PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL [*LORDS*]

Fifth Sitting

Tuesday 20 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 24 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 20 March 2018

(Morning)

[David Hanson *in the Chair*]

Data Protection Bill [*Lords*]

9.25 am

The Chair: We begin consideration of the Bill today with schedule 9, to which no amendments have been tabled.

Schedule 9 agreed to.

Schedule 10

Conditions for sensitive processing under Part 4

Amendment made: 117, in schedule 10, page 187, line 5, at end insert—

'Safeguarding of children and of individuals at risk

3A (1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual.'—*(Victoria Atkins.)*

Schedule 10 makes provision about the circumstances in which the processing of special categories of personal data is permitted. This amendment adds to that Schedule certain processing of personal data which is necessary for the protection of children or of adults at risk. See also Amendments 85 and 116.

Schedule 10, as amended, agreed to.

Clauses 87 to 93 ordered to stand part of the Bill.

Clause 94

Right of access

Amendments made: 35, in clause 94, page 55, line 8, leave out 'day' and insert 'time'

This amendment is consequential on Amendment 71.

36, in clause 94, page 55, line 9, leave out 'day' and insert 'time'

This amendment is consequential on Amendment 71.

37, in clause 94, page 55, line 10, leave out 'days'

This amendment is consequential on Amendment 71.

38, in clause 94, page 55, line 11, leave out 'the day on which' and insert 'when'

This amendment is consequential on Amendment 71.

39, in clause 94, page 55, line 12, leave out 'the day on which' and insert 'when'

This amendment is consequential on Amendment 71.

40, in clause 94, page 55, line 13, leave out 'the day on which' and insert 'when' —*(Victoria Atkins.)*

This amendment is consequential on Amendment 71.

Clause 94, as amended, ordered to stand part of the Bill.

Clause 95 ordered to stand part of the Bill.

Clause 96

Right not to be subject to automated decision-making

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

Liam Byrne (Birmingham, Hodge Hill) (Lab): We are rattling through the Bill this morning and will soon reach clause 109, to which we have tabled some amendments. Clause 96, within chapter 3 of part 4, on intelligence services processing, touches on the right not to be subject to automated decision making. I do not want to rehearse the debate that we shall have later, but I think that this is the appropriate point for an explanation from the Minister. Perhaps she will say something about the kind of administration that the clause covers, and its relationship, if any—there may not be one, but it is important to test that question—to automated data-gathering by our intelligence services abroad, and the processing and use of that data.

The specific instance that I want to take up concerns the fact that about 700 British citizens have gone to fight in foreign conflicts—for ISIS in particular. The battery of intelligence-gathering facilities that we have allows us to use remote data-sensing to detect, track and monitor them, and to assemble pictures of their patterns of life and behaviour. It is then possible for our intelligence services to do stuff with those data and patterns, such as transfer them to the military or to foreign militaries in coalitions of which we are a member. For the benefit of the Committee, will the Minister spell out whether the clause, and potentially clause 97, will bite on that kind of capability? If not, where are they aimed?

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): An intelligence services example under clause 96 would be a case where the intelligence services wanted to identify a subject of

interest who might have travelled to Syria in a certain time window and where the initial selector was age, because there was reliable reporting that the person being sought was a certain age. The application of the age selector would produce a pool of results, and a decision may be taken to select that pool for further processing operations, including the application of other selectors. That processing would be the result of a decision taken solely on the basis of automated processing.

Liam Byrne: I do not think the clause actually says anything about age selection. How do we set boundaries around the clause? Let us say that minors—people under the age of 18—want to travel to Syria or some other war zone. Is the Minister basically saying that the clause will bite on that kind of information and lead to a decision chain that results in action to intervene? If that is the case, will she say a little more about the boundaries around the use of the clause?

Victoria Atkins: The right hon. Gentleman asked me for an example and I provided one. Age is not in the clause because the Government do not seek in any way to create burdens for the security services when they are trying to use data to protect this country. Given his considerable experience in the Home Office, he knows that it would be very peculiar, frankly, for age to be listed specifically in the clause. The clause is drafted as it is, and I remind him that it complies with Council of Europe convention 108, which is an international agreement.

Liam Byrne: The point is that the clause does create a burden. It does not detract from a burden; it creates an obligation on intelligence services to ensure that there is not automatic decision making. We seek not to add burdens, but to question why the Minister is creating them.

Victoria Atkins: The clause complies with Council of Europe convention 108. I do not know whether I can say any more.

The Chair: I think we have come to a natural conclusion.

Question put and agreed to.

Clause 96 accordingly ordered to stand part of the Bill.

Clause 97

RIGHT TO INTERVENE IN AUTOMATED DECISION-MAKING

Amendments made: 41, in clause 97, page 56, line 34, leave out "21 days" and insert "1 month".

Clause 97(4) provides that where a controller notifies a data subject under Clause 97(3) that the controller has taken a decision falling under Clause 97(1) (automated decisions required or authorised by law), the data subject has 21 days to request the controller to reconsider or take a new decision not based solely on automated processing. This amendment extends that period to one month.

Amendment 42, in clause 97, page 56, line 39, leave out "21 days" and insert "1 month".—*(Victoria Atkins.)*

Clause 97(5) provides that where a data subject makes a request to a controller under Clause 97(4) to reconsider or retake a decision based solely on automated processing, the controller has 21 days to respond. This amendment extends that period to one month.

Clause 97, as amended, ordered to stand part of the Bill.

Clause 98

RIGHT TO INFORMATION ABOUT DECISION-MAKING

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

Liam Byrne: This is a vexed and difficult area. The subject of the clause is the right to information about decision making, which is very difficult when it comes to the intelligence services, and I have had experiences, as have others I am sure, of constituents who come along to an advice bureau and claim to have been subject either to intelligence services investigation or, in some cases, to intelligence services trying to recruit them. Sometimes—this is not unknown—an individual's immigration status might be suspect. I had one of these cases about five or six years ago, where the allegation was that the intelligence services were conspiring with the UK Border Agency and what at that time was the Identity and Passport Service to withhold immigration documents to encourage the individual to become a source. The challenge for Members of Parliament trying to represent such individuals is that they will get a one-line response when they write to the relevant officials to say, "I am seeking to represent my constituent on this point."

A right to information about decision-making will be created under clause 98. I ask the Minister, therefore, when dealing with very sensitive information, how is this right going to be exercised and who is going to be the judge of whether that right has been fulfilled satisfactorily? There is no point approving legislation that is superfluous because it will have no effect in the real world. The clause creates what looks like a powerful new right for individuals to request information about decisions taken by the intelligence agencies, which might have a bearing on all sorts of things in their lives. Will the Minister explain how, in practice, this right is to become a reality?

Victoria Atkins: If I may give an example, where a terrorist suspect is arrested and believes he is the subject of MI5 surveillance, revealing to them whether they were under surveillance and the process by which the suspect was identified as a potential terrorist would clearly aid other terrorists in avoiding detection. The exercise of the right is subject to the operation of the national security exemption, which was debated at length last week. It might be that, in an individual case, the intelligence services need to operate the "neither confirm nor deny" principle, and that is why the clause is drafted as it is.

Liam Byrne: The clause is drafted in the opposite way. Subsection (1)(b) says that

"the data subject is entitled to obtain from the controller, on request, knowledge of the reasoning underlying the processing."

In other words, the data subject—in this case, the individual under surveillance—has the right to obtain from the controller, in the hon. Lady's example of the intelligence agencies, knowledge of the reasoning underlying the way their data was processed.

Let us take, for example, a situation where CCTV footage was being captured at an airport or a border crossing and that footage was being run through facial

[Liam Byrne]

recognition software, enabling special branch officers to intervene and intercept that individual before they crossed the border. That is an example of where information is captured and processed, and action then results in an individual, in this case, being prevented from coming into the country.

I have often had cases of constituents who have come back from Pakistan or who might have transitioned through the middle east, perhaps Dubai, and they have been stopped at Birmingham airport because special branch officers have said their name is on a watch list. Watch lists are imperfect—that is probably a fairly good description. They are not necessarily based on the most reliable and up-to-date information, but advances in technology allow a much broader and more wide-ranging kind of interception to take place at the border. If we are relying not on swiping someone's passport and getting a red flag on a watch list but on processing data coming in through CCTV and running it through facial recognition software, that is a powerful new tool in the hands of the intelligence agencies. Subsection (1)(b) will give one of my constituents the right to file a request with the data controller—presumably, the security services—and say, "Look, I think your records are wrong here. You have stopped me on the basis of facial recognition software at Birmingham airport; I want to know the reasoning behind the processing of the data."

