PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL [*LORDS*]

Third Sitting

Thursday 15 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

Monday 19 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

Thursday 15 March 2018

(Morning)

[Mr Gary Streeter *in the Chair*]

Data Protection Bill [*Lords*]

Schedule 6

The applied GDPR and the applied Chapter 2

11.30 am

Darren Jones (Bristol North West) (Lab): I beg to move amendment 152, in schedule 6, page 179, line 17, leave out paragraph 2 (as inserted by paragraph 49) and insert—

"2 The Commissioner must, in carrying out the Commissioner's functions under this Regulation, incorporate with any modifications which he or she considers necessary in any guidance or code of practice which the Commissioner issues, decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board established under Article 68 of the GDPR.

2A The Commissioner must, in carrying out the Commissioner's functions under this Regulation, have regard to any implementing acts adopted by the Commission under Article 67 of the GDPR (exchange of information)."

It is a pleasure to serve under your chairmanship, Mr Streeter. I declare my interests as set out in the Register of Members' Financial Interests.

Amendment 152, like the amendments we tabled on Tuesday, would assist the Government in securing a finding of adequacy from the European Commission so that, if the UK leaves the European Union, we can continue to exchange data with it. As the Committee knows, I like to refer to my version of the general data protection regulation as much as to the Bill, even though it is not the subject of our debate today.

I welcome the Government's commitments on the Floor of the House to seeking something "akin to" adequacy, then adequacy, and then something "beyond adequacy". I thank the Minister , the hon. Member for Stourbridge, for her response to my question on Second Reading about wanting "beyond adequacy" to represent a useful position for our Information Commissioner on the European data protection board. Some of us have concerns about that because of the practicalities of what happens with third countries. Indeed, I asked the Information Commissioner herself about it at an evidence session of the Select Committee on Science and Technology, and she confirmed that third countries traditionally have little influence on the article 29 working party—the predecessor of the EDPB—even if they have a seat at the table.

I think our shared view is that in seeking "beyond adequacy", we want not only to have a seat at the table as a potential third country but to have influence. In order to have that influence, we need to go slightly above and beyond what other third countries do and show close co-operation between the UK and the European Union.

Article 45 of the GDPR sets out guidelines on how the European Commission will assess and agree decisions on adequacy. It has to be happy that our legal framework is in line with its own. Of course, there will be an initial conversation as part of trade negotiations with the European Union. Under paragraph 3, the Commission is then to undertake

"a periodic review, at least every four years"

to ensure that we continue to be compliant. Paragraph 4 refers to ongoing monitoring of developments in third countries in their application of data protection laws and privacy rights.

As I have said on Second Reading and in previous debates on data protection laws, my concern is that we should lockstep the developments in our legislation, guidance and codes of conduct to show that they are still in line with the leading European Union legislative framework for data protection, so that we can continue to flow important amounts of data. Some 70% of our data flow is with the EU, and the UK accounts for a huge proportion—around 11%—of global data flow. We must maintain that. Under article 50 of the GDPR, in deciding on adequacy, the European Commission must seek

"mechanisms to facilitate the effective enforcement of legislation".

This is our opportunity to show the European Union that we are committed to data protection principles. Amendment 152 would tweak the wording of paragraph 2 of article 61 of the applied GDPR. I was pleased to see that paragraph; in earlier debates I raised some concerns that—for political reasons that I will not go into today—the Bill might not go as far as admitting that we need to track and implement EU law in the area. However, I want to strengthen the paragraph 2 wording, which says that our Information Commissioner must

"have regard to"

various things that happen at European Union level, including

"decisions, advice, guidelines, recommendations and best practices issued by the European Data Protection Board".

The amendment seeks to strengthen that slightly, while recognising that the Government, and probably also the Information Commissioner, would like a little flexibility.

Liam Byrne (Birmingham, Hodge Hill) (Lab): This is a wise and carefully crafted amendment. Does my hon. Friend agree that it is especially needed because the Government have rather unwisely decided not to incorporate article 8 into British law, which means there is a risk of courts in Europe and Britain interpreting data protection regimes differently, leading to divergence in future?

Darren Jones: I agree. I am attempting not to get too much into the party politics in a bid to seek the Government's agreement to the amendment, but there is an important distinction to be made. We have a layering of risks in seeking to achieve adequacy. On Tuesday we debated at length the Government's decision to repeal fundamental rights of the European charter, which we know from European guidelines is something they look to. We will come to issues of national security today, which is also an issue for third countries, as we have seen with Canada.

This small amendment would help mitigate some of that risk by making it clear to our friends in the European Union that we in Britain are proud about the influence we had in drafting the general data protection regulation, which is a world-leading set of laws and rules for the

future of our digital economy, and we continue to want to play a part in that, to help lead the conversation in the world and at European Union level. In co-operation with our friends in Europe, we seek to maintain that. While the Government may wish for divergence in other areas, I take the view that they do not in this area because we have been at the forefront of developments.

The amendment seeks only to tweak what is already in the Bill. As Members will see, it says that we would

"incorporate, with any modifications which he or she"—

that is the Information Commissioner—

"considers necessary in any guidance or code of practice… decisions…issued by the European Data Protection Board".

There is a nuanced difference; the Bill as drafted speaks of having "regard to", while the amendment speaks of incorporating, with any modifications that the Information Commissioner feels fit. It may seem like I am getting stuck in semantics—I do quite like to do that—but the amendment would deliver an important tone to the European Commission. On passing the Bill, we would be saying that when we are negotiating on data, where we have a shared interest at European and UK level, we want to get it right, and we will have gone beyond the basics of adequacy of other third countries because of our close relationship. We will hopefully have a seat on the European data protection board, where we seek to have influence, and we will take that responsibility seriously and, therefore, we will incorporate decisions of the board into the guidance of UK laws to lockstep our development in the area. As I said, it is made clear in the general data protection regulation that that is to be monitored on a continuous basis and more formally on a periodic basis.

I would not want us to lose adequacy in the future by diverging from European Union law. I want us to have an influential position on the European data protection board, which means being involved in the detail and taking the obligation of carrying that through on our side of the fence. The amendment seeks to bring that tone of co-operation and would help us and the Government in seeking adequacy so that we can secure these important data flows into the future.

Liam Byrne: It is a privilege to serve under your chairmanship, Mr Streeter. I rise to support my hon. Friend on his excellent, very helpful amendment. Earlier in the week we had a debate about the wisdom of incorporating article 8 into the Bill. I want to underline that we now have two different foundations for privacy that will operate post-Brexit in Europe and in the UK. The law is not fixed in aspect; it is a dynamic body of thought and ideas, and in the years to come there is a risk that courts in Europe and in the UK will diverge in how they interpret those fundamental principles.

That risk is all the more profound in this area of public policy because technology is moving so quickly. Therefore, if the Government wanted to do away with the risk to any future adequacy agreements, they would look for any and every opportunity to create bridges between the EU data protection regime and the British regime. The more bridges that are put in place, and the more girders that yoke us together in this field of public policy, the better.

Companies will consider whether regulatory harmonisation in data protection will continue when they make investment decisions in the technology space in the UK. I am afraid that that is now a fact of economic life. The simpler and faster the Government can help companies take those decisions, by putting beyond dispute and doubt any future adequacy agreement, the better. It is in our common interest to try to create stronger links than the Bill offers. I hope that the Government will accept the amendment.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): It is a pleasure to serve under your chairmanship, Mr Streeter. I thank the hon. Member for Bristol North West, who has great knowledge of these issues and has put his thoughts on his amendment very well to the Committee. As the Prime Minister said in her Mansion House speech, the ability to transfer data across international borders is crucial to a well-functioning economy, and that will remain the case after we leave the European Union. We are committed to ensuring that uninterrupted data flows between the UK and the EU continue. One way we can help to ensure that we have the foundations for that relationship is to continue to apply our exceptionally high standards for the protection of personal data.

