PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL [*LORDS*]

First Sitting

Tuesday 13 March 2018

(Morning)

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Saturday 17 March 2018

The Committee consisted of the following Members:

Chairs: †David Hanson, Mr Gary Streeter

† Adams, Nigel *(Lord Commissioner of Her Majesty's Treasury)*
† Atkins, Victoria *(Parliamentary Under-Secretary of State for the Home Department)*
† Byrne, Liam *(Birmingham, Hodge Hill)* (Lab)
† Clark, Colin *(Gordon)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Haigh, Louise *(Sheffield, Heeley)* (Lab)
† Heaton-Jones, Peter *(North Devon)* (Con)
† Huddleston, Nigel *(Mid Worcestershire)* (Con)
† Jack, Mr Alister *(Dumfries and Galloway)* (Con)
† James, Margot *(Minister of State, Department for Digital, Culture, Media and Sport)*
† Jones, Darren *(Bristol North West)* (Lab)
† Lopez, Julia *(Hornchurch and Upminster)* (Con)
† McDonald, Stuart C. *(Cumbernauld, Kilsyth and Kirkintilloch East)* (SNP)
† Murray, Ian *(Edinburgh South)* (Lab)
† O'Hara, Brendan *(Argyll and Bute)* (SNP)
† Snell, Gareth *(Stoke-on-Trent Central)* (Lab/Co-op)
† Warman, Matt *(Boston and Skegness)* (Con)
† Wood, Mike *(Dudley South)* (Con)
† Zeichner, Daniel *(Cambridge)* (Lab)

Kenneth Fox, *Committee Clerk*

† attended the Committee

Public Bill Committee

Tuesday 13 March 2018

(Morning)

[Mr David Hanson *in the Chair*]

Data Protection Bill [*Lords*]

9.25 am

The Chair: Welcome. The annunciators in the Committee Room are not working, so we will go by the *Hansard* clock on my left until they are repaired. I remind colleagues to switch off their mobile phones, and that tea and coffee are not permitted in Committee sittings.

Ordered,

That—

(1) the Committee shall (in addition to its first meeting at 9.25 am on Tuesday 13 March) meet—

(a) at 2.00 pm on Tuesday 13 March;

(b) at 11.30 am and 2.00 pm on Thursday 15 March;

(c) at 9.25 am and 2.00 pm on Tuesday 20 March;

(d) at 11.30 am and 2.00 pm on Thursday 22 March;

(e) at 9.25 am and 2.00 pm on Tuesday 27 March.

(2) the proceedings shall be taken in the following order: Clauses 1 to 10; Schedule 1; Clauses 11 to 15; Schedules 2 to 4; Clauses 16 and 17; Schedule 5; Clauses 18 to 22; Schedule 6; Clauses 23 to 30; Schedule 7; Clauses 31 to 35; Schedule 8; Clauses 36 to 86; Schedules 9 and 10; Clauses 87 to 112; Schedule 11; Clauses 113 and 114; Schedule 12; Clauses 115 and 116; Schedule 13; Clauses 117 and 118; Schedule 14; Clauses 119 to 153; Schedule 15; Clause 154; Schedule 16; Clauses 155 to 181; Schedule 17; Clauses 182 to 204; Schedule 18; Clauses 205 to 208; new Clauses; new Schedules; remaining proceedings on the Bill;

(3) the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 27 March. —*(Margot James.)*

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Margot James.)*

The Chair: Copies of written evidence will be made available in the Committee Room shortly.

We now begin line-by-line consideration of the Bill. Mr Streeter—my fellow Chair—and I have selected the amendments for consideration today; the selection list is available in the Committee Room. Amendments that have been grouped for debate are generally on the same or a similar issue.

For the benefit of new Members on the Committee, I should say that decisions on amendments are made not necessarily in the order in which they are debated, as shown on the selection list, but rather in the order in which they appear on the amendment paper. Some of the provisions that we debate today will therefore not be voted on until a later day. I will use my discretion to determine whether to have separate stand part debates on clauses to which a number of amendments have been tabled. I am sure it will all become clear in due course.

Clause 1

Overview

Question proposed, That the clause stand part of the Bill.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): It is a pleasure to serve under your chairmanship, Mr Hanson. Clause 1 is a signposting overview of the Bill. It is not intended to have any effect other than to help us to navigate such a large Bill; I trust that hon. Members agree that it achieves its purpose.

Liam Byrne (Birmingham, Hodge Hill) (Lab): It is a pleasure to serve under your chairmanship, Mr Hanson. Looking around the Committee Room, I see that you have an extremely unruly bunch of hon. Members to police in the next couple of weeks, but I know that you will do so with skill and care.

The Opposition do not wish to object to clause 1, which is basically the foundation stone of the Bill. We wish only to underline the Bill's peculiarity in that it seeks to incorporate a piece of European legislation into British law without actually reproducing the legislation in question. Throughout the debate, we will hear references to the general data protection regulation—GDPR—a text that appears nowhere in the Bill. I hope that over the coming weeks the Committee will therefore focus on a series of principles for data protection. The Opposition will move amendments to enshrine those principles more firmly into our law. Beyond that, I have no objections to this foundation stone of the Bill.

Question put and agreed to.

Clause 1 accordingly agreed to.

Clause 2

Protection of personal data

Question proposed, That the clause stand part of the Bill.

The Chair: With this it will be convenient to discuss new clause 12— *Right to protection of personal data*—

"(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."

This new clause would incorporate Article 8 of the Charter of Fundamental Rights of the European Union (Protection of personal data) into the Bill.

Liam Byrne: New clause 12, which I tabled with other Opposition members of the Committee, seeks to achieve something very simple: to incorporate article 8 of the EU charter of fundamental rights into British law. It is beyond dispute that both sides of the House share the objective of ensuring friction-free trade with our neighbour, the European Union, over the years to come. The role of this Bill in enabling that trade is of fundamental

significance. Something like 70% of our exports of goods and services rely on the smooth transfer of data, and we know that the European data economy will be worth something like £643 billion by 2020. Despite all the efforts of the Secretary of State for International Trade, the reality is that the EU data economy, sitting next door to us, remains one of the most important, if not the most important, global markets from which we should aspire to profit over the years to come.

One of the great risks of Brexit is that technology firms will relocate, which is already beginning to take place. Many such firms will choose to headquarter in the Republic of Ireland. It is therefore in everybody's interest that our trade and data protection regimes allow the smooth export of digitally enabled services. I hope that is not a contentious point.

In new clause 12, we propose to incorporate into British law what is, in effect, at the cutting edge of global data protection measures. It is not a trivial or frivolous new clause. Her Majesty's Opposition did not make it up; it was crafted with techUK—an organisation that represents 950 companies, which employ something like 800,000 people and make up about half of the UK tech industry. When techUK proposes a fundamental measure of reform, it is important that we listen.

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. I hope that, having looked at this amendment and appreciated some of the refinements we made in the other place, the Government will decide that they will not put dogma in the way of agreeing to it. It is too important to leave to doubt.

In the debate on clause 1, I said that this principle was all the more important, because right hon. and hon. Members are being asked to agree to a Bill that does not feature the GDPR, which it seeks to incorporate into British law. Hon. Members can look it up if they like, but the Government have not set it out in a schedule or anywhere else. The fact that the Bill does not include the GDPR makes it all the more important that the House agrees a series of principles that are good now and for the future. Principles are paramount, and in this Bill the principle of privacy is first among equals.

The question of privacy is not disputed. It is a principle that has been agreed by our own Supreme Court in a recent case that was brought by the right hon. Member for Haltemprice and Howden (Mr Davis), who is now the Secretary of State for Brexit. Together with my hon. Friend the Member for West Bromwich East (Tom Watson), he brought the case of David Davis and others *v.* Secretary of State for the Home Department to the High Court, which confirmed the right of privacy in this country. This is not something that is necessarily party political; this is something on which there is strong cross-party consensus. These principles will become all the more important as the EU (Withdrawal) Bill is given effect because the Bill has thousands of ideas and proposals but kills off only one piece of legislation: the EU charter of fundamental rights.