If, as the Minister says, the response from the data controller is, "We can neither confirm nor deny what happened in this case," then, frankly, the clause is pretty nugatory. Will the Minister give an example of how the right is going to be made a reality? What are the scenarios in which a constituent might be able to exercise this right? I am not interested in the conventions and international agreements this happy clause tends to agree with, but I would like to hear a case study of how a constituent could exercise this right successfully.

Victoria Atkins: The right hon. Gentleman says he is not interested in conventions and so on, but I am afraid that is the legal framework within which Parliament and this country have to act. The clause confers—as do the other clauses in chapter 3—rights upon citizens, but those rights are subject, as they must be, to the national security exemption set out in chapter 6, clause 110.

I am slightly at a loss as to where the right hon. Gentleman wishes to go with this. I am not going to stand here and dream up scenarios that may apply. The rights and the national security exemption are set out in the Bill; that is the framework we are looking at, and that is the framework within which the security services must operate. Of course one has a duty to one's constituents, but that is balanced with a duty to one's country. This is precisely the section of the Bill that is about the balance between the rights of our citizens and the absolute necessity for our security services to protect us and act in our interests when they are required to do so.

Liam Byrne: I am not asking the Minister to dream up a scenario in Committee. All good Ministers understand every single dimension of a clause they are required to take through the House before they come anywhere near a Committee, because they are the Bill Minister.

We are not debating here whether the security services have sufficient power; we had that debate earlier. We are talking about a power and a right that are conferred on data subjects under subsection (1)(b). I am slightly concerned that the Minister, who is responsible for this Bill and this matter of policy, has not been able to give us a well-rehearsed scenario, which presumably she and her officials will have considered before the Bill came anywhere near to being drafted. How will this right actually be exercised by our constituents? It could be that the Committee decides, for example, that the rights we are conferring on the data subject are too sweeping. We might be concerned that there are insufficient safeguards in place for the intelligence agencies to do their jobs. This is a specific question about how data subjects, under the clause, are going to exercise their power in a way that allows the security services to do their job. That is not a complicated request; it is a basic question.

Victoria Atkins: As I say, the framework is set out in the Bill, and the exemption exists in the Bill itself. I have already given an example about a terror suspect. With respect, I am not going to enter into this debate about the right hon. Gentleman's constituent—what he or she might have requested, and so on. The framework is there; the right is there, balanced with the national security exemption. I am not sure there is much more I can add.

Liam Byrne: The Minister says she does not want to enter into a debate. I kindly remind her that she is in a debate. The debate is called—

Victoria Atkins: Mr Hanson, I did not say that.

The Chair: Order. Liam Byrne has the floor. If he wishes to give way, he may do so.

Victoria Atkins: On a point of order, Mr Hanson. I did not say that I do not want a debate. Will the right hon. Gentleman please use his language carefully, as I know he has long experience of doing? I said I was not sure how fruitful it would be to have examples, to and fro, about constituents. That is quite a different matter from a debate. I have debated with him; I have said the answer; it is for him—

9.45 am

The Chair: Order. We have a point of order—which, in due course, the good offices of *Hansard* will resolve—as to what was said by the right hon. Gentleman and how the Minister interpreted it. At the moment, we are dealing with clause 98 and Mr Liam Byrne has the floor. As he wishes, he can give way or continue.

Liam Byrne: I am grateful, Mr Hanson, for that complete clarity. This is the debate that we are having today: how will clause 98(1)(b) become a reality? It creates quite powerful rights for a data subject to seek information from the intelligence agencies. I gave an example from my constituency experience of how the exercise of this right could run into problems.

All I ask of the Minister responsible for the Bill and this area of policy, who has thought through the Bill with her officials and is asking the Committee to agree

the power she is seeking to confer on our constituents, and who will have to operate the policy in the real world after the Bill receives Royal Assent, is that she give us a scenario of how the rights she is conferring on a data subject will function in the real world.

However, Mr Hanson, I think we might have exhausted this debate. It is disappointing that the Minister has not been able to come up with a scenario. Perhaps she would like to intervene now to give me an example.

Victoria Atkins: Part 4 sets out a number of rights of data subjects, clause 98 being just one of them. This part of the Bill reflects the provisions of draft modernised convention 108, which is an international agreement, and the Bill faithfully gives effect to those provisions. A data subject wishing to exercise the right under clause 98 may write to that effect to the Security Service, which will then either respond in accordance with clause 98 or exercise the national security exemption in clause 110. That is the framework.

Liam Byrne: That is probably about as much reassurance as the Committee is going to get this afternoon. It is not especially satisfactory or illuminating, but we will not stand in the way and we will leave the debate there, Mr Hanson.

The Chair: This might seem like a long day, but it is still morning. On that note, we will proceed.

Question put and agreed to.

Clause 98 accordingly ordered to stand part of the Bill.

Clause 99

Right to object to processing

Amendments made: 43, in clause 99, page 57, line 28, leave out "day" and insert "time".

This amendment is consequential on Amendment 71.

44, in clause 99, page 58, line 3, leave out "day" and insert "time".

This amendment is consequential on Amendment 71.

45, in clause 99, page 58, line 5, leave out "the day on which" and insert "when".

This amendment is consequential on Amendment 71.

46, in clause 99, page 58, line 6, leave out "the day on which" and insert "when".—*(Victoria Atkins.)*

This amendment is consequential on Amendment 71.

Clause 99, as amended, ordered to stand part of the Bill.

Clauses 100 to 108 ordered to stand part of the Bill.

Clause 109

Transfers of personal data outside the United Kingdom

Liam Byrne: I beg to move amendment 159, in clause 109, page 61, line 13, after "is" insert "provided by law and is".

This amendment would place meaningful safeguards on the sharing of data by the intelligence agencies.

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

Amendment 160, in clause 109, page 61, line 18, at end insert—

'(3) The transfer falls within this subsection if the transfer—

(a) is based on an adequacy decision (see section 74),

(b) if not based on an adequacy decision, is based on there being appropriate safeguards (see section 75), or

(c) if not based on an adequacy decision or on there being appropriate safeguards, is based on special circumstances (see section 76 as amended by subsection (5)).

(4) A transfer falls within this subsection if—

(a) the intended recipient is a person based in a third country that has (in that country) functions comparable to those of the controller or an international organisation, and

(b) the transfer meets the following conditions—

(i) the transfer is strictly necessary in a specific case for the performance of a task of the transferring controller as provided by law or for the purposes set out in subsection (2),

(ii) the transferring controller has determined that there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer,

(iii) the transferring controller informs the intended recipient of the specific purpose or purposes for which the personal data may, so far as necessary, be processed, and

(iv) the transferring controller documents any transfer and informs the Commissioner about the transfer on request.

(5) The reference to law enforcement purposes in subsection (4) of section 76 is to be read as a reference to the purposes set out in subsection (2)."

New clause 14—*Subsequent transfers*—

'(1) Where personal data is transferred in accordance with section 109, the transferring controller must make it a condition of the transfer that the data is not to be further transferred to a third country or international organisation without the authorisation of the transferring controller.

(2) A transferring controller may give an authorisation under subsection (1) only where the further transfer is necessary for the purposes in subsection (2).

(3) In deciding whether to give the authorisation, the transferring controller must take into account (among any other relevant factors)—

(a) the seriousness of the circumstances leading to the request for authorisation,

(b) the purpose for which the personal data was originally transferred, and

(c) the standards for the protection of personal data that apply in the third country or international organisation to which the personal data would be transferred.'

This new clause would place meaningful safeguards on the sharing of data by the intelligence agencies.

Liam Byrne: I rise to speak to amendments 159 and 160, which relate to two significant developments in defence policy that have unfolded over the past couple of years. Our intelligence agencies have acquired pretty substantial new capabilities through all kinds of technological advances, which allow them remotely to collect and process data in a completely new way.

[Liam Byrne]

It is now possible, through satellite technology and drones, to collect video footage of battle zones and run the information collected through facial recognition software, which allows us to track much more forensically and accurately the movement, habits, working lives and leisure of bad people in bad places. We are fighting against organisations such as Daesh, in a coalition with allies, but over the past year one of our allies has rather changed the rules of engagement, which allows it to take drone strikes with a different kind of flexibility from that under the Obama regime.

The change in the American rules of engagement means that, on the one hand, the American Administration has dramatically increased the number of drone strikes—in Yemen, we have had an increase of about 288% in the past year—and, on the other, as we see in other theatres of conflict such as the war against al-Shabaab in Africa, repeated strikes are allowed for. Therefore, even when the circumstances around particular individuals have changed—new intelligence may have come to light about them—the Trump Administration have basically removed the safeguards that President Obama had in place that require an individual to be a "continuing and imminent threat" before a strike is authorised. That safeguard has been lifted, so the target pool that American forces can take aim at and engage is now much larger, and operational commanders have a great deal more flexibility over when they can strike.