Amendment 152 relates to the applied GDPR, which exists to extend GDPR standards to personal data processed for purposes outside the scope of EU law that may be otherwise left unregulated. The amendment is to schedule 6 of the Bill, which creates the applied GDPR by modifying the text of the GDPR so that it makes sense for matters outside the scope of EU law. The extension of GDPR standards is vital, because having a complete data protection regulatory framework will provide the UK with a strong foundation from which to protect people's personal data and secure the future free flow of data with the EU and the rest of the world. Applying consistent standards ensures that those bodies—mostly public authorities—who process personal data, both in and out of the scope of EU law, experience no discernible operational difference when doing so.

However, the applied GDPR, although very close, is not identical to the GDPR known as the real GDPR. The differences are primarily the inevitable result of extending text designed for the EU to matters over which the UK and other member states retain competence. Reference to member states becomes a reference to our country; reference to the supervisory authorities becomes a reference to the Information Commissioner, and so on. Similarly, the applied GDPR, as a purely domestic piece of regulation, is outside the scope of the functions of the European data protection board and the EU Commission.

Decisions and guidance issued by the European Data Protection Board will have an important bearing on the GDPR as implemented in the UK. To ensure that the interpretation of the applied element of the GDPR remains consistent with the interpretation of the real GDPR, it is right that the Information Commissioner should have regard to decisions and guidance issued by the European Data Protection Board in carrying out her functions, as the UK regulator and enforcer of the applied GDPR. However, the amendment goes further, by requiring her to incorporate them into her guidance and codes of practice. The effect of that is to extend the ambit of the European data protection board so that, uniquely among member states, it would have within its purview processing outside the scope of EU law, when that processing was undertaken in the UK.

[Margot James]

We do not agree that such an extension is required for the UK to achieve the relationship that we are seeking. By contrast, the current requirement in paragraph 49 of the schedule, for the commissioner to have regard to decisions and guidance issued by the European Data Protection Board in carrying out her functions means that she can and, in some cases, should incorporate into her guidance what she recognises as relevant and necessary. We are confident that that, founded on the commissioner's discretion, remains the best approach. On that basis, I hope that the hon. Member for Bristol North West feels able to withdraw his amendment.

11.45 am

Daniel Zeichner (Cambridge) (Lab): It is a pleasure to serve under your chairmanship, Mr Streeter. I listened closely to the Minister—I am struggling with the real and the applied GDPRs, as I am sure we all are—and the sense I get is that that will lead to potential divergence, which could have further consequences. We have reached an important point in the discussion. If we have divergence a few years down the line, does that not put adequacy at risk?

Margot James: I reassure the hon. Gentleman that divergence, if it occurs, will apply only to the applied GDPR, which is outside the scope of EU law, and therefore may well apply in a similar sense to member states as well as to us, when we become a third country.

Darren Jones: I thank the Minister for her useful reply. She is right, of course, that the applied GDPR is different from the real GDPR. As I said, I am seeking to establish a beyond-adequacy outcome, which is the Government's intention, according to their comments on Second Reading.

From other third countries, we know that adequacy decisions look at areas of non-EU competence—we will get into the detail of that later in the context of national security and the ongoing conversations with Canada; we already had a conversation on Tuesday about fundamental rights. Under the regulation, the European Commission has the power to look at the whole legislative environment in a third country, even where it is not an area of EU competence. That is an important point to be clear on.

The relationship may be unique compared with other third countries, but we are in a unique position as we leave the European Union. If we want to have strong, sustainable, ongoing adequacy, it is important that we take steps to establish that.

Liam Byrne: The Minister seemed to rest her argument on the need to preserve the Information Commissioner's discretion, which implies that she is trying to protect the commissioner's ability to go her own way. That will not help us to secure, lock down or nail to the floor an adequacy agreement in years to come. It will put an adequacy agreement at risk.

Darren Jones: My right hon. Friend is exactly right. Of course, the Information Commissioner is an excellent commissioner. We are privileged to have Elizabeth in the role here in the UK, not least with her experience, as a Canadian, of being in a third country. That is why I put some flexibility into my amendment—to recognise that situations may arise about which we cannot hypothesise today in which the commissioner will need some flexibility. Under my amendment, she has the power to add modifications that she considers necessary. The Government's concerns about the lack of flexibility are not reflected in the drafting of my amendment, as I have tried to deal with that.

The idea that the amendment increases the European data protection board's power is incorrect, because this is UK law, not European Union law. The amendment merely says that we will go only slightly further, with flexibility, by recognising that in the decisions that we want to be a part of—that is a really important point here—and to influence, we will take the obligations as well as the responsibilities, should we be invited to.

Daniel Zeichner: Could the Bill not also put the Information Commissioner in an extraordinarily difficult position? Decisions that she may make in the future could have huge political consequences. I would be surprised if she wanted to take that on.

Darren Jones: I agree with my hon. Friend. The reality may be that under the wording in the Bill, the Information Commissioner has no choice but to apply and incorporate the European data protection board's decisions if it is to keep up and maintain adequacy.

That is why the amendment is not something to worry about. It seeks to do what will probably happen in practice, but it puts our commitment to that relationship in the Bill. When we say to Europe that, uniquely, unlike any other third country and despite not being a member of the European Union, we want to have a position of influence on the EDPB, we can also say that we recognise that no one else has that level of influence, but in seeking to have it, we have made commitments to that future relationship in UK legislation.

I do not think any other Members here are members of the European Scrutiny Committee, but I spent the whole of yesterday afternoon losing votes on amendments to a report, and I rather enjoyed myself, so I will press this amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 8, Noes 10.

Division No. 6]

AYES

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

NOES

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

Question accordingly negatived.

Margot James: I beg to move amendment 115, in schedule 6, page 180, line 2, leave out sub-paragraph (b) and insert—

"(b) in paragraph 2, for 'Member States' substitute 'The Secretary of State';

(c) after that paragraph insert—

'3 The power under paragraph 2 may only be exercised by making regulations under section (Duty to review provision for representation of data subjects) of the 2018 Act.'"

This amendment is consequential on NC2.

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

Government amendments 63 to 68.

Amendment 154, in clause 183, page 106, line 24, at end insert—

"(4A) In accordance with Article 80(2) of the GDPR, a person who satisfies the conditions in Article 80(1) and who considers that the rights of a data subject under the GDPR have been infringed as a result of data processing, may bring proceedings, on behalf of the data subject and independently of the data subject's mandate—

(a) pursuant to Article 77 (right to lodge a complaint with a supervisory authority),

(b) to exercise the rights referred to in Article 78 (right to an effective judicial remedy against a supervisory authority),

(c) to exercise the rights referred to in Article 79 (right to an effective judicial remedy against a controller or processor).

(4B) An individual who considers that rights under the GDPR, this Act or any other enactment relating to data protection have been infringed in respect of a class of individuals of which he or she forms part may bring proceedings in respect of the infringement as a representative of the class (independently of the mandate of other members of the class), and—

(a) for the purposes of this subsection 'proceedings' includes proceedings for damages, and any damages recovered are to be distributed or otherwise applied as directed by the court,

(b) in the case of a class consisting of or including children under the age of 18, an individual may bring proceedings as a representative of the class whether or not the individual's own rights have been infringed,

(c) the court in which proceedings are brought may direct that the individual may not act as a representative, or may act as a representative only to a specified extent, for a specified purpose or subject to specified conditions,

(d) a direction under paragraph (c) may (subject to any provision of rules of court relating to proceedings under this subsection) be made on the application of a party or a member of the class, or of the court's own motion, and

(e) subject to any direction of the court, a judgment or order given in proceedings in which a party is acting as a representative under this subsection is binding on all individuals represented in the proceedings, but may only be enforced by or against a person who is not a party to the proceedings with the permission of the court.

