13 March 2018 cc49-52

> Frankly, that is a hopeless safeguard, particularly when it comes to policing, because the police are authorised to do so much by law. The police can stop people, search people and put through procedures that would deny people bail. The police can add people to databases. If those decisions are taken by an algorithm, all sorts of problems will arise. We think that there should be much stronger safeguards.
>
> Through the amendments, basically we want to try to separate the business of automatic data processing from the possibilities of automatic decision taking. It is fine for data to be processed using algorithms in a way that is automated, but not for decision taking to be automated. We want to leave unfettered the rights of businesses and the Government to process data in an automatic way, but we want fetters around the business of decision taking. It is okay to use algorithms to inform decisions but not to take decisions. The idea of a post hoc review, as many of us know from our own casework, is a nice idea that is not a reality open to many citizens in this country. There is no substitute for preventing a decision being wrong in the first place…[47]

Margot James said that she attached "far greater meaning" to the Bill's safeguards than Mr Byrne:

> (…) The safeguards embed transparency, accountability and a right to request that the decision be retaken, and for the data subject to be notified should a decision be made solely through artificial intelligence.
>
> (…) we have translated the GDPR protections into law through the Bill. As I said, the data subject has the right to request that the decision be retaken with the involvement of a sentient individual.
>
> That will dovetail with other requirements. By contrast, the amendments are designed to prevent any automated decision-making from being undertaken under article 22(2)(b) if it engages the rights of the data subject under the Human Rights Act 1998.[48]

The amendment was negatived on division by 10 votes to 9.[49]

Brendan O'Hara moved **amendment 130** to provide protection for individuals who are subject to purely automated decision-making:

> (…) I urge the Government to look again at the parts of the Bill about automated decision making, to ensure that when it is carried out, a human being will have to decide whether it is reasonable and appropriate to continue on that course. That human intervention will provide transparency and capability, and it will ensure that the state does not infringe on an individual's freedoms—those fundamental rights of liberty and privacy—which are often subjective. Because they are subjective, they are beyond the scope of an algorithm.
>
> There are serious human rights, accountability and transparency issues around fully automated decision making as the Bill stands. Amendment 130 says that any human involvement has to be "meaningful". We define meaningful human oversight as being significant, of consequence and purposeful. As I have said, that is far beyond the scope of an algorithm. If an individual's rights are to be scrutinised and possibly fundamentally affected, it is an issue of basic

47 Public Bill Committee 13 March 2018 c51
48 Public Bill Committee 13 March 2018 cc53-4
49 Public Bill Committee 13 March 2018 c55

> fairness that the decision is made, or at least overseen, by a sentient being.[50]

Margot James resisted the amendment:

> (…) Amendment 130 also seeks to clarify what is meant by a decision
>
> "based solely on automated processing"
>
> to ensure that human intervention must be meaningful.
>
> We consider the amendment unnecessary, as the phrase, especially when read with recital 71 of the GDPR, already provides for this…
>
> However, even if it were not the case, we could not go around altering definitions under the GDPR; it is not in our gift to do so.[51]

Brendan O'Hara said that he would put his amendment to a division at Report stage.[52]

Employment and automated decision making

Liam Byrne moved **new clauses 7 and 8 to 11** relating to algorithmic decision-making in the context of employment:[53]

> (…) Central to the new clauses is a concern that unaccountable and highly sophisticated automated or semi-automated systems are now making decisions that bear on fundamental elements of people's work, including recruitment, pay and discipline…[54]
>
> (…) This battery of new clauses sets out to do five basic things. First, they set out some enhancements and refinements to the Equality Act 2010, in a way that ensures that protection from discrimination is applied to new forms of decision making, especially when those decisions engage core rights, such as rights on recruitment, terms of work, or dismissal. Secondly, there is a new right to algorithmic fairness at work, to ensure equal treatment. Thirdly, there is the right to an explanation when a decision is taken in a way that affects core elements of work life, such as a decision to hire, fire or suspend someone. Fourthly, there is a new duty for employers to undertake an algorithmic impact assessment, and fifthly, there are new, realistic ways for individuals to enforce those rights in an employment tribunal. It is quite a broad-ranging set of reforms to a number of different parts of legislation.[55]

Victoria Atkins said that the Government did not support the new clauses. She said that the Equality Act already protected workers against direct or indirect discrimination by computer or algorithm-based decisions:

> (…) The Act is clear that in all cases, the employer is liable for the outcome of any of their actions, or those of their managers or supervisors, or those that are the result of a computer, algorithm or mechanical process. If, during a recruitment process, applications from people with names that suggest a particular ethnicity were rejected for that reason by an algorithm, the employer would be liable for race discrimination, whether or not they designed the algorithm with that intention in mind.

---

50 Public Bill Committee 13 March 2018 cc52-3
51 Public Bill Committee 13 March 2018 c54
52 Public Bill Committee 13 March 2018 c55
53 Public Bill Committee 22 March 2018 cc311-5
54 Public Bill Committee 22 March 2018 c314
55 Public Bill Committee 22 March 2018 c315

> The right hon. Gentleman placed a great deal of emphasis on advertising and, again, we share his concerns that employers could seek to treat potential employees unfairly and unequally. The Equality and Human Rights Commission publishes guidance for employers to ensure that there is no discriminatory conduct and that fair and open access to employment opportunities is made clear in the way that employers advertise posts.
>
> The same principle applies in the provision of services. An automated process that intentionally or unintentionally denies a service to someone because of a protected characteristic will lay the service provider open to a claim under the Act, subject to any exceptions.[56]

Mr Byrne withdrew the new clauses but said that he might return to the issue at Report stage.[57]

2.5 Exemptions - immigration control

The Bill

Clause 15 and **Schedules 2, 3 and 4** relate to exemptions, restrictions and adaptations of the GDPR.

Part 1 Paragraph 4 of **Schedule 2** contains new exemptions to data subjects' rights for the purposes of maintaining effective immigration control or for the investigation or detection of activities that would undermine it.

The exemption has attracted criticism from, among others, Liberty and the Open Rights Group. When the Bill was considered in the Lords, amendments were moved – unsuccessfully – to remove paragraph 4 from Schedule 2. For discussion, see pp30-3 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Debate in Public Bill Committee

Liam Byrne moved **amendment 156** to remove paragraph 4 from Schedule 2.[58] He pointed to the importance of subject access requests in immigration cases and said that the Bill's provision for immigration control could lead to "terrible injustices":

> (…) SARs are one of the most powerful instruments by which anybody in this country, whether a citizen or someone applying to become a citizen, or applying for a legal right to remain, can acquire information that is crucial to the delivery of justice. Many of us are incredibly sympathetic to the job that the Home Office does. Many of us will want a tougher regime in policing immigration, in particular illegal immigration, but I suspect every member of the Committee is also interested in the good conduct of justice and administrative justice. As someone who served in the Home Office for two years, I had to take some very difficult decisions, including to release subject access request information that I absolutely did not want to go into the public domain. Sometimes it was right to release that information because it helped ensure that justice was done in the courts of this land.