We now see some of the consequences of that policy, with the most alarming statistics being on the number of civilians caught up in some of those strikes. That is true in Yemen and in the fight against al-Shabaab, and I suspect it is true in Syria, Afghanistan and, in some cases, Pakistan. We must ensure that the data sharing regime under which our intelligence agencies operate does not create a legal threat to them because of the way the rules of engagement of one of our allies have changed.

The Joint Committee on Human Rights has talked about that, and it has been the subject of debates elsewhere in Parliament. The JCHR concluded in its 2016 report that

"we owe it to all those involved in the chain of command for such uses of lethal force—intelligence personnel, armed services personnel, officials, Ministers and others—to provide them with absolute clarity about the circumstances in which they will have a defence against any possible future criminal prosecution, including those which might originate from outside the UK."

We need to reflect on some of those legal risks to individuals who are serving their country. The amendment would ensure that—where there was a collection, processing and transfer of information by the UK intelligence services to one of our allies, principally America, and they ran that information against what is widely reported as a kill list and ordered drone strikes without some of the safeguards operated by previous Administrations—first, the decision taken by the intelligence agency here to share that information was legal and, secondly, it would be undertaken in a way that ensured that our serving personnel were not subject to legal threats or concerns about legal threats.

Mike Wood (Dudley South) (Con): Does the right hon. Gentleman agree that the legal framework that we rightly expect to apply to our law enforcement offers and agencies does not necessarily apply directly to our intelligence and security services? That, however, would be the effect of the amendment.

Liam Byrne: I am not sure that that would be the effect of the amendment. While I agree with the thrust of the hon. Gentleman's argument, I am cognisant of the fact that in 2013 the Court of the Appeal said that it was "certainly not clear" that UK personnel would be immune from criminal liability for their involvement in a programme that entailed the transfer of information to America and a drone strike ordered using that information, without the same kinds of safeguard that the Obama Administration had. The amendment would ensure a measure—nothing stronger than that—of judicial oversight where such decisions were taken and where information was transferred. We must ensure a level of judicial oversight so that inappropriate decisions are not taken. It is sad that we need such a measure, but it reflects two significant changes over the past year or two: first, the dramatic increase in our ability to capture and process information, and, secondly, the crucial change in the rules of engagement under the Trump Administration.

Mike Wood: The right hon. Gentleman is being kind and generous with his time. He says that the amendments would not replicate the frameworks for law enforcement, yet amendment 160 would do exactly that by applying clauses 74, 75 and 76 to the test for data sharing for intelligence and security services. Those exact safeguards were designed for law enforcement, not for intelligence and security sharing.

Liam Byrne: The point for the Committee is that the thrust of the amendment is not unreasonable. Where there is a multiplication of the power of intelligence agencies to capture and process data, it is not unreasonable to ask for that greater power to bring with it greater scrutiny and safeguards. The case for this sensible and cautious amendment is sharpened because of the change in the rules of engagement operated by the United States. No member of the Committee wants a situation where information is transferred to an ally, and that ally takes a decision that dramatically affects the human rights of an individual—as in, it ends those rights by killing that person. That is not something that we necessarily want to facilitate.

As has been said, we are conscious of the difficulty and care with which our politicians have sometimes had to take such decisions. The former Prime Minister very sensibly came to the House to speak about his decision to authorise a drone strike to kill two British citizens whom he said were actively engaged in conspiring to commit mass murder in the United Kingdom. His judgment was that those individuals posed an imminent threat, but because they were not operating in a place where the rule of law was operational, there was no possibility to send in the cops, arrest them and bring them to trial.

The Prime Minister was therefore out of options, but the care that he took when taking that decision and the level of legal advice that he relied on were extremely high. I do not think any member of the Committee is confident that the care taken by David Cameron when he made that decision is replicated in President Trump's White House.

We must genuinely be concerned and cautious about our intelligence agencies transferring information that is then misused and results in drone strikes that kill individuals, without the safeguards we would expect. The last thing anyone would want is a blowback, in either an American or a British court, on serving officers in our military or intelligence services because the requisite safeguards simply were not in place.

My appeal to the Committee is that this is a point of principle: enhanced power should bring with it enhanced oversight and surveillance, and the priority for that is the fact that the rules of engagement for the United States have changed. If there is a wiser way in which we can create the kinds of safeguard included in the amendment we will be all ears, but we in the House of Commons cannot allow the situation to go unchecked. It is too dangerous and too risky, and it poses too fundamental a challenge to the human rights that this place was set up to champion and protect.

10 am

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I agree that these amendments ask a legitimate and important question about the level of safeguards on international data sharing by UK intelligence agencies. As it stands, clause 109 contains two fairly otiose sub-clauses to do with the sharing of personal data abroad by our intelligence agencies. In contrast, there is a whole chapter and a full seven clauses putting in place safeguards in relation to transfer to third countries by law enforcement agencies. These amendments borrow some of the safeguards placed on law enforcement agencies and there seems to be no good reason why that is not appropriate. I take the point that it does not necessarily follow that what is good for law enforcement agencies is definitely good for intelligence services. However, it is for the Government to tell us why those safeguards are not appropriate. If there are different ways for us to go about this, I am all ears, like the right hon. Gentleman. The right hon. Gentleman quite rightly raised the example of drones and US attacks based on information shared by personnel. At the moment, the lack of safeguards and of a very clear legal basis for the transfer of information can be lethal for billions and is dangerous for our personnel, as the Joint Committee on Human Rights has pointed out. We support the thrust of these amendments.

Darren Jones (Bristol North West) (Lab): I declare my interests as set out in the Register of Members' Interests.

The Chair: Order. The hon. Gentleman declared his interests in previous Committees, but I have been advised that he needs to specify what the interests are, as well as declaring them.

Darren Jones: Thank you, Mr Hanson. The two items on the register are, first, that I was a legal counsel at BT before my election as a Member of Parliament, where I was responsible for data protection law. Secondly, I had a relationship with a law firm called Kemp Little to maintain my practising certificate while I was a Member of Parliament.

My argument in support of amendment 160 is one that I have rehearsed in previous debates. In line with recommendations from the Joint Committee on Human Rights, today we benefit from an exemption under European treaties that say that national security is a member state competence and therefore not one with which the European Union can interfere. However, if the UK leaves the European Union, the European Commission reserves the right to review the entire data processing legislation, including that for intelligence services of a third country when seeking to make a decision on adequacy—as it has done with Canada. Where the amendment talks about adequacy, it would be helpful—

Victoria Atkins: Does the EU have an adequacy agreement with Canada?

Darren Jones: It does, but it has been reviewed by the European Commission. One of the concerns the Commission has had with Canada is its intelligence-sharing arrangements with the United States of America, which is why this amendment is so pertinent and why it is right to support the Government in seeking this adequacy decision. I make the point again that we will no longer benefit from the exemption if we leave the European Union and I hope that the Government keep that in mind.

Victoria Atkins: Before I start, I want to clarify what the hon. Gentleman has just said about adequacy decisions. Canada does have an adequacy decision from the EU for transfers to commercial organisations that are subject to the Canadian Personal Information Protection and Electronic Documents Act. I am not sure that security services are covered in that adequacy decision, but it may be that we will get assistance elsewhere.

As the right hon. Member for Birmingham, Hodge Hill is aware, amendments 159, 160 and new clause 14 were proposed by a campaigning organisation called Reprieve in its recent briefing on the Bill. They relate to concerns about the sharing of personal data with the US and seek to apply the data sharing protections designed specifically for law enforcement data processing, provided for in part 3 of the Bill, to processing by the intelligence services, provided for in part 4. That is, they are seeking to transpose all the law enforcement measures into the security services. However, such safeguards are clearly not designed for, and do not provide, an appropriate or proportionate basis for the unique nature of intelligence services processing, which we are clear is outside the scope of EU law.

Before I get into the detail of these amendments, it is important to put on record that the international transfer of personal data is vital to the intelligence services' ability to counter threats to national security. Provision of data to international partners bolsters their ability to counter threats to their security and that of the UK. In a globalised world, threats are not necessarily contained within one country, and the UK cannot work in isolation. As terrorists do not view national borders as a limit to their activities, the intelligence services must be in a position to operate across borders and share information quickly—for example, about the nature of the threat that an individual poses—to protect the UK.

In the vast majority of cases, intelligence sharing takes place with countries with which the intelligence services have long-standing and well-established relationships.