(4C) Subsections (4A) and (4B)—

(a) apply in respect of infringements occurring (or alleged to have occurred) whether before or after the commencement of this section,

(b) apply to proceedings begun before the commencement of this section as if references in subsections (4A) and (4B) to bringing proceedings included a reference to continuing proceedings, and

(c) are without prejudice to the generality of any other enactment or rule of law which permits the bringing of representative proceedings."

This amendment would create a collective redress mechanism whereby a not-for-profit body, organisation or association can represent multiple individuals for infringement of their rights under the General Data Protection Regulation.

Amendment 155, in clause 205, page 120, line 38, at end insert—

"(ca) section 183 (4A) to (4C);"

This amendment would create a collective redress mechanism whereby a not-for-profit body, organisation or association can represent multiple individuals for infringement of their rights under the General Data Protection Regulation.

Government amendments 73 and 74.

Government new clause 1—*Representation of data subjects with their authority: collective proceedings.*

Government new clause 2—*Duty to review provision for representation of data subjects.*

Margot James: These Government amendments concern the issue of class representation for data protection breaches. Article 80(1) of the GDPR enables a not-for-profit organisation to represent a data subject on their behalf, if the data subject has mandated them to do so. The Bill gives effect to the same right in clause 183. Where a not-for-profit organisation wants to bring a claim on behalf of multiple people, as things stand it will need to make multiple applications to the court. That is not efficient, and it would be better if all the claims could be made in a single application.

New clause 1 gives the Secretary of State the power to set out provisions allowing a non-profit organisation to bring a claim on behalf of multiple data subjects under article 80(1). We have taken the practical view that that will be an effective way for a non-profit group to seek a remedy in the courts on behalf of a large number of data subjects. The Bill does not give effect to article 80(2), which allows not-for-profit bodies to represent individuals without their mandate. We believe that opt-out collective proceedings should be established on the basis of clear evidence of benefit, with a careful eye on the pitfalls that have befallen so-called class-action lawsuits in other jurisdictions. The Government have, however, listened to the concerns raised and accept that further consideration should be given to the merits of implementing the provisions in article 80(2).

New clause 2 provides a statutory requirement for the Secretary of State to conduct a review of the operation of article 80(1), which will consider how it and the associated provisions in the Bill have operated in practice and assess the merits of implementing article 80(2) in the future. The review will involve consultation among relevant stakeholders, such as the Information Commissioner, businesses, privacy groups, the courts, tribunals and other Departments. The new clause requires the Secretary of State to conduct the review and present its findings to Parliament within 30 months of the Bill's coming into force. That is necessary to provide enough time for there to be sufficient evidence to scrutinise the options provided in article 80(1) in the civil courts. Were the review period to be substantially shorter, it would increase the likelihood of there being a paucity of evidence, which would undermine the effectiveness and purpose of the review. Upon the conclusion of the review period, the Secretary of State will have the

[Margot James]

power, if warranted, to implement article 80(2), allowing non-profit organisations to exercise the rights awarded to data subjects under articles 77, 78, 79 and 82 on their behalf without first needing their authorisation to do so.

Amendments 63 to 68, 73, 74 and 115 are consequential amendments that tidy up the language of the related clause, clause 183. They provide additional information about the rights of data subjects that may be exercised by representative bodies. I commend the amendments to the Committee.

Liam Byrne: I will speak to amendments 154 and 155, which are in my name and those of my hon. Friends. The broad point I want to start with is a philosophical point about rights. If rights are to be real, two things need to be in place: first, a level of transparency so that we can see whether those rights are being honoured or breached; and, secondly, an efficient form of redress. If we do not have transparency and an effective, efficient and open means of redress, the rights are not real, so they are theoretical.

We think there are some unique circumstances in the field of data protection that require a slightly different approach from the one that the Government have proposed. The Government have basically proposed an opt-in approach with a review. We propose an opt-out approach. We think that the argument is clear cut, so we do not see why the Government have chosen to implement something of a half-measure.

The Bill gives us the opportunity to put in place an effective, efficient and world-leading form of redress to ensure that data protection rights are not breached. The reality is that large-scale data breaches are now part and parcel of life. They affect not only the private sector but the private sector, which is partnering with Government. We have seen a number of data breaches among Government partners where financial information has been leaked. The reality is that data protection breaches around the world are growing in number and size.

What is particularly egregious is that many private sector companies admit to the scale of a data breach only many years after the offence has taken place. Yahoo! is a case in point. It had one of the biggest data breaches so far known, but it took many months before the truth came out. That has been true of Government partners, too. Sometimes a lesser offence is admitted to. There is muttering about a particular problem and then, as the truth unfolds, we hear that a massive data breach has taken place. The reality is that these firms are by and large going unpunished. Although the Bill proposes some new remedies of a significant scale, unless those remedies can be sought by ordinary citizens in a court, they frankly are not worth the paper they are printed on.

To underline that point, I remind the Committee that often we look to the Information Commissioner to take the lead in prosecuting these offences. My hon. Friend the Member for Bristol North West was right to celebrate the strength of our current Information Commissioner, but the Government have not blessed the Information Commissioner with unlimited resources, and that will not change in the foreseeable future. What that means is that in the last year for which we have information—2016-17—the Information Commissioner issued only 16 civil monetary penalties for data breaches. That is a very small number. We think we need a regime that allows citizens to bring actions in court. That would multiply the power of the Information Commissioner.

Article 80 of the GDPR addresses that problem in a couple of ways, and the Minister has alluded to them. Article 81 basically allows group or class actions to be taken, and article 82 says that the national law can allow representative bodies to bring proceedings. The challenge with the way in which the Government propose to activate that power is that the organisation bringing the class action must seek a positive authorisation and people must opt in. The risk is that that will create a burden so large that many organisations will simply not step up to the task.

12 noon

A world-leading charity and consumer rights organisation such as Which?, for example, would have a board of trustees to which it would be accountable. It would have to satisfy the trustees that it was not about to embark on something very difficult and expensive. I think most trustees would regard bringing a class action against Google, Facebook, Apple or Microsoft as a reasonably high risk action. If they then have to get a positive opt-in from a large number of people, like the 100,000 affected by the Morrisons data breach, it simply will not happen.

The mechanism that the Government propose breaks down in two particular ways in the real world. First, it takes no account of the gigantic asymmetry between the fearsome five data giants, or indeed many of the other large organisations that control tons and tons of our data, and the humble individual. I mentioned earlier in our proceedings that the big five data giants have a combined market capitalisation of $2.4 trillion. They have billions and billions in cash sitting on their balance sheets. Their legal power is practically unlimited and certainly unprecedented. The role of the plucky organisation being empowered by the Bill to bring a class action is, I am afraid, under some pressure. There is a gigantic inequality of legal arms.

The second reality on which the Government's argument founders is the fact that data breaches, by their very nature, involve data being leaked about tens and tens of thousands of people. The idea that a small charity or a small representative body can round up positive authorisation from tens of thousands of people who have had their rights violated in order to then take Facebook, Google, Apple, Microsoft, Morrisons or Experian to court is laughable. I therefore ask the Government to reflect again on the unique asymmetry that such legal cases confront, and on the evidence of organisations such as Which?, which have had to try to bring cases such as that of Lloyd against Google. That evidence tells us loud and clear that a regime that requires opt-in will simply not work in practice. Our amendment would switch the emphasis. It would allow representative bodies to bring cases, allow people to opt out of cases and allow a collective opt-out.