A British tradition helped shape the EU charter of fundamental rights. We are the country of the Magna Carta and we are the country that helped craft the European convention on human rights after world war two to ensure there was never a return to the horrors of the 1930s and 1940s. Our lawyers played a fundamental role in shaping the EU charter of fundamental rights, but now, in the EU (Withdrawal) Bill, the Government decide to kill off the whole thing.

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. If we bring that into doubt, we jeopardise an adequacy agreement for the future. I fear that, by setting their face against this new clause 12, the Government are, in some way and for some reason, trying to preserve the illusion of harmony between our regime and the regime of the European Union in order to camouflage the flexibility that might allow it to depart from regulatory harmonisation in the years to come. To coin a phrase, they are trying to have their cake and eat it.

That is not a reasonable position. The Minister will reassure us that that is not the intention of Her Majesty's Government today. No doubt, she will tell us there is no will to try and win a race to the bottom in the data protection regime and many of us may be sympathetic to her position, as she is quite famously a reasonable Minister. However, the Tory party is not a stable place and the worry on all parts is not only how long the Minister will enjoy her office but what will come after her and what Government will come after this Government. There will be Governments of many colours over the course of the next 70 or 80 years and in this Committee we do not want to risk leaving unfettered a future Government who may take a less reasonable position than the famously reasonable Minister. That is why we want to move the incorporation of article 8 into British law.

We currently have a Bill without a data protection instrument and without clear data protection principles. That is a high-risk situation when, today, we have a low-risk regime. Nobody is particularly troubled by the current privacy regimes; we have been operating under article 8 of the EU charter of fundamental rights for some time and, certainly, no arguments I have heard suggest that it is troublesome in any way. What is wrong with continuing with it?

When we first crafted this new clause, there were some issues to which we were alert. A number of noble peers expressed a concern that we were creating too absolutist a right, a right without balancing test and provisions. That has been corrected in the new clause presented to this Committee today. We would therefore like to press it to a vote, as we want to ensure this fundamental right is part and parcel of British law for the years to come. It de-risks an adequacy agreement for data protection for the future. We have enjoyed the

[Liam Byrne]

provisions of article 8 for some years, and there is no reason to suggest that they may be more troublesome in the years ahead. We do not think the Government want to depart from a harmonisation of regulations in this area over the years to come so the flexibility that this Bill currently offers will not be taken up. Let us put the matter beyond dispute and beyond doubt and let us incorporate article 8 into the Bill.

The Chair: I remind Members—particularly new Members—that new clause 12 is being debated now, but will not be voted on, if Members wish to have a vote, until we have completed consideration of the Bill. Today's debate is on clause 2 and new clause 12, but the vote on the new clause will come later.

Brendan O'Hara (Argyll and Bute) (SNP): I rise in support of new clause 12, 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. As we have heard from the right hon. Member for Birmingham, Hodge Hill, if the United Kingdom fails to secure an adequacy agreement, I fear there will be a flight of high-tech, high-skilled jobs from the United Kingdom to other parts of the European Union.

For the UK to be able to take full advantage of this vital continued free flow of data with the rest of the European Union post Brexit, the most straightforward route is an adequacy agreement. As I have heard argued before, that decision is not as straightforward as one would hope. An adequacy agreement is not simply in the Commission's gift to give; it is a legal judgment.

If I could point again to the data protection lawyer, Rosemary Jay, who said that the EU had to go through a legislative process, and it was simply not in the EU's gift to do this in any informal way. The Commission has to go through a legislative process in order to give the UK an adequacy agreement. There are further complications because, with an adequacy agreement, the European Commission has to consider a variety of issues, such as the rule of law, respect for human rights, and legislation on national public security and criminal law. That being so, as it currently stands, the Investigatory Powers Act may well prove a block to achieving adequacy. The Act has already been accused of violating the European Union's charter of fundamental rights. Eduardo Ustaran, the internationally recognised expert, has said:

"What the UK needs to do is convince the Commission—and perhaps one day the European Court of Justice—that the Investigatory Powers Act is compatible with fundamental rights. That's a tall order".

While I can understand that the Government are absolutely desperate to secure an adequacy agreement, the harsh reality is that, in these challenging circumstances and with this challenging legal process, it is not going to be as simple as perhaps we had hoped.

No one wants this situation to arise; it is absolutely essential that we have this deal, but, as GDPR evolves over time—as it surely will—in order to maintain that adequacy status, should we attain it, the UK will have to keep its data protection law in line with GDPR. The EU charter of fundamental rights and freedoms is absolutely central to EU data protection law. If we exclude ourselves now from article 8, the chances of achieving adequacy are seriously jeopardised, and the chances of maintaining adequacy are further jeopardised. I urge the Government please to consider the long and short-term consequences of not accepting this new clause. Without article 8, I cannot see how we will achieve or maintain adequacy, and if we cannot achieve and maintain adequacy, the consequences for UK high-tech businesses are unfathomable.

Darren Jones (Bristol North West) (Lab): Thank you, Mr Hanson. It is a pleasure to serve under your chairmanship on my first Bill Committee.

I rise to support the comments made by my right hon. Friend the Member for Birmingham, Hodge Hill about the importance of adequacy and its link to article 8 of the charter of fundamental rights, and therefore in support of new clause 12. The Bill is pragmatic in seeking to bring GDPR principles into areas of non-EU competence and to provide a legislative parking space for GDPR if the UK leaves the European Union. However, we cannot get away from the fact that GDPR in itself has a legal basis that is anchored to the European charter of fundamental rights. In trying to copy and paste that level of protection into UK law, we must therefore also bring with it the fundamental rights to which it is attached.

9.45 am

The Joint Committee on Human Rights shares that view. Its report, following the passing of the Bill in the other place, was clear that article 8 of the charter is a fundamental legal right to the principles of data protection and privacy. It noted that with third countries such as Canada—the EU-Canada agreement, which this Government may seek to replicate with the European Union—the Grand Chamber of the European Union looked at article 8 of the European charter of fundamental rights when deciding on adequacy. Therefore, it would be sensible to assume that the same approach will be taken with the UK when it becomes a third country in the coming months.

There was a broad conversation about this issue in a general debate before Christmas on data protection, before the Bill was laid. Ministers on the Treasury Benches said that the Department for Exiting the European Union would set out why we did not need to include article 8 of the charter, given that it is present in other areas of UK law. On 5 December the same Department released its analysis, which acknowledged that article 8 of the charter had "no direct equivalent" in the European convention on human rights, and referred back instead to the Data Protection Bill.

Mike Wood (Dudley South) (Con): The hon. Gentleman is selectively quoting from that analysis. As he will see, it also says that the European Court of Human Rights —I think that the case concerned Finland—held that

article 8 of the European convention on human rights encompassed data protection rights that were protected in article 8 of the charter.

Darren Jones: Of course the hon. Gentleman is right that the article includes principles of data protection, but we are trying to make the Government's job in seeking the decision on adequacy with the European Union as easy as possible. This seems an easy way to facilitate that. Clearly, there is a dereliction of fundamental rights through not copying and pasting this across into UK law. Although there are data protection principles under the European convention on human rights, article 8 states:

> "Everyone has the right to respect for his private and family life, his home and his correspondence."

That does not sound very modern or digital to me. Although rights flow from that, the charter rights on communications—specifically electronic communications—seem much more fit for the future. I welcome the Secretary of State's comments that the Bill seeks to make our country fit for the future. Let us rely not on a world of manual correspondence, but on one of electronic communications.

The new clause is not ideological; it does not seek to rebalance power between business controllers and individual citizens. It merely seeks to replicate what is in law today: a basic and fundamental human right that seems to me and to others to be perfectly sensible. Only yesterday, I was in Brussels with the European Scrutiny Committee, meeting Mr Barnier. He talked positively about wanting to get agreement on data adequacy, given its importance—not least because 11% of global data flows come to the UK, 70% of which are with the EU. It would be a disaster for this country if we did not have adequacy, so let us make our job easier to effect that shared aim across the Floor of the Committee and with our counterparts in Europe of seeking a decision on adequacy. Let us put this new clause into the Bill, so that we maintain the position that our data subjects have today: a fundamental right, which is in the European charter of fundamental rights, and in the future will be in this Bill.