[Victoria Atkins]

In all cases, however, the intelligence services apply robust necessity and proportionality tests before sharing any information. The inherent risk of sharing information must be balanced against the risk to national security of not sharing such information.

Liam Byrne: Will the Minister tell us more about the oversight and scrutiny for the tests that she has just set out that the intelligence services operate? Perhaps she will come on to that.

Victoria Atkins: I am coming on to that.

Any cross-border sharing of personal data must be consistent with our international obligations and be subject to appropriate safeguards. On the first point, the provisions in clause 109 are entirely consistent with the requirements of the draft modernised Council of Europe data protection convention—convention 108—on which the preventions of part 4 are based. It is pending international agreement.

The provisions in the convention are designed to provide the necessary protection for personal data in the context of national security. The Bill already provides that the intelligence services can make transfers outside the UK only when necessary and proportionate for the limited purposes of the services' statutory functions, which include the protection of national security; for the purpose of preventing or detecting serious crime; or for the purpose of criminal proceedings.

In addition, on the point the right hon. Gentleman just raised, the intelligence services are already under statutory obligations in the Security Service Act 1989 and the Intelligence Services Act 1994 to ensure that no information is disclosed except so far as is necessary for those functions or purposes. All actions by the intelligence services, as with all other UK public authorities, must comply with international law.

Louise Haigh (Sheffield, Heeley) (Lab): Will the Minister give way?

Victoria Atkins: Yes, but I am coming on to further safeguards, if that is the point the hon. Lady wants to raise.

Louise Haigh: Under those pieces of legislation, are the intelligence services subject to the Information Commissioner, and will they be subject to the commissioner under the Bill's provisions?

Victoria Atkins: I am about to come on to the safeguards that govern the intelligence services' information acquisition and sharing under the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. They ensure that any such processing is undertaken only when necessary, lawful and proportionate, and that any disclosure is limited to the minimum number of individuals, in accordance with arrangements detailed in those Acts.

Those Acts, and the provisions in the relevant codes of practice made under them, also provide rigorous safeguards governing the transfer of data. Those enactments already afford proportionate protection and safeguards when data is being shared overseas. Sections 54, 130, 151 and 192 of the 2016 Act provide for safeguards relating to disclosure of material overseas.

Those provisions are subject to oversight by the investigatory powers commissioner, and may be challenged in the investigatory powers tribunal. They are very powerful safeguards, over and above the powers afforded to the Information Commissioner, precisely because of the unique nature of the material with which the security services must act.

Peter Heaton-Jones (North Devon) (Con): Is the point not that those who would seek to do us harm do not have the courtesy to recognise international borders, as recent events have shown? It is vital that our intelligence services can share information across those same borders.

Victoria Atkins: It is absolutely vital. What is more, not only is there a framework in the Bill for overseeing the work of the intelligence services, but we have the added safeguards of the other legislation that I set out. The burden on the security services and the thresholds they have to meet are very clear, and they are set out not just in the Bill but in other statutes.

I hope that I have provided reassurance that international transfers of personal data by the intelligence services are appropriately regulated both by the Bill, which, as I said, is entirely consistent with draft modernised convention 108 of the Council of Europe—that is important, because it is the international agreement that will potentially underpin the Bill and agreements with our partners and sets out agreed international standards in this area—and by other legislation, including the 2016 Act. We and the intelligence services are absolutely clear that to attempt to impose, through these amendments, a regime that was specifically not designed to apply to processing by the intelligence services would be disproportionate and may critically damage national security.

I am sure that it is not the intention of the right hon. Member for Birmingham, Hodge Hill to place unnecessary and burdensome obstacles in the way of the intelligence services in performing their crucial function of safeguarding national security, but, sadly, that is what his amendments would do. I therefore invite him to withdraw them.

Liam Byrne: I am grateful to the Minister for that explanation and for setting out with such clarity the regime of oversight and scrutiny that is currently in place. However, I have a couple of challenges.

I was slightly surprised that the Minister said nothing about the additional risks created by the change in rules of engagement by the United States. She rested some of her argument on the Security Services Act 1989 and the Intelligence Services Act 1994, which, as she said, require that any transfers of information are lawful and proportionate. That creates a complicated set of ambiguities for serving frontline intelligence officers, who have to make fine judgments and, in drafting codes of practice, often look at debates such as this one and at the law. However, the law is what we are debating. Where the Bill changed the law to create a degree of flexibility, it would create a new risk, and that risk would be heightened by the change in the rules of engagement by one of our allies.

The Minister may therefore want to reflect on a couple of points. First, what debate has there been about codes of practice? Have they changed given the increased surveillance capacity that we have because of the development of our capabilities? How have they changed in the light of the new rules of engagement issued by President Trump?

Peter Heaton-Jones: The right hon. Gentleman is being generous in giving way. I am listening carefully to what he says. I am concerned that he seems to be inviting us to make law in this country based almost solely on the policies of the current US Administration. I do not understand why we would do that.

Liam Byrne: The reason we would do that is that there has been an exponential increase in drone strikes by President Trump's Administration and, as a result, a significant increase in civilian deaths in Pakistan, Afghanistan, Syria and Iraq, Yemen and east Africa. It would be pretty odd for us not to ensure that a piece of legislation had appropriate safeguards, given what we now know about the ambition of one of our most important allies to create flexibility in rules of engagement.

Matt Warman (Boston and Skegness) (Con): I agree with the right hon. Gentleman on that point, but is not the more important point that our legislation cannot be contingent on that of any other country, however important an ally it is? Our legislation has to stand on its own two feet, and we should seek to ensure that it does. To change something, as he attempts to, purely on the basis of changes over the past couple of years would set a dangerous precedent rather than guard against a potential pitfall.

10.15 am

Liam Byrne: The hon. Gentleman makes a good point, and he is right to say that our legislation has to stand on its own two feet. It absolutely has to, and what is more, it has to be fit for the world in which we live today, which I am afraid has two significant changes afoot. One is a transformation in the power of our intelligence agencies to collect and process data, and in my view that significant advance is enough to require a change in the level of oversight, and potentially a judicial test for the way we share information. As it happens—I was careful to say this—the risk and necessity of that change is merely heightened by the fact that the rules of engagement with one of our most important allies have changed, and that has had real-world consequences. Those consequences create a heightened threat of legal challenge in foreign and indeed domestic courts to our serving personnel.

For some time, our defence philosophy has been—very wisely—that we cannot keep our country safe by defending from the goal line, and on occasion we have to intervene abroad. That is why in my view Prime Minister Cameron took the right decision to authorise lethal strikes against two British citizens. He was concerned first that there was an imminent threat, and secondly that there was no other means of stopping them. Those important tests and safeguards are not operated by our allies.

The change to the American rules of engagement, which allow a strike against someone who is no longer a "continuing and imminent threat", means that one of our allies now operates under completely different rules of engagement to those set out before the House of Commons by Prime Minister David Cameron, which I think met with some degree of approval. If we are to continue to operate safely a policy of not defending from the goal line, if we are to protect our ability to work with allies and—where necessary and in accordance with international law—to take action abroad, and if we are to continue the vital business of safely sharing information with our allies in the Five Eyes network, a degree of extra reassurance should be built into legislation to ensure that it is fit for the future.

Mr Alister Jack (Dumfries and Galloway) (Con): I am confused. Is the right hon. Gentleman suggesting that the actions by Americans, based on the data sharing, which we know is run with international safeguards, could have legal consequences for our personnel in the intelligence agencies serving here?

Liam Byrne: Yes, and it is not just me—the Court of Appeal is arguing that. The Court of Appeal's summary in 2013 was that there was a risky legal ambiguity. Its conclusion that it is certainly not clear that UK personnel are immune from criminal liability for their involvement in these programmes is a concern for us all. The Joint Committee on Human Rights reflected on that in 2016, and it concluded pretty much the same thing:

> "In our view, we owe it to all those involved in the chain of command for such uses of lethal force…to provide them with absolute clarity about the circumstances in which they will have a defence against any possible future criminal prosecution, including those which might originate from outside the UK."

This is not a theoretical legal threat to our armed forces and intelligence agencies; this is something that the Court of Appeal and the Joint Committee on Human Rights have expressed worries about.

The new powers and capabilities of our intelligence agencies arguably create the need for greater levels of oversight. This is a pressing need because of the operational policy of one of our allies. We owe it to our armed forces and intelligence agencies to ensure a regime in which they can take clear, unambiguous judgments where possible, and where they are, beyond doubt, safe from future legal challenge. It is not clear to me that the safeguards that the Minister has set out meet those tests.

Perhaps the Minister will clarify one outstanding matter, about convention 108, on which she rested much of her argument. Convention 108 is important. It was written in 1981. The Minister told the Committee that it had been modernised, but also said that that was in draft. I should be grateful for clarification of whether the United Kingdom has signed and is therefore bound by a modernised convention that is currently draft.