The reason why the regime that we propose is much better than the one that Ministers proposed is to do with the protection of children's data rights, which we all want to emphasise. I do not think any of us here is such a fantasist that we imagine that groups of children will take Facebook to court because it might have leaked their data somewhere. We will therefore rely on

representative organisations to bring class actions on behalf of children. How on earth will Which? round up thousands of the nation's children to secure their positive opt-in to a class action, which it is in the national interest to bring? That would be completely impossible. The measures that the Government propose are not only weak for adults but completely ineffective for children.

The Government's proposals will allow for a reversal of the regime once we have taken into account the way the world works. Let us think about what that involves, though: allowing the system to fail before getting round to fixing it. The idea is that we introduce a regime knowing that it will not work, and watch the wholesale abuse and breach of people's data rights. We then reflect on the reality that it is impossible for those people to secure justice under the regime that the Government have proposed. Then we decide that we will have a review, which will take a few months. Then Ministers will have to take a decision, and they will probably bring some proposals back to the House. At some point in the 2020s—perhaps the late 2020s—we may get round to having an effective regime to protect people's data rights.

This is one of the defining questions on the Bill—the Government's attitude to the amendments will define whether they are taking the defence of data rights seriously. We now know enough, from cases such as Lloyd against Google, about what works and does not work. The way the Which? trustees had to reflect on class actions brought against companies such as Google tells us enough about how the regime needs to operate.

If the Government are serious about taking on the double asymmetry—the asymmetry between the humble individual and the gigantic tech giants, and that between a single case and thousands of people having their data breached—they will accept the amendments. They were drawn up and tested very carefully. We sought expert legal counsel to get them right. We are grateful to the House for the fact that they have been framed nice and clearly. I urge Ministers not to fail this basic test of judgment as to whether they are serious about protecting our data rights, and to accept the amendments.

Brendan O'Hara (Argyll and Bute) (SNP): It is a pleasure to serve under your chairmanship this afternoon, Mr Streeter.

I support amendment 154. We strongly recommend that if the Government are, as they claim to be, serious about providing the best possible data protection regime to achieve the gold standard that they often talk about for UK citizens, they should look again at the issue of collective redress and make provision for suitably qualified non-profit organisations to pursue data protection infringements and breaches of their own accord, as provided for by the GDPR.

The right hon. Member for Birmingham, Hodge Hill rightly said that the amendments would allow representative bodies to bring such cases, but would also allow individuals to opt out. Currently there is not a level playing field. If the Bill is not amended, the already uneven playing field will become impossibly uneven for individuals whose rights are breached or infringed—probably by a tech giant.

Collective redress was one of the most controversial and hotly debated issues when the Bill was in the House of Lords. The Government resisted all attempts to change it there. There have been slight amendments since then, and an understanding has been reached, but I feel that what the Government propose does not go nearly far enough to address the concerns expressed by Scottish National party and Labour Members.

Anna Fielder, a former chair of Privacy International, wrote:

> "Weak enforcement provisions were one of the widely acknowledged reasons why the current data protection laws, in the UK and elsewhere in Europe, were no longer fit for purpose in the big data age. As a result, it has been more convenient for organisations collecting and processing personal information to break the law and pay up if found out, than to observe the law—as profits made from people's personal information vastly outweighed even the most punitive of fines."

That is the situation we are in, and it is incumbent on legislators to level the playing field—not to make it even more uneven. However, as the Bill currently stands, it only enables individuals to request that such suitably qualified non-profit organisations take up cases on their behalf, rather than allowing the organisations themselves to highlight where they believe a breach of data protection law has occurred.

All too often, as has been pointed out on numerous occasions, individuals are the last people to know that their data has been unlawfully and in many cases illegally used. They depend on suitably qualified non-profit organisations, which are there to conduct independent research and investigations, to inform them that that is the case. Indeed, there was a very striking example recently in Germany, where the consumer federation took one of the tech giants to court over a number of platform breaches of current German data protection law, and it won. However, there are numerous examples across the world of organisations and groups highlighting bad or illegal practices that would hitherto probably have gone unnoticed here.

Privacy International recently published a report on the use and possible abuse of personal data connected to the rental car market. Which? has carried out research on online toys that are widely available in this country, which could pose serious child safety risks. The Norwegian consumer council has done similar work on toys, as well as exposing unlawful practices by health and dating apps.

Across the world, there are groups that do collective redress work very successfully in Belgium, Italy, Portugal, Spain, Sweden, Canada and Australia. I urge the Government to reconsider the matter and to see the great consumer benefits and protections that would come from accepting amendment 154. It would give not-for-profit organisations the right to launch complaints with a supervisory authority, as well as seeking judicial remedy, when it considered that the rights of a data subject under the GDPR had been breached.

I repeat that at the moment we have an uneven playing field. If the Bill goes through unamended it will become an impossible playing field for consumers, so I urge the Government to accept the amendment.

Darren Jones: I promise not to speak at every opportunity today, Mr Streeter; I am conscious that it is a Thursday and that Members have constituencies to get to, but on this point I will just add my support to the amendment tabled by my right hon. Friend the Member for Birmingham, Hodge Hill.

[Darren Jones]

The Bill puts us in a position that we should not have been in in the first place. The Government's original view was that they were not going to implement article 80 of the GDPR; they have now gone one step in that direction, and I support the aim that we go the whole hog.

I recognise from my work previous to being an MP that a lot of tech companies are not evil; they want to do the right thing and go about being successful as businesses. It was partly my job in the past to look at these areas of law on behalf of companies, and to work with campaigning groups, regulators and others. It was about being an internal voice to make sure that there was the correct balance within businesses between considering consumers and being pro-business. This amendment would help to facilitate that conversation, because if bodies such as Which? that are private enforcers on behalf of consumers had these legal rights, then of course there would be an obligation on businesses to have ongoing dialogue and relationships. They would have to make sure that consumers' concerns were at the forefront and that they were doing things in the right way.

The balance to be struck is really important. The Information Commissioner's Office, for example, has lost quite a lot of staff to other companies recently. The Minister's Department had to increase the salary bands for ICO staff to try to keep them there. In other sectors of the regulated economy, having private enforcers on behalf of consumers as a collective group works perfectly well for existing regulators.

In the telecommunications sector, in which I have worked in the past, there is Ofcom, which regulates the telecom sector, but there is also Which?, working as a private enforcer under the Consumer Rights Act 2015, which can act on behalf of consumers as a group. That works perfectly well and as my right hon. Friend said, private enforcers will not just start bringing these super-complaints every week, because the risk would be too high. They will only bring these super-complaints when they have failed in their dialogue and have no choice.

12.15 pm

Under the Consumer Rights Act 2015, where this mechanism exists today, we do not have endless vexatious super-complaints. There are actually some very effective super-complaints that work well in the interests of consumers, however. Some of the data breaches have involved groups as big as tens of millions of people.

I know from my own experience in other parts of law that we cannot always identify the individual involved. Sometimes they have moved on, or their contact details have changed, and we physically cannot get compensation to them. Under the Consumer Rights Act, again with the mechanism that came from European law—it is a principle that has been copied across from the GDPR—compensation can be given to others on behalf of consumers as a group. It is given to consumer charities or consumer regulators to help facilitate their work. We ought to be alive to that possibility in data protection law.

That mechanism is normal and widely used at European Union law level to balance power between consumers and businesses. We have adopted it into UK law, as the Minister will know from her previous role as the Minister responsible for consumer law and small business. I do not see why we cannot use it now, so I support the amendment. It simply says, let us get on with it instead of waiting to see whether it works, because we know that it works perfectly well today in other areas of law.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): It is a pleasure to serve under your chairmanship, Mr Streeter. We have had three excellent speeches already in support of amendments 154 and 155, so I will not try to replicate them. As the right hon. Member for Birmingham, Hodge Hill said, this is one of the pivotal debates on the Bill. I would like to be positive, but all I can bring myself to say about the Government's new clause and amendments is that they are marginally better than nothing. However, they do not go far enough and they will leave the UK significantly behind other EU countries in terms of collective redress and the pursuit of the gold standard of data protection. They will leave the Bill falling short of what the Government themselves promised on effective redress.