---

56 Public Bill Committee 22 March 2018 c318
57 Public Bill Committee 22 March 2018 cc319-20
58 Public Bill Committee 13 March 2018 cc59-61

> The Minister has some very strong safeguards in the Bill. There are strong safeguards that create exemptions for her where the interest is in crime prevention, such as, for example, illegal immigration. However, the power that the provision seeks, at which we take aim in our amendments, is a step too far and risks the most terrible injustices. It risks the courts being fouled up and our being challenged in all sorts of places, including the European Court of Human Rights in the years to come. It is an unwise provision…and a step too far.[59]

The SNP supported the amendment.[60]

For the Government, Victoria Atkins argued that paragraph 4 of Schedule 2 was "a necessary and proportionate measure to protect the integrity of our immigration system".[61] When responding to Members' concerns she said:

> (…) I am asked whether this will have an impact on someone's application, either at appeal or reconsideration. Of course, information is obtained so that a person can be brought in...When the need, as set out under the exemption, no longer exists, the rights kick back in again. This relates only to the first two data protection principles under the GDPR…this is not the permanent exemption from rights as perhaps has been feared by some; it is simply to enable the process to work. Once a person has been brought into the immigration system, all the protections of the immigration system remain.
>
> (…) Let me be clear on what paragraph 4 of schedule 2 does not do. It categorically does not set aside the whole of the GDPR for all processing of personal data for all immigration purposes. It makes it clear that the exemption applies only to certain GDPR articles. The articles that the exemption applies to are set out in paragraph 4(2) of schedule 2. They relate to various rights of data subjects provided for in chapter 3 of the GDPR, such as the rights to information and access to personal data, and to two of the data protection principles—namely the first one, which relates to fair and transparent processes, and the purpose limitation, which is the second one.
>
> (…) Contrary to the impression that has perhaps been given or understood, paragraph 4 does not give the Home Office a free hand to invoke the permitted exceptions as a matter of routine. The Bill is clear that the exceptions may be applied only to the extent that the application of the rights of data subjects, or the two relevant data protection principles, would be likely to prejudice
>
> "the maintenance of effective immigration control, or…the investigation or detection of activities that would undermine the maintenance of effective immigration control".
>
> That is an important caveat.[62]

Liam Byrne asked why the exemption was needed given that there were already exemptions relating to the prevention or detection of crime. Victoria Atkins responded:

> (…) We do not see the immigration system as some form of criminality or as only being open to the principles of criminal law. He will know that we deal with immigration in both the civil law and

---

59 Public Bill Committee 13 March 2018 c61
60 Public Bill Committee 13 March 2018 cc61-5
61 Public Bill Committee 13 March 2018 c65
62 Public Bill Committee 13 March 2018 cc67-8

> criminal law contexts. The exemption he has raised in terms of paragraph 2 of the schedule deals with the criminal law context, but we must also address those instances where the matter is perhaps for civil law.
>
> We know that in the vast majority of immigration cases, people are dealt with through immigration tribunals or through civil law. They are not dealt with through criminal law. That is the point; we must please keep open the ability to deal with people through the civil law system, rather than rushing immediately to criminalise them. If, for example, they have overstayed, sometimes it is appropriate for the criminal law to become involved, but a great number of times it is for the civil law to be applied to deal with that person's case either by way of civil penalty or by finding an arrangement whereby they can be given discretion to leave or the right to remain. We have the exemption in paragraph 4 so that we do not just focus on the criminal aspects that there may be in some immigration cases. We must ensure that we also focus on the much wider and much more widely used civil law context.
>
> It is important to recognise that the exemptions will not and cannot be targeted at whole classes of vulnerable individuals, be they victims of domestic abuse or human trafficking, undocumented children or asylum seekers. The enhanced data rights afforded by the GDPR will benefit all those who are here lawfully in the United Kingdom, including EU citizens. The relevant rights will be restricted only on a case-by-case basis where there is evidence that the prejudice I have mentioned is likely to occur.[63]

In response to questions about subject access rights and the impact of the immigration exemption on EU citizens, Victoria Atkins said:

> (…) The exemption will not be enacted on the basis of nationality. It is enacted on a case-by-case basis to uphold the integrity of the immigration system. There will be no question of EU nationals being in any way targeted by it.
>
> (…) In the case of subject access requests, each request would need to be considered on its own merits. For example, we could not limit the information given to visa applicants on how their personal data would be processed as part of that application. Rather, the restrictions would be applied only where there was a real likelihood of prejudice to immigration controls as a result of disclosing the information concerned.[64]

She also responded to the charge that the exemption has no basis in EU law:

> (…) Article 23 of the GDPR allows member states to restrict the application of certain provisions of the regulation to safeguard important objectives of general public interest. Immigration control constitutes one such objective. We see immigration as an important matter of public interest, and the GDPR allows member states to exempt rights where that is the case. We are not alone in our belief that immigration is an important matter of general public interest. The Irish Government clearly stated that in their own Data Protection Bill. Clause 54 of the Irish Bill gives powers to make regulations restricting certain rights and obligations under the GDPR to safeguard

63 Public Bill Committee 13 March 2018 cc68-9
64 Public Bill Committee 13 March 2018 c69

> important objectives of general public interest. The list of such objectives in the Bill includes matter relating to immigration.[65]

Liam Byrne was not satisfied with the Minister's explanations and put his amendment to a division. It was negatived by 10 votes to 9.[66]

2.6 Power to make further exemptions

The Bill

Clause 16 would give the Secretary of State the power to make regulations altering the application of the GDPR, including adding or varying the derogations in Schedules 2 to 4 and omitting provisions subsequently added by regulations. The regulations would be subject to the affirmative procedure.