Margot James: I thank speakers for their thoughtful contributions. I share many of their concerns, as do the Government, particularly with regard to adequacy, which I will talk about in more detail. I think we are all agreed that after Britain leaves the European Union we must be able to negotiate an adequacy agreement for the free flow of data between us and the EU. That is absolutely essential.

First, the GDPR implements the right to data protection and more. It is limited in scope, but the Bill also implements data protection rights on four areas beyond GDPR. It applies GDPR standards to personal data beyond EU competence, such as personal data processed for consular purposes or national security. Secondly, the Bill applies the standards to non-computerised and unstructured records held by public authorities that the GDPR ignores. Thirdly, the Bill regulates data processed for law enforcement purposes. Fourthly, it covers data processed by the intelligence services.

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. I think this is common ground. We share Opposition Members' concern for the protection of personal data. It must be processed lawfully, individuals have rights, and the Information Commissioner will enforce them.

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.

Liam Byrne: The Minister is rehearsing the argument that was made in the other place before the requirements that we put into our amendments. She can see as well as me that the new clause was rewritten so that, under subsection (2), it is to be interpreted only

> "in accordance with the provisions, exceptions and derogations of this Act;".

So the idea that we are creating some kind of new and unfettered right is nonsense. We had this debate in the other place. We made refinements and they have been presented in the new clause.

If there is no dispute about the importance of adequacy and of putting it beyond risk, what is the problem with putting the question beyond doubt and dispute and incorporating the same foundation that is enjoyed in the European Union into British law?

Margot James: New clause 12 takes article 8 of the charter outside that context and creates a free-standing right. That is the potential for confusion. New clause 12 says nothing about the consequences of incompatibility with the new right to the protection of personal data. That would create, legal, regulatory and economic uncertainty. We are endeavouring not just to ensure adequacy after we leave the European Union, but to go beyond the mere requirement for adequacy, as the Prime Minister set out in her speech almost two weeks ago.

Further, how would the courts approach other legislation in the light of this new right? One has to ask how they would approach other rights. Could this new right be balanced against other rights?

Liam Byrne: It is not a new right; it is a roll-over of an existing right. I have not heard of a case prosecuted in British courts where there was a problem with balancing the right that we currently enjoy with anything else. We simply seek to roll this right over into the future.

Margot James: That brings me on to my other point: not only does this roll-over, as the right hon. Gentleman puts it, threaten to create confusion and undermine other rights, but it is unnecessary. The charter of fundamental rights merely catalogues rights that already exist in EU law; it is not the source of those rights. The rights, including to data protection, which is, importantly, what we are here to debate, 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.

Darren Jones: 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.

On the Minister's original comments about the consequences of the new clause, I think they are clear in the drafting. Subsection (2), as my right hon. Friend the Member for Birmingham, Hodge Hill said, states that processing personal data must comply with GDPR and the derogations in the Bill, and the consequences of subsection (3) are that the Information Commissioner should ensure compliance. In ensuring compliance, the commissioner will look to GDPR and the Bill to understand the consequences of a breach of a fundamental right that already exists.

Margot James: The source of the rights that we are discussing are EU legislation and case law. Those rights will be protected in UK domestic law after we leave the European Union by the European Union (Withdrawal) Bill. We have fully protected the right to data protection in our law. We have considered new clause 12 carefully, and it creates a new right. As I said, the arguments are well rehearsed, which is why we created clause 2 with the agreement of the Opposition spokespeople in the House of Lords.

The Government are determined to ensure the future free flow of data when we leave the European Union. We have heard much about the importance of, and the need for, an adequacy agreement, and I agree with everybody who has spoken on that. The general consensus is that, to achieve that, we need to faithfully implement the GDPR, and avoid the courts finding parts of the GDPR potentially incompatible with a new right. If that happened, rather than enabling the free flow of data, we would risk undermining it.

Twelve countries have negotiated adequacy arrangements with the European Union, including Canada, Israel, Uruguay, New Zealand and the United States. None of those countries was obliged by the EU Commission to put the charter of fundamental rights into their law, so I think Members can rest assured that the new clause is entirely unnecessary to achieve adequacy on our departure.

Brendan O'Hara: Does the Minister not accept that the countries she just listed were in an entirely different situation from the one that the United Kingdom finds itself in at the moment, where it is withdrawing from, rather than joining? One cannot compare like with like, because they are two entirely different situations. I believe that we are putting ourselves outside the scope of the GDPR and of achieving adequacy. The countries that she talked about took many years to achieve an adequacy agreement. The United Kingdom does not have that time. If the United Kingdom does not achieve adequacy on day one post-Brexit, does she not agree that the economy of the United Kingdom will suffer greatly as a result?

10 am

Margot James: I do not agree with the hon. Gentleman. I share his concern that we need to negotiate an adequacy agreement effectively; I am at one with him on that matter. For the reasons I have outlined, I do not believe that, if our clause is passed unamended, it will undermine that right when we come to negotiate an agreement. He made the point that those other countries are in a different position. They are already third countries in relation to us, and will be so when we leave. We will become a third country when we leave the European Union. I accept that the situation is different, but it puts us at an advantage. We are incorporating the GDPR in its entirety into UK legislation, and I assure the hon. Gentleman that we have that safeguard.

Future free flow of data is absolutely at the top of our agenda for the forthcoming EU negotiations. As I said earlier, my right hon. Friend the Prime Minister made that clear in her Mansion House speech two weeks ago. We want to secure an agreement with the EU that provides stability and confidence for EU and UK businesses and individuals, and ensures we achieve our aims of maintaining and developing the UK's strong trading and economic links with the European Union.

Ultimately, as some Opposition Members said, importing text from the EU charter of fundamental rights is unnecessary. The general principles of EU law will be retained when we leave the EU via the European Union (Withdrawal) Bill for the purposes of the interpretation of the retained EU law. The GDPR will be retained. Indeed, the Bill will firmly entrench it in our law. The right to the protection of personal information is a general principle of EU law, and has been recognised as such since the 1960s. The withdrawal Bill requires our courts to interpret the GDPR consistently with the general principle reflected in article 8 and retained CJEU case law, so far as it is possible to do so.

Darren Jones: Does the Minister recognise that, under the European Union (Withdrawal) Bill, the application of the EU acquis—EU law—is based on legislation that existed before the point of exit? It will not continue to apply to new legislation and developments after the point of exit. The new clause needs to be in the Bill to maintain that position for the future; we must not just look back into the past.

Margot James: The European Union (Withdrawal) Bill fully protects the rights to data protection in our law. As I said earlier, we are seeking not only adequacy

after Brexit, but a continuing role in conjunction with the bodies in Europe that govern the GDPR, with the idea that we continue to contribute our expertise and benefit from theirs.

Liam Byrne: I am afraid we have heard a very weak argument against new clause 12. The Minister sought to prosecute two lines of argument: first, that new clause 12 risks confusion in the courts; and, secondly, that it is not needed. Let me take each in turn.

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, and she had a couple of different lines of attack. First, 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. That will be bad for Britain, bad for British businesses and bad for technology jobs in all our constituencies.

The challenge we have with regulating in this particular field is that sometimes we have to be anticipatory in the way we structure regulations. Anyone who has spent any time with the British FinTech industry, which Ministers are keen to try and enhance, grow and develop for the years to come, will know that FinTech providers need to be able to test and reform bits of regulation in conjunction not only with the Information Commissioner but with other regulators such as the Financial Conduct Authority. For those regulators to be able to guarantee a degree of regulatory certainty, sometimes they will need to look beyond the letter of a particular piece of legislation, such as the Data Protection Bill when it becomes an Act, and reflect on the spirit of that legislation. The spirit is captured best by fundamental rights. The challenge we have is in the thousands of decisions that our regulators must take in the future. How do we put beyond doubt or dispute the preservation of regulatory lockstep with our single most important market next door?