Only amendments 154 and 155 will provide a comprehensive opt-out regime and enable adults and children who are victims of data breaches properly to vindicate their rights to proper protection of their personal data. The amendments will provide a mechanism whereby serious breaches of data protection, which can affect the most vulnerable in society, are seriously addressed and result in real change that will benefit thousands if not millions of consumers across the UK.

The Bill provides a hugely significant opportunity to legislate for a cost-effective and efficient mechanism for redress in cases of mass data breaches, which we all know are increasingly common and which the Information Commissioner's Office has limited resources to deal with. The measure is essential to make the Bill fit for purpose and I wholeheartedly support both amendments.

The Chair: Before I call the Minister to respond, it might help the Committee to know that, although we are properly debating Opposition amendments 154 and 155 at the moment, if they are to be put to a Division, that cannot happen until we reach clause 183. However, that does not prevent the Minister from indicating she might accept them at this stage. That is entirely up to her.

Margot James: I thank right hon. and hon. Members for their contributions. We certainly agree with the need for a transparent system of rights over people's personal data and a system of enforcement of those rights. We could not agree more with the thinking behind that, but we need to pause for thought before implementing article 80(2). The GDPR represents significant change, but we should test the effectiveness of the new enforcement scheme, including, as we have already discussed, article 80(1), before we make further changes of the type proposed this morning under amendments 154 and 155.

Amendment 154 applies article 80(2) with immediate effect and gold-plates it. We have a number of concerns with that approach. First, we are wary of the idea that data subjects should be prevented from enforcing their own data rights simply because an organisation or, in this instance, an individual they had never met before, got there first. That is not acceptable. It contradicts the

theme of the Bill and the GDPR as a whole, which is to empower individuals to take control of their own data. As yet we have no evidence that that is necessary.

Liam Byrne: Let us take Uber—one of the most recent of the 200 data breaches listed on Wikipedia. In that case, 57 million records were leaked. How is one of those drivers going to take Uber to court to ensure justice?

Margot James: The GDPR places robust obligations on the data controller to notify all data subjects if there has been a breach that is likely to result in a high risk to their rights. That example is almost unprecedented and quite different—

Liam Byrne: It is not unprecedented. Look at the Wikipedia page on data breaches. There are 200 of them, including Uber, Equifax, AOL, Apple, Ashley Madison, Betfair—the list goes on and on. I want an answer to a very simple question. How is a humble Uber driver, who is busting a gut to make a living, going to find the wherewithal to hire a solicitor and take Uber to court? What is the specific answer to that question?

Margot James: If a data subject is sufficiently outraged, there is nothing to stop them contacting a group such as Which? and opting into a group action. Furthermore, a range of enforcement options are open to the ICO. It can issue enforcement notices to compel the controller to stop doing something that is in breach of people's data rights. As I said, there is nothing to stop a data subject opting into a group action.

Liam Byrne: There is only one major precedent for the kind of scenario the Minister has sketched out today, which is Various Claimants *v.* Wm Morrisons Supermarket plc—a case she knows well. That case illustrates the difficulties of opt-in. It is by far the largest group of data protection claimants ever put together. Even then, the total number of people who could be assembled was 5,000 out of 100,000 people whose data rights were breached. That was incredibly difficult and took a huge amount of time. Even if the claim succeeds, the 95% of people not covered by the claim will not receive justice. I am not quite sure what new evidence the Minister is waiting for so that she has enough evidence to activate the kind of proposals we are talking about today.

Margot James: As I said, the GDPR represents significant change. We believe we should test the effectiveness of the new enforcement scheme before we make further changes of the kind the right hon. Gentleman is suggesting. The Morrisons case was effective. The collective redress mechanism—group litigation orders—was used and was effective. The Information Commission will have new powers under the Bill to force companies to take action when there has been a breach of data.

There are other problems with amendment 154. First, like the right hon. Member for Birmingham, Hodge Hill, we are concerned about children's rights. We would be concerned if a child's fundamental data rights were weighed up and stripped away by a court without parents or legal guardians having had the opportunity to make the decision to seek redress themselves or seek the help of a preferred non-profit organisation. Once that judgment has been finalised, there will be no recourse for the child or the parent. They will become mere observers, which is unacceptable and makes a travesty of the rights they are entitled to enforce on their own account.

Secondly, we must remember that the non-profit organisations referred to in the amendment are, by definition, active in the field of data subjects' rights. Although many will no doubt have data subjects' interests at heart, some may have a professional interest in achieving a different outcome—for example, chasing headlines to promote their own organisation. That is why it is essential that data subjects are capable of choosing the organisation that is right for them or deciding not to partake in a claim that an organisation has advertised. The amendment would also allow an individual to bring a collective claim on behalf of other data subjects without their consent.

Brendan O'Hara: Does the Minister not accept, as I said earlier, that individuals are often the last people to know that their data has been breached and their rights have been infringed? For collective rights in hugely complicated areas, there must be a presumption that those rights are protected, and the Bill does not do that. I do not believe it reflects the principle that individuals are often the last people to know, and that they are the ones who need protecting.

Margot James: The Information Commissioner has powers to force companies to notify data subjects of any breach of data, and there is a legal requirement on companies so to do.

The amendment would allow an individual to bring a collective claim on behalf of other data subjects without their consent. We oppose it because it does not give people the protection of knowing that the entity controlling their claim is a non-profit organisation with a noble purpose in mind. I am pleased to say that, as I outlined this morning, the Government's position was supported in the other place by the Opposition Front Benchers and the noble Baroness Kidron.

Liam Byrne: I am incredibly disappointed with the Minister's response, and I am not quite sure I believe that she believes what she has been reading out. I hope that between now and Report, or whenever the amendment is pressed to a vote, she will have the opportunity to consult Which? and her officials. The reality is that for complex public policy decisions, whether relating to organ donation or auto-enrolment pensions, we have well-established procedures for opting out, rather than opting in. There has been strong cross-party support for that over the past seven or eight years, and it reflects a reality in new economic thinking. Behavioural economics shows that opt-out is often better than opt-in.

If the Government pursue that line of argument on Report, in the other place and through to Royal Assent, we will not permit the Minister ever again to refer to the Bill as a gold standard in data protection. It is a shoddy, tarnished bronze. She has sought to ensure that the legal playing field is tilted in the favour of large organisations and tech giants, and away from consumers and children. That will lead to a pretty poor state of affairs. We now have enough precedents to know that the regime she is

[Liam Byrne]

proposing will not work. This is not a theoretical issue; it has already been tested in the courts. Her proposal will not fix the asymmetry that potentially leaves millions of people without justice.

The idea that the Minister can present the Morrisons case as some kind of success when 95% of the people whose data rights were breached did not receive justice because they did not opt in to the class action betrays it all. She is proposing a system of redress that is good for the few and bad for the many. If that is her politics, so be it, but she will not be able to present the Bill as the gold standard if she persists with that argument.

The Chair: As I said, we will deal with the Opposition amendments later in our proceedings.

Amendment 115 agreed to.

Schedule 6, as amended, agreed to.

Clauses 23 and 24 ordered to stand part of the Bill.

Clause 25

MANUAL UNSTRUCTURED DATA USED IN LONGSTANDING HISTORICAL RESEARCH

Amendment made: 17, in clause 25, page 15, line 40, leave out "individual" and insert "data subject".—*(Margot James.)*

Clause 25 makes provision about the processing of manual unstructured data used in longstanding historical research. This amendment aligns Clause 25(1)(b)(i) with similar provision in Clause 19(2).