The regulation making powers were debated and amended when the Bill was considered in the House of Lords – see p40 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Debate in Public Bill Committee

During the clause stand part debate, Stuart McDonald and Liam Byrne raised concerns about the delegated powers in clause 16. Margot James said that the Government had "carefully reviewed" the use of the powers after recommendations from the Delegated Powers and Regulatory Reform Committee and that an "appropriate balance" had now been struck:

> Clause 16 includes order making powers to ensure that the Secretary of State can update from time to time the particular circumstances in which data subjects' rights can be disapplied. That might be necessary if, for example, the functions of a regulator are expanded and exemptions are required to ensure that those new functions cannot be prejudiced by a data subject exercising his or her right to object to the processing.
>
> We believe it is very important that the power to update the schedules is retained. Several of the provisions in schedules 2 to 4 did not appear in the Data Protection Act 1998 and have been added to the Bill to address specific requirements that have arisen over the last 20 years…[67]

Clause 16 was agreed on division by 10 votes to 9.[68]

2.7 The applied GDPR

The Bill

The GDPR only applies to the processing of data in the course of an activity which is subject to Union law.[69] **Part 2 Chapter 3** of the Bill extends GDPR standards to areas outside EU competence (the "applied GDPR" scheme)

---

65 Public Bill Committee 13 March 2018 c71
66 Public Bill Committee 13 March 2018 c74
67 Public Bill Committee 13 March 2018 c81
68 Public Bill Committee 13 March 2018 c82
69 Article 2(2) of the GDPR

"to create a simple framework under which data controllers and processors can apply a single standard".[70] For further background, see pp20-1 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Schedule 6 specifies how the GDPR standards will be applied to areas outside the scope of Union law.

Paragraph 49 of Schedule 6 replaces Articles 60 to 76 of the GDPR (co-operation and consistency) with a shorter replacement Article (new Article 61) in the applied GDPR:

> 49 For Articles 60 to 76 substitute—
>
> *"Article 61*
>
> **Co-operation with other supervisory authorities etc**
>
> 1 The Commissioner may, in connection with carrying out the Commissioner's functions under this Regulation—
>
> (a) co-operate with, provide assistance to and seek assistance from other supervisory authorities;
>
> (b) conduct joint operations with other supervisory authorities, including joint investigations and joint enforcement measures.
>
> 2 The Commissioner must, in carrying out the Commissioner's functions under this Regulation, have regard to—
>
> (a) decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board established under Article 68 of the GDPR;
>
> (b) any implementing acts adopted by the Commission under Article 67 of the GDPR (exchange of information)."

Debate in Public Bill Committee

Darren Jones moved **amendment 152** to paragraph 49. This would replace the second paragraph with:

> "2 The Commissioner must, in carrying out the Commissioner's functions under this Regulation, incorporate with any modifications which he or she considers necessary in any guidance or code of practice which the Commissioner issues, decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board established under Article 68 of the GDPR.
>
> 2A The Commissioner must, in carrying out the Commissioner's functions under this Regulation, have regard to any implementing acts adopted by the Commission under Article 67 of the GDPR (exchange of information)."[71]

According to Mr Jones, the amendment would "assist" the Government in obtaining an adequacy decision from the European Commission:[72]

> This is our opportunity to show the European Union that we are committed to data protection principles. Amendment 152 would tweak the wording of paragraph 2 of article 61 of the applied GDPR…I want to strengthen the paragraph 2 wording, which says that our Information Commissioner must

---

70 Para 33 of the Explanatory Notes to Bill 153
71 Public Bill Committee 15 March 2018 c87
72 Public Bill Committee 15 March 2018 c87

> "have regard to"
>
> various things that happen at European Union level, including
>
> "decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board".
>
> The amendment seeks to strengthen that slightly, while recognising that the Government, and probably also the Information Commissioner, would like a little flexibility.
>
> (…) On passing the Bill, we would be saying that when we are negotiating on data, where we have a shared interest at European and UK level, we want to get it right, and we will have gone beyond the basics of adequacy of other third countries because of our close relationship... [73]

Margot James argued that the amendment was not needed to maintain the uninterrupted flow of data between the UK and the EU:

> (…) schedule 6 of the Bill…creates the applied GDPR by modifying the text of the GDPR so that it makes sense for matters outside the scope of EU law. The extension of GDPR standards is vital, because having a complete data protection regulatory framework will provide the UK with a strong foundation from which to protect people's personal data and secure the future free flow of data with the EU and the rest of the world. Applying consistent standards ensures that those bodies—mostly public authorities—who process personal data, both in and out of the scope of EU law, experience no discernible operational difference when doing so.
>
> (…) Decisions and guidance issued by the European Data Protection Board will have an important bearing on the GDPR as implemented in the UK. To ensure that the interpretation of the applied element of the GDPR remains consistent with the interpretation of the real GDPR, it is right that the Information Commissioner should have regard to decisions and guidance issued by the European Data Protection Board in carrying out her functions, as the UK regulator and enforcer of the applied GDPR. However, the amendment goes further, by requiring her to incorporate them into her guidance and codes of practice. The effect of that is to extend the ambit of the European data protection board so that, uniquely among member states, it would have within its purview processing outside the scope of EU law, when that processing was undertaken in the UK.
>
> We do not agree that such an extension is required for the UK to achieve the relationship that we are seeking… [74]

Darren Jones did not agree that his amendment would increase the European data protection board's power:

> (…) this is UK law, not European Union law. The amendment merely says that we will go only slightly further, with flexibility, by recognising that in the decisions that we want to be a part of—that is a really important point here—and to influence, we will take the obligations as well as the responsibilities, should we be invited to. [75]

The amendment was negatived on division by 10 votes to 8. [76]

---

73 Public Bill Committee 15 March 2018 cc90-1
74 Public Bill Committee 15 March 2018 cc92-3
75 Public Bill Committee 15 March 2018 c94
76 Public Bill Committee 15 March 2018 c94

National security certificates

The Bill

Clauses 26 to 28 create an exemption from certain provisions in the applied GDPR scheme and in Parts 5, 6 and 7 of the Bill if the exemption is required for the purpose of safeguarding national security or for defence purposes. The provisions from which there is an exemption are listed in **clause 26(2)** and include most of the data protection principles, the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions.[77]

Under **clause 27**, a Minister of the Crown would be able to certify that an exemption was required in relation to specified personal data for the purpose of safeguarding national security.