The Uruguayan defence offered by the Minister will reassure few people. We should not be aspiring to the Uruguayan regime; we should be aspiring to something much deeper, more substantive and more harmonious. The Minister's proposal will create a field day for lawyers. We all like lawyers; some of our Committee members are former lawyers—recovering lawyers in some cases. Lawyers should enjoy a profitable and successful future, but we in this House do not necessarily need to maximise their profit-making possibilities in the future. However, that is exactly what the Minister is doing by creating a pot pourri of legislation, which lawyers and judges will have to pick their way through. It is much simpler, much lower-risk, much safer and better for economic growth if we put beyond doubt, dispute and question the harmonisation of our data protection regime with our single most important market. That is why we need to incorporate article 8.

Darren Jones: I have a copy of the general data protection regulation here. Recital 1 on the first page states:

"The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union—".

Is it not the case, to use some imagery here, that at the moment the GDPR is built on a foundation as on page one of this fundamental right in the same way as a house is built on strong foundations? Are we now not seeking to build the same house but without the foundations? Does this risk us sinking our decision on adequacy?

Liam Byrne: My hon. Friend is right. He speaks with tremendous knowledge on this particular subject. There is a real risk that one of our most important industries will have its foundations wrecked by the inadequacies of this piece of legislation. There is no risk of confusion, there is no creation of a new and unchecked, unfettered right. We can draw no comfort from the EU (Withdrawal) Bill. There is a great risk of regulatory confusion and divergence over the years to come. I simply cannot understand why the Government would seek to put dogma and not the future protection of the British technology industry first.

This is not a trivial or frivolous issue; it has been put forward by the industry association representing half of technology jobs in this country. I hope that the Committee is persuaded by these arguments. We will seek to prosecute these arguments in a vote, at your discretion, Mr Hanson, but I hope that before we get to that point, the Government will see sense and accept the amendment.

The Chair: As I said, the vote on new clause 12, should there be one, will take place at a later date.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

Clause 3

Terms relating to the processing of personal data

Margot James: I beg to move amendment 1, in clause 3, page 2, line 25, leave out "personal data" and insert "information".

This amendment and Amendment 2 enable the definition of "processing" to be used in relation to any information, not just personal data.

The Chair: With this it will be convenient to discuss Government amendments 2 to 6 and 69.

Margot James: These amendments make a series of minor and technical changes to clause 3, which covers terminology relating to use of personal data. I do not propose to go through each one in detail, because they are designed to improve clarity and consistency of language, and no more. Amendments 1 and 2 amend the definition of "processing" in subsection (4), by replacing the term "personal data" with "information". This has no material impact on the use of the term "processing" in parts 2 to 7 of the Bill, where the meaning of "processing" is to be understood within the context of the applicable regime, but the amendments ensure consistency with terminology in other legislation.

Amendments 3 and 6 are linked; amendment 6 adds a new paragraph (c) to subsection (14), confirming that the terms "controller" and "processor" have the same meaning in parts 5 to 7 of the Bill as they do in parts 2 to 4 respectively, unless otherwise stated. Amendment 3 adds a cross-reference to this new paragraph in subsection (6). Again, these are both technical in nature. Amendment 4 ensures that references in parts 5 to 7 of the Bill to chapter 2 of part 2 will be read as including the applied GDPR under chapter 3 of part 2, unless stated otherwise.

Amendment 69 removes similar wording from clause 184, because amendment 4 means that it is no longer required. Finally, amendment 5 improves the phraseology relating to the processing of personal data in subsection (14)(b).

Amendment 1 agreed to.

Amendments made: 2, in clause 3, page 2, line 26, leave out "personal data, or on sets of personal data" and insert "information, or on sets of information".

See the explanatory statement for Amendment 1.

Amendment 3, in clause 3, page 2, line 41, after "83" insert "and see also subsection (14)(c)".

This amendment is consequential on Amendment 6.

Amendment 4, in clause 3, page 3, line 27, at end insert —

"(aa) references to Chapter 2 of Part 2, or to a provision of that Chapter, include that Chapter or that provision as applied by Chapter 3 of Part 2;".

This amendment makes clear that references to Chapter 2 of Part 2 in Parts 5 to 7 of the bill include that Chapter as applied by Chapter 3 of Part 2.

Amendment 5, in clause 3, page 3, line 28, leave out "processing and personal data are to processing and personal data" and insert "personal data, and the processing of personal data, are to personal data and processing".

This amendment is consequential on Amendment 1.

Amendment 6, in clause 3, page 3, line 29, at end insert —

"(c) references to a controller or processor are to a controller or processor in relation to the processing of personal data to which Chapter 2 or 3 of Part 2, Part 3 or Part 4 applies."—*(Margot James.)*

This amendment and amendment 3 make clear that references to controllers and processors in Parts 5 to 7 of the bill are to controllers and processors in relation to processing to which the GDPR, the applied GDPR or Part 3 or 4 of the bill applies.

Clause 3, as amended, ordered to stand part of the Bill.

Clauses 4 to 6 ordered to stand part of the Bill.

Clause 7

Meaning of "public authority" and "public body"

10.15 am

Margot James: I beg to move amendment 7, in clause 7, page 5, line 8, leave out "a body specified" and insert "body specified or described".

This amendment and Amendment 8 make clear that regulations under Clause 7 may identify an authority or body by describing a type of authority or body, as well as by specifying an authority or body.

The Chair: With this it will be convenient to discuss Government amendments 8, 18, 19 and 62.

Margot James: Clause 7 defines the meaning of "public authority" for the purposes of the GDPR. Generally speaking, "public authority" will have the same meaning as the definition used in the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002. Those Acts list a wide range of public authorities, including Departments, local authorities and NHS bodies. As the new legislation beds in, the list of authorities imported from those Acts may need to be adapted to function properly in a data protection setting rather than a freedom of information setting. Clause 7(1) therefore allows the Secretary of State to specify in regulations that additional bodies are public authorities for the purposes of data protection legislation. Conversely, subsection (3) allows the Secretary of State to specify that certain bodies are not to be treated as public authorities, even if they are defined as such for the purposes of freedom of information legislation.

Amendments 7 and 8 clarify that the Secretary of State may describe bodies that are or are not public authorities in addition to specifying them. They are technical amendments designed to improve the terminology used in relation to the Secretary of State's regulation-making powers. Amendments 18 and 19 make corresponding provisions in relation to part 3 of the Bill.

Amendment 62 is designed to ensure that regulations made under clause 7 will not be considered as hybrid instruments. Regulations made under the clause are already subject to the affirmative resolution procedure, and the general duty to consult before making regulations, which is set out in clause 179, also applies. In this setting, the hybrid procedure would add nothing but bureaucracy.

Liam Byrne: The amendments look like tidying-up amendments, but it would help if the Minister put on the record the extent to which they will allow the Bill to bite effectively on the nation's schools. Obviously, schools collect a great deal of data. They often hold not only exam data but data relating to eligibility for free school meals, and most schools operate systems such as ParentPay, which means that they capture children's biometrics. Anything to do with the protection of children's data has to be treated incredibly seriously. The school system in this country has been balkanised—often, academies are set up as private sector entities in complex chains and have problematic governance arrangements—so I think we would all benefit from the Minister saying a few words about the Bill's bite on schools, academies

and colleges. Will she also say a little more about her plans to ensure that there are statutory codes of practice to which everyone who provides education services must adhere?

Margot James: I thank the right hon. Gentleman for his comments. Obviously, we share his concern about the protection of children. He cites important and highly sensitive personal data such as biometrics. Schools, like all bodies, must have a legal basis—the public interest or the normal course of their business—for processing personal data.

The right hon. Gentleman raises safeguarding. Later in our deliberations, my hon. Friend the Under-Secretary of State for the Home Department will introduce Government amendments to strengthen the safeguarding aspects of the processing of personal data. Schools are public authorities, and GDPR protections intended for authorities will apply, as I said. Schedule 3 provides further and specific protection on the points that he raises.