Clause 25, as amended, ordered to stand part of the Bill.

Clause 26

NATIONAL SECURITY AND DEFENCE EXEMPTION

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

12.30 pm

Louise Haigh (Sheffield, Heeley) (Lab): It is a pleasure to serve under your chairmanship once again, Mr Streeter. I think it was about 18 months ago that we were in this very room, debating the Bill that became the Digital Economy Act 2017. We discussed at length the trade-off between the rights of data subjects, privacy, transparency and the need for Government access to data. In that context we were debating the rights of viewers of online pornography, rather than matters of national security. I note that the Government have had to delay the introduction of the regulations, because they failed to get to grips with the issues that we raised in Committee. I do not envy the new Minister, or, indeed, my right hon. Friend the shadow Minister, their task of attempting to get things right. It was one of the low points of my political career when I had to negotiate with the present Secretary of State for Digital, Culture, Media and Sport on what sexual acts would be blocked. I wish them both luck in taking the matter forward, and am glad I am dealing only with national security issues in the Bill that we are considering today.

As we come to crucial clauses that give Ministers and the security services a great deal more latitude, it is important for the Opposition to lay out key principles on national security certificates. Of course we support the legitimate interests of the intelligence services, as dictated by their statutory functions, including the safeguarding of national security. Of course we recognise that protecting citizens from harm often means striking a difficult balance between operational requirements and the rights of individuals who may fall within the scope of the investigations. We know that the security services take that seriously.

It is the Opposition's duty, however, to scrutinise the Government's approach, to ensure that any powers that explicitly allow the setting aside of citizens' data rights under the Bill are proportionate and necessary, and that they will be overseen through appropriate safeguards. Clauses 26 and 27 provide for a national security certification regime allowing restriction of and exemption from a wide range of rights under the GDPR and the Bill on the basis of national security, and for defence purposes.

The Government state that national security falls outside the scope of EU law and, therefore, the GDPR, and that therefore any processing of personal data relating to national security will be governed by the applied GDPR. Article 4(2) of the treaty on the European Union provides that national security remains the sole responsibility of each member state. Despite that, EU data protection legislation provides for derogations for national security. If national security were entirely outside the scope of the EU treaty, such derogations would be unnecessary, so, as the Joint Committee on Human Rights argued, the provisions imply the retention of some level of EU scrutiny over derogations from EU data protection rights on the grounds of national security. It is thus not at all clear that the Government's assertions about blanket national security exemptions are correct.

Furthermore, there is no clear definition of which entities will be covered by the extremely broad exemptions under subsection 1, which refers to "national security" and "defence purposes". I am concerned that a measure allowing broad exemptions to the rights of citizens does not stipulate which entities will be entitled to jettison those rights. As was debated at length in the other place, there are no clear definitions of national security, or of the extended exemption for defence purposes, which goes beyond the Data Protection Act 1998, in the Bill or the explanatory notes. As the right hon. and learned Member for Rushcliffe (Mr Clarke) remarked during the passage of the Investigatory Powers Act 2016,

> "National security can easily be conflated with the policy of the Government of the day."—[*Official Report*, 15 March 2016; Vol. 607, c. 850.]

As the Joint Committee on Human Rights concluded,

> "it is unclear why the authorities require such a breadth of exemptions from their obligations under the data protection regime."

Before we move on to discuss our amendments to clause 26, I should be grateful if the Minister could assure us about the definitions of "national security" and "defence purposes" and in particular which entities they apply to.

The Chair: I think the amendments are to clause 27 of the Bill.

Brendan O'Hara: I rise to speak to amendment 161 and amendments 162 to 169.

The Chair: That is the next clause.

Brendan O'Hara: My apologies.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): It is a pleasure to serve under your chairmanship, Mr Streeter. Clause 26 creates an exemption for certain provisions in the Bill only if that exemption is required for the purpose of safeguarding national security or for defence purposes. Where processing does not meet these tests, the exemption cannot apply. It is possible to exempt from most but not all the data protection principles the rights of data subjects, certain obligations on data controllers and processors, and various enforcement provisions, where required to safeguard national security or for defence purposes. In relation to national security, the exemption mirrors the existing national security exemption provided for in section 28 of the 1998 Act. The statutory framework has long recognised that the proportionate exemptions from the data protection principles and the rights of data subjects are necessary to protect national security. The Bill does not alter that position.

The exemption for defence purposes is intended to ensure the continued protection, security and capability of our armed forces and of the civilian staff who support them—not just their combat effectiveness, to use the outdated language of the 1998 Act. In drafting this legislation, we concluded that this existing exemption was too narrow and no longer adequately captured the wide range of vital activities that are undertaken by the Ministry of Defence and its partners. We have seen that all too obviously in the last two weeks.

Liam Byrne: On that point, will the Minister give way?

Victoria Atkins: If the right hon. Gentleman is going to disagree with me that combat effectiveness would be a very narrow term to describe the events in Salisbury, of course I will give way.

Liam Byrne: I actually wanted to ask about interpreters who support our armed forces. There is cross-party consensus that sometimes it is important to ensure that we grant leave to remain in this country to those very brave civilians who have supported our armed forces abroad as interpreters. Sometimes, those claims have been contested by the Ministry of Defence. Is the Minister confident and satisfied that the Ministry of Defence would not be able to rely on this exemption to keep information back from civilian staff employed as interpreters in support of our armed forces abroad when they seek leave to remain in this country?

Victoria Atkins: I cannot possibly be drawn on individual applications for asylum. It would be wholly improper for me to make a sweeping generalisation on cases that are taken on a case-by-case basis. I refer back to the narrow definition that was in the 1998 Act and suggest that our enlarging the narrow definition of combat effectiveness would mean including the civilian staff who support our brave troops.

The term "defence purposes" is intended to be limited in both application and scope, and will not encompass all processing activities conducted by the Ministry of Defence. Only where a specific right or obligation is found to incompatible with a specific processing activity being undertaken for defence purposes can that right or obligation be set aside. The Ministry of Defence will continue to process personal information relating to both military and civilian personnel in a secure and appropriate way, employing relevant safeguards and security in accordance with the principles of the applied GDPR. It is anticipated that standard human resources processing functions such as the recording of leave and the management of pay and pension information will not be covered by the exemption.

Liam Byrne: I am sorry to press the Minister on this point, and she may want to write to me as a follow-up, but I think Members on both sides of the House have a genuine interest in ensuring that interpreters who have supported our troops abroad are able to access important information, such as the terms of their service and the record of their employment, when making legitimate applications for leave to remain in this country—not asylum—or sometimes discretionary leave.

Victoria Atkins: I am very happy to write to the right hon. Gentleman about that. The exemption does not cover all processing of personal data by the Ministry of Defence, but I am happy to write to him on that subject.

It may assist the Committee if I give a few examples of processing activities that might be considered to fall into the definition of defence purposes requiring the protection of the exemption. Such processing could include the collation of personal data to assist in assessing the capability and effectiveness of armed forces personnel, including the performance of troops; the collection and storage of information, including biometric data necessary to maintain the security of defence sites, supplies and services; and the sharing of data with coalition partners to support them in maintaining their security capability and the effectiveness of their armed forces. That is not an exhaustive list. The application of the exemption should be considered only in specific cases where the fulfilment of a specific data protection right or obligation is found to put at risk the security capability or effectiveness of UK defence activities.

The hon. Member for Sheffield, Heeley asked for a definition of national security. It has been the policy of successive Governments not to define national security in statute. Threats to national security are constantly evolving and difficult to predict, and it is vital that legislation does not constrain the security and intelligence agencies' ability to protect the UK from new and emerging threats. For example, only a few years ago it would have been very difficult to predict the nature or scale of the threat to our national security from cyber-attacks.