Debate in Public Bill Committee

For Labour, Louise Haigh moved **amendments 161 to 169**.[78] She said that the Bill's provisions on national security certificates gave Ministers "broad powers to remove individuals' rights with absolutely no oversight".[79] Labour's amendments were designed to "create a framework around which these necessary and proportionate powers can be used appropriately by Ministers and the security services".[80] Louise Haigh explained:

> Amendment 161 would introduce a framework to give citizens judicial protection in the initial instance and greater rights. The provisions of clause 26(1) allow individuals to press for their rights only after the fact. The amendments would mirror the provisions of the Investigatory Powers Act 2016, which gives the Investigatory Powers Commissioner's office independent judicial oversight of public authorities' use of investigatory powers. Crucially, that office will consider whether it agrees with Ministers' decisions to authorise intrusive investigatory powers before they can come into effect. Judicial commissioners act independently of Government and can be removed from office only by resolution of each House, and in limited circumstances by the Prime Minister, for example through bankruptcy, disqualification as a company director, or conviction of an offence that carries a sentence of imprisonment.
>
> If, under the 2016 Act, the exercise of a range of investigatory powers by public authorities—including the interception of communications, the acquisition and retention of communications data, equipment interference, intrusive surveillance, property interference, directed surveillance, covert human intelligence sources and bulk personal data sets—can be monitored prior to any potential breach of rights, it is not clear why a similar safeguard cannot take its place in the more limited provisions of this Bill.
>
> Crucially, amendment 162 stipulates that the judicial commissioners should be entitled to make an assessment for a national security certificate based on the tests outlined today; namely, whether it is necessary and proportionate to issue a certificate…

---

77 Para 166 of the Explanatory Notes to Bill 153
78 Public Bill Committee 15 March 2018 cc109-13
79 Public Bill Committee 15 March 2018 c111
80 Public Bill Committee 15 March 2018 c111

> Citizens must have confidence that in the exercise of their duties, Ministers and the intelligence services are questioned to ensure that they are making the right decisions based on evidence. Amendments 163 and 165 would require the national security certificate to identify the personal data to which the certificate applies, and would require a Minister to provide a justification of why they are seeking an exemption under the Bill…
>
> The Bill as it stands gives Ministers huge powers to set aside data rights, with no justification and providing only the bare minimum of information. A general description of the data in question would not alone be enough for the tribunal or the judicial commissioners to make a determination on whether the certificate was justified. Amendment 167 would allow the tribunal to consider the facts of the case, and it should be considered with the other amendments that I have spoken to…
>
> Finally, amendment 169 recognises the need for Ministers to be able to appeal the decision of the judicial commissioners in the event that they reject the application for a certificate. That appeal would go to the Information Commissioner and would stipulate that the judicial commissioner must set out the reasons why such an application was rejected…[81]

The amendments were supported by the SNP.[82] There was lengthy debate on the amendments. For the Government, Victoria Atkins claimed that the Bill's provisions relating to national security exemptions and certificates "were wholly in line with the provisions in the Data Protection Act 1998 and its predecessor, the Data Protection Act 1984":

> (…) What we are doing in the Bill is preserving an arrangement that has been on the statute book for more than 30 years and has been operated by successive Governments. The national security exemption is no different in principle from the other exemptions provided for in the Bill. If it is right that certain provisions of data protection legislation can be disapplied for reasons of, for example, crime prevention or taxation purposes, or in pursuit of various regulatory functions, without external approval, surely it is difficult to take issue with the need for an exemption on the grounds of national security on the same basis.[83]

On the national security exemption, she said:

> (…) To be absolutely clear, a national security exemption is applied not by a Minister but by a data controller. Data controllers—be they the intelligence services, the Ministry of Defence or any other body—are well placed to make the determination, given that they will have a detailed understanding of the operational context and the extent to which departure from the requirement of the general data protection regulation—or parts 3 or 4 of the Bill as the case may be—is necessary to safeguard national security. In short, a data controller decides whether the national security exemption should be applied in a particular case, and the certificate is the evidence of the need for such an exemption in the event that someone challenges it.[84]

---

81 Public Bill Committee 15 March 2018 cc111-2
82 Public Bill Committee 15 March 2018 cc113-4
83 Public Bill Committee 15 March 2018 c121
84 Public Bill Committee 15 March 2018 c123

On judicial oversight, she argued:

> The Government fully accept that national security certificates should be capable of being subject to judicial oversight. Indeed, the current scheme—both under the 1998 Act and this Bill—provides for just that. However, the amendments would radically change the national security certificate regime, because they would replace the existing scheme with one that required a Minister of the Crown to apply to a judicial commissioner for a certificate if an exemption was sought for the purposes of safeguarding national security, and for a decision to issue a certificate to be approved by a judicial commissioner.
>
> This, again, is the debate that we had when we were considering the Investigatory Powers Act 2016. There were some who would have preferred a judicial commissioner to make the decision about warrantry before the Secretary of State. However, Parliament decided that it was not comfortable with that, because it would have meant a great change. For a member of the judiciary to certify on national security issues, rather than a member of the Executive—namely the Prime Minister or a Secretary of State—would have great constitutional implications…The House decided that the decision itself must be a matter for a Minister of the Crown, because in the event—God forbid—that there is a national security incident, the House will rightly and properly demand answers from the Government of the day…[85]

Victoria Atkins also noted that the Information Commissioner had not raised any issues in respect of the provisions in clause 27.[86]

Louise Haigh was not "reassured" by the Minister's response:

> (…) The safeguards and oversights are not built into the Bill in the way they were in the Investigatory Powers Act 2016. There is no clear argument why those safeguards should be in place for collection, but not for processing. The Minister has constantly relayed that that decision is based on 30 years'-worth of data but, as has already been said, the scope for the collection and processing of data is so far transformed, even from when the Data Protection Act was written in 1998, that the oversights and safeguards need to be transformed as well. That is why we are proposing these amendments…[87]

Amendment 161 was negatived on division by 10 votes to 7.[88]

2.8 Representation of data subjects

The GDPR

Article 80(1) of the GDPR gives data subjects the right to mandate a not-for-profit body, organisation or association (such as a consumer protection body) to exercise rights and bring claims on their behalf. This is a new feature of data protection law.