Victoria Atkins: I am happy to clarify that. Convention 108 is in the process of being modernised by international partners. I have made it clear, last week and this week, that the version in question is modernised, and is a draft version; but it is the one to which we are committed, not least because the Bill reflects its provisions. Convention 108 is an international agreement and sets the international standards, which is precisely why we are incorporating those standards into the Bill.

I know that the Leader of Her Majesty's Opposition appears to be stepping away from the international community, over the most recent matters to do with Russia, but the Bill and convention—*[Interruption.]*

[Victoria Atkins]

Well, he is. However, convention 108 is about stepping alongside our international partners, agreeing international standards and putting the thresholds into legislation. The right hon. Gentleman keeps talking about the need for legislation fit for the world we live in today; that is precisely what convention 108 is about.

The Chair: Order. The right hon. Member for Birmingham, Hodge Hill indicates that this is an intervention. I thought he had sat down and wanted the Minister to respond. However, if it is an intervention, it is far too long.

Liam Byrne: I am grateful. Some of us in this House have been making the argument about the risk from Russia for months, and the permissive environment that has allowed the threats to multiply is, I am afraid, the product of much of the inattention of the past seven years.

On the specific point about convention 108, I am glad that the Minister has been able to clarify the fact that it is not operational.

Victoria Atkins: On the language—

Liam Byrne: I will give way to the Minister in a moment. The convention was written in 1981. Many people in the Government have argued in the past that we should withdraw not only from the European Union but from the European convention on human rights and therefore also the Council of Europe.

Victoria Atkins: That is not Government policy.

Liam Byrne: I did not say it was Government policy. I said that there are people within the Administration, including the Secretary of State for Environment, Food and Rural Affairs, who have made the argument for a British Bill of Rights that would remove Britain from the European convention on human rights and, therefore, the Council of Europe. I very much hope that that ambiguity has been settled and that the policy of the current Government will remain that of the Conservative party from now until kingdom come; but the key point for the Committee is that convention 108 is in draft. The modernisation is in draft and is not yet signed. We have heard an express commitment from the Minister to the signing of the thing when it is finalised. We hope that she will remain in her position, to ensure that that will continue to be Government policy; but the modernised version that has been drafted is not yet a convention.

Darren Jones: Does my right hon. Friend recognise that the modernisation process started in 2009, with rapporteurs including one of our former colleagues, Lord Prescott? When a process has taken quite so many years and the document is still in draft, it raises the question of how modern the modernisation is.

Liam Byrne: Some members of the Committee—I am one of them—have been members of the Parliamentary Assembly of the Council of Europe for some time. We know how the Council of Europe works. It is not rapid: it likes to take its time deliberating on things. The Minister may correct me, but I do not think that there is a deadline for the finalisation of the draft convention. So, to ensure that the Government remain absolutely focused on the subject, we will put the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 8]

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 109 ordered to stand part of the Bill.

Clauses 110 to 112 ordered to stand part of the Bill.

Schedule 11

OTHER EXEMPTIONS UNDER PART 4

Amendments made: 118, in schedule 11, page 190, line 4, leave out

"day falls before the day on which"

and insert "time falls before".

This amendment is consequential on Amendment 71.

Amendment 119, in schedule 11, page 190, line 7, leave out "day" and insert "time".

This amendment is consequential on Amendment 71.

Amendment 120, in schedule 11, page 190, line 9, leave out "the date of".

This amendment is consequential on Amendment 71.

Amendment 121, in schedule 11, page 190, line 17, leave out "day" and insert "time".—*(Victoria Atkins.)*

This amendment is consequential on Amendment 71.

Schedule 11, as amended, agreed to.

Clause 113

POWER TO MAKE FURTHER EXEMPTIONS

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

Stuart C. McDonald: Clause 113 is one of the broad Henry VIII powers that we are consistently opposing and voting against and will continue to oppose and vote against. In chapter 6 of part 4 of the Bill are set out various exemptions that would disapply a number of aspects of data protection if that were required for national security. In schedule 11 are set out further exemptions, including for prevention and detection of crime, parliamentary privilege, legal professional privilege and so on. Huge swathes of data protection principles and subjects' rights disappear in those circumstances.

We have already had a number of good debates on whether we have struck the right balance between the rights of data subjects and the national interest, national security interests and so on. In our view, it rather undermines our role in scrutinising Government legislation and finding the right balance if we then hand over what is pretty much a carte blanche to change the balance that we have decided on, with the minimum of scrutiny, through broad Henry VIII powers. We therefore continue to oppose broad Henry VIII powers in the Bill and encourage hon. Members to support taking this clause out of the Bill.

Victoria Atkins: I thank the hon. Gentleman for raising this point. Clause 113 is analogous to clause 16, which we have already debated, and provides for the Secretary of State, by regulations subject to the affirmative procedure, to add further exemptions from the provisions of part 4 or to omit exemptions added by regulations. This clause reflects amendments made in the House of Lords in response to the Delegated Powers and Regulatory Reform Committee's concerns that the powers in the Bill as introduced, which provided for adding, varying or omitting further exemptions in relation to schedule 11, were inadequately justified and too widely drawn. However, maintaining the power to add further exemptions, or to omit exemptions that have been added, provides the flexibility required, if necessary, to extend exemptions in the light of changing public policy requirements.

10.30 am

Any regulations will be subject to the affirmative procedure, so they will have to be debated and approved by both Houses. I hope that gives the hon. Gentleman some comfort. In addition, clause 179 requires the Home Secretary to consult the Information Commissioner and other interested parties that they consider appropriate before bringing forward any regulations. Again, those are further procedural safeguards.

Question put and agreed to.

Clause 113 accordingly ordered to stand part of the Bill.

Clause 114 ordered to stand part of the Bill.

Schedule 12 agreed to.

Clauses 115 and 116 ordered to stand part of the Bill.

Schedule 13

OTHER GENERAL FUNCTIONS OF THE COMMISSIONER

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I beg to move amendment 122, in schedule 13, page 194, line 36, leave out from beginning to end of line 4 on page 195.

This amendment is consequential on the omission of Clause 121 (see Amendment 47).

The Chair: With this it will be convenient to discuss clause 121 stand part.

Margot James: Amendment 122 and clause 121 deal with measures inserted into the Bill with the intention of protecting and valuing certain personal data held by the state—an issue championed by Lord Mitchell, to whom I am grateful for taking the time to come to see me to further explain his amendments, and for giving me the opportunity to explain how we plan to address the issues he raised.

Lord Mitchell's amendments require the Information Commissioner to maintain a register of publicly controlled data of national significance and to prepare a code of practice that contains practical guidance in relation to personal data of national significance, which is defined as data that, in the Commissioner's opinion,

"has the potential to further…economic, social or environmental well-being"

and

"financial benefit…from processing the data or the development of associated software."

Lord Mitchell has made it clear that his primary concern relates to the sharing of health data by the NHS with third parties. He believes that some information sharing agreements have previously undervalued NHS patient data, and that the NHS, along with other public authorities, needs additional guidance on optimising the benefits derived from such sharing agreements.

We agree that the NHS is a prime state asset, and that its rich patient data records have great potential to further medical research. Its data could be used to train systems using artificial intelligence to diagnose patients' conditions, to manage risk, to target services and to take pre-emptive and preventive action—all developments with huge potential. I have discussed this matter with ministerial colleagues; not only do we want to see these technological developments, but we want the NHS, if it is to make any such deals, to make fair deals. The benefits of such arrangements are often not exclusively monetary.

NHS patient data is only ever used within the strict parameters of codes of practice and the standards set out by the National Data Guardian and other regulatory bodies. We of course recognise that we must continue in our efforts to make the best use of publicly held data, and work is already being carried out to ensure that the value of NHS patient data is being fully recognised. NHS England and the Department of Health and Social Care have committed to working with representatives of the public and of industry to explore how to maximise the benefits of health and care data for patients and taxpayers.

Lord Mitchell's provision in clause 121 proposes that the commissioner publish a code of practice. However, if there is a problem, a code would seem to be an unduly restrictive approach. Statutory codes are by necessity prescriptive, and this is an area where the public may benefit from a greater degree of flexibility than a code could provide in practice, especially to encourage innovation in how Government use data to the benefit of both patients and taxpayers.

The Government are releasing public data to become more transparent and to foster innovation. We have released more than 40,000 non-personal datasets. Making the data easily available means that it will be easier for people to make other uses of Government-collected data, including commercial exploitation or to better understand how government works and to hold the Government to account. The benefits of each data release are quite different, and sometimes they are unknown until later. Lord Mitchell's primary concern is

[Margot James]

health data, but can guidance on how that is used be equally applicable to the vast array of data we release? Such guidance would need to be so general that it would be useless.