Liam Byrne: Will the Minister set on the record explicitly the fact that academies are covered in the same way as schools? An academy may be set up by a private sector organisation, set up as a charitable body, or set up in a way that is outwith the formal education system. Ofsted has raised concerns about unregulated schools, for example. Can she confirm whether organisations that provide education services—whether they are academies, charities or local education authority schools—are governed by the codes? Crucially, can she confirm that she will publish the code of practice?

Margot James: I certainly can confirm that the schools that the right hon. Gentleman has cited—academies run by private sector organisations and/or charities—are public authorities for the purposes of the Bill, and will be subject to the same protections.

Question put and agreed to.

Amendment made: 8, in clause 7, page 5, line 13, after "specified" insert "or described".—*(Margot James.)*

See the explanatory statement for Amendment 7.

Clause 7, as amended, ordered to stand part of the Bill.

Clause 8

LAWFULNESS OF PROCESSING: PUBLIC INTEREST ETC

Daniel Zeichner (Cambridge) (Lab): I beg to move amendment 140, in clause 8, page 5, line 23, after "includes" insert

"but is not limited to,".

The Chair: With this it will be convenient to discuss amendment 141, in clause 8, page 5, line 29, at end insert

"or

(e) the exercise of research functions by public bodies."

This amendment would ensure that university researchers and public bodies with a research function are able to use the 'task in the public interest' lawful basis for processing personal data, where consent is not a viable lawful basis.

Daniel Zeichner: It is a pleasure to serve under your chairmanship, Mr Hanson. I shall begin by declaring an interest: I chair the all-party parliamentary group on data analytics, the secretariat to which is provided by Policy Connect. In that capacity, I have had the pleasure of having many discussions about GDPR with experts over the past couple of years. I reflect on what a very good process it is that British parliamentarians in the European Parliament are able to intervene on such matters at early stages, to make sure that when the legislation finally comes to us it already has our slant on it. That may not be possible in future when we come to discuss such legislation.

I represent a university city, so research is a key part of what we do. It is on that basis that I tabled the amendments, and I am grateful to the Wellcome Trust and the Sanger Institute, which have given me advice on how the amendments would help them by providing certainty for the work that they do. The purpose of amendment 141 is to ensure that university researchers and public bodies with a research function are able to use what is called the "task in the public interest" lawful basis for processing personal data, where consent is not a viable lawful basis. I apologise for going into some detail, but it is important for universities and researchers that there is clarity.

As the Bill is drafted, clause 8 provides a definition of lawfulness of processing personal data under GDPR article 6(1)(e). Subsections (a) to (d) of clause 8 set out a narrow list of activities that could be included in the scope of public interest. I am told that that list is imported from schedule 2(5) of the Data Protection Act 1998, but I am also told that the drafters have omitted a version of the final and most general sub-paragraph from that list, which reads:

"for the exercise of any other functions of a public nature exercised in the public interest by any person."

It is speculated that that may have been taken out of the list to tighten up, and to avoid a tautology in defining, "public interest", but the worry is that taking it out has made the clause too restrictive. The explanatory notes indicate that the list in clause 8—that is, subsections (a) to (d)—is not intended to be exhaustive, but the Wellcome Trust and the Sanger Institute worry that it has narrowed the public interest terminology to a very narrow concept, which will be confined to public and judicial administration.

There was a very lengthy and very good debate in the other place on this matter. 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.

The amendment tries to enable research functions to be conducted by public bodies such as universities without doing what the Government fear, which is to broaden the definition of "public interest" too far. The wording retains the structure of the DPA list, from which the current clauses were imported, but it narrows

[Daniel Zeichner]

it down in two ways. It specifies the purpose of processing, that is, research functions, which must be the reason for the processing and specifies who is doing the processing—the basis of it only being available to public bodies, as defined in the previous clause.

We are aware that the Government are worried about adding further subsections to the list. I think they said that it could open the floodgates in some way. However, I am told that there is not really any evidence to suggest that the current wording of paragraph 5 of schedule 2 of the Data Protection Act, which has a very broad notion of public interest, has in any way "opened the floodgates". To give some sense of the concerns that have arisen, the processes by which university researchers seek permission to do things are quite complicated. Some of the bodies have already issued guidance. I am told that the Health Research Authority issued guidance on GDPR before Christmas. It advised that a clause on using legitimate interests should be included in the Bill.

There is confusion in the research sector, and there is a wider worry that if this is not clear, it is open to legal challenge. While some institutions will be able to take that risk, the worry is that smaller research bodies would conclude that, given the lack of clarity, it would not be worth taking that risk. I hope that the Government will think hard about the suggestion. It comes from the research institutions themselves and would give clarity and reassurance. I hope that the Minister will accept the amendment.

Liam Byrne: I want to say a few words in support of my hon. Friend and these important amendments. I think there is an acknowledgement on both sides of the Committee that if we are to prosper in the world that is coming, we are going to need to increase the amount of money that we spend on research and development and make sure that a research-driven economy reaches every corner of the country.

The world of innovation and research is changing very quickly. I think it is next year that China becomes the world's largest science spender for the first time in several centuries. If we are to compete in this new world, we need to invest more in our R&D base. The Government have made some helpful commitments in this area. Their proposals are not quite as ambitious as the Labour amendments, but none the less all progress is welcome.

I hope that the Minister will reflect on the reality—the way in which research is conducted in our country is changing. In the past, I have called that a shift from the cathedral to the campus. Once upon a time, big firms put a lot of people in a large building and prayed for the best. Now, they are building business parks and creating ecosystems of innovation where they may have a shared research and development facility, otherwise known as a university. There may be big international companies with global reach organised around them, but there are also scores of much smaller firms. They may be as small as a couple of post-docs in a shared lab. If we look at facilities such as BT at Dashwood Park, the Crick Institute or GSK in Stevenage, we see big global companies with hundreds of smaller companies around them which are undertaking research with much greater speed and much lower risk, but with an impact that could change the world.

We cannot jeopardise the conduct of that research. My hon. Friend the Member for Cambridge is right to point out that where there is doubt about the law, or the powers and freedoms of research firms, there is a risk that such firms simply will not undertake such work in the UK, and instead will seek relationships either with global companies or, increasingly, with universities that have R&D facilities elsewhere. We want to create the world's best place to undertake new science, and that means having a research regime that is the best in the world. We therefore need a data protection regime that helps and does not hinder, which is why the Government should accept these carefully crafted amendments.

10.30 am

Margot James: I recognise the expertise of the hon. Member for Cambridge in this area, and I am glad of the opportunity to debate the matter fully with him, as I am conscious that I did not address the points he made in his good contribution on Second Reading. We all agree on the importance of scientific research, and one of the things I am most proud of in the industrial strategy is the huge increase in public funding for research and development. We welcome the interest in the Bill shown by the Wellcome Trust and other organisations. They are concerned that universities processing personal data in the context of ground-breaking medical research will not have a clear legal basis for doing so. The Government recognise how important that is, but we believe that the amendment is not necessary and that there is no need specifically to mention the research functions of public bodies in clause 8.

It might be helpful if I explain what clause 8 is designed to do. If an organisation is to process personal data, it must have a legal basis for doing so under article 6 of the GDPR. The clearest basis is where the data subject has given his or her consent to the processing, but article 6 also permits processing without someone's consent in certain circumstances, including where

"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

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 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 to much 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". Given those reassurances, I hope that the hon. Gentleman will not feel it necessary to press his amendment to a vote.

Daniel Zeichner: I thank the Minister for her kind words—particularly about Second Reading. I think that we were all puzzled about what was going on at about five minutes to 10; I am none the wiser. I am slightly disappointed by her response, because this is not a party political discussion. We all want to get to the same place. In many ways, the discussion we have just had is not that dissimilar from the previous one about educational institutions, schools and academies. There are many grey areas relating to what universities are, and what their status and that of the research bodies associated with them is. My worry is that if we just take the Minister's reassurances rather than amend the Bill, the uncertainty to which I alluded—it is not my uncertainty; it is what staff at esteemed research institutions say they feel—will be a problem. We should try to improve the Bill to get the clarity we need.

The Chair: The hon. Gentleman needs to indicate to the Chair whether he wishes to withdraw the amendment or press it to a Division.

Daniel Zeichner: I think we will go to a vote, Mr Hanson.

Question put, That the amendment be made.

The Committee divided: Ayes 8, Noes 10.

Division No. 1]

AYES

Byrne, rh Liam	McDonald, Stuart C.
Elmore, Chris	O'Hara, Brendan
Haigh, Louise	Snell, Gareth
Jones, Darren	Zeichner, Daniel

NOES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

Question accordingly negatived.

Margot James: I beg to move amendment 9, in clause 8, page 5, line 29, at end insert—

"( ) an activity that supports or promotes democratic engagement."

This amendment adds a reference to processing of personal data that is necessary for activities that support or promote democratic engagement to Clause 8 (lawfulness of processing: public interest etc).

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. As my noble Friend Lord Ashton set out in the other place, the Government believe that there is a strong public interest in political parties and elected representatives and officials being able to engage with the public both inside and outside elections, which may sometimes include the processing of personal data.

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.

The amendment does not seek to create a partisan advantage for any one side or to create new exemptions from the data protection legislation. It is intended to provide greater clarity. It is also independent of any particular technology, given that in a short time we have moved from physical post to email, Twitter, text messages, WhatsApp, Facebook and so forth.

The Government are always open to suggestions of what else could be done to ensure legal and operational clarity for political parties and elected representatives. Further work might be needed to ensure that their current activities have the legal basis required to rely on the public interest condition. The Government will shortly engage with political parties via the parliamentary parties panel to discuss the matter further and in more detail.

Liam Byrne: I was surprised and not a little troubled that the Minister did not include the opportunity of creating Member-specific apps in her list—especially those which suck out the pictures from someone's phone without their permission. Presumably that was not included in her list because that is already illegal.

I am grateful to the Minister for tabling the amendment and for her earlier correspondence with my noble Friend Lord Kennedy. She undertook to reflect on that correspondence and bring forward amendments. She helpfully set out a list of some of the activities that may be undertaken by a political party that fall within the ambit of the amendment. She gave a pretty comprehensive list, but will she put beyond doubt whether canvassing and collecting canvass returns were in her mind when she tabled the amendment and are therefore covered by the amendment? That would be extremely helpful.

The amendment is well intentioned. The health of our democracy is important to all parties. We look forward to the conversations that she will broker through the parliamentary parties panel.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): We, too, are grateful to the Minister for tabling the amendment and for her letter to you on 12 March, Mr Hanson, which has been shared with the Committee.

From our point of view, the description of democratic engagement as a new lawful basis for processing in the public interest, under article 6(1)(e) of the GDPR, is useful. In fact, there might even be an argument for including the non-exhaustive list, which I think is due to appear in the explanatory notes, in the Bill. Will the Minister think about that? I appreciate that it has been kept in very general terms.

In her letter, the Minister asked for views on whether the basis for processing data from electoral registers is currently appropriate as defined. Those registers are supplied to parties with the main condition that they are used for electoral purposes. The Law Commission, which recently reported on the review of electoral law, expressed the view that the legislation should be more precise about what that means. Again, the list in the letter that the Minister sent to you, Mr Hanson, looks like a good starting point for that.

10.45 am

The Electoral Commission has said that general political fundraising using the electoral register is not lawful, so it might be helpful to have that on the face of the Bill or in regulations. The main issue with the test of "for electoral purposes" is that every activity needs to be related to an election for it to be processed under the supplied conditions. In practice, parties engage in general campaigning, including issue-based campaigning, which is not necessarily directed at elections. In broad terms, we welcome the amendment and we make these points merely to take forward further debate.

Margot James: I thank the right hon. Member for Birmingham, Hodge Hill and his noble Friends for their constructive participation in the development of the amendment. He mentioned the app of the Secretary of State for Digital, Culture, Media and Sport; I assure him that it is compliant in every way with current data protection law and will be compliant with the provisions of the Bill. I commend my right hon. Friend for setting a new standard in the way that he communicates with his constituents.

I reassure the right hon. Member for Birmingham, Hodge Hill that canvassing and collecting canvassing returns are covered by the amendment. That is absolutely vital. I reassure the hon. Member for Cumbernauld, Kilsyth and Kirkintilloch East that it covers campaigning activity and communications between elections, concerning issues as well as elections. As I said in my short preamble, the detail of the matter can be further discussed at a meeting of the parliamentary parties panel and it is within everybody's rights to contribute their thoughts to panel members for those important forthcoming discussions.

Amendment 9 agreed to.

Clause 8, as amended, ordered to stand part of the Bill.

Clause 9

CHILD'S CONSENT IN RELATION TO INFORMATION SOCIETY SERVICES

Question proposed, That the clause stand part of the Bill.

Liam Byrne: The clause is an important topic of debate because it enshrines the Government's derogation from European frameworks in law and sets the minimum age of consent for data processing at 13 rather than 16.

That derogation was invented before social media companies arrived at their current strength and delivered the very wide and sophisticated range of tools that help ensure that children become almost addicted to social media devices. In the debate on this topic over the last two or three months there have been fresh revelations from leaders of social media firms that they forbid their children to engage in the apps that their companies deliver. We have had revelations from engineers who have worked at companies such as Facebook, Twitter and Instagram that a great deal of thought goes into how they create devices and forms of interaction that encourage that basic addiction to their apps.

We are at the beginning of what I hope is a period of re-regulation and better regulation of these firms, so that we can do away with many of the risks that affect our children. In a way, I was encouraged to see the Secretary of State's interview with *The Times* on Saturday, in which he said very clearly that he would like to see better regulation of social media firms in this country before his own children are tempted to engage in this exciting online world. Many of us have children who are already engaged in this and, as a parent, I have real concerns about the freedom with which social media companies can develop and deliver these techniques, as well as their freedom to take a rather relaxed view of taking down often unfortunate and extremist content. I know that we will have this debate later, and we have tabled amendments to encourage the Government to set a deadline for reforming the electronic commerce directive.

It is important to draw a little more out of the Government about how they see the safeguards coming into place around clause 9. We have not sought to challenge the derogation the Government seek to enshrine in the Bill, but we ensured widespread support for Baroness Kidron's amendment on the creation of an age-appropriate code. However, rather than simply wave clause 9 through, it is incumbent on the Minister to say a little about how she will ensure that there are adequate safeguards in place to protect our children from the very threats the Secretary of State lit up in lights on Saturday.

Margot James: I support the general tone of the right hon. Gentleman's comments. I too was pleased to see the interview with the Secretary of State, his focus on the addictive nature of some of these apps and the idea that there could be within the technology a means of limiting the time children spend on them, which parents could click on. The Information Commissioner's Office will publish guidance shortly on how clause 9 will work and what those safeguards will be. She will take into consideration an age-appropriate design, as suggested by Baroness Kidron.

Overall, where online services referred to in the Bill as "information society services" choose to rely on consent as the basis for their processing, article 8 of the GDPR sets the age below which a website must obtain the parents' and not the child's consent. Most websites will be captured by this additional safeguard, ranging from online banking to search engines to social media, with social media probably being the most relevant to the age group in question.

The GDPR gives member states the flexibility to set this age within a prescribed range of between 13 and 16. The Bill sets it at 13, with an exception for preventive and counselling services, for which the test is based purely on the child's capacity to understand what they are being asked to consent to. The Government are satisfied that the Information Commissioner's Office has adequate enforcement powers, including large fines for any offences committed in this area.

Darren Jones: The Minister said that Europe provides that the age range is between 13 and 16. In fact, the GDPR says the age for consent is 16, but that member states can derogate down to 13. I do not wish to be an annoying lawyer, but it is an important distinction. Our colleagues in Europe are saying that the age they deem to be appropriate is 16, but they are giving member states flexibility to go lower. Interestingly, article 8(2) talks about how reasonable efforts need to be taken to verify age and consent

"taking into consideration available technology."

My view is that, on these types of issues, there should be better technology for age verification as part of using online services and, where children's data is being used to commercialise and monetise for the purposes of advertising, there should be additional safeguards for children.

I ask the Minister only to keep an open mind in the future, so that when we get to a position where technology providers can verify the age of children—I appreciate that is perhaps currently a little difficult—if industry does not move voluntarily to this position, the Government consider regulating in that regard.

Margot James: The hon. Gentleman is right that the GDPR stipulates 16 as the minimum age for consenting to data processing without parental consent, but that it provides for member states to derogate from that. At least seven, including Spain, Ireland and Denmark, have done just that. Like us, they have proposed a much younger age of 13, so we are not an outlier on the issue.

Currently, the minimum age in this country for allowing personal data to be used without parental consent is 12, so in a sense we are derogating from that policy by setting the minimum age at 13 in the Bill. The hon. Gentleman is right to point out that it is very difficult for technology companies to implement meaningful verification mechanisms for those younger than 18, who may not have anything like a credit card or driving licence. I have no doubt that the Government will keep an open mind on the matter, in line with other developments that will take place long after the Bill is passed.

Question put and agreed to.

Clause 9 accordingly ordered to stand part of the Bill.

Clause 10

Special categories of personal data and criminal convictions etc data

Stuart C. McDonald: I beg to move amendment 129, in clause 10, page 6, line 19, leave out subsections (6) and (7).

This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.

The Chair: With this it will be convenient to discuss the following:

Amendment 132, in clause 35, page 21, line 29, leave out subsections (6) and (7).

This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.

Amendment 134, in clause 86, page 50, line 33, leave out subsections (3) and (4).

This amendment would remove delegated powers that would allow the Secretary of State to vary the conditions and safeguards governing the general processing of sensitive personal data.

Stuart C. McDonald: The amendments stand not only in my name and that of my hon. Friend the Member for Argyll and Bute, but in the names of Labour Members, for whose support we are very grateful.

There cannot be anyone in this Committee Room who does not know what a Henry VIII power is. If my email inbox is anything to go by, half the country knows what a Henry VIII clause is now, even if they did not know before the European Union (Withdrawal) Bill commenced its progress through the House. Amendments 129, 132 and 134 would remove Henry VIII powers from clauses 10, 35 and 86 respectively. To explain why those powers are not appropriate and need to be removed, I need to explain briefly what those clauses concern and why the powers are therefore too significant and wide.

Clause 10 needs to be read alongside article 9 of the GDPR, which states unambiguously:

"Processing of personal data revealing 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 shall be prohibited."

Such data includes some of the most sensitive information that we can imagine. Article 9 then sets out situations in which the prohibition does not apply. Some of the exceptions that it lists, such as those in which

"processing relates to personal data which are manifestly made public by the data subject",

apply directly, so the Bill need not address them. Others need to be interpreted in accordance with EU or member state law before they can be relied on; for instance, paragraph 2(g) of article 9 states that the prohibition shall not apply if

"processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law".

Clause 10, which applies schedule 1, establishes the basis in member state law for lifting the prohibition on processing such sensitive information. For example, part 2 of schedule 1 includes 18 conditions—ranging from parliamentary and ministerial functions to preventing money laundering and detecting unlawful acts—that provide the basis in UK law for the substantial public interest exception to apply to the processing of special categories of personal data.

Clause 35 is in part 3, which is headed "Law enforcement processing". It states that the first of the data protection principles by which law enforcement bodies must abide

"is that the processing of personal data for any of the law enforcement purposes must be lawful and fair".

The specific conditions that must be met with respect to sensitive data are set out in schedule 8, which is similar to schedule 1. They include cases in which the processing is necessary

[Stuart C. McDonald]

"for the administration of justice"

or

"to protect the vital interests of the data subject or of another individual."

Clause 86 is in part 4, "Intelligence services processing". It essentially does for that activity what clause 35 does for law enforcement, and it applies schedule 10. In short, we have a carefully framed set of exceptions to the prohibition on processing of this extremely sensitive information, and those exceptions provide a lawful basis for the processing of information that we normally would not dream of processing because of its highly intrusive and sensitive nature.

11 am

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. Any adjustments to this fine balance deserve the greatest of scrutiny; we on this Bill Committee are essentially wasting our time if we are just handing the Government a blank cheque to hand out powers as and when they see fit. We seek support for our amendments to remove these Henry VIII powers from the Bill.

Liam Byrne: We support these amendments very strongly, and if possible we would like to test the Committee's will on this. The Bill has a succession of Henry VIII powers at a number of different clauses, which in effect give the Secretary of State the power to vary and amend regulations that are incredibly important. We cannot detach this debate from the earlier debate on the incorporation of article 8. We now have a Bill that is pretty weak on the fundamental principles of law that it seeks to enshrine; the Government want to set their face against incorporating some protections that we have in the European charter of fundamental rights. Therefore, the idea that we leave out some fundamental protections of rights, but then hand over to the Minister unfettered power to make regulations as he or she sees fit, does not seem to be in Parliament's best interest. We think that the Government need to think again.

The powers in this particular clause create the possibility that exemptions to data protection rights, which have not been considered or debated in Parliament, go through effectively at the whim of the Minister. Those powers are enshrined in clause 10, and in clauses 35 and 86; we will come on to those debates, but the powers that clause 10 proposes to grant the Minister are in effect unilaterally to vary the conditions and safeguards governing the general processing of sensitive personal data—the general data set out in schedule 1—and then to add new conditions to schedules 1, 8 and 10.

That means that we would basically give the Secretary of State the power to expand the permissible reasons to allow processing of sensitive personal data, both generally and particularly for law enforcement and intelligence agencies. That is something that has been considered extensively in the other place. The House of Lords Constitution Committee said:

"The Government's desire to future-proof legislation…must be balanced against the need for Parliament to scrutinise and, where necessary, constrain executive power."

The Delegated Powers and Regulatory Reform Committee said that

"it is not good enough for Government to say that they need 'flexibility' to pass laws by secondary instead of primary legislation without explaining in detail why".

The Ministers slightly let the cat out of the bag when Baroness Chisholm spoke up for the Government and said that if they were to accept the Committee's recommendations in full that would

"leave the Government unable to accommodate developments in data processing and the changing requirements of certain sectors"—[*Official Report, House of Lords,* 11 December 2017; Vol. 787, c. 1464.]

That includes, for example, the insurance sector. That is patently nonsense. It would not constrain the Government's ability to introduce wise regulations in this place; it would simply constrain the Government's ability to do that unilaterally without effective recourse to Parliament. We are seeking a very clear Government explanation as to why the Secretary of State, not Parliament, should be empowered to alter the data protection regime to keep it up to date, and that explanation needs to be all the more robust following the remarks that the Minister has made about her attitude towards incorporating the fundamental right of privacy in British law.

We think that the amendments would be sensible constraints on Henry VIII powers. There is wide consensus across both Houses that they are necessary. They will not damage or diminish the Secretary of State's ability to keep regulation up to date. Many of us have been in this place long enough to know that it is perfectly within the Executive's power to keep regulatory reform on track if the political will is there. We are asking for a defence of Parliament's right to oversee, scrutinise and, where necessary, constrain the powers of the Secretary of State to regulate in this field.

Margot James: Following recommendations by the Delegated Powers and Regulatory Reform Committee, we have considered carefully the use of the Bill's order-making powers and amended the Bill in the House of Lords to provide additional safeguards for the exercise of those powers, but Members of the Lords on all sides of the House agreed that it was essential to retain the order-making powers in the Bill as amended.

I will explain how the powers will be used in practice. Article 9 of the GDPR prohibits the processing of special categories of personal data unless one of the exemptions in paragraph 2 of article 9 applies. The exemptions include, for example, the situation where processing is necessary for reasons of substantial public interest. Schedule 1 to the Bill provides a series of processing conditions for special categories of data under article 9 and criminal convictions data under article 10. Most of those processing conditions have been imported from the Data Protection Act 1998 and statutory instruments made under that Act, but some of them are new—for example, the conditions on anti-doping

in sport or processing for insurance purposes. They have been added to reflect the way in which the use of data has changed over the past 20 years.

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.

It is interesting to note that the hon. Member for Sheffield, Heeley has tabled an amendment to schedule 1 that would add a completely new processing condition in relation to maintaining the missing persons register. My hon. Friend the Under-Secretary of State for the Home Department will touch on the merits of that proposal later, but the fact that others in the Committee are considering further changes to schedule 1 illustrates the point that schedule 1 cannot simply freeze the regimes in parts 3 and 4 of the Bill. I urge colleagues to resist the amendment.

Stuart C. McDonald: It is vital that we get the balance right: we are talking about very sensitive information and processing of that information. It is absolutely right for hon. Members to table amendments to the Bill and for them to be considered, including proposals on the missing persons register. The fact that hon. Members are suggesting changes at this stage does not mean that we are saying that we want to fix things for all time now and never suggest changes again. We are saying that we are not happy with the process whereby changes are brought about. The Minister has not explained why she believes that changes could not be brought about satisfactorily by changes to legislation from time to time. She has not explained why there would be urgent situations in which the only possibility would be a "Take it or leave it" statutory instrument. In the light of the seriousness of the data that we are speaking about and the inadequacy of the Minister's explanation, we would like to press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 2]

AYES

Byrne, rh Liam	Murray, Ian
Elmore, Chris	O'Hara, Brendan
Haigh, Louise	Snell, Gareth
Jones, Darren	Zeichner, Daniel
McDonald, Stuart C.	

NOES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

Question accordingly negatived.

Clause 10 ordered to stand part of the Bill.

Schedule 1

SPECIAL CATEGORIES OF PERSONAL DATA AND CRIMINAL CONVICTIONS ETC DATA

Margot James: I beg to move amendment 76, in schedule 1, page 123, line 21, at beginning insert "Except as otherwise provided,".

This amendment is consequential on Amendments 79, 82 and 90.

The Chair: With this it will be convenient to discuss Government amendments 77 to 83 and 87 to 91.

Margot James: Part 2 of schedule 1 sets out a series of processing activities that are considered to be or have the potential to be in the substantial public interest. That is important in ensuring that such activities can continue even in the absence of explicit consent and even where they require special categories of personal data to be processed.

I am pleased to introduce amendment 78 today. It will help businesses and other organisations ensure that boardrooms and senior management levels are truly representative of the workforce they manage and the communities they serve. In my former role at the Department for Business, Energy and Industrial Strategy, I worked closely with Sir John Parker, to whom I pay great tribute for the work that he has done in this area. I worked with him to examine how we could ensure that more FTSE 100 companies and others did more to attract talent from a wide range of racial and ethnic backgrounds.

In November 2016, Sir John published a report that showed that although 14% of the population identified as black, Asian or other minority ethnic status, only 1.5% of directors in FTSE 100 boardrooms were UK citizens from such a minority. Although significant progress has been made in recent years to improve the gender balance in the boardrooms of such companies, the severe under-representation of people from minority ethnic backgrounds cannot be tolerated in modern society. Sir John's report included a series of recommendations to improve ethnic diversity in the boardroom. He encouraged companies to make better use of executive search firms to identify potential candidates and invite them to be interviewed for managerial vacancies.

Amendment 78 will add a new processing condition to schedule 1 to allow organisations to process personal data about potential candidates' racial or ethnic origin and identify suitable candidates for potential board or managerial positions. The processing condition will apply only until such point as it is reasonable to expect the organisation to get the potential candidate's consent to the continued processing of their racial and ethnic origin data. If the data subject gave a positive indication that she or he did not consent to the processing of such data, the controller would have to cease processing the data.

I hope that hon. Members welcome the steps we are taking to implement the recommendations of the Parker review. We believe that it is in the interest of society as a whole to ensure that businesses and other organisations recruit the best person for the job if they are going to compete in today's economy. People from all backgrounds should be given equal opportunities to contribute.

11.15 am

I am also pleased to introduce amendment 83, concerning patient support, which honours a commitment made by the Government to my noble Friend, Baroness Neville-Jones during the Bill's passage through the Lords. She spoke passionately on behalf of the patient support group Unique, which maintains a register of patients suffering from very rare and sometimes life-limiting chromosomal disorders. Over the years, it has built up a database of around 18,000 patients, which it uses to provide invaluable guidance and support to new and existing members, who may not know what to expect from the different stages of a particular disorder. It even uses the database to advise GPs and other medical professionals about probable symptoms so that they can help patients at the time of diagnosis. Amendment 83 adds a new processing condition to the schedule to provide Unique and groups like it with the legal certainty they require to continue their vital work.

During the Lords stages of the Bill, Thomson Reuters provided their lordships with a helpful briefing note setting out how it compiles reports on persons suspected of terrorism, bribery, money laundering, modern slavery and other reprehensible activities. It shares that information with banks to help them avoid mixing with such people and to allow them to comply with their regulatory obligations and other internationally recognised guidelines. In response to support for the proposal on both sides of the House of Lords, the Government committed to working with Thomson Reuters to bring forward amendments at a later stage of the Bill's passage.

Amendment 81 is the culmination of that work. It adds a new processing condition to the schedule to allow organisations such as Thomson Reuters, and banks themselves, to screen customers and suppliers for criminal activities and other seriously improper conduct. The condition can be used only in circumstances where the controller cannot reasonably be expected to obtain the data subject's consent to process data—for example, where the controller processes data from sanction lists and therefore does not have contact details for individuals. I am pleased to introduce the amendment, which should help the UK's fight against organised economic crime by making it more difficult for offenders to launder the proceeds of their crime. I am grateful for the help that Thomson Reuters provided my officials with developing the provision.

Moving to the technical amendments in the group, amendment 88 corrects a mistake in the drafting of paragraph 16 of the schedule relating to processing in connection with occupational pensions.

Liam Byrne: Oh dear!

Margot James: It does happen. That is not a new provision, but one that was imported from the current law. Unfortunately, some crucial words were accidentally lost in the process of importing it. The amendment reinstates them.

Schedule 1 sets out UK domestic legislation to allow the processing of particularly sensitive data in certain circumstances. The Government's view is that the processing of such data must be undertaken with adequate and appropriate safeguards to ensure that individuals' most sensitive data is appropriately protected. One of those safeguards is the new requirement for an appropriate policy document to be maintained in most circumstances when special categories of data and criminal convictions data are processed. That is set out in paragraph 5 and part 4 of the schedule.

Since the Bill's introduction, we have reflected on whether there are cases where the requirement to hold an appropriate policy document is so disproportionate that, rather than improving protections, it effectively prevents the necessary processing from taking place. Amendments 79, 82 and 90 remove the requirement for a controller to have an appropriate policy document where processing involves the disclosure of special category data to a competent authority for the detection or prevention of an unlawful act, the disclosure of special category data for specific purposes in connection with journalism, or the disclosure of special category data to an anti-doping authority. Amendment 80 defines what is meant by "competent authority". The aim of those amendments is to avoid a scenario in which an individual who never normally processes data under schedule 1 wishes to report a crime, report something of public interest to the media or report doping activities in sport and, in so doing, processes special categories of data and would have to have in place an appropriate policy document.

Amendment 76 reflects that change to the requirement to have an appropriate policy document by inserting the words, "Except as otherwise provided" in paragraph 5 of the schedule. Amendments 87 and 89 make it clear that, in the context of schedule 1, "withholding consent" means doing something purposeful, not just neglecting to reply to a letter from the data controller. That avoids a world in which data controllers have an incentive not to bother requesting consent in the first place.

Paragraph 31 of the schedule requires the controller to have an appropriate policy document in place when relying on a processing condition in part 2 of the schedule to process criminal convictions data. However, all the provisions in part 2 are subject to the policy document requirement except where noted, so there is no reason to state it again in paragraph 31. Amendment 91 removes that duplicate requirement. It is simply a tidying-up amendment to improve the coherence of the Bill.

Darren Jones: On a point of order, Mr Hanson. I think I was remiss in not declaring my interest at the start of my contributions to today's proceedings. With your permission, I seek to rectify that.

The Chair: That is indeed a point of order. The record will show that the hon. Gentleman has now declared his interest in relation to his contributions to the debate.

Ordered, That the debate be now adjourned.—*(Nigel Adams.)*

11.22 am

Adjourned till this day at Two o'clock.