Under **Article 80(2)** Member States may provide that any of these organisations has the right to lodge a complaint with a supervisory authority independently of a data subject's mandate. The Government has decided not to implement this subsection. This was criticised when the Bill

85 Public Bill Committee 15 March 2018 cc124-5
86 Public Bill Committee 15 March 2018 c131
87 Public Bill Committee 15 March 2018 cc131-2
88 Public Bill Committee 15 March 2018 c132

was considered in the Lords and amendments were moved – unsuccessfully – to implement Article 80(2). For further detail see pp61-2 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Debate in Public Bill Committee

The Government tabled a set of amendments (**115 and 63 to 68, 73 and 74**) and two new clauses relating to class representation for data protection breaches. **New clause 1** would give the Secretary of State the power to set out provisions allowing a non-profit organisation to bring a claim on behalf of multiple data subjects under article 80(1). According to Margot James, the Government had taken the view that this "will be an effective way for a non-profit group to seek a remedy in the courts on behalf of a large number of data subjects".[89]

New clause 2 would require the Secretary of State to conduct a review of the operation of article 80(1). This would involve consultation with stakeholders such as the Information Commissioner, businesses, privacy groups, the courts, tribunals and other government departments. The review would also assess the merits of implementing article 80(2) in the future. The Secretary of State would have to conduct the review and present the findings to Parliament within 30 months of the Bill coming into force.[90]

For Labour, Liam Byrne moved **amendments 154 and 155** that would implement Article 80(2).[91] He argued that the Government's approach was mistaken:

> …Article 80(1) basically allows group or class actions to be taken, and article 80(2) says that the national law can allow representative bodies to bring proceedings. The challenge with the way in which the Government propose to activate that power is that the organisation bringing the class action must seek a positive authorisation and people must opt in. The risk is that that will create a burden so large that many organisations will simply not step up to the task…
>
> The mechanism that the Government propose breaks down in two particular ways in the real world. First, it takes no account of the gigantic asymmetry between the fearsome five data giants, or indeed many of the other large organisations that control tons and tons of our data, and the humble individual… Their legal power is practically unlimited and certainly unprecedented. The role of the plucky organisation being empowered by the Bill to bring a class action is, I am afraid, under some pressure. There is a gigantic inequality of legal arms.
>
> The second reality on which the Government's argument founders is the fact that data breaches, by their very nature, involve data being leaked about tens and tens of thousands of people. The idea that a small charity or a small representative body can round up positive authorisation from tens of thousands of people who have had their rights violated in order to then take Facebook, Google, Apple, Microsoft, Morrisons or Experian to court is laughable…Our amendment would switch the emphasis. It would allow

89 Public Bill Committee 15 March 2018 c96
90 Public Bill Committee 15 March 2018 c96
91 Public Bill Committee 15 March 2018 cc97-8

> representative bodies to bring cases, allow people to opt out of cases and allow a collective opt-out.[92]

Mr Byrne also said that Labour's amendments would put in place a better system for protecting children:

> (…) I do not think any of us here is such a fantasist that we imagine that groups of children will take Facebook to court because it might have leaked their data somewhere. We will therefore rely on representative organisations to bring class actions on behalf of children. How on earth will Which? round up thousands of the nation's children to secure their positive opt-in to a class action, which it is in the national interest to bring? That would be completely impossible. The measures that the Government propose are not only weak for adults but completely ineffective for children.[93]

The SNP supported Labour's amendments.[94] For the Government, Margot James raised a number of concerns:

> (…) Amendment 154 applies article 80(2) with immediate effect and gold-plates it. We have a number of concerns with that approach. First, we are wary of the idea that data subjects should be prevented from enforcing their own data rights simply because an organisation or, in this instance, an individual they had never met before, got there first. That is not acceptable. It contradicts the theme of the Bill and the GDPR as a whole, which is to empower individuals to take control of their own data. As yet we have no evidence that that is necessary.
>
> (…) There are other problems with amendment 154. First, like the right hon. Member for Birmingham, Hodge Hill, we are concerned about children's rights. We would be concerned if a child's fundamental data rights were weighed up and stripped away by a court without parents or legal guardians having had the opportunity to make the decision to seek redress themselves or seek the help of a preferred non-profit organisation. Once that judgment has been finalised, there will be no recourse for the child or the parent. They will become mere observers, which is unacceptable and makes a travesty of the rights they are entitled to enforce on their own account.
>
> Secondly, we must remember that the non-profit organisations referred to in the amendment are, by definition, active in the field of data subjects' rights. Although many will no doubt have data subjects' interests at heart, some may have a professional interest in achieving a different outcome—for example, chasing headlines to promote their own organisation. That is why it is essential that data subjects are capable of choosing the organisation that is right for them or deciding not to partake in a claim that an organisation has advertised. The amendment would also allow an individual to bring a collective claim on behalf of other data subjects without their consent.[95]

---

92 Public Bill Committee 15 March 2018 cc97-8
93 Public Bill Committee 15 March 2018 cc98-9
94 Public Bill Committee 15 March 2018 cc99-100
95 Public Bill Committee 15 March 2018 cc102-4

Liam Byrne said that he was "incredibly disappointed" with the Minister's response and hoped that the Government would reconsider its position before Report stage.[96]

The Government's amendments were agreed without division.[97] New clauses 1 and 2 are now clauses 181 and 182 of Bill 190.

2.9 Data protection impact assessments

The Bill

Part 3 of the Bill covers law enforcement processing. **Chapter 4** would impose a range of general and specific obligations on data controllers and processors. These would include the carrying out of data protection impact assessments where processing would be likely to result in a "high risk" to the rights and freedoms of an individual (**clause 64**). Where an impact assessment indicates there is a high risk, the data controller or processor would be required to consult with the Information Commissioner before conducting the processing operation (**clause 65**).

Debate in Public Bill Committee

Louise Haigh moved **amendments 142 to 149** and **new clauses 3 and 4** to strengthen the requirement to conduct impact assessments:[98]

> (…) Given the breadth and reach of new technology, it is right that impact assessments are conducted where the new technology may present a risk, rather than a "high risk", as envisaged in the Bill. That is what we seek to achieve with the amendments. New technology in law enforcement presents a unique challenge to the data protection and processing environment. The trialling of technology, including facial recognition and risk assessment algorithms, as already discussed, has not been adequately considered by Parliament to date, nor does it sit easily within the current legal framework. I do not doubt that such technologies have a significant role to play in making law enforcement more effective and efficient, but they have to be properly considered by Parliament, and they need to have adequate oversight to manage their appropriate use…[99]

New clause 3 would require the intelligence services to undertake a risk assessment in cases where there is a "high risk" to the rights and freedoms of individuals. **New clause 4** would require the intelligence services to have prior consultation with the Information Commissioner when proposing processing.