Clause 26 does not provide for a blanket exemption. It can be applied only when it is required to safeguard national security or for defence purposes.

Daniel Zeichner: What weight does the Minister give to the written evidence that the Committee received from the Information Commissioner's Office? It is obviously expert on this issue, and it addresses some of the points she made. It concludes that there is no threshold for when "defence purposes" are to be used, and that there is no guidance

"for when it is appropriate to rely on the exemption."

[Daniel Zeichner]

What weight does the Minister give to that, and what is her response to the concern raised by the Information Commissioner's Office?

Victoria Atkins: Again, surely it is for the Executive—elected officials—to take responsibility for decisions that are made by data controllers in the Ministry of Defence. Obviously, the Department has considered the Information Commissioner's representations, but this is not a blanket exemption. The high threshold can be met only in very specific circumstances.

Question put and agreed to.

Clause 26 accordingly ordered to stand part of the Bill.

Clause 27

NATIONAL SECURITY: CERTIFICATE

Louise Haigh: I beg to move amendment 161, in clause 27, page 17, line 2, leave out subsection (1) and insert—

"A Minister of the Crown must apply to a Judicial Commissioner for a certificate, if exemptions are sought from specified provisions in relation to any personal data for the purpose of safeguarding national security."

This amendment would introduce a procedure for a Minister of the Crown to apply to a Judicial Commissioner for a National Security Certificate.

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

Amendment 162, in clause 27, page 17, line 5, at end insert—

"(1A) The decision to issue the certificate must be—

(a) approved by a Judicial Commissioner,

(b) laid before Parliament,

(c) published and publicly accessible on the Information Commissioner's Office website.

(1B) In deciding whether to approve an application under subsection (1), a Judicial Commissioner must review the Minister's conclusions as to the following matters—

(a) whether the certificate is necessary on relevant grounds,

(b) whether the conduct that would be authorised by the certificate is proportionate to what it sought to be achieved by that conduct, and

(c) whether it is necessary and proportionate to exempt all provisions specified in the certificate."

This amendment would ensure that oversight and safeguarding in the application for a National Security Certificate are effective, requiring sufficient detail in the application process.

Amendment 163, in clause 27, page 17, leave out lines 6 to 8 and insert—

"(2) An application for a certificate under subsection (1)—

(a) must identify the personal data to which it applies by means of a detailed description, and".

This amendment would require a National Security Certificate to identify the personal data to which the Certificate applies by means of a detailed description.

Amendment 164, in clause 27, page 17, line 9, leave out subsection (2)(b).

This amendment would ensure that a National Security Certificate cannot be expressed to have prospective effect.

Amendment 165, in clause 27, page 17, line 9, at end insert—

"(c) must specify each provision of this Act which it seeks to exempt, and

(d) must provide a justification for both (a) and (b)."

This amendment would ensure effective oversight of exemptions of this Act from the application for a National Security Certificate.

Amendment 166, in clause 27, page 17, line 10, leave out "directly" and insert

"who believes they are directly or indirectly"

This amendment would broaden the application of subsection (3) so that any person who believes they are directly affected by a National Security Certificate may appeal to the Tribunal against the Certificate.

Amendment 167, in clause 27, page 17, line 12, leave out

", applying the principles applied by a court on an application for judicial review,"

This amendment removes the application to the appeal against a National Security Certificate of the principles applied by a court on an application for judicial review.

Amendment 168, in clause 27, page 17, line 13, leave out

"the Minister did not have reasonable grounds for issuing"

and insert

"it was not necessary or proportionate to issue".

These amendments would reflect that the Minister would not be the only authority involved in the process of applying for a National Security Certificate.

Amendment 169, in clause 27, page 17, line 16, at end insert—

"(4A) Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Judicial Commissioner must give the Minister of the Crown reasons in writing for the refusal.

(4B) Where a Judicial Commissioner refuses to approve a Minister's application for a certificate under this Chapter, the Minister may apply to the Information Commissioner for a review of the decision.

(4C) It is not permissible for exemptions to be specified in relation to—

(a) Chapter II of the applied GDPR (principles)—

(i) Article 5 (lawful, fair and transparent processing),

(ii) Article 6 (lawfulness of processing),

(iii) Article 9 (processing of special categories of personal data),

(b) Chapter IV of the applied GDPR—

(i) GDPR Articles 24 – 32 inclusive,

(ii) GDPR Articles 35 – 43 inclusive,

(c) Chapter VIII of the applied GDPR (remedies, liabilities and penalties)—

(i) GDPR Article 83 (general conditions for imposing administrative fines),

(ii) GDPR Article 84 (penalties),

(d) Part 5 of this Act, or

(e) Part 7 of this Act."

This amendment would require a Judicial Commissioner to intimate in writing to the Minister reasons for refusing the Minister's application for a National Security Certificate and allows the Minister to apply for a review by the Information Commissioner of such a refusal.

Louise Haigh: With our amendments we seek to provide some oversight of and protections against the very broad definitions in this part of the Bill. I am afraid we are not content with the Minister's assertions in her response on the previous clause.

As they currently stand, national security certificates give Ministers broad powers to remove individuals' rights with absolutely no oversight. If this is a matter for the Executive, as the Minister has just said, they must be subject to oversight and accountability when making such decisions, and as it stands there is absolutely none at all. The rights at risk from the exemption are the right to be informed when personal data is collected from individuals, which is in article 13 of the GDPR; the right to find out whether personal data against them is being processed, in article 15; and the right to object to automated decision making, in articles 21 and 22. Furthermore, the Information Commissioner's inspection, authorisation and advisory powers are set aside, which is why she and her office raised concerns, as my hon. Friend the Member for Cambridge set out.

It is not difficult to envisage examples of why those exemptions may be necessary. The Minister has laid some of them out: for instance, during the course of an ongoing national security investigation, the right of an individual to be informed that their data is being processed would not be appropriate. With these exemptions, there will inevitably be a need for appropriate safeguards to protect the rights of citizens. We are not yet convinced that the Bill contains them. That is what these amendments seek to tackle.

12.45 pm

As we have set out, any powers exercised in the interests of national security and defence must be necessary, proportionate and overseen by appropriate safeguards. Amendments 161 to 169 create a framework around which these necessary and proportionate powers can be used appropriately by Ministers and the security services. The current framework laid out in the Bill is extraordinarily narrow; yes, there will be a tribunal to determine the rights of the citizen, but the provisions of the Bill allow for that to happen only after the rights themselves have been infringed; they allow Ministers to detail the reasons for the certificate in only the vaguest possible terms; and they give the individual the power to appeal against the decision only within the narrow confines of the principles of a judicial review.

Amendment 161 would introduce a framework to give citizens judicial protection in the initial instance and greater rights. The provisions of clause 26(1) allow individuals to press for their rights only after the fact. The amendments would mirror the provisions of the Investigatory Powers Act 2016, which gives the Investigatory Powers Commissioner's office independent judicial oversight of public authorities' use of investigatory powers. Crucially, that office will consider whether it agrees with Ministers' decisions to authorise intrusive investigatory powers before they can come into effect. Judicial commissioners act independently of Government and can be removed from office only by resolution of each House, and in limited circumstances by the Prime Minister, for example through bankruptcy, disqualification as a company director, or conviction of an offence that carries a sentence of imprisonment.

If, under the 2016 Act, the exercise of a range of investigatory powers by public authorities—including the interception of communications, the acquisition and retention of communications data, equipment interference, intrusive surveillance, property interference, directed surveillance, covert human intelligence sources and bulk personal data sets—can be monitored prior to any potential breach of rights, it is not clear why a similar safeguard cannot take its place in the more limited provisions of this Bill.