Even if we stay focused on NHS data and what might help to ensure that the value of it is properly exploited, Lord Mitchell's proposal has some significant problems. First, by definition, data protection legislation deals with the protection of personal data, not general data policy. Companies who enter into data sharing agreements with the NHS are often purchasing access to anonymised patient data—that is to say, not personal data. Consequently, the code in clause 121 cannot bite. Secondly, maintaining a register of data of national significance is problematic. In addition to the obvious bureaucratic burden of identifying the data that would fall under the definition, generating a list of data controllers who hold data of national significance is likely to raise a number of security concerns. The NHS has been the victim of cyber-attacks, and we do not want to produce a road map to resist those who want to harm it.

Thirdly, we do not believe that the proposed role is a proper one for the Information Commissioner, and nor does she. It is not a question of legislative enforcement and, although she may offer valuable insight on the issues, such responsibilities do not comfortably fit with her role as regulator of data protection legislation. We have consulted the commissioner on the amendments and she agrees with our assessment. In her own terms, she considers herself not to be best placed to advise on value for money and securing financial benefits from the sharing of such personal data with third parties. Those matters are far removed from her core function of safeguarding information rights. She adds that others in Government or the wider public sector whose core function it is to drive value from national assets may be a more natural home for providing such best practice advice.

Ian Murray (Edinburgh South) (Lab): I have the great pleasure of representing a constituency with one of the best medical research facilities in the world. One of the greatest impediments for that facility is getting access to anonymised NHS data for its research. Is the Minister saying that her amendment, which would remove the Lords amendment, would make it easier or more difficult for third parties to access that anonymised data?

Margot James: I am ill-qualified to answer the hon. Gentleman's question. Hypothetically, it would probably make it more difficult, but that is not our purpose in objecting to clause 121, which we do not see as being consistent with the role of the Information Commissioner, for the reasons I set out. However, he raises an interesting question.

I agree with Lord Mitchell that the issues that surround data protection policy, particularly with regard to NHS patient data, deserve proper attention both by the Government and by the National Data Guardian for Health and Care, but we have not yet established that there is any evidence of a problem to which his provisions are the answer. We are not sitting on our laurels. As I have already said, NHS England and the Department of Health and Social Care are working to ensure that they understand the value of their data assets. Further work on the Government's digital charter will also explore this issue. When my right hon. friend the Prime Minister launched the digital charter on 25 January, she made it clear that we will set out principles on the use of personal data.

Amendment 122 removes Lord Mitchell's amendment from schedule 13. We do this because it is the wrong tool; however, we commit to doing everything we can to ensure that we further explore the issue and find the right tools if needed. *[Interruption.]* I have just received advice that the amendments will make no difference in relation to the hon. Gentleman's question, because anonymised data is not personal data.

I commend amendment 122 and give notice that the Government will oppose the motion that clause 121 stand part of the Bill.

Liam Byrne: I am grateful that the Minister made time to meet my former noble Friend Lord Mitchell. These are important amendments and it is worth setting out the background to why Lord Mitchell moved them and why we give such priority to them.

In 2009-10, we began to have a debate in government about the right approach to those agencies which happen to sit on an enormous amount of important data. The Government operate about 200 to 250 agencies, and some are blessed with data assets that are more valuable than those of others—for example, the Land Registry or Companies House sit on vast quantities of incredibly valuable transactional data, whereas other agencies, such as the Meteorological Office, the Hydrographic Office and Ordnance Survey, sit on sometimes quite static data which is of value. Some of the most successful American companies are based on Government data—for example, The Weather Channel is one of the most valuable and is based on data issued from, I think, the US meteorological survey. A number of Government agencies are sitting on very valuable pots of data.

The debate that we began to rehearse nearly 10 years ago was whether the right strategy was to create public-private partnerships around those agencies, or whether more value would be created for the UK economy by simply releasing that data into the public domain. I had the great pleasure of being Chief Secretary to the Treasury and the Minister for public service reform. While the strong advice inside the Treasury was that it was better to create public-private partnerships because that would release an equity yield up front, which could be used for debt reduction, it was also quite clear to officials in the Cabinet Office and those interested in public service reform more generally that the release of free data would be much more valuable. That is the side of the argument on which we came down.

After the White Paper, "Smarter Government", that I brought to the House, we began the release of very significant batches of data. We were guided by the arguments of Tim Berners-Lee and Professor Nigel Shadbolt, who were advising us at the time, that this was the right approach and it was very good to see the Government continue with that.

There are still huge data pots locked up in Government which could do with releasing, but the way in which we release them has to have an eye on the way we create value for taxpayers more generally. Beyond doubt, the

area of public policy and public operations where we have data that is of the most value is health. The way in which, in the United States, Apple and other companies have now moved into personal health technology in a substantial way betrays the reality that this is going to be a hugely valuable and important market in years to come. If we look at the US venture industry we can see significant investment now going into health technology companies.

10.45 am

Lord Mitchell's amendment is designed to steer the Government in a particular direction. He would be the first to accept that it is imperfect and that the Information Commissioner is not the perfect custodian of the task, but the question is: how do we make progress and why is this so important? It is important because the Government have made mistakes in the way they have thought about the value of intellectual property in some of the joint ventures they have created in the last seven years. Let us look, for example, at the Government's approach to Hinkley Point and the investment it sought from Chinese investors. Frankly, the Chinese cannot believe the structure of the deal because it is so generous to Chinese investors. A huge amount of investment is sought to modernise the nuclear industry in one of the most important economies in the world, and all the intellectual property flows back to the Chinese investors. If the deal were being set up in France or Germany, or indeed in China, it would be set up as a joint venture in which the intellectual property rights were invested in the joint venture, and the Government were therefore a party who would enjoy the upside of the use of that data in the future.

What Lord Mitchell is super-conscious of is that our NHS records stretch back to 1948, so the longitudinal health data we have in this country is pretty much without parallel anywhere in the world. Some regions, such as the NHS in the west midlands, operate an extremely extensive payer database of the use of medications in a super-diverse population. The dynamic and longitudinal data assets that we are sitting on in parts of the NHS are unbelievably valuable. In the arguments he rehearsed in the other place, Lord Mitchell made the point that the data the NHS is sitting on is like our North sea oil—in fact, it is probably more valuable than the North sea oil assets discovered in the early 1970s. He has told me that at least two sources have related to him that the annual value of those longitudinal data records is of the order of $50 billion. I cannot vouch for that figure or for the source, but I know Lord Mitchell has done his homework on this. He is seeking to ensure that something almost like a sovereign wealth fund is created for data assets in this country—in particular, a sovereign wealth fund created for NHS data assets.

We would like to avoid the kind of mistakes that were made in assembling the Hinkley Point joint venture. Lord Mitchell's amendment is quite simple: he seeks the creation of a register of significant data assets. The Minister says it is difficult to put that together, but life is a bit difficult sometimes. That is why we have highly paid Ministers and poorly paid officials, to work together to assemble the arguments and the data.

The precedent we have is back in, I think, 1998-99, when the last Labour Government put together what came to be called the Domesday book of Government assets. We are now looking for a similar kind of catalogue assembled for significant data assets. Rather unfashionably for a Labour MP, at that time I was an investment banker working for a small bank called Rothschild & Co. in London. I know that will ruin my pro-Corbyn credentials.

Margot James: They were never very impressive.

Liam Byrne: The Minister is very generous. From that vantage point in the City, I was able to watch the level of ingenuity, creativity and innovation that was unlocked simply by the Government telling the world, "Here are the assets that are in public hands." All sorts of ideas were floated for using those assets in a way that was better for taxpayers and public service delivery.

To the best of my knowledge, we do not have a similar data catalogue today. What Lord Mitchell is asking is for Ministers to do some work and create one. They can outsource that task to the Information Commissioner. Perhaps the Information Commissioner is not the best guardian of that particular task, but I am frustrated and slightly disappointed that the Minister has not set out a better approach to achieving the sensible and wise proposals that Lord Mitchell has offered the Government.

The reason why it is so important in the context of the NHS is that the NHS is obviously a complicated place. It is an economy the size of Argentina's. The last time I looked, if the NHS were a country, it would be the 13th biggest economy on earth. It is a pretty complicated place and there are many different decision makers. Indeed, there are so many decision makers now that it is impossible to get anything done within the NHS, as any constituency MP knows. So how do we ensure that, for example, in our neck of the woods, Queen Elizabeth Hospital Birmingham does not strike its own data sharing agreement with Google or DeepMind? How do we ensure that the NHS in Wales does not go in a particular direction? How do we ensure that the trust across the river does not go in a particular direction? We need to bring order to what is potentially an enormous missed opportunity over the years to come.

The starting point is for the Government, first, to ensure we have assembled a good catalogue of data assets. Secondly, they should take some decisions about whether the organisations responsible for those data assets are destined for some kind of public-private partnership, as they were debating in relation to Companies House and other agencies a couple of years ago, or whether—more wisely—we take the approach of creating a sovereign wealth fund to govern public data in this country, where we maximise the upside for taxpayers and the opportunities for good public service reform.

The example of Hinkley Point and the unfortunate example of the Google partnership with DeepMind, which ran into all kinds of problems, are not good precedents. In the absence of a better, more concrete, lower risk approach from the Government, we will have to defend Lord Mitchell's wise clause in order to encourage the Government to come back with a better solution than the one set out for us this morning.

Margot James: I enjoyed the right hon. Gentleman's speech, as it went beyond some of the detail we are debating here today, but I was disappointed with the

[Margot James]

conclusion. I did not rest my argument on it being just too difficult to organise such a database as proposed by Lord Mitchell; there are various reasons, chief among them being that we are here to debate personal data. A lot of the databases the right hon. Gentleman referred to as being of great potential value do not contain personal data. Some do, some do not: the Land Registry does not, Companies House does, and so forth. Also, the Information Commissioner has advised that this is beyond her competence and her remit and that she is not resourced to do the job. Even the job of defining what constitutes data of public value is a matter for another organisation and not the Information Commissioner's Office. That is my main argument, rather than it being too difficult.

Liam Byrne: Happily, what sits within the scope of a Bill is not a matter for Ministers to decide. First, we rely on the advice of parliamentary counsel, which, along with the Clerks, was clear that this amendment is well within the scope. Secondly, if the Information Commissioner is not the right individual to organise this task—heaven knows, she has her hands full this week—we would have been looking for a Government amendment proposing a better organisation, a better Ministry and a better Minister for the work.

Margot James: I can only be the Minister I am. I will try to improve. I was not saying that Lord Mitchell's amendment is not within the scope of the Bill; I was making the point that some of the databases and sources referred to by the right hon. Gentleman in his speech went into the realms of general rather than personal data. I therefore felt that was beyond the scope of the Information Commissioner's remit.

I share the right hon. Gentleman's appreciation of the value and the uniqueness of the NHS database. We do not see it just in terms of its monetary value; as the hon. Member for Edinburgh South made clear in his intervention, it has tremendous potential to improve the care and treatment of patients. That is the value we want to realise. I reassure the right hon. Gentleman and put it on record that it is not my place as a Minister in the Department for Digital, Culture, Media and Sport, or the place of the Bill, to safeguard the immensely valuable dataset that is the NHS's property.

Louise Haigh: Before the Minister concludes, given that she has focused so much on NHS data, can she update the Committee on the Government's progress on implementing Dame Fiona Caldicott's recommendations about health and social care data?

Margot James: I cannot give an immediate update on that, but I can say that Dame Fiona Caldicott's role as Data Guardian is crucial. She is working all the time to advise NHS England and the Secretary of State for Health and Social Care on how best to protect data and how it can deliver gains in the appropriate manner. I do not feel that that is the place of the Bill or that it is my role, but I want to reassure the Committee that the Secretary of State for Health and Social Care, to whom I am referring Lord Mitchell, is alive to those issues and concerns. The NHS dataset is a matter for the Department of Health and Social Care.

Amendment 122 agreed to.

Schedule 13, as amended, agreed to.

Clauses 117 and 118 ordered to stand part of the Bill.

Schedule 14 agreed to.

Clauses 119 and 120 ordered to stand part of the Bill.

Clause 121

CODE ON PERSONAL DATA OF NATIONAL SIGNIFICANCE

11 am

The Chair: We debated clause 121 with schedule 13. For those who are interested, the Minister proposed that the clause should not stand part of the Bill, but the question remains "That the clause stand part of the Bill." For the avoidance of confusion—I have only been here 26 years—those who, like the Minister, do not want the clause to stand part of the Bill should vote no.

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

The Committee divided: Ayes 9, Noes 10.

Division No. 9]

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 121 disagreed to.

Clauses 122 and 123 ordered to stand part of the Bill.

Clause 124

AGE-APPROPRIATE DESIGN CODE

Amendment made: 48, in clause 124, page 68, line 24, leave out "with the day on which" and insert "when"

This amendment is consequential on Amendment 71.—(Margot James.)

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

Liam Byrne: The debate rehearsed in the other place was whether we should acquiesce in a derogation that the Government have exercised to set the age of consent for personal data sharing at 13, as opposed to 16, which other countries have adopted. There was widespread concern that 13 was too young. Many members of the Committee will have experienced pressing the agree button when new terms and conditions are presented to us on our updates to software on phones, or privacy

settings presented to us by Facebook; privacy settings, it is now alleged, are not worth the paper that they were not written on.

Debates in the other place centred on what safeguards could be wrapped around children if that derogation were exercised and the age of consent left at 13. With Baroness Kidron, we were keen to enshrine in legislation a step towards putting into operation the objectives of the 5Rights movement. Those objectives, which Baroness Kidron has driven forward over the past few years, are important, but the rights therein are also important. They include not only rights that are enshrined in other parts of the Bill—the right to remove, for example—but important rights such as the right to know. That means that someone has the right to know whether they are being manipulated in some way, shape or form by social media technologies.

One of the most interesting aspects of the debate in the public domain in the past few months has been the revelation that many of the world's leading social media entrepreneurs do not allow their children to use social media apps, because they know exactly how risky, dangerous and manipulative they can be. We have also heard revelations from software engineers who used to work for social media companies about the way they deliberately set out to exploit brain chemistry to create features of their apps that fostered a degree of addiction. The right to know is therefore very powerful, as is the right to digital literacy, which is another important part of the 5Rights movement.

It would be useful to hear from the Minister of State, who—let me put this beyond doubt—is an excellent Minister, what steps she plans to take to ensure that the age-appropriate design code is set out pretty quickly. We do not want the clause to be passed but then find ourselves in a situation akin to the one we are in with section 40 of the Crime and Courts Act 2013 where, five years down the line, a misguided Secretary of State decides that the world has changed completely and that this bit of legislation should not be commenced.

We would like the Minister to provide a hard timetable—she may want to write to me if she cannot do so today—setting out when we will see an age-appropriate design code. We would also like to hear what steps she will take to consult widely on the code, what work she will do with her colleagues in the Department for Education to ensure that the code includes some kind of ventilation and education in schools so that children actually know what their rights are and know about the aspects of the code that are relevant to them, and, crucially, what steps she plans to take to include children in her consultation when she draws up the code.

This is an important step forward, and we were happy to support it in the other place. We think the Government should be a little more ambitious, which is why we suggest that the rights set out by the 5Rights movement should become part of a much broader and more ambitious digital Bill of Rights for the 21st century, but a start is a start. We are pleased that the Government accepted our amendment, and we would all be grateful if the Minister told us a little more about how she plans to operationalise it.

Margot James: I thank the right hon. Gentleman for his generous remarks. To recap, the idea that everyone should be empowered to take control of their data is at the heart of the Bill. That is especially important for groups such as children, who are likely to be less aware of the risks and consequences associated with data processing. Baroness Kidron raised the profile of this issue in the other place and won a great deal of support from peers on both sides of that House, and the Government then decided to introduce a new clause on age-appropriate design to strengthen children's online rights and protections.

Clause 124 will require the Information Commissioner to develop a new statutory code that contains guidance on standards of age-appropriate design for online services that are likely to be accessed by children. The Secretary of State will work in close consultation with the commissioner to ensure that that code is robust, practical and meets children's needs in relation to the gathering, sharing and storing of their data. The new code will ensure that websites and apps are designed to make clear what personal data of children is collected, how it is used and how both children and parents can stay in control of it. It will also include requirements for websites and app makers on privacy for children under 18.

The right hon. Gentleman cited examples of the consultation he hopes to see in preparation for the code. In developing the code, we expect the Information Commissioner to consult a wide range of stakeholders, including children, parents, persons who represent the interests of children, child development experts and trade associations. The right hon. Gentleman mentioned the Department for Education, and I see no reason why it should not be included in that group of likely consultees.

The commissioner must also pay close attention to the fact that children have different needs at different ages, as well as to the United Kingdom's obligations under the United Nations Convention on the Rights of the Child. The code interlocks with the existing data protection enforcement mechanism found in the Bill and the GDPR. The Information Commissioner considers many factors in every regulatory decision, and non-compliance with that code will weigh particularly heavily on any organisation that is non-compliant with the GDPR. Organisations that wish to minimise their risk will apply the code. The Government believe that clause 124 is an important and positive addition to the Bill.

Liam Byrne: Will the Minister say a word about the timetable? When can we expect the consultation and code of practice to be put into operation?

Margot James: There should be no delay to the development of the code and the consultation that precedes it. If I get any additional detail on the timetable, I will write to the right hon. Gentleman.

Question put and agreed to.

Clause 124, as amended, ordered to stand part of the Bill.

Clause 125

APPROVAL OF DATA-SHARING, DIRECT MARKETING AND AGE-APPROPRIATE DESIGN CODES

Amendment made: 49, in clause 125, page 69, line 9, leave out "with the day on which" and insert "when" *—(Margot James.)*

This amendment is consequential on Amendment 71.

Clause 125, as amended, order to stand part of the Bill.

Clauses 126 to 130 ordered to stand part of the Bill.

Clause 131

DISCLOSURE OF INFORMATION TO THE COMMISSIONER

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

Liam Byrne: Clause 131 deals with disclosure of information to the Information Commissioner, and this is probably a good point at which to ask whether the Information Commissioner has the right level of power to access information that is pertinent to her investigations into the misuse of information. Thanks to *The Guardian*, *The New York Times*, and particularly the journalist Carole Cadwalladr, we have had the most extraordinary revelations about alleged misbehaviour at Cambridge Analytica over the past couple of years. Indeed, Channel 4 News gave us further insight into its alleged misdemeanours last night.

We have a situation in social media land that the Secretary of State has described as the "wild west". Some have unfairly called the Matt Hancock app one of the features of that wild west, but I would not go that far, despite its slightly unusual privacy settings. None the less, there is now cross-party consensus that the regulatory environment that has grown up since the 2000 e-commerce directive is no longer fit for purpose. Yesterday, the Secretary of State helpfully confirmed that that directive will be modernised, and we will come on to discuss new clauses that suggest setting a deadline for that.

One deficiency of today's regulatory environment is the inadequate power that the Information Commissioner currently has to access information that is important for her investigations. We have a wild west, we have hired a sheriff, but we have not given the sheriff the power to do her job of keeping the wild west in order. We now have the ridiculous situation that the Information Commissioner must declare that she is going to court to get a warrant to investigate the servers of Cambridge Analytica, and to see whether any offence has been committed.

11.15 am

The offence is potentially incredibly serious. We are talking about data collected through an app called "My Digital World" that ran on Facebook and allowed the individuals in question to collect data on around 50 million people. Certainly, 50 million data records were assembled for a particular purpose. The allegation is that the data was then repurposed by Cambridge Analytica and put in the service of winning election campaigns, including the election of the President of the United States. This is not immaterial, and it is not a trivial offence or a public policy question. We should not glide over it, shrug our shoulders and say, "Well that is just part and parcel of the new world we live in." This is something we should take incredibly seriously. The way in which Facebook has, quite frankly, stonewalled investigations by this House through the excellent Department for Digital, Culture, Media and Sport Select Committee is all the more concerning. Essentially, Facebook told Members of this House that they were unable to check on allegations because they did not know what records to go and check. A company that makes a profit of $4 billion every single quarter has said to the House that it was unable to find the resources to investigate the kind of misdemeanours that have now been laid at their door and that of Cambridge Analytica.

I am concerned that the way our regulators operate together is simply inadequate. Many of the allegations about misuse of data during election campaigns and referendums will touch on whether the data was collected, repurposed illegally and then used to target so-called dark social ads in an inappropriate way, but there is also sometimes a need to explore where the money came from to buy those ads. Where money has, potentially, been laundered onshore there is a requirement for the Financial Conduct Authority to investigate. Sometimes it will require further investigations in, for example, Financial Conduct Authority countries such as Gibraltar. At the moment, there is no information sharing gateway between the Financial Conduct Authority, the Electoral Commission and the Information Commissioner. It is actually impossible for any regulator to create a single picture of what on earth has gone on. That challenge gets even harder when the Information Commissioner does not have the power to get the information she needs to do her job.

Darren Jones: Does my hon. Friend agree that this is also a question of access to the judiciary? Last night, the Information Commissioner had to wait until this morning to get a warrant because no judges or emergency judges were available. At the same time, we assume that Facebook was able to exercise its contractual right to enter the offices of Cambridge Analytica. Emergency judges are available for terrorism or deportation cases. Should there not be access to emergency judges in cases of data misuse for quick regulatory enforcement too?

Liam Byrne: If I wanted to hide something from a newspaper and I thought that the newspaper was going to print it inappropriately, I would apply for an emergency injunction to stop the newspaper running it. I do not understand why the Information Commissioner has had to broadcast her intentions to the world, because that has given Cambridge Analytica a crucial period of time in which to do anything it likes, frankly, to its data records. The quality of the Information Commissioner's investigation must be seriously impaired by the time that it has taken to get what is tantamount to a digital search warrant.

Is the Minister satisfied in her own mind that clause 131 and its associated clauses are powerful enough? Will she say more about the Secretary of State's declaration to the House last night that he would be introducing amendments to strengthen the Commissioner's power in the way that she requested? When are we going to see those amendments? Are we going to see them before this Committee rises, or at Report stage? Will there be a consultation on them? Is the Information Commissioner going to share her arguments for these extra powers with us and with the Secretary of State? We want to see a strong sheriff patrolling this wild west, and right now we do not know what the Government's plan of action looks like.

Margot James: I just want to recap on what clause 131 is about. It is intended to make it clear that a person is not precluded by any other legislation from disclosing to the commissioner information that she needs in relation to her functions, under the Bill and other legislation. The only exception relates to disclosures prohibited by the Investigatory Powers Act 2016 on grounds of national security. It is therefore a permissive provision enabling people to disclose information to the commissioner.

However, the right hon. Member for Birmingham, Hodge Hill has taken the opportunity to question the powers that the Information Commissioner has at her disposal. As my right hon. Friend the Secretary of State said yesterday in the Chamber, we are not complacent. I want to correct something that the right hon. Member for Birmingham, Hodge Hill said. My right hon. Friend did not say that he would table amendments to the Bill on the matter in question. He did say that we were considering the position in relation to the powers of the Information Commissioner, and that we might table amendments, but we are in the process of considering things at the moment. I presume that that goes for the right hon. Gentleman as well; if not, he would surely have tabled his own amendments by now, but he has not.

Liam Byrne: The Minister will notice that I have tabled a number of new clauses that would, for example, bring election law into the 21st century. I think that the Secretary of State left the House with the impression yesterday that amendments to strengthen the power of the Information Commissioner would be pretty prompt. It is hard to see another legislative opportunity to put that ambition into effect, so perhaps the Minister will tell us whether we can expect amendments soon.

Margot James: I can certainly reassure the right hon. Gentleman that we are looking at the matter seriously and, although I cannot commit to tabling amendments, I do not necessarily rule them out. I have to leave it at that for now.

On a more positive note, we should at least acknowledge that, although the Bill strengthens the powers of the Information Commissioner, her powers are already the gold standard internationally. Indeed, we must bear it in mind that the data privacy laws of this country are enabling American citizens to take Cambridge Analytica to court over data breaches.

I want to review some of the powers that the Bill gives the commissioner, but before I do so I will answer a point made by the right hon. Member for Birmingham, Hodge Hill. He said that the commissioner had had difficulties and had had to resort to warrants to pursue her investigation into a political party in the UK and both the leave campaigns in the referendum. She is doing all that under existing data protection law, which the Bill is strengthening. That is encouraging.

Liam Byrne: I did not want to intervene, but I have been struggling with the matter myself. There are allegations that a significant donor to Leave.EU was supported in that financial contribution by organisations abroad. As I spoke to the Financial Conduct Authority and tabled questions to the Treasury, it was revealed that there were no data sharing gateways between the Electoral Commission and the FCA.

Margot James: I shall come back to the right hon. Gentleman on the relationship between the Information Commissioner and the FCA. I am sure that the information that he has already ascertained from the Treasury is correct, but there may be other ways in which the two organisations can co-operate, if required. The allegations are very serious and the Government are obviously very supportive of the Information Commissioner as she grapples with the current investigation, which has involved 18 information notices and looks as if it will be backed up by warrants as well. I remind the Committee that that is happening under existing data protection law, which the Bill will strengthen.

Question put and agreed to.

Clause 131 accordingly ordered to stand part of the Bill.

11.25 am

The Chair adjourned the Committee without Question put (Standing Order No. 88).

Adjourned till this day at Two o'clock.