For the Government, Victoria Atkins resisted the amendments.[100] She claimed that the new clauses were "inappropriate" and could "prejudice the lawful and proportionate action that is required to safeguard UK national security and UK citizens".[101] On the issue of "high risk", she said:

> (…) Clause 64 separates out the processing most likely significantly to affect an individual's rights and freedom, which requires an

96 Public Bill Committee 15 March 2018 c104
97 Public Bill Committee 15 March 2018 c105
98 Public Bill Committee 15 March 2018 cc143-7
99 Public Bill Committee 15 March 2018 c145
100 Public Bill Committee 15 March 2018 c148
101 Public Bill Committee 15 March 2018 c154

> additional level of assessment to reflect the higher risk. The amendments would water down the importance of those assessments. That is not to say that consideration of the impact on rights and freedoms can be overlooked. It will, of course, remain necessary for the controller to carry out that initial assessment to determine whether a full impact assessment is required. Good data protection is not achieved by putting barriers in the way of processing. It is about considering the risk intelligently and applying appropriate assessments accordingly.
>
> On the question of high risk, officers or data controllers will go through that process when considering whether a data protection impact assessment is correct…[102]

Victoria Atkins said that she would write to Louise Haigh on some of the points raised during the debate (e.g. photo recognition software, mobile fingerprint scanning, oversight of the surveillance camera commissioner). Louise Haigh agreed to withdraw the amendments.[103]

2.10 Data sharing by the intelligence agencies

The Bill

National security is outside the scope of EU law. **Part 4** of the Bill would provide for a specific data protection regime for processing by the intelligence services (the Security Service, Secret Intelligence Service, and Government Communications Headquarters), based on the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Debate in Public Bill Committee

Liam Byrne moved **amendment 159** (and 160) to ensure that the sharing of data by the intelligence agencies was legal.[104] He argued that the amendments were needed because of technological advances and a change in the American rules of engagement:

> (…) It is now possible, through satellite technology and drones, to collect video footage of battle zones and run the information collected through facial recognition software, which allows us to track much more forensically and accurately the movement, habits, working lives and leisure of bad people in bad places. We are fighting against organisations such as Daesh, in a coalition with allies, but over the past year one of our allies has rather changed the rules of engagement, which allows it to take drone strikes with a different kind of flexibility from that under the Obama regime.
>
> The change in the American rules of engagement means that, on the one hand, the American Administration has dramatically increased the number of drone strikes…and, on the other…repeated strikes are allowed for. Therefore, even when the circumstances around particular individuals have changed—new intelligence may have come to light about them—the Trump Administration have basically removed the safeguards that President Obama had in place that require an individual to be a "continuing and imminent threat" before a strike is authorised. That safeguard has been lifted, so the

102 Public Bill Committee 15 March 2018 cc150-1
103 Public Bill Committee 15 March 2018 c154
104 Public Bill Committee 20 March 2018 cc169-71

> target pool that American forces can take aim at and engage is now much larger, and operational commanders have a great deal more flexibility over when they can strike…
>
> (…)
>
> The amendment would ensure that—where there was a collection, processing and transfer of information by the UK intelligence services to one of our allies, principally America, and they ran that information against what is widely reported as a kill list and ordered drone strikes without some of the safeguards operated by previous Administrations—first, the decision taken by the intelligence agency here to share that information was legal and, secondly, it would be undertaken in a way that ensured that our serving personnel were not subject to legal threats or concerns about legal threats.[105]

For the Government, Victoria Atkins argued that the amendments would "place unnecessary and burdensome obstacles in the way of the intelligence services" in safeguarding national security.[106] She said that the *Investigatory Powers Act 2016*, the *Regulation of Investigatory Powers Act 2000* and codes of practice made under these Acts, provided "rigorous safeguards governing the transfer of data".[107]

Victoria Atkins also referred to the draft modernised convention 108 of the Council of Europe:

> (…) international transfers of personal data by the intelligence services are appropriately regulated both by the Bill, which, as I said, is entirely consistent with draft modernised convention 108 of the Council of Europe - that is important, because it is the international agreement that will potentially underpin the Bill and agreements with our partners and sets out agreed international standards in this area – and by other legislation, including the 2016 Act…[108]

Liam Byrne noted that there was no deadline for the finalisation of the draft convention and put amendment 159 to a division to "ensure that the Government remain absolutely focused on the subject". The amendment was negatived by 10 votes to 8.[109]

2.11 Register of publicly controlled data of national significance

The Bill

Clause 121 would require the Information Commissioner to prepare a code of practice on "personal data of national significance". This would set out best practice on information sharing between publicly funded data controllers and third parties. It would also include guidance on calculating the value for money of any such information sharing agreements and on how to secure the financial benefits from the sharing.

105 Public Bill Committee 20 March 2018 c171
106 Public Bill Committee 20 March 2018 c176
107 Public Bill Committee 20 March 2018 c175
108 Public Bill Committee 20 March 2018 c176
109 Public Bill Committee 20 March 2018 c180

The clause is not supported by the Government.[110] It was added to the Bill at Report stage in the Lords following an amendment moved by Lord Mitchell (Cross Bench).[111] For further detail see pp54-5 of the Library's Briefing Paper (CBP 8214, 1 March 2018).

Debate in Public Bill Committee

For the Government, Margot James raised a number of concerns about clause 121:

> (…) First, by definition, data protection legislation deals with the protection of personal data, not general data policy. Companies who enter into data sharing agreements with the NHS are often purchasing access to anonymised patient data—that is to say, not personal data. Consequently, the code in clause 121 cannot bite. Secondly, maintaining a register of data of national significance is problematic. In addition to the obvious bureaucratic burden of identifying the data that would fall under the definition, generating a list of data controllers who hold data of national significance is likely to raise a number of security concerns. The NHS has been the victim of cyber- attacks, and we do not want to produce a road map to resist those who want to harm it.
>
> Thirdly, we do not believe that the proposed role is a proper one for the Information Commissioner, and nor does she. It is not a question of legislative enforcement and, although she may offer valuable insight on the issues, such responsibilities do not comfortably fit with her role as regulator of data protection legislation. We have consulted the commissioner on the amendments and she agrees with our assessment...[112]

Liam Byrne spoke in favour of the clause:

> (…) The Government operate about 200 to 250 agencies, and some are blessed with data assets that are more valuable than those of others—for example, the Land Registry or Companies House sit on vast quantities of incredibly valuable transactional data, whereas other agencies, such as the Meteorological Office, the Hydrographic Office and Ordnance Survey, sit on sometimes quite static data which is of value…
>
> (…) There are still huge data pots locked up in Government which could do with releasing, but the way in which we release them has to have an eye on the way we create value for taxpayers more generally. Beyond doubt, the area of public policy and public operations where we have data that is of the most value is health…
>
> What Lord Mitchell is super-conscious of is that our NHS records stretch back to 1948, so the longitudinal health data we have in this country is pretty much without parallel anywhere in the world…The dynamic and longitudinal data assets that we are sitting on in parts of the NHS are unbelievably valuable…He is seeking to ensure that something almost like a sovereign wealth fund is created for data assets in this country—in particular, a sovereign wealth fund created for NHS data assets…[113]

---

110 Para 311 of the Explanatory Notes to Bill 153
111 Amendment 107B, HL Deb 10 January 2018 c204
112 Public Bill Committee 20 March 2018 c183
113 Public Bill Committee 20 March 2018 cc184-5

Margot James responded:

> (…) A lot of the databases the right hon. Gentleman referred to as being of great potential value do not contain personal data. Some do, some do not: the Land Registry does not, Companies House does, and so forth. Also, the Information Commissioner has advised that this is beyond her competence and her remit and that she is not resourced to do the job. Even the job of defining what constitutes data of public value is a matter for another organisation and not the Information Commissioner's Office…[114]

The Committee voted by 10 votes to 9 to remove clause 121 from the Bill.[115]

2.12 Press regulation

The Bill

Clause 142 was added to the Bill following a Lords amendment moved by Baroness Hollins. The clause would require an "Inquiry into issues arising from data protection breaches committed by or on behalf of news publishers". Baroness Hollins said that the "spirit" of her amendment "would be fully satisfied by the completion of the second part of the Leveson inquiry".