Crucially, amendment 162 stipulates that the judicial commissioners should be entitled to make an assessment for a national security certificate based on the tests outlined today; namely, whether it is necessary and proportionate to issue a certificate. They should assess whether the certificate is necessary on relevant grounds, whether conduct authorised by the certificate would be proportionate, and whether it is necessary and proportionate to exempt all the provisions in question. The Government believe that the provisions in the Bill do not give controllers carte blanche to set aside rights and obligations, and that rights and obligations will be considered on a case-by-case basis, but they allow for obligations to be set aside with no oversight.

Citizens must have confidence that in the exercise of their duties, Ministers and the intelligence services are questioned to ensure that they are making the right decisions based on evidence. Amendments 163 and 165 would require the national security certificate to identify the personal data to which the certificate applies, and would require a Minister to provide a justification of why they are seeking an exemption under the Bill. It is not a big ask to require a Minister to state what data they are processing and for what purposes.

The Bill as it stands gives Ministers huge powers to set aside data rights, with no justification and providing only the bare minimum of information. A general description of the data in question would not alone be enough for the tribunal or the judicial commissioners to make a determination on whether the certificate was justified. Amendment 167 would allow the tribunal to consider the facts of the case, and it should be considered with the other amendments that I have spoken to. Judicial review, taken together with the limited information that the Government want to detail in the certificate, would leave only a very narrow angle open for a data subject whose rights had been unlawfully breached in a way that was neither necessary nor proportionate. That would allow the tribunal to consider the true facts of the case.

Finally, amendment 169 recognises the need for Ministers to be able to appeal the decision of the judicial commissioners in the event that they reject the application for a certificate. That appeal would go to the Information Commissioner and would stipulate that the judicial commissioner must set out the reasons why such an application was rejected.

As we have stated, we recognise how vital it is, operationally, for intelligence services and law enforcement to carry out their duties in the interest of national security, and no provision should get in the way of keeping our citizens from harm. The rights of data subjects must be protected, however, and where there are issues of national security, we have to get that balance right. We are seeking to help the Government do that by bringing the Bill into line with the safeguards that were added to the Investigatory Powers Act, to ensure necessity and proportionality without hindering operational requirement.

For an interference with rights to be in accordance with law, it must include safeguards against arbitrary interference. We contest that the provisions regarding

national security certificates fall short of that requirement. These clauses, unamended, would leave the Government wide open to legal challenge. We hope that the Minister will see the merit of our amendments and correct the Bill at this stage.

Brendan O'Hara: It may come as no surprise that I rise to speak in support of amendments 161 to 169. They are intended to challenge the Government's plan to introduce a national security certification regime that will allow the restriction of and exemptions from a wide range of fundamental rights on the basis of national security and defence. Although it is absolutely right that, as a country, the UK has the ability to act in its own national security interest, I and many others are worried that the scale and scope of what is proposed in the Bill goes much further than the 1998 Act by widening the national security definition to include a further and, I would suggest, undefined range of defence purposes.

The Minister gave three or four examples earlier, but stressed that it was not an exhaustive list. Given the broad and indefinite nature of those national security exemptions, we are concerned that they do not meet the test of being both necessary and proportionate. How much confidence can we have that an individual's fundamental rights will be best protected when the exemptions will be signed off by a Government Minister with little or no judicial oversight? It is also concerning that there appears to have been little or no attention to the harmful impact of exempting vast amounts of information from data protection safeguards by relying upon national security certificates.

As we heard earlier, the list of rights that are exempted, set out in clause 26, includes the right to be informed when data is being collected, the right to find out when personal data is being processed and the right to object to automated decision making. Those exemptions are to be exercised by a certificate, which, as I say, will be signed by a Minister, who will certify that an exemption from those rights and obligations is necessary for the purpose of safeguarding national security.

That means that, as the Bill is currently drafted, people's rights could be removed by a politician without any form of judicial oversight. That cannot be right. We would argue most strongly that there has to be judicial oversight of any such decision, to prevent the removal of individual data protection rights from being permitted purely at the say-so of a Government Minister. I ask the Minister, how do the Government define national security and defence purposes in the context of the Bill? I certainly was not satisfied with the explanation we heard earlier on. I believe that these undefined terms are unnecessarily open-ended and broad, and open to vague interpretation. They could very well result in the removal of an individual's rights unnecessarily. The lack of a clear definition of national security and defence purposes also means that people will be unable to foresee or understand when their rights will be overridden by the application of these exemptions. Surely that is incompatible with an individual citizen's fundamental rights.

These exemptions, on the surface, are not limited to the UK's intelligence and security services. As we heard when debating part 2 of the Bill, which deals with general processing, they broadly permit public authorities, and even private corporations on occasion, to invoke national security and defence as a reason to cast aside privacy rights. Can the Minister explain if, how, and under what circumstances a public authority or private company could invoke national security and defence as a reason to cast aside privacy rights?

That brings me to necessity and proportionality, which are fundamental principles when looking at exemptions from data protection, and which will be examined extremely closely by the European Commission and its legal team when it decides on the UK's suitability for adequacy after Brexit. The principles of necessity and proportionality are enshrined in the European convention on human rights. A Minister must take them into account when they consider restricting or limiting an individual's rights, such as those under article 8, the right to privacy.

As the Bill stands, no conditions or tests are imposed on a Minister's decision to withdraw an individual's personal data protection rights by issuing a national security certificate. There is no limitation on how a national security certificate should run or how long it should operate for. There is no obligation to review the ongoing necessity of having a live certificate. In effect, a certificate is open-ended and indefinite. My concern is that that may allow the state to use a certificate for activities for which it was not considered relevant or appropriate by the Minister when it was first issued or signed.

That loophole cannot be considered proportionate or necessary. The certificates have to be time-limited. That does not mean that once a certificate has expired it cannot be re-certified, but it would ensure that certificates that are no longer necessary or that have been used beyond their original remit do not continue indefinitely. Perhaps the Minister could explain why she thinks such a system could not work, and why it would not be in the best interest of the state and of protecting an individual's rights.

As with everything we do, including everything we have done in this area in the past couple of years, the Bill has to be seen against the backdrop of Brexit. Not only do we have to comply with the GDPR, but we have to do so in a way that means the United Kingdom will achieve the vital, much sought after adequacy decision from the European Commission. We also have to keep our laws consistent with EU law to maintain that adequacy status. I fear that the widespread use of exemptions and, perhaps more worryingly, the undefined range of defence purposes could deal a severe blow to the UK achieving an adequacy decision from the European Commission.

Can the Minister tell me whether the Government have been given cast-iron guarantees that the new and undefined range of defence purposes will be consistent with EU law, to allow us not just to achieve adequacy but to maintain adequacy post Brexit?

The Chair: I will call the Minister to respond, but before she responds to that point, she wishes to correct the record in relation to a previous point, which I am happy to permit.

Victoria Atkins: On reflection, I would not wish the hon. Member for Cambridge to understand my earlier answer to mean that a Minister makes a decision on defence purposes. I apologise to him if that was not clear. It is

the data controller at the Ministry of Defence who makes that decision. The data controller is accountable to Ministers and in due course to domestic courts. I hope that clarifies that.

The Chair: And now the response to amendment 161.

Victoria Atkins: I think I am going to be cut off for lunch, Mr Streeter.

The Chair: It is up to the Committee what time we adjourn for lunch, of course, and the Minister may wish to speak quite rapidly.

The Lord Commissioner of Her Majesty's Treasury (Nigel Adams): Much as I would like the Minister to speak rapidly, I will move the Adjournment.

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

12.59 pm

Adjourned till this day at Two o'clock.