Clauses 168 and 169 were added to the Bill following Lords amendments moved by Earl Attlee. These "would incentivise media operators to sign up to an independent press regulator in respect of data protection claims". It would be "achieved in the same way as the yet-to-be-commenced section 40 of the *Crime and Courts Act 2013*".

The Government does not support the clauses added by the Lords. In a statement on 1 March 2018, Matt Hancock, the Secretary of State, announced that the Government was formally closing the Leveson inquiry. He also said that section 40 would not be commenced and would be repealed at the "earliest opportunity".

For further detail see the Library Paper, *Press regulation after Leveson: unfinished businesses?* (CBP 7576, 12 March 2018) and pp34-40 of Library Briefing Paper (CBP 8214, 1 March 2018).

Public Bill Committee debate

There was lengthy debate on the clauses relating to press regulation.[116]

Liam Byrne spoke in support of clause 142:

> (…) Imagine our surprise when the Secretary of State decided to close the Leveson inquiry, saying that the world had changed and that all criminal behaviour and conduct in the fourth estate magically and mystically came to a definitive, categorical and unequivocal end in 2010. That, however, appears not to be the case. Subsequent to the Secretary of State's declaration that the world had suddenly returned to order and honesty, we heard the revelations of John Ford, a professional blagger employed by the *Sunday Times*, who set out

114 Public Bill Committee 20 March 2018 c187
115 Public Bill Committee 20 March 2018 c188
116 Public Bill Committee 20 March 2018 cc198-215

> several detailed allegations and examples of criminal behaviour relating to sensitive information, including on members of the Cabinet and their personal bank accounts. Furthermore, he claims that the practice persists today…
>
> (…) When the Secretary of State presented his decision to the House, most hon. Members who were lucky enough to hear his statement left the Chamber feeling fairly clear that he had explained that Sir Brian Leveson supported his decision to close down Leveson 2. Imagine our surprise when it subsequently emerged that Sir Brian "fundamentally disagrees" with the Government's decision to end part 2 of the inquiry
>
> When Sir Brian Leveson said that some of the terms of reference could be changed, he was recommending that they be expanded, not restricted, so that the inquiry could look further into how social media companies collect and use data, as well as how they are used as conduits for fake news…[117]

He also spoke in support of clauses 168 and 169:

> (…) bad behaviour by the press has destroyed people's reputations without any real chance of recovery. In a world of social media, when reputations are destroyed, the smears stick to people like tar. They do not go away; they stay with people and scar them for life.
>
> That underlines the reality that there needs to be some kind of low-cost, readily accessible form of arbitration and settlement when the press, so help them, get things wrong. People make mistakes; to err is human, so we have to ensure that human institutions have a means of fixing things when mistakes are made. Many of the victims who suffer at the hands of the press may be poor people, not rich people, who do not have access to expensive lawyers who can file emergency injunctions to stop publication overnight, as we know many celebrities have…[118]

Liam Byrne said that the amendments would be re-tabled on Report if the Government defeated them in Committee.[119]

For the SNP, Brendan O'Hara moved **amendment 137**. This would require the UK Government to obtain the consent of the Scottish Government before establishing any inquiry under clause 142. He also moved **amendments 138 and 139** to ensure that clauses 168 and 169 would only extend to England and Wales and not apply in Scotland.[120]

For the Government, Margot James referred to the Secretary of State's statement of the 1 March 2018. She said that she would not repeat his arguments but did state that the "Government's firm focus is on the problems faced by the media right now".[121] The Minister also noted that the Lords amendments would undermine the Scotland and Northern Ireland devolution settlements and was therefore "sympathetic" to the SNP's amendments. However, she said that amendment 137 was unnecessary because there was already a consultation requirement in the *Inquiries Act 2005*. In

117 Public Bill Committee 20 March 2018 c201
118 Public Bill Committee 20 March 2018 cc207-8
119 Public Bill Committee 20 March 2018 c208
120 Public Bill Committee 20 March 2018 cc198-200
121 Public Bill Committee 20 March 2018 c212

addition, the Government would push for the removal of clauses 168 and 169 in their entirety.[122]

The SNP's amendment 137 was negatived on division by 10 votes to 9.[123]

The Committee voted to remove clause 142 from the Bill (10 votes to 7).[124]

The Committee voted to remove clauses 168 and 169 from the Bill (10 votes to 7).[125]

2.13 E-commerce Directive

Background

The *Electronic Commerce (EC Directive) Regulations 2002* implemented Directive 2000/31/EC (8 June 2000) of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce.

Public Bill Committee debate

Liam Byrne moved **new clause 13**. This would require the Secretary of State to review the application and operation of the Regulations that were now "hopelessly out of date":

> (…) There is widespread recognition that the e-commerce directive, which is used to regulate information services providers, is hopelessly out of date. It was agreed in around 2000. In effect, it allows information services providers to be treated as platforms rather than publishers. Since then, we have seen the growth of big tech and the new data giants that now dominate the digital economy, and they are misbehaving. Worse, they have become platforms for hate speech, social division and interference in democracy…
>
> (…) The Secretary of State for Digital, Culture, Media and Sport reminded us as recently as this morning that as we come out of the European Union we will have a new opportunity to update the e-commerce directive. The House basically must put in place a new framework to regulate information services providers in a new way…
>
> (…) The new clause would set a deadline for Government proposals to modernise the e-commerce directive. We will have to have a debate and make a choice about how close we bring the obligations and the liabilities of social media firms to the regulations we have for newspapers. Despite the hopelessly weak regulatory regime that the Government are intent on delivering in this country, there is no way on earth that even an IPSO-regulated newspaper could get away with the kind of nonsense that we see on social media—the kind of hate speech and viciousness that, more often than not I might add, is directed at women rather than men.
>
> The new clause urges the Government to get on with that and states that by 31 January 2019—a little under a year's time—we would have

122 Public Bill Committee 20 March 2018 c214
123 Public Bill Committee 20 March 2018 c215
124 Public Bill Committee 20 March 2018 c215
125 Public Bill Committee 20 March 2018 cc228-9

> not the final law or regulations, but a review and a set of proposals on how the e-commerce directive needed to be reformed…[126]

Margot James acknowledged that the 2000 Directive was outdated, in particular with regard to its limited liability provisions. However, she said that the Bill was not the place to look at these matters:

> (…) The Government have made it clear through our digital charter that we are committed to making the UK the safest place to be online, as well as the best place to grow a digital business. As the Prime Minister has said, when we leave the EU we will be leaving the digital single market, including the e-commerce directive. That gives us an opportunity to make sure that we get matters corrected for the modern age: supporting innovation and growth, and the use of modern technology, but doing so in a way that commands the confidence of citizens, protects their rights and makes their rights as enforceable online as they currently are offline.
>
> (…) There is an important debate to be had on the e-commerce directive and on platform liability, and we are committed to working with others, including other countries, to understand how we can make the best of existing frameworks and definitions. Consideration of the Bill in Committee and on Report are not the right places for that wide debate to be had…[127]

Liam Byrne put his new clause to a division where it was negatived by 10 votes to 7.[128]

2.14 Jurisdiction

The Bill

Under **clause 177**, jurisdiction in England and Wales and Northern Ireland is exercisable by the county court or the High Court. In Scotland it is exercisable by the sheriff or the Court of Session. This mirrors the jurisdiction provisions under the 1998 Act.

Debate in Public Bill Committee

Darren Jones moved **amendment 151** to add the following sub-section to clause 177:

> "(4) Notwithstanding any provision in section 6 of the European Union (Withdrawal) Act 2018, a court or tribunal shall have regard to decisions made by the European Court after exit day so far as they relate to any provision under this Act.".

He said that the amendment would assist in obtaining an adequacy decision from the European Commission:

> (…) I appreciate that there may be some political challenges in stating the aim that the UK will mirror the European Court's jurisdiction, but the reality is that developing European data protection law, either directly from the courts or through the European data protection board, will in essence come from the application of European law at the European Court of Justice. The amendment does not seek to cause political problems for the Government, but merely says that we ought to have regard to European case law in UK courts, in order

126 Public Bill Committee 22 March 2018 cc320-1
127 Public Bill Committee 22 March 2018 c322
128 Public Bill Committee 22 March 2018 c323

> to provide the obligation to our learned friends in the judiciary to have regard to European legal decision making and debates in applying European-derived law in the United Kingdom. This short amendment seeks merely to put that into the Bill, to assist the Government in their negotiations on adequacy with the European Commission.[129]

Margot James said that the Government was committed to getting an adequacy agreement but resisted the amendment:

> (…) Courts will be allowed to follow the jurisprudence of the ECJ in this area of data protection. Nothing I am saying is prompting a departure from that position. We see the amendment as going further than we would like to go. By contrast, the Government's proposed approach to CJEU oversight respects the referendum result and is clear, consistent and achievable.[130]

Darren Jones responded:

> The Minister's arguments do not seem to stack up. If I were saying in the amendment that we must apply ECJ case law directly and that the UK courts had no power to disregard EU jurisprudence I would probably agree, but that is not what it seeks to do. I am not convinced it goes beyond the Government's policy position nor what is said in the EU (Withdrawal) Bill…[131]

The amendment was negatived on division by 10 votes to 9.[132]

2.15 Digital Bill of Rights

Liam Byrne spoke at length on his **new clause 5** that would introduce a Bill of Data Rights in the Digital Environment.[133] This would include articles on:

- Equality of Treatment
- Security
- Free Expression
- Equality of Access
- Privacy
- Ownership and Control
- Algorithms
- Participation
- Protection
- Removal

Compensation would be payable for a breach of any of the rights.

The application of the rights to someone aged under 18 would have to be read in conjunction with the rights set out in the United Nations

129 Public Bill Committee 20 March 2018 c234
130 Public Bill Committee 20 March 2018 c237
131 Public Bill Committee 20 March 2018 c237
132 Public Bill Committee 20 March 2018 c238
133 Public Bill Committee 22 March 2017 cc297-304

Convention on the Rights of the Child. Where an information society service processed data of those aged under 18, it would have to do so under the age appropriate design code.[134]

Mr Byrne said the proposed Bill of Rights was "an attempt to provoke the Government into being more ambitious in their strategy for the digital world".[135]

For the Government, Margot James referred to the digital charter:

> (…) Citizens rightly want to know that they will be safe and secure online. Tackling these challenges in an effective and responsible way is absolutely critical. The digital charter is our response. It is a rolling programme of work to agree norms and rules for the online world and to put them into practice. In some cases, that will be through shifting expectations of behaviour and resetting a settlement with internet companies. In some cases, we will need to agree completely new standards; in others, we will want to update our laws and regulations. Our starting point is that we expect the same rights and behaviour online as we do offline, with the same ease of enforcement.
>
> The charter's core purpose is to make the internet work for everyone—for citizens, businesses and society as a whole—and it is based on liberal values…[136]

Liam Byrne withdrew his clause after saying he was glad that the Government agreement with the sentiment behind it.[137]

134 Public Bill Committee 22 March 2017 cc297-8
135 Public Bill Committee 22 March 2017 c298
136 Public Bill Committee 22 March 2017 c307
137 Public Bill Committee 22 March 2017 c308

Appendix: Committee membership

Membership of the Committee was as follows.

Chairs:

David Hanson, Gary Streeter

Members:

Nigel Adams (Conservative)

Victoria Atkins (Conservative, Parliamentary Under-Secretary at the Home Office)

Liam Byrne (Labour)

Colin Clark (Conservative)

Chris Elmore (Labour)

Louise Haigh (Labour)

Peter Heaton-Jones (Conservative)

Nigel Huddleston (Conservative)

Alister Jack (Conservative)

Margot James (Conservative, Minister of State at the Department for Digital, Culture, Media and Sport)

Darren Jones (Labour)

Julia Lopez (Conservative)

Stuart C. McDonald (Scottish National Party)

Ian Murray (Labour)

Brendan O'Hara (Scottish National Party)

Gareth Snell (Labour (Co-op))

Matt Warman (Conservative)

Mike Wood (Conservative)

Daniel Zeichner (Labour)

BRIEFING PAPER
Number 8251
13 April 2018

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer