PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL *[LORDS]*

Fourth Sitting

Thursday 15 March 2018

(Afternoon)

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

(Afternoon)

[Mr David Hanson *in the Chair*]

Data Protection Bill [*Lords*]

2 pm

The Chair: By the miracle of assistance from the Clerks, I am aware that we have had a debate this morning and that the Minister is now to respond to that debate, which I did not hear, but which I am sure was a full one.

Clause 27

National security: certificate

Amendment proposed (this day): 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."—*(Louise Haigh.)*

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

Question again proposed, That the amendment be made.

The Chair: I remind the Committee that with this we are discussing 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.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): Thank you, Mr Hanson. It is a pleasure to serve under your chairmanship again.

I will first provide some context for this part of the Bill. The provisions in the Bill relating to national security exemptions and certificates are wholly in line with the provisions in the Data Protection Act 1998 and its predecessor, the Data Protection Act 1984. What we are doing in the Bill is preserving an arrangement that has been on the statute book for more than 30 years and has been operated by successive Governments.

The national security exemption is no different in principle from the other exemptions provided for in the Bill. If it is right that certain provisions of data protection legislation can be disapplied for reasons of, for example, crime prevention or taxation purposes, or in pursuit of various regulatory functions, without external approval, surely it is difficult to take issue with the need for an exemption on the grounds of national security on the same basis.

Louise Haigh (Sheffield, Heeley) (Lab): The Minister is absolutely right that the provisions mirror those in the DPA. That is exactly why we take issue with them. They mirror unacceptable preventions of rights in the tribunal appeal process, but do not mirror the rights in the Investigatory Powers Act 2016. Why were safeguards put in place in that Act, but will not apply in this Bill?

Victoria Atkins: If I understand the hon. Lady's argument correctly, she has presented the judicial commissioners as permitting, for example, warrant to be granted. Having sat through the Joint Committee on the Draft Investigatory Powers Bill and then the Public Bill Committee, I can tell her that I am afraid that is not how that Act works. What happens is that the Secretary of State grants the warrant and then that decision is overseen by the judicial commissioner. I will come on to the difference between the Investigatory Powers Act and this Bill in due course, because the terminology used draws on that in the Investigatory Powers Act, but that Act is very different from this Bill, which is about the processing of data, in its engagement with people and their rights.

Darren Jones (Bristol North West) (Lab): Will the Minister give way on that point?

Victoria Atkins: If I may, I will make some progress. Along with existing provisions in section 28 of the 1998 Act, clause 27 provides for a certificate signed by a Minister of the Crown certifying that exemption from specified data protection requirements is required for the purposes of safeguarding national security. There are equivalent provisions in parts 3 and 4 of the Bill. Such a certificate is conclusive evidence of that fact, for example in any legal proceedings. That is the point about the certificates—they only come into play if the exemption or restriction is actually applied.

The certificate provides evidence that the exemption or restriction is required for the purpose of safeguarding national security. It therefore has relevance only in the event that, first, the exemption or restriction is applied to the data in question and, secondly, there is a need to rely on the certificate as conclusive evidence in proceedings to establish that the exemption or restriction is required for the statutory purpose.

Louise Haigh: But what the national security certificate does not require is a statement of what data is being processed or the exemptions under which the Ministry of Defence or the intelligence services require it. That is what our amendments seek to introduce. If the Bill proceeds unamended, national security certificates would require only very broad details and no information on what data was being processed. It would therefore not be very likely that a tribunal would be able to oppose the decision on the basis of a judicial review.

Victoria Atkins: I have a copy of a live certificate granted by the then Secretary of State, David Blunkett, on 10 December 2001. In the certificate, he sets out in summary the reasons why the certificate has been granted, including:

"The work of the security and intelligence agencies of the Crown requires secrecy."

I assume hon. Members do not disagree with that. Another reason is:

"The general principle of neither confirming nor denying whether the Security Service processes data about an individual, or whether others are processing personal data for, on behalf of with a view to assist or in relation to the functions of the Security Service, is an essential part of that secrecy."

Again, I assume that hon. Members do not disagree with that. As I said, this is a live certificate that has been given to the Information Commissioner, and is in the public domain for people to see and to check should they so wish. Those reasons are given in that certificate.

Louise Haigh: That is wonderful, but the Bill does not require that. It is great that my noble Friend Lord Blunkett put that on his national security application, but the Bill does not require that in law, so I am afraid that it is not a sufficient argument against the amendments that we have tabled.

Victoria Atkins: What we are doing is transposing the requirements of the Data Protection Act 1998 into the Bill. It is difficult to see a situation in which a national security certificate will be granted on the basis that the work of the security and intelligence agencies of the Crown does not require secrecy.

Peter Heaton-Jones (North Devon) (Con): Is there not a bigger, more general overall point here, which is that we should not be considering doing anything in Committee that risks making it more difficult for the security services to protect us? This week of all weeks, surely that should be uppermost in our minds.

Victoria Atkins: Very much so—indeed, this debate ran through the passage of the Investigatory Powers Act 2016, which was one of the most scrutinised pieces of legislation. Senior parliamentarians who served on the Committee on that Act during long careers in this House, including the then Minister, my right hon. Friend the Member for South Holland and The Deepings (Mr Hayes), said that it was an incredibly well scrutinised Bill. There was constant debate about the battle, or tension, between ensuring the national security of our country in the most transparent way possible, and the fact that by definition there has to be some secrecy and confidentiality about the ways in which the security agencies work.

[Victoria Atkins]

What was important in the debates on that Act, as it is in those on the current Bill, was making it clear that the idea that rogue civil servants or security agents can run around with people's information with no checks is very wrong. We are replicating in the Bill the system that has been used for the past 30 years, because we consider that that system has the appropriate and necessary safeguards in the often very fast-moving context of a national security situation.

Louise Haigh: Will the Minister give way?

Victoria Atkins: I will make a little progress, then I will take more interventions.

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

Louise Haigh: Will the Minister give way?

Victoria Atkins: I will give an example first, because I think it is so important. I fear that a bit of misunderstanding has crept in. Let us take the example of a subject access request. Mr Smith asks an intelligence service whether it is processing personal data concerning him and, if so, for information about that data under clause 94. The intelligence service considers whether it is processing personal data, which it will have obtained under its other statutory powers, such as the Regulation of Investigatory Powers Act 2000 or the Investigatory Powers Act 2016.

If the agency determines that it is processing personal data relating to Mr Smith, it then considers whether it is able to disclose the data, or whether a relevant exemption is engaged. For the agency, the key consideration will be whether disclosing the data would damage national security, for example by disclosing sensitive capabilities or alerting Mr Smith to the fact that he is a subject of investigation. If disclosure does not undermine national security and no other exemption is relevant, the intelligence service must disclose the information. However, if national security would be undermined by disclosure, the agency will need to use the national security exemption in relation to processing any personal data relating to Mr Smith.

If the intelligence service does not process any personal data relating to Mr Smith, it will again have to consider whether disclosing that fact would undermine national security, for example by revealing a lack of capability, which could be exploited by subjects of investigation. That is why, on occasion, when such requests are made, a "neither confirm nor deny" response may be necessary, because either confirming or denying may in itself have ramifications, not only in relation to Mr Smith but in relation to other aspects of national security.

Mr Smith may complain to the Information Commissioner about the response to his request for information. The intelligence service may then be required to demonstrate to the commissioner that the processing of personal data complies with the requirements of part four of the Bill, as set out in clause 102, and that it has responded to the request for information appropriately.

If, in legal proceedings, Mr Smith sought to argue that the national security exemption had been improperly relied upon, a national security certificate could be used as conclusive evidence that the national security exemption was required to safeguard national security. Any person who believed they were directly affected by the certificate could of course appeal against it to the upper tribunal, as set out in clause 111.

Liam Byrne (Birmingham, Hodge Hill) (Lab): The Minister is setting out the mechanics of the system with admirable clarity. The point in dispute, though, is not the mechanics of the process but whether the data controller is able—unilaterally, unchecked and unfettered—to seek a national security exemption. Anyone who has worked with the intelligence agencies, either as a Minister or not, knows that they take parliamentary oversight and the defence of parliamentary supremacy extremely seriously.

What we are seeking with this amendment is to ensure that a data controller does not issue a national security certificate unchecked, and that instead there is an element of judicial oversight. The rule of law is important. It should be defended, protected and enhanced, especially when the data collection powers of the intelligence services are so much greater than they were 30 years ago when data protection legislation was first written.

Victoria Atkins: The Government fully accept that national security certificates should be capable of being subject to judicial oversight. Indeed, the current scheme—both under the 1998 Act and this Bill—provides for just that. However, the amendments would radically change the national security certificate regime, because they would replace the existing scheme with one that required a Minister of the Crown to apply to a judicial commissioner for a certificate if an exemption was sought for the purposes of safeguarding national security, and for a decision to issue a certificate to be approved by a judicial commissioner.

This, again, is the debate that we had when we were considering the Investigatory Powers Act 2016. There were some who would have preferred a judicial commissioner to make the decision about warrantry before the Secretary of State. However, Parliament decided that it was not comfortable with that, because it would have meant a great change. For a member of the judiciary to certify on national security issues, rather than a member of the Executive—namely the Prime Minister or a Secretary of State—would have great constitutional implications.

There were great debates about the issue and the House decided, in its wisdom, that it would maintain the constitutional tradition, which is that a member of the Executive has the ultimate responsibility for national

security, with, of course, judicial oversight by judicial commissioners and by the various tribunals that all these powers are subject to. The House decided that the decision itself must be a matter for a Minister of the Crown, because in the event—God forbid—that there is a national security incident, the House will rightly and properly demand answers from the Government of the day. With the greatest respect, a judicial commissioner cannot come to the Dispatch Box to explain how the Government and those assisting them in national security matters have responded to that situation. That is why we have this fine constitutional balance, and why we have adopted in the Bill the regime that has been in place for 30 years.

2.15 pm

We are keen to deal with the point about the Investigatory Powers Act and the obtaining of information. The nature of the conduct carried out in the case of an authorised warrant under the IPA is entirely different from the operation of the national security exemption and the use of national security certificates. Warrants authorise operational activity, which may have an impact on the right to respect for a private life when that is necessary and proportionate for a statutory purpose. They are about obtaining information, not processing it. In the context of the Bill, the application of an exemption would prevent an individual from ascertaining what personal data is being processed by a data controller.

The hon. Member for Sheffield, Heeley mentioned equipment interference, but there are other types of warrantry in the Investigatory Powers Act, such as for interception of communications. That is about the obtaining of information—that can be quite intrusive, which is why Parliament has placed a number of judicial and other oversights on it—but this Bill is about the processing of personal data. It is quite a different thing.

In the impact on the data subject, the national security exemption is similar in kind to the other exemptions in the Bill, which have been approved in the other place and in this Committee's debates thus far.

Louise Haigh: Does the Minister accept that in response to the case of Watson and others against the Government, the Government conceded that additional safeguards, including a far more robust system of independent oversight, were necessary? That test of judicial review is simply not sufficient as oversight. It cannot contest the merits of the case and applies only to the very limited, narrow appeal right of judicial review. It is just not sufficient.

Victoria Atkins: I will come on, if I may, to the judicial review test. I have quite a lot about that.

Darren Jones: Before the Minister does that, will she give way?

Victoria Atkins: I am grateful to have more time for my officials to scribble a response.

Darren Jones: I am happy to help the Minister. She keeps referring to the framework that has been in place for the last 30 years. That has been a time when we have been a member of the European Union. In reviewing this situation, the House of Lords European Union Committee made the point that under the treaty on the functioning of the European Union, there is absolute jurisdiction for national member states to take decisions on national security. That is not an EU area of jurisdiction. The treaty says that we are protected as a member of the EU, but if we leave the European Union we are not protected by that exemption under the treaty. That is why, for third countries, the European Commission looks at the whole legislative framework. Do we not risk the adequacy decision by taking this approach? In the future, we will not have the answer of saying that it is an issue of exemption from the European Commission.

Victoria Atkins: National security must always be a matter for any member state in the EU, but also once we leave the EU. Sorry, I may have misunderstood the hon. Gentleman, but how we deal with national security is, of course, a matter for the state.

Darren Jones: I am happy to clarify for the Minister. The status quo is that the European Union will not look at areas of national security because they are the jurisdiction of member states. When we leave the European Union, the Commission will look at the entirety of legislation around data protection and privacy rights, because there are no exemptions that it needs to take into account. The noble Lords made the point that our

"data protection standards would be assessed without the benefit of the protection afforded by the national security exemption"

under the treaty. Do we not risk our adequacy by taking these exemptions?

Victoria Atkins: No, because those who have drafted the Bill have sought, at all times, to comply with the law enforcement directive and with the modernised, draft Council of Europe convention 108. The Bill very much meets those standards, not just on law enforcement but across parts 3 and 4.

Liam Byrne: I have spoken to the outgoing Council of Europe information commissioner about the issue, and he has put on the record his grave reservations about the regime that we have in place, because we simply do not have the right kind of judicial oversight of the information gathering powers that are now available to our intelligence services. Our intelligence services are very good, and they need to be allowed to do their job, but they will be allowed to do that job more effectively—and without additional risks to our adequacy—if there is some kind of judicial oversight in the right timeframe of the decisions that are taken.

Victoria Atkins: That is where the distinction between obtaining information and processing it is so important. The gathering that the right hon. Gentleman refers to falls under the Investigatory Powers Act 2016. Retaining it and processing it in the ways that the Bill seeks to provide for is the data protection element. The 2016 Act has all the extra judicial oversights that have been passed by the House.

Liam Byrne: Quite helpfully, we are coming to the nub of the question. It is now incumbent on the Minister to lay out for the Committee why the oversight regime for obtaining information should be so remarkably different from the regime for processing it.

Victoria Atkins: The obtaining of information is potentially intrusive and often extremely time-sensitive. For the processing of information, particularly in the case of a subject access request, once we have met the criteria for obtaining it, separate judicial oversight through the upper tribunal is set out in the Bill, as well as ministerial oversight. They are two separate regimes.

There is extra oversight in the 2016 Act because obtaining information can be so intrusive. The right hon. Gentleman will appreciate that I cannot go into the methodology—I am not sure I am security-cleared enough to know, to be honest—but obtaining information has the potential to be particularly intrusive, in a way that processing information gathered by security service officials may not be.

Liam Byrne: I reassure the Minister that I went through the methodologies during my time at the Home Office. The justification that she still needs to lay out for the Committee—she is perhaps struggling to do so—is why there should be one set of judicial oversight arrangements for obtaining information and another for processing it. Why are they not the same?

Victoria Atkins: There might be many reasons why we process information. The end result of processing might be for national security reasons or law enforcement reasons—my officials are scribbling away furiously, so I do not want to take away their glory when they provide me with the answer.

I have an answer on the Watson case, raised by the hon. Member for Sheffield, Heeley, which dealt with the retention of communications by communications service providers. Again, that is an entirely different scenario from the one we are talking about, where the material is held by the security services.

Amendment 161 goes further than the 2016 Act, because it places the decision to issue a certificate with the judicial commissioner. As I have said, national security certificates come into play only to serve in legal proceedings as conclusive evidence that an exemption from specified data protection requirements is necessary to protect national security—for example, to prevent disclosure of personal data to an individual under investigation, when such disclosure would damage national security. The certificate does not authorise the required use of the national security exemption, which is properly a matter for the data controller to determine.

Amendments 163 and 164 relate to the form of a national security certificate. Amendment 163 would require a detailed rather than general description of the data identified on a national security certificate, but we believe this change to be unnecessary and unhelpful, given that much data can be adequately described in a general way. Amendment 164, which would prevent a certificate from having prospective effect, appears to be dependent on the prior judicial authorisation scheme proposed in amendments 161 and 162, and again contrasts with the prospective nature of certificates currently under the Data Protection Act 1998.

Prospective certificates of the type issued under the 1998 Act are the best way of ensuring that the use of the national security exemption by the intelligence services and others is both sufficiently foreseeable for the purposes of article 8 of the European convention on human rights, and accountable. The accountability is ensured by the power to challenge certificates when they are issued, and that is something that has real teeth. The accountability is strengthened by the provision in clause 130 for the publication of certificates. The documents we are discussing will therefore be in the public domain—indeed, many of them are already. But it will now be set out in statute that they should be in the public domain.

Amendments 166 to 168 relate to the appeals process. Amendment 166 would broaden the scope for appealing a national security certificate from a person "directly affected" by it to someone who

"believes they are directly or indirectly affected"

by it. I wonder whether the Opposition did any work on the scope of the provision when drafting it, because the words "indirectly affected" have the potential to cause an extraordinary number of claims. How on earth could that phrase be defined in a way that does not swamp the security services with applications from people who consider that they might be indirectly affected by a decision relating to a national security matter? I do not see how that can be considered practicable.

Louise Haigh: As I have already said, the issue is that the judicial review process for appeal is incredibly narrow and limited. Under section 28 of the DPA, where an individual requests to access his or her data that is subject to a certificate, they will merely be informed that they have been given all the information that is required under the Act. They would not be informed that their data is being withheld on the grounds of a national security certificate. That means that it is impossible for them to know whether they even have the right to appeal under a judicial review, and they do not have the information available to allow them to take that judicial review case forward. That is why the amendment is drafted in this way. If the Minister would like, she can suggest some alternative wording that would solve the problem.

Victoria Atkins: We get to the nub of the problem. Is the hon. Lady seriously suggesting that the security services should notify someone who puts in an access request that they are the subject of an investigation? That is the tension facing the security services. That is why we have internationally met standards, with regard to article 108 of the convention, which the Bill complies with. That is why we have to build in all these safeguards, to try to ensure that those people who intend ill will to this country do not benefit from our natural wish to be as transparent as possible when dealing with people's personal data.

Louise Haigh: I have already explained that there would of course be an exemption for not informing individuals if they were under surveillance or being processed, but there are not sufficient oversights, safeguards or appeals. In the absence of any of those three, the Minister has to accept that there are absolutely no checks and balances on the exemptions listed under the clause.

Victoria Atkins: There most certainly are: they have the right to appeal to the upper tribunal.

Louise Haigh: Under judicial review?

Victoria Atkins: Yes. The upper tribunal reviews the material and applies the judicial review test. Again, we had this debate in relation to the Investigatory Powers Act 2016, which Parliament passed, in relation to the test that applied in the later appeal stages, following the grant of a warrant. This Bill has been drafted to comply with the modernised convention 108 of the Council of Europe. This is why it is in this way. It reflects the past 30 years'-worth of practice but meets international standards as they exist at the moment, which I hope reassures the hon. Member for Bristol North West.

2.30 pm

If someone is the subject of investigation or suspicion, and the security services neither confirm nor deny, when someone who is not under suspicion puts in an application, the great tension for the security services is whether they answer differently in one case from another. In such circumstances that would have ramifications, because people will work out that this answer has been given or this answer has not been given. Of course there is a tension. That is why the exemptions exist and why so much emphasis is placed on the data controller, and that is why it meets the international standard as expected by the modernised Council of Europe convention.

Peter Heaton-Jones: On the specific narrow point, is it not the case that clause 130 already provides for the publication of certificates, so the amendment is simply not necessary? On the wider point—at the risk of repeating my earlier one—I fear that we are at risk of stumbling into a law of unintended consequences where we will make it more difficult for our security services to do the job that we want them to do. While we have been sitting here, I saw on my phone that the international community has recognised that what happened in Salisbury is the first recorded attack using a nerve agent on a European country since 1945. Let us remember that.

Victoria Atkins: That is a particularly sobering development. I know that we all feel the gravity of our responsibilities when considering the Bill in the context of national security today. I am grateful to my hon. Friend.

Matt Warman (Boston and Skegness) (Con): The Minister and I served on the Draft Investigatory Powers Bill Joint Committee and we had many debates on this subject. It struck me that the House was at its best when we passed the Investigatory Powers Bill on Third Reading, with the support of the Labour party, having had these debates. It is frustrating that today of all days, as my hon. Friend says, we should go over that ground again having already reached a useful consensus.

Victoria Atkins: On the judicial review point, the test was debated at length in the Joint Committee, in the Public Bill Committee and on the Floor of the House. The House passed that Act with cross-party consensus, as my hon. Friend has said, so I do not understand why we are having the same debate.

Liam Byrne: Anyone who has spent time working with our intelligence agencies knows that they see their mission as the defence of parliamentary democracy. They believe in scrutiny and oversight, which is what we are trying to insert in the Bill. The reason the Investigatory Powers Bill was passed in that way was because we were successful in ensuring that there were stronger safeguards. The Minister has been unable to explain today why the safeguarding regime should be different for the processing of data as opposed to the obtaining of data. We have heard no convincing arguments on that front today. All that we are seeking to do is protect the ability of the intelligence agencies to do their job by ensuring that a guard against the misuse of their much broader powers is subject to effective judicial oversight, and not in public but in a court.

Victoria Atkins: For the security services to have obtained data under the Investigatory Powers Act, they will have passed through the various safeguards that Parliament set out in that Act. Once that data is obtained, it follows that the permission that the judicial commissioner will have reviewed will still flow through to the processing of that information. Our concern here is certain requirements of the data protection regime. The decision to disseminate information under that regime must rest with the intelligence agencies, with oversight. The Bill provides for those decisions to be appealed. That is as it should be. It should not be for a judicial commissioner to take over the decision of the data controller, who is processing applications and information in real time, often in situations that require them to act quickly. Likewise, whether to grant a certificate, which will be in the public domain, must be a decision for a member of the Executive, not the judiciary.

I assume that no work has been done to measure the scope of amendment 166, but allowing the clause to cover people indirectly affected could have enormous consequences for the security services, which already face great pressures and responsibilities.

Amendments 167 and 168 would remove the application of judicial review principles by the upper tribunal when considering an appeal against a certificate. They would replace the "reasonable grounds for issuing" test with a requirement to consider whether issuing a certificate was necessary and proportionate. Again, that would be an unnecessary departure from the existing scheme, which applies the judicial review test and has worked very well for the past 30 years.

In applying judicial review principles, the upper tribunal can consider a range of issues, including necessity, proportionality and lawfulness. As we set out in our response to the report of the House of Lords Constitution Committee, that enables the upper tribunal to consider matters such as whether the decision to issue the certificate was reasonable, having regard to the impact on the rights of the data subject and the need to safeguard national security. The Bill makes it clear that the upper tribunal has the power to quash the certificate if it concludes that the decision to issue it was unreasonable.

I hope that I have answered the concerns of the right hon. Member for Birmingham, Hodge Hill about how certificates are granted and about the review process when a subject access request is made and the certificate is applied. We must recognise that the Bill does not weaken a data subject's rights or the requirements that must be met if an exemption is to be relied on; it reflects the past 30 years of law. Perhaps I missed it, but I do not think that any hon. Member has argued that the Data Protection Act 1998 has significant failings.

Liam Byrne: As the Minister well knows, the debate internationally is a result of the radical transformation of intelligence agencies' ability to collect and process data. There is an argument, which has been well recognised in the Council of Europe and elsewhere, that where powers are greater, oversight should be stronger.

Victoria Atkins: Yes, and that is precisely why Parliament passed the Investigatory Powers Act 2016.

Liam Byrne: It is about obtaining information, not processing it.

Victoria Atkins: The safeguards that apply once the information has been obtained—

Liam Byrne: There aren't any safeguards!

The Chair: Order. I realise that the right hon. Gentleman feels strongly about the issue, but if he wishes to intervene, he must stand. If not, he must remain quiet and take it on the chin.

Victoria Atkins: The Government have listened to the concerns of the House of Lords. We added clause 130 in the Lords to provide for the publication of national security certificates by the Information Commissioner, so that they would be easily accessible to anyone who wished to mount a subject access request, and could be tested accordingly. In her briefing to noble Lords about the Bill, the Information Commissioner said that the clause was

"very welcome as it should improve regulatory scrutiny and foster greater public trust and confidence in the use of national security certificate process."

It will also ensure that any person who believes that they are directly affected by a certificate will be better placed to exercise their appeal rights.

The Bill's approach to national security certificates is tried and tested. We rely on those 30 years of experience of the regime being in place. In her written submission to the Committee, the Information Commission has not raised any issues in respect of the provisions in clause 27.

I hope that I have reassured the hon. Member for Sheffield, Heeley. I suspect from the interventions that she may well press the amendment to a vote, but I invite her to withdraw it. We have scrutinised this matter, and the Government are clear that the Bill reflects the past 30 years of the regime. It has worked and the Information Commissioner has not raised any concerns about clause 27.

Louise Haigh: I am afraid that the Minister is correct; she has not reassured Opposition Members. The amendment is not about putting obstacles in the way of our intelligence agencies going about their operational capabilities—that is the last thing we want to do—but the Minister has been unable to give us a clear argument as to why there should be stronger safeguards on the collection of data than on processing. That the Home Office would like to have the data is not a sufficient argument.

Victoria Atkins: Please do not trivialise the matter. It is not the case that the Home Office would like the data; this is national security. This is the regime that our security services use at the moment. It is the regime they need. That is why the Government are pressing the issue. Again, I would have thought that this week of all weeks is the week to back our security services, not to put more barriers in their way.

Louise Haigh: The intelligence agencies, as my right hon. Friend the Member for Birmingham, Hodge Hill has said, take parliamentary oversight and scrutiny seriously. The safeguards and oversights are not built into the Bill in the way they were in the Investigatory Powers Act 2016. There is no clear argument why those safeguards should be in place for collection, but not for processing. The Minister has constantly relayed that that decision is based on 30 years'-worth of data but, as has already been said, the scope for the collection and processing of data is so far transformed, even from when the Data Protection Act was written in 1998, that the oversights and safeguards need to be transformed as well. That is why we are proposing these amendments.

The Joint Committee on Human Rights has suggested that the exemptions put forward in the Bill are not legal and introduce arbitrary interferences into people's privacy rights. It is this Committee's responsibility to ensure that the amendments pass. That is not trivialising the issue, but ensuring that there is a proper debate about security and the individual's data subject rights. That is why we will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 10.

Division No. 7]

AYES

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

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 27 ordered to stand part of the Bill.

The Chair: Members will note that there are a number of clauses on the selection list to which no amendments have been tabled. I propose to start grouping such clauses together in order to speed progress. However, Members still have the right to tell me that they wish to speak to, or vote on, an individual clause.

Clauses 28 and 29 ordered to stand part of the Bill.

Clause 30

Meaning of "competent authority"

Amendments made: 18, in clause 30, page 19, line 4, after "specified" insert "or described".

This amendment changes a reference to persons specified in Schedule 7 into a reference to persons specified or described there.

Amendment 19, in clause 30, page 19, line 10, leave out from "add" to end of line and insert

"or remove a person or description of person".—*(Margot James.)*

This amendment makes clear that regulations under Clause 30 may identify a person by describing a type of person, as well as by specifying a person.

Clause 30, as amended, ordered to stand part of the Bill.

Schedule 7 agreed to.

Clauses 31 to 34 ordered to stand part of the Bill.

Clause 35

THE FIRST DATA PROTECTION PRINCIPLE

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

Liam Byrne: Very briefly, subsection (1) includes the phrase

"must be lawful and fair".

Could the Minister say a little more about the word "fair"? What definition is she resting on, and who is the judge of it?

Victoria Atkins: "Lawful" means any processing necessary to carry out a particular task, where that task is authorised either by statute or under common law. It would cover, for example, the taking and retention of DNA and fingerprints under the Police and Criminal Evidence Act 1984, or the police's common law powers to disclose information required for the operation of the domestic violence disclosure scheme.

The Government recognise the importance of safeguarding sensitive personal information about individuals. Subsections (3) to (5) therefore restrict the processing of sensitive data, the definition of which includes information about an individual's race or ethnic origin, and biometric data such as their DNA profile and fingerprints.

Further safeguards for the protection of sensitive personal data are set out in clause 42. The processing of sensitive personal data is permitted under two circumstances. The first is where the data subject has given his or her consent. The second is where the processing is strictly necessary for a law enforcement purpose and one or more of the conditions in schedule 8 to the Bill has been met. Those conditions include, for example, that the processing is necessary to protect the individual concerned or another person, or is necessary for the administration of justice. In both cases, the controller is required to have an appropriate policy document in place. We will come on to the content of such policy documents when we debate clause 42.

Liam Byrne: I am grateful for the Minister's extensive definition, given in response to a question I did not ask. I did not ask for the definition of "lawful" but for the definition of "fair".

Victoria Atkins: I am so sorry; I thought it was apparent from my answer. "Fair" is initially a matter for the data controller, but ultimately the Information Commissioner has oversight of these provisions and the commissioner will cover that in her guidance.

Question put and agreed to.

Clause 35 accordingly ordered to stand part of the Bill.

Schedule 8

CONDITIONS FOR SENSITIVE PROCESSING UNDER PART 3

Amendment made: 116, in schedule 8, page 184, line 32, 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 8 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 117.

Schedule 8, as amended, agreed to.

Clauses 36 to 40 ordered to stand part of the Bill.

Clause 41

SAFEGUARDS: ARCHIVING

Amendment made: 20, in clause 41, page 23, line 34, leave out "an individual" and insert "a data subject".—*(Victoria Atkins.)*

Clause 41 makes provision about the processing of personal data for archiving purposes, for scientific or historical research purposes or for statistical purposes. This amendment aligns Clause 41(2)(b) with similar provision in Clause 19(2).

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

Liam Byrne: We had a good debate on what I think was a shared objective across the Committee: to ensure that those running our big national archives—whether they are large or small organisations—should not be jeopardised by frivolous claims or, indeed, a multiplicity of claims from individuals who might seek to change the records held there in one way or another. I mentioned

[Liam Byrne]

to the Minister in an earlier debate that we were anxious, despite the reassurances she sought to give the Committee, that a number of organisations, including the BBC, were deeply concerned about the Bill's impact on their work. They were not satisfied that the exemptions and safeguards in the Bill would quite do the job.

My only reason for speaking at this stage is to suggest to Ministers that if they were to have discussions with some of those organisations about possible Government amendments on Report to refine the language, and provide some of the reassurance people want, that would attract our support. We would want to have such conversations, but it would be better if the Government could find a way to come forward with refinements of their own on Report.

Victoria Atkins: I am happy to explore that. The reason for the clause is to enable processing to be done to create an archive for scientific or historical research, or for statistical purposes. The reason law enforcement is mentioned is that it may be necessary where a law enforcement agency needs to review historic offences, such as allegations of child sexual exploitation. I would of course be happy to discuss that with the right hon. Gentleman to see whether there are further avenues down which we should proceed.

Liam Byrne: I am grateful to the Minister for that response. I am happy to write to her with the representations that we have received, and perhaps she could reflect on those and write back.

Question put and agreed to.

Clause 41, as amended, accordingly ordered to stand part of the Bill.

Clause 42

SAFEGUARDS: SENSITIVE PROCESSING

Amendment made: 21, in clause 42, page 24, line 29, leave out "with the day" and insert "when".—*(Victoria Atkins.)*

This amendment is consequential on Amendment 71.

Clause 42, as amended, ordered to stand part of the Bill.

Clauses 43 to 46 ordered to stand part of the Bill.

Clause 47

RIGHT TO ERASURE OR RESTRICTION OF PROCESSING

Victoria Atkins: I beg to move amendment 22, in clause 47, page 28, line 20, leave out second "data".

This amendment changes a reference to a "data controller" into a reference to a "controller" (as defined in Clauses 3 and 32).

I can be brief, because this drafting amendment simply ensures that clause 47, as with the rest of the Bill, refers to a "controller" rather than a "data controller". For the purposes of part 3, a controller is defined in clause 32(1) so it is not necessary to refer elsewhere to a "data controller".

Amendment 22 agreed to.

Clause 47, as amended, ordered to stand part of the Bill.

Clause 48 ordered to stand part of the Bill.

Clause 49

RIGHT NOT TO BE SUBJECT TO AUTOMATED DECISION-MAKING

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

Liam Byrne: We had a good debate on possible amendments to the powers of automatic decision making earlier and this is an important clause in that it creates a right not to be subject to automated decision making. Clause 49(1) states:

"A controller may not take a significant decision based solely on automated processing unless that decision is required or authorised by law."

I hope Ministers recognise that

"required or authorised by law"

is an incredibly broad set of questions. I would like to provoke the Minister into saying a little more about what safeguards she believes will come into place to ensure that decisions are not taken that jeopardise somebody's human rights and their right to appeal and justice based on those human rights. It could be that the Minister decides to answer those questions in the debate on clause 50, but it would be useful for her to say a little more about her understanding of the phrase "significant decision" and a little more about what kind of safeguards will be needed to ensure that decisions that are cast in such a broad way do not impact on people in a negative way.

Victoria Atkins: Clause 49 establishes the right for individuals not to be subject to a decision based exclusively on automated processing, where that decision has an adverse impact on the individual. It is important to protect that right to enhance confidence in law enforcement processing and safeguard individuals against the risk that a potentially damaging decision is taken without human intervention. The right hon. Gentleman asked about the definition of a significant decision. It is set out in the Bill.

We are not aware of any examples of the police solely using automated decision-making methods, but there may be examples in other competent authorities. The law enforcement directive includes that requirement, so we want to transpose it faithfully into statute, and we believe we have captured the spirit of the requirement.

3 pm

Louise Haigh: There is the example of Durham police force—an excellent police force in many regards—using automated decision making to decide who does and does not remain in custody, and when people receive their charge. A human is involved in that decision-making process at the moment, but the Bill would enable that to be taken away and allow it to be done purely on an automated basis. I am sure the Minister understands our concerns about removing humans from that decision-making process.

Victoria Atkins: I have to say that I am not familiar with that example. I look to my officials—

The Chair: Order. The hon. Lady has on a number of occasions referred to her officials. She should remember at all times that, as far as the Committee is concerned, there are no officials in this room, even though self-evidently there are.

Victoria Atkins: I wonder whether that is captured in the spirit of the Bill. Forgive me, Mr Hanson. This is my first Bill Committee as a Minister and I was not aware of that. Many apologies.

I am not familiar with that example. It would be a very interesting exercise under the PACE custody arrangements. I will look into it in due course. These protections transpose the law enforcement directive, and we are confident that they meet those requirements.

Question put and agreed to.

Clause 49 accordingly ordered to stand part of the Bill.

Clause 50

AUTOMATED DECISION-MAKING AUTHORISED BY LAW: SAFEGUARDS

Amendments made: 23, in clause 50, page 30, line 11, leave out "21 days" and insert "1 month".

Clause 50(2)(b) provides that where a controller notifies a data subject under Clause 50(2)(a) that the controller has taken a "qualifying significant decision" in relation to the data subject based solely on automated processing, 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 24, in clause 50, page 30, line 17, leave out "21 days" and insert "1 month".—*(Victoria Atkins.)*

Clause 50(3) provides that where a data subject makes a request to a controller under Clause 50(2)(b) 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.

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

Liam Byrne: I remain concerned that the safeguards the Government have proposed to ensure people's human rights are not jeopardised by the use of automated decision making are, frankly, not worth the paper they are written on. We know that prospective employers and their agents use algorithms and automated systems to analyse very large sets of data and, through the use of artificial intelligence and machine learning, make inferences about whether people are appropriate to be considered to be hired or retained by a particular company. We have had a pretty lively debate in this country about the definition of a worker, and we are all very grateful to Matthew Taylor for his work on that question. Some differences emerged, and the Business, Energy and Industrial Strategy Committee has put its views on the record.

The challenge is that our current labour laws, which were often drafted decades ago, such as the Sex Discrimination Act 1975 and the Race Relations Act 1965, are no longer adequate to protect people in this new world, in which employers are able to use such large and powerful tools for gathering and analysing data, and making decisions.

We know that there are problems. We already know that recruiters use Facebook to seek candidates in a way that routinely discriminates against older workers by targeting job advertisements. That is not a trivial issue; it is being litigated in the United States. In the United Kingdom, research by Slater and Gordon, a group of employment lawyers, found that one in five bosses admits to unlawful discrimination when advertising jobs online. Women and people over 50 are most likely to be stopped from seeing an advert. Around 32% of company executives admitted to discriminating among those over 50; 23% discriminated against women; and 62% of executives who had access to profiling tools admitted to using them to actively seek out people based on criteria such as age, gender and race. Female Uber drivers earn 7% less than men when pay is determined by algorithms. A number of practices in the labour market are disturbing and worrying, and they should trouble all of us.

The challenge is that clause 50 needs to include a much more comprehensive set of rights and safeguards. It should clarify that the Equality Act 2010 and protection from discrimination applies to all new forms of decision making that engage core labour rights around recruitment, terms of work or dismissal. There should be new rights about algorithmic fairness at work to ensure equal treatment where an algorithm or automated system takes a decision that impinges on someone's rights. There should be a right to explanation where significant decisions are taken based on an algorithm or an automated decision. There is also a strong case to create a duty on employers, if they are a large organisation, to undertake impact assessments to check whether they are, often unwittingly, discriminating against people in a way that we think is wrong.

Over the last couple of weeks, we have seen real progress in the debate about gender inequalities in pay. Many of us will have looked in horror at some of the news that emerged from the BBC and at some of the evidence that emerged from ITV and *The Guardian.* We have to contend with the reality that automated decision-making processes are under way in the labour market that could make inequality worse rather than better. The safeguards that we have in clause 50 do not seem up to the job.

I hope the Minister will say a bit more about the problems that she sees with future algorithmic decision making. I am slightly troubled that she is unaware of some live examples in the Home Office space in one of our most successful police forces, and there are other examples that we know about. Perhaps the Minister might say more about how she intends to improve the Bill with regard to that issue between now and Report.

Victoria Atkins: I will pick up on the comments by the right hon. Gentleman, if I may.

In the Durham example given by the hon. Member for Sheffield, Heeley, I do not understand how a custody sergeant could sign a custody record without there being any human interaction in that decision-making process. A custody sergeant has to sign a custody record and to review the health of the detainee and whether they have had their PACE rights. I did not go into any details about it, because I was surprised that such a situation could emerge. I do not see how a custody sergeant could be discharging their duties under the Police and Criminal Evidence Act 1984 if their decision as to custody was based solely on algorithms, because a custody record has to be entered.

Louise Haigh: I thank the Minister for allowing me to clarify. I did not say that it was solely an algorithmic decision already. Durham is using an algorithm known as the harm assessment risk tool. A human makes a decision based on the algorithm's recommendations. The point I was making was that law enforcement is using algorithms to make very important decisions that limit an individual's right to freedom, let alone the right to privacy or anything else, but the Bill will enable law

[Louise Haigh]

enforcement to take that further. I appreciate what the Minister is saying about PACE and the need for a custody sergeant, but the Bill will enable law enforcement to take that further and to remove the human right—

Victoria Atkins: This has been a moment of genuine misunderstanding. Given how the hon. Lady presented that, to me it sounded as if she was saying that the custody record and the custody arrangements of a suspect—detaining people against their will in a police cell—was being done completely by a computer. That was how it sounded. There was obviously an area of genuine misunderstanding, so I am grateful that she clarified it. She intervened on me when I said that we were not aware of any examples of the police solely using automated decision making—that is when she intervened, but that is not what she has described. A human being, a custody sergeant, still has to sign the record and review the risk assessment to which the hon. Lady referred. The police are using many such examples nowadays, but the fact is that a human being is still involved in the decision-making process, even in the issuing of penalties for speeding. Speeding penalties may be automated processes, but there is a meaningful element of human review and decision making, just as there is with the custody record example she gave.

There was a genuine misunderstanding there, but I am relieved, frankly, given that the right hon. Member for Birmingham, Hodge Hill was making points about my being unaware of what is going on in the Home Office. I am entirely aware of that, but I misunderstood what the hon. Lady meant and I thought she was presenting the custody record as something that is produced by a machine with no human interaction.

Liam Byrne: Will the Minister give way?

Victoria Atkins: No, with respect—

Liam Byrne: This is a Bill Committee, line-by-line scrutiny.

Victoria Atkins: Line-by-line scrutiny, but I was acting in good faith on an intervention that the hon. Member for Sheffield, Heeley made when I was talking about any examples of the police solely using automated decision making.

Liam Byrne: On a point of order, Mr Hanson.

The Chair: I hope it is, Mr Byrne.

Liam Byrne: May I ask for your guidance on this question? We are in a Bill Committee that is tasked with scrutinising the Bill line by line. Is it customary for Ministers to refuse to give way on a matter of detail?

The Chair: Ultimately, whether the Minister gives way is a matter for the Minister—that is true for any Member who has the Floor—but it is normal practice to debate aspects of legislation thoroughly. Ultimately, however, it remains the choice of the Minister or any other Member with the Floor whether to give way.

Victoria Atkins: I think it is fair to say that I have given way on interventions, but the right hon. Gentleman seemed to be seeking to argue with me as to my understanding of what his colleague, the hon. Member for Sheffield, Heeley, had said. Frankly, that is a matter for me to understand.

The Chair: Order. We are debating clause 50 of the Bill, so may I suggest that in all parts of the Committee we focus our minds on the clause?

Victoria Atkins: I am grateful—

Liam Byrne: Will the Minister give way on that point?

Victoria Atkins: I have lost track of which point the right hon. Gentleman wants me to give way on.

Liam Byrne: Let me remind the Minister. What we are concerned about on the question of law enforcement is whether safeguards that are in place will be removed under the Bill. That is part and parcel of a broader debate that we are having about whether the safeguards that are in the Bill will be adequate. So let me return to the point I made earlier to the Minister, which is that we would like her reflections on what additional safeguards can be drafted into clauses 50 and 51 before Report stage.

Victoria Atkins: Clause 49 is clear that individuals should not be subject to a decision based solely on automated processing if that decision significantly or adversely has an impact on them, legally or otherwise, unless required by law. If that decision is required by law, clause 50 specifies the safeguards that controllers should apply to ensure that the impact on the individual is minimised. Critically, that includes informing the data subject that a decision has been taken and giving that individual 21 days in which to ask the controller to reconsider the decision, or to retake the decision with human intervention.

A point was made about the difference between automated processing and automated decision making. Automated processing is when an operation is carried out on personal data using predetermined fixed parameters that allow for no discretion by the system and do not involve further human intervention in the operation to produce a result or output. Such processing is used regularly in law enforcement to filter large datasets down to manageable amounts for a human operator to use. Automated decision making is a form of automated processing that allows the system to use discretion, potentially based on algorithms, and requires the final decision to be made without human interference. The Bill seeks to clarify that, and the safeguards are set out in clause 50.

Question put and agreed to.

Clause 50, as amended, accordingly ordered to stand part of the Bill.

Clause 51

Exercise of rights through the Commissioner

3.15 pm

Victoria Atkins: I beg to move amendment 25, in clause 51, page 31, line 2, leave out from first "the" to end of line 3 and insert

"restriction imposed by the controller was lawful;".

This amendment changes the nature of the request that a data subject may make to the Commissioner in cases where rights to information are restricted under Clause 44(4) or 45(4). The effect is that a data subject will be able to request the Commissioner to check that the restriction was lawful.

The Chair: With this it will be convenient to discuss Government amendment 26.

Victoria Atkins: These technical amendments are required to ensure that the provisions in clause 51 do not inadvertently undermine criminal investigations by the police or other competent authorities. Under the Bill, where a person makes a subject access request, it may be necessary for the police or other competent authority to give a "neither confirm nor deny" response, for example in order to avoid tipping someone off that they are under investigation for a criminal offence. In such a case, the data subject may exercise their rights under clause 51 to ask the Information Commissioner to check that the processing of their personal data complies with the provisions in part 3. It would clearly undermine a "neither confirm nor deny" response to a subject access request if a data subject could use the provisions in part 3 to secure confirmation that the police were indeed processing their information.

It is appropriate that the clause focuses on the restriction of a data subject's rights, not on the underlying processing. The amendments therefore change the nature of the request that a data subject may make to the commissioner in cases where rights to information are restricted under clause 44(4) or clause 45(4). The effect of the amendments is that a data subject will be able to ask the commissioner to check that the restriction was lawful. The commissioner will then be able to respond to the data subject in a way that does not undermine the original "neither confirm nor deny" response.

Liam Byrne: This is a significant amendment—I understand the ambition behind the clause—so it is worth dwelling on it for a moment. I would like to check my understanding of what the Minister said. In a sense, if an investigation is under way and the individual under investigation makes a subject access request to the police and gets a "neither confirm nor deny" response, the data subject will be able to ask the Information Commissioner to investigate. Will the Minister say a little more about what message will go from the police to the Information Commissioner and the content of the message that will go from the Information Commissioner to the data subject? I have worked on such cases in my constituency. Often, there is an extraordinary spiral of inquiries and the case ultimately ends up in a judicial review in court. Will the Minister confirm that I have understood the mechanics accurately and say a little more about the content of the messages from the police to the Information Commissioner and from the Information Commissioner to the person who files the request?

Victoria Atkins: I can help the right hon. Gentleman in one respect: he has understood the mechanics. I am afraid that I cannot give him examples, because it will depend on the type of criminal offence or the type of investigation that may be under way. I cannot possibly give him examples of the information that may be sent by the police to the Information Commissioner, because that will depend entirely on the case that the police are investigating.

Liam Byrne: Perhaps I can pose the question in a sharper way. I do not think that is entirely the case. It must be possible for the Minister to be a little more specific, and perhaps a little more knowledgeable, about the content of the message that will go from the Information Commissioner to the data subject. Will that be a standard message? Will it be in any way detailed? Will it reflect in any way on the information that the police provide? Or will it simply be a blank message such as "I, the Information Commissioner, am satisfied that your information has been processed lawfully"? I do not think the Information Commissioner is likely to ask for too much detail about the nature of the offence, but she will obviously ask whether data has been processed lawfully. She will want to make checks in that way. Unless the Information Commissioner is able to provide some kind of satisfactory response to the person who has made the original request, we will end up with an awful administrative muddle that will take of lot of the courts' time. Perhaps the Minister could put our minds at rest on that.

Victoria Atkins: The Information Commissioner will get the information but, by definition, she does not give that information to the subject, because law enforcement will have decided that it meets the criteria for giving a "neither confirm nor deny" response from their perspective. The commissioner then looks at the lawfulness of that; if she considers it to be lawful, she will give the same response—that the processing meets part 3 obligations.

Amendment 25 agreed to.

Amendment made: 26, in clause 51, page 31, line 11, leave out from first "the" to end of line 12 and insert "restriction imposed by the controller was lawful;"—*(Victoria Atkins.)*

This amendment is consequential on Amendment 25.

Clause 51, as amended, ordered to stand part of the Bill.

Clause 52 ordered to stand part of the Bill.

Clause 53

Manifestly unfounded or excessive requests by the data subject

Amendments made: 27, in clause 53, page 31, line 39, leave out "or 47" and insert ",47 or 50".

Clause 53(1) provides that where a request from a data subject under Clause 45, 46 or 47 is manifestly unfounded or excessive, the controller may charge a reasonable fee for dealing with the request or refuse to act on the request. This amendment applies Clause 53(1) to requests under Clause 50 (automated decision making). See also Amendment 28.

Amendment 28, in clause 53, page 32, line 4, leave out "or 47" and insert ",47 or 50".—*(Victoria Atkins.)*

Clause 53(3) provides that where there is an issue as to whether a request under Clause 45, 46 or 47 is manifestly unfounded or excessive, it is for the controller to show that it is. This amendment applies Clause 53(3) to requests under Clause 50 (automated decision making). See also Amendment 27.

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

Liam Byrne: We have just agreed a set of amendments that, on the face of it, look nice and reasonable. We can all recognise the sin that the Government are taking aim at, and that the workload of the Information Commissioner's Office and of others has to be kept under control, so we all want to deter tons of frivolous and meaningless requests. None the less, a lot of us have noticed that, for example, the introduction of fees for industrial tribunals makes it a lot harder for our constituents to secure justice.

[Liam Byrne]

I wonder, having now moved the amendment successfully, whether the Minister might tell us a little more about what will constitute a reasonable fee and what will happen to those fees. Does she see any relationship between the fees being delivered to her Majesty's Government and the budget that is made available for the Information Commissioner? Many of us are frankly worried, given the new obligations of the Information Commissioner, about the budget she has to operate with and the resources at her disposal. Could she say a little more, to put our minds at rest, and reassure us that these fees will not be extortionate? Where sensible fees are levied, is there some kind of relationship with the budget that the Information Commissioner might enjoy?

Victoria Atkins: Clause 35 establishes the principle that subject access requests should be provided free of charge in most cases. That will be the default position in most cases. In terms of the fees, that will not be a matter to place in statute; certainly, I can write to the right hon. Gentleman with my thoughts on how that may develop. The intention is that in the majority of cases, there will be no charge.

Question put and agreed to.

Clause 53, as amended, accordingly ordered to stand part of the Bill.

Clause 54

MEANING OF "APPLICABLE TIME PERIOD"

Amendments made: 29, in clause 54, page 32, line 14, leave out "day" and insert "time".

This amendment is consequential on Amendment 71.

Amendment 30, in clause 54, page 32, line 15, leave out "day" and insert "time".—*(Victoria Atkins.)*

This amendment is consequential on Amendment 71.

Clause 54, as amended, ordered to stand part of the Bill.

Clauses 55 to 63 ordered to stand part of the Bill.

Clause 64

DATA PROTECTION IMPACT ASSESSMENT

Louise Haigh: I beg to move amendment 142, in clause 64, page 37, line 2, leave out "is likely to" and insert "may".

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

Amendment 143, in clause 64, page 37, line 2, leave out "high".

Amendment 144, in clause 64, page 37, line 15, leave out "is likely to" and insert "may".

Amendment 145, in clause 64, page 37, line 15, leave out "high".

Amendment 146, in clause 65, page 37, line 19, leave out subsection (1) and insert—

"(1) This section applies where a controller intends to—

(a) create a filing system and process personal data forming part of it, or

(b) use new technical or organisational measures to acquire, store or otherwise process personal data."

Amendment 147, in clause 65, page 37, line 23, leave out "would" and insert "could".

Amendment 148, in clause 65, page 37, line 23, leave out "high".

Amendment 149, in clause 65, page 37, line 44, at end insert—

"(8) If the Commissioner is not satisfied that the controller or processor (where the controller is using a processor) has taken sufficient steps to remedy the failing in respect of which the Commissioner gave advice under subsection (4), the Commissioner may exercise powers of enforcement available to the Commissioner under Part 6 of this Act."

New clause 3—*Data protection impact assessment: intelligence services processing—*

"(1) Where a type of processing proposed under section 103(1) may result in a risk to the rights and freedoms of individuals, the controller must, prior to the processing, carry out a data protection impact assessment.

(2) A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.

(3) A data protection impact assessment must include the following—

(a) a general description of the envisaged processing operations;

(b) an assessment of the risks to the rights and freedoms of data subjects;

(c) the measures envisaged to address those risks;

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Part, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing could result in a risk to the rights and freedoms of individuals, the controller must take into account the nature, scope, context and purposes of the processing."

New clause 4—*Prior consultation with the Commissioner: intelligence services processing—*

"(1) This section applies where a controller proposes that a particular type of processing of personal data be carried out under section 103(1).

(2) The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section [Data protection impact assessment: intelligence services processing] indicates that the processing of the data could result in a risk to the rights and freedoms of individuals (in the absence of measures to mitigate the risk).

(3) Where the controller is required to consult the Commissioner under subsection (2), the controller must give the Commissioner—

(a) the data protection impact assessment prepared under section [Data protection impact assessment: intelligence services processing], and

(b) any other information requested by the Commissioner to enable the Commissioner to make an assessment of the compliance of the processing with the requirements of this Part.

(4) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe any provision of this Part, the Commissioner must provide written advice to the controller and, where the controller is using a processor, to the processor.

(5) The written advice must be provided before the end of the period of 6 weeks beginning with receipt of the request for consultation by the controller or the processor.

(6) The Commissioner may extend the period of 6 weeks by a further period of one month, taking into account the complexity of the intended processing.

(7) If the Commissioner extends the period of 6 weeks, the Commissioner must—

(a) inform the controller and, where applicable, the processor of any such extension before the end of the period of one month beginning with receipt of the request for consultation, and

(b) provide reasons for the delay.

(8) If the Commissioner is not satisfied that the controller or processor (where the controller is using a processor) has taken sufficient steps to remedy the failing in respect of which the Commissioner gave advice under subsection (4), the Commissioner may exercise powers of enforcement available to the Commissioner under Part 6 of this Act."

Louise Haigh: The amendments in my name, and in the names of my right hon. and hon. Friends, are all designed to strengthen the requirement to conduct impact assessments, and to require permission from the Information Commissioner for the purposes of data processing for law enforcement agencies. Impact assessments are a critical feature of the landscape of data protection, particularly where new technology has evolved. It is vital that we have in place enabling legislation and protective legislation to cover new technologies and new methods of data collection and processing.

Since the introduction of the Data Protection Act 1998, the advance of technology has considerably increased the ability of organisations to collect data, as we have discussed. The impact assessment as envisaged allows for an assessment to be conducted where there are systematic and extensive processing activities, including profiling, and where decisions have legal effects, or similarly significant effects, on individuals. In addition, an assessment can be conducted where there is large-scale processing of special categories of data, or personal data in relation to criminal convictions or offences, and where there is a high risk to rights and freedoms—for example, based on the sensitivity of the processing activity.

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

Facial recognition surveillance was mentioned in Committee on Tuesday. The Minister was right to say that it is being trialled by the Metropolitan police, but it has been trialled for three years running. I suggest that it is no longer a trial. It is also being used by South Wales police and other police forces across the country, particularly when policing large events. The Metropolitan police use it in particular for Notting Hill carnival.

In September last year, the Policing Minister made it clear in response to a written question that there is no legislation regulating the use of CCTV cameras with facial recognition. The Protection of Freedoms Act 2012 introduced the regulation of overt public space surveillance cameras. As a result, the surveillance camera code of practice was issued by the Secretary of State in 2013. However, there is no reference to facial recognition in the Act, even though it provides the statutory basis for public space surveillance cameras.

Neither House of Parliament has ever considered or scrutinised automated facial recognition technology. To do so after its deployment—after three years of so-called trialling by the Metropolitan police—is unacceptable, particularly given the technology's significant and unique impact on rights. The surveillance camera commissioner has noted that "clarity regarding regulatory responsibility" for such facial recognition software is "an emerging issue". We urgently need clarity on whether the biometric commissioner, the Information Commissioner or the surveillance camera commissioner has responsibility for this use of technology. Our amendments suggest that the Information Commissioner should have scrutiny powers over this, but if the Minister wants to tell me that it should be any of the others, we will be happy to support that.

3.30 pm

Clearly, there needs to be some scrutiny of this very important and invasive technology, which provides recommendations to law enforcement agencies to act, to stop and search and, potentially, to detain people. There are still no answers as to what databases law enforcement agencies are matching faces against, what purposes the technology can and cannot be used for, what images are captured and stored, who can access those images and how long they are stored for.

In 2013, the Government said that the Home Office would publish a forensics and biometrics strategy. Five years on, that strategy has still not been published. The deadline has been missed by quite some time. I appreciate that they have said that they will publish it by June 2018, but in the meantime many of these emerging technologies are being used with absolutely no oversight and, as the Minister said, no legal basis. That simply cannot be acceptable.

There are other issues with the use of facial recognition technology. It is used extensively in the United States, and several studies have found that commercial facial recognition algorithms have in-built biases and issues around demographic accuracy. In particular, they are more likely to misidentify women and black people. That might be because of bias coded into the software by programmers, or it might be because of an underrepresentation of people from black and minority ethnic backgrounds and women in the training datasets. Either way, the technology that the police are currently using in this country has not been tested against such biases.

Surely that testing is urgently needed when we consider the issues that the Home Secretary and the Prime Minister have tried to tackle around the disproportionate use of stop-and-search powers against black and minority ethnic populations, and the issues around trust in the police that that has engendered. Why are we not concerned about the same issues with this very invasive technology that could recreate those exact same biases?

The facial recognition software used by the South Wales police has not been tested against those biases either, but this is not just about facial recognition software. Significant technologies and algorithms are being used by law enforcement agencies across the country. We have already discussed the algorithm used to make

recommendations on custody. Automatic number plate recognition has been rolled out across many forces—we will discuss a code of practice for that when we come to a later amendment. Fingerprint-scanning mobile devices have recently been rolled out across West Yorkshire police. I mentioned earlier, in relation to another amendment, that South Yorkshire police is now tagging individuals who frequently go missing.

It was brought to my attention this morning that South Yorkshire police and Avon and Somerset police have a technology that allows them to track the movements of mobile phone users within a given area and intercept texts and calls. These are called international mobile subscriber identity—IMSI—catchers. They mimic cell towers, which mobile phones connect to in order to make and receive phone calls and text messages. When they are deployed, every mobile phone within an 8 sq km area will try to connect to the dummy tower. The IMSI catchers will then trace the location and unique IMSI number of each phone, which can then be used to identify and track people.

Those are all worrying invasions into the privacy of individuals who have not been identified by the police as being about to commit criminal activity, nor are wanted by the police or law enforcement agencies. In that last example, they are just people who happen to be within the 8 sq km area in which the police would like to track and intercept people's phones.

It may be that every one of those technologies is being used proportionately and necessarily, and that we would all be happy about the way that they are being used. However, if there is no basis in law and no commissioner overseeing the use of these technologies, and if Parliament has never discussed them, surely this is the opportunity to ensure that that happens, to give people confidence that the police and other enforcement agencies will be using them proportionately and not excessively.

Furthermore, the police national database currently contains over 21 million images of individuals, over 9 million of whom have never been charged or convicted of any offence. The biometrics commissioner has already said that it is completely unacceptable for the Home Office to retain those images when it has no good reason to do so. Doing so would also be a clear breach of clause 47, which covers the right to erasure, when there is no reasonable need for the police national database to contain those images. That raises issues around facial recognition software, because if we are matching people's faces against a database where there is no legal right for those faces to be held, that would already be a breach of the Bill as un-amended.

I hope the Minister will accept that there are good reasons for these amendments or, if she can, assure me that these existing and emerging technologies will be covered by the Bill, and that a relevant commissioner will oversee this, both before any technology or new method of data collection and data processing is rolled out by law enforcement, and afterwards, when an individual's data rights have been potentially abused. We need clear principles around what purposes any of these technologies can or cannot be used for, what data is captured and stored, who can access that data, how long it is stored for and when it is deleted. I am not convinced that the Bill as it stands protects those principles.

Liam Byrne: I rise briefly to support my hon. Friend's excellent speech. The ambition of Opposition Members on the Committee is to ensure that the Government have in place a strong and stable framework for data protection over the coming years. Each of us, at different times in our constituencies, have had the frustration of working with either local police or their partners and bumping into bits of regulation or various procedures that we think inhibit them from doing their job. We know that at the moment there is a rapid transformation of policing methods. We know that the police have been forced into that position, because of the pressure on their resources. We know that there are police forces around the world beginning to trial what is sometimes called predictive policing or predictive public services, whereby, through analysis of significant data patterns, they can proactively deploy police in a particular way and at a particular time. All these things have a good chance of making our country safer, bringing down the rate of crime and increasing the level of justice in our country.

The risk is that if the police lack a good, clear legal framework that is simple and easy to use, very often sensible police, and in particular nervous and cautious police and crime commissioners, will err on the side of caution and actually prohibit a particular kind of operational innovation, because they think the law is too muddy, complex and prone to a risk of challenge. My hon. Friend has given a number of really good examples. The automatic number plate recognition database is another good example of mass data collection and storage in a way that is not especially legal, and where we have waited an awfully long time for even something as simple as a code of practice that might actually put the process and the practice on a more sustainable footing. Unless the Government take on board my hon. Friend's proposed amendments, we will be shackling the police, stopping them from embarking on many of the operational innovations that they need to start getting into if they are to do their job in keeping us safe.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): I will speak briefly in support of amendments 142 to 149, as well as new clauses 3 and 4. As it stands, clause 64 requires law enforcement data controllers to undertake a data protection impact assessment if

"a type of processing is likely to result in a high risk to the rights and freedoms of individuals".

That assessment would look at the impact of the envisaged processing operations on the protection of personal data and at the degree of risk, measures to address those risks and possible safeguards. If the impact assessment showed a high risk, the controller would have to consult the commissioner under clause 65.

It is important to be clear that the assessment relates to a type of processing. Nobody is asking anyone to undertake an impact assessment every time the processing occurs. With that in mind, the lower threshold for undertaking an assessment suggested in the amendments seems appropriate. We should be guarding not just against probable or high risks, but against any real risk. The worry is that if we do not put these tests in place, new forms of processing are not going to be appropriately scrutinised. We have had the example of facial recognition technology, which is an appropriate one.

New clauses 3 and 4 do a similar job for the intelligence services in part 4, so they also have our support.

Darren Jones: I rise to support the amendments in the name of my hon. Friend the Member for Sheffield, Heeley. I had the pleasure of cross-examining Baroness Williams of Trafford, who is the Minister responsible for some of these issues, on the Select Committee on Science and Technology in our inquiry on the biometric strategy and why there has been such a delay in the Government publishing that document. We had grave concerns about the delay in the strategy, but also about the way in which IT systems and servers in different forces act in different ways, which make things potentially very difficult.

The amendments would add safeguards to legitimate purposes—to prevent them from going too far. They should be welcomed by the Government and included in the Bill. There are a number of situations where, in this developing area of technology, which could be very useful to us as a country, as my hon. Friends have said, we need to ensure that the appropriate safeguards are in place. On facial recognition, we know from information received by the Science and Technology Committee that there is too high a number of facial records on the police national database and other law enforcement databases, when there is no legitimate reason for them to be there. We understand that it is difficult to delete them, but that is, with respect, not a good enough answer.

The Select Committee also heard—I think I mentioned this in an earlier sitting—that we have to be careful about the data that the Government hold. The majority of the adult population already has their facial data on Government databases, in the form of passport and driving licence imagery. When we start talking about the exemptions to being able to share data between different Government functions and law enforcement functions, and the exemptions on top of that for the ability to use those things, we just need to be careful that it does not get ahead of us. I know it is difficult to legislate perfectly for the future, but these safeguards would help to make it a safer place.

I will mention briefly the IMSI-catchers, because that covers my constituency of Bristol North West. It was the Bristol Cable, a local media co-operative of which I am a proud member—I pay £1 a month, so I declare an interest—that uncovered some of the issues around IMSI-catchers with bulk collection of information. It is really important that when we are having debates, as we have had with algorithms and artificial intelligence, we recognise that human intervention and the understanding of some of these systems is sometimes difficult. There are very few people who understand how algorithms actually work or how the systems actually work. As they become more advanced and learn and make decisions by themselves, the idea of human intervention or a human understanding of that is increasingly difficult.

In a situation where human resource is extremely stretched, such as in the police service, the tendency will understandably be to rely on the decisions of the systems within the frameworks that are provided, because there is not time to do full human intervention properly. That is why the safeguards are so important—to prevent things getting ahead of us. I hope the Government support the amendments, which I think are perfectly sensible.

Victoria Atkins: I have just a small correction. The hon. Member for Sheffield, Heeley said in error that the Home Office were holding on to the photographs. It is not the Home Office. It is individual police forces that hold that.

Louise Haigh: No, it is on the police national computer. That falls under the responsibility of the Home Office, not individual forces.

Victoria Atkins: That is run by the police. I do not want the misapprehension to be established that there is an office in the Home Office in Marsham Street where these photographs are held on a computer. It is on the police national computer, which is a secure system that people have to have security clearance to get into. It is not completely accurate to say that the Home Office has possession of it.

3.45 pm

I want to reassure the hon. Lady, because the picture she painted of the various systems she described was that they are unregulated, but that is not the case. Where they involve the processing of personal data, they will be caught by the Bill and the 1998 Act. Other statutory provisions may also apply—for example, the provisions of PACE relating to biometric information—and the surveillance camera commissioner will have a role in relevant cases. Facial recognition systems, in particular, are covered by the 1998 Act and the Bill, because they relate to personal data. Any new systems that are developed will be subject to a data protection impact assessment.

Law enforcement processing of ANPR data for the purpose of preventing, detecting, investigating and prosecuting crime will be conducted under part 3 of the Bill. When the data is processed by other organisations for non-law enforcement purposes, such as the monitoring of traffic flows, the data will be processed under part 2 of the Bill.

Part 3 of the Bill puts data protection impact assessments on a statutory footing for the first time. The purpose of such impact assessments is to prompt a controller to take action and put in place safeguards to mitigate the risk to individuals in cases in which processing is likely to result in a high risk to the rights and freedoms of their personal data. For example, under clause 64 the police will be required to carry out a data protection impact assessment before the new law enforcement data service—the next-generation police national computer—goes live. Clauses 64 and 65 faithfully transpose the provisions of the law enforcement directive, and the provisions in part 4 faithfully give effect to draft Council of Europe convention 108.

Amendments 142 to 145 would extend the scope of the requirements in clause 64 so that a formal impact assessment would have to be carried out irrespective of the likelihood or significance of the risk. That would place overly burdensome duties on controllers and their resources, with limited benefit to the data subject.

Louise Haigh: I would be grateful if the Minister can confirm that all the examples we raised today will fall under the "high risk" category in the Bill.

Victoria Atkins: I will deal with the definition of high risk in a moment. Clause 64 separates out the processing most likely significantly to affect an individual's rights and freedom, which requires an additional level of assessment to reflect the higher risk. The amendments would water down the importance of those assessments.

[Victoria Atkins]

That is not to say that consideration of the impact on rights and freedoms can be overlooked. It will, of course, remain necessary for the controller to carry out that initial assessment to determine whether a full impact assessment is required. Good data protection is not achieved by putting barriers in the way of processing. It is about considering the risk intelligently and applying appropriate assessments accordingly.

On the question of high risk, officers or data controllers will go through that process when considering whether a data protection impact assessment is correct. I will write to the hon. Lady to clarify whether the bodies and lists she mentioned will be defined as high risk. The fact is that they are none the less regulated by various organisations.

Matt Warman: The crucial point—I do not think the Opposition disagree with it—is that, although some things contain an element of risk, there are also huge benefits. Surely nobody wishes to do anything that prevents law enforcement from using hugely advantageous new technology, which will allow it to divert its resources to even more valuable areas.

Victoria Atkins: Indeed. A pertinent example of that is the development of artificial intelligence to help the police categorise images of child sexual exploitation online. That tool will help given the volume of offences now being carried out across the world. It will also help the officers involved in those cases, because having to sit at a computer screen and categorise some of these images is soul-breaking, frankly. If we can use modern technology and artificial intelligence to help categorise those images, that must surely be a good thing.

Louise Haigh: There is absolutely no argument over that. As a former special constable myself, I have no wish to put obstacles in the way of law enforcement. There is a particular need to develop technology to help digital investigations, and I think the Government have been delaying that. Human failures in those investigations have led to the collapse of several trials over the past couple of months.

The Minister says that the surveillance camera commissioner has a role. The commissioner has said that there needs to be further clarity on regulatory responsibility. It is not clear whether it is the surveillance camera commissioner, the biometrics commissioner or the Information Commissioner who has responsibility for facial recognition software. Does she accept that the Government urgently need to provide clarity, as well as guidance to the National Police Chiefs Council and police forces, about the use of this potentially invasive software?

Victoria Atkins: Specifically on clause 64, which is about the data protection impact assessment, the judgment as to whether the proposed processing is high risk must be a matter for the controller. On the face of it, many of the systems that the hon. Lady described in her speech will involve high risk, but with respect the decision is not for me to make as a Minister on my feet in Committee. We must allow data controllers the freedom and responsibility to make those assessments. They are the ones that make the decisions and what flows from that in terms of processing.

If the hon. Lady will write to me on the more general, wider point about oversight of the surveillance camera commissioner and so on, I would be happy to take that up outside of Committee.

Louise Haigh: The issue about whether it is high risk is of course a matter for the data controller, but we are scrutinising this Bill, and the Minister is asking us to support a test of high risk. I am sure the whole Committee would agree that all the cases that have been suggested today involve an incredibly high risk. They involve deprivation of liberty and invasion of privacy. The idea that we would accept a definition of high risk that does not cover those examples is too much for the Opposition to support. That is why the amendment exists. We need to test exactly what the Government envisage in the definition of high risk.

Victoria Atkins: May I just clarify whether the hon. Lady intends to amend her amendment to list the various categories she listed in her speech? I have been very clear that high risk is defined as including processing where there is a particular likelihood of prejudice to the rights and freedoms of data subjects. I would be very cautious about listing examples in the Bill through an amendment, because as we have all acknowledged, criminality and other things develop over time. It would be very bold to put those categories in the Bill.

Louise Haigh: No one is suggesting that such examples should go in the Bill. I appreciate this is the Minister's first Bill Committee, but the job of the Opposition is to test the definitions in the Bill and ensure that it is fit for purpose. My concern is that the definition of high risk is set too high to cover law enforcement agencies and will allow egregious breaches of individuals' data rights, privacy rights and right to liberty. It is our job as the Opposition—there is nothing wrong with us exercising this role—to ensure that the Bill is fit for purpose. That is what we are seeking to do.

Victoria Atkins: I am extremely grateful to the hon. Lady for clarifying her role. My answer is exactly as I said before. High risk includes processing where there is a particular likelihood of prejudice to the rights and freedoms of data subjects. That must be a matter for the data controller to assess. We cannot assess it here in Committee for the very good reason put forward by members of the Committee: we cannot foresee every eventuality. Time will move on, as will technology. That is why the Bill is worded as it is, to try to future-proof it but also, importantly, because the wording complies with our obligations under the law enforcement directive and under the modernised draft Council of Europe convention 108.

Liam Byrne: Does the Minister not have some sympathy with the poor individuals who end up being data controllers for our police forces around the country, given the extraordinary task that they have to do? She is asking those individuals to come up with their own frameworks of internal guidance for what is high, medium and low risk. The bureaucracy-manufacturing potential of the process she is proposing will be difficult for police forces. We are trying to help the police to do their job, and she is not making it much easier.

Victoria Atkins: Clause 65(2) states:

"The controller must consult the Commissioner prior to the processing if a data protection impact assessment prepared under section 64 indicates that the processing of the data would result in a high risk".

There are many complicated cases that the police and others have to deal with. That is why we have guidance rather than putting it in statute—precisely to give those on the frontline the flexibility of understanding, "This situation has arisen, and we need to calibrate the meaning of high risk and take that into account when we look at the prejudices caused to a person or a group of people." That is precisely what we are trying to encompass. Presumably, that is what the Council of Europe and those involved in drafting the law enforcement directive thought as well.

Of course, there will be guidance from the Information Commissioner to help data controllers on those assessments, to enable us to get a consistent approach across the country. That guidance will be the place to address these concerns, not on the face of the Bill.

Louise Haigh: Can the Minister confirm that the Metropolitan police consulted the Information Commissioner before trialling facial recognition software? I appreciate that she might not be able to do so on her feet, so I will of course accept it if she wishes to write to me.

Victoria Atkins: I am afraid that I will have to write to the hon. Lady on that.

The intention behind this part of the Bill is not to place unnecessary barriers in the way of legitimate processing. Nor, we all agree, should we place additional burdens on the commissioner without there being a clear benefit. These provisions are in the Bill to address the need for an intelligent application of the data protection safeguards, rather than assuming that a one-size-fits-all approach results in better data protection.

Amendment 149 would insert a new subsection (8) to clause 65, which would permit the commissioner to exercise powers of enforcement if she was not satisfied that the controller or processor had taken sufficient steps to act on her opinion that intended processing would infringe the provisions in part 3. It is worth noting that the purpose of clause 65 is to ensure consultation with the commissioner prior to processing taking place. It is therefore not clear what enforcement the commissioner would be expected to undertake in this instance, as the processing would not have taken place. If, however, the controller sought to process the data contrary to the commissioner's opinion, it would be open to her to take enforcement action in line with her powers already outlined in part 6.

I do not know, Mr Hanson, whether we have dealt with new clauses 3 and 4.

The Chair: New clauses 3 and 4 are being considered as part of this group, but would not be voted on until after the consideration of the clauses of the Bill have been completed. If you wish to respond to them, Minister, you can do so now.

Victoria Atkins: I am grateful; I will deal with them now. New clauses 3 and 4 would place additional obligations on the intelligence services. New clause 3 would require the intelligence services to undertake a data protection impact assessment in cases where there is

"a risk to the rights and freedoms of individuals",

whereas new clause 4 would require the intelligence services to have prior consultation with the Information Commissioner when proposing processing. Neither new clause reflects the unique form of processing undertaken by the intelligence services, its sensitive nature and the safeguards that already exist.

I should stress that the "data protection by design" requirements of clause 103 are wholly consistent with draft modernised Council of Europe convention 108, which was designed to apply to the processing of personal data in the national security context, and which therefore imposes proportionate requirements and safeguards. Under clause 103, in advance of proposing particular types of processing, the intelligence services will be obliged to consider the impact of such processing on the rights and freedoms of data subjects. That requirement will be integrated into the design and approval stages of the delivery of IT systems that process personal data, which is the most effective and appropriate way to address the broad aim. Furthermore, clause 102 requires the controller to be able to demonstrate, particularly to the Information Commissioner, that the requirements of chapter 4 of part 4 of the Bill are complied with, including the requirement in clause 103 to consider the impact of processing.

4 pm

The impact assessment requirements of the general data protection regulation and the law enforcement directive were not designed for national security processing, which is out of the scope of EU law. Given the need to respond swiftly and decisively in the event of terrorist acts or actions by hostile states, any unnecessary delay to the intelligence services' ability to deal with such threats could clearly have serious consequences. The new clauses are therefore inappropriate and could prejudice the lawful and proportionate action that is required to safeguard UK national security and UK citizens. Having explained our reasoning behind clauses 64 and 65, I hope that the hon. Member for Sheffield, Heeley will withdraw her amendment.

Louise Haigh: I remain concerned that the Bill leaves gaps that will enable law enforcement agencies and the police to go ahead and use technology that has not been tested and has no legal basis. As my right hon. Friend the Member for Birmingham, Hodge Hill said, that leaves the police open to having to develop their own guidance at force level, with all the inconsistencies that would entail across England and Wales.

The Minister agreed to write to me on a couple of issues. I do not believe that the Metropolitan police consulted the Information Commissioner before trialling the use of photo recognition software, and I do not believe that other police forces consulted the Information Commissioner before rolling out mobile fingerprint scanning. If that is the case and the legislation continues with the existing arrangements, that is not sufficient. I hope that before Report the Minister and I can correspond so as potentially to strengthen the measures. With that in mind, and with that agreement from the Minister, I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 64 ordered to stand part of the Bill.

Clauses 65 and 66 ordered to stand part of the Bill.

Clause 67

NOTIFICATION OF A PERSONAL DATA BREACH TO THE COMMISSIONER

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

Liam Byrne: The Committee is looking for some guidance and for tons of reassurance from the Minister about how the clause will bite on data processors who do not happen to base their operations here in the United Kingdom. This morning we debated the several hundred well-known data breaches around the world and highlighted some of the more recent examples, such as Yahoo!—that was probably the biggest—and AOL. More recently, organisations such as Uber have operated their systems with such inadequacy that huge data leaks have occurred, directly infringing the data protection rights of citizens in this country. The Minister will correct me if I am wrong, but I am unaware of any compensation arrangements that Uber has made with its drivers in this country whose data was leaked.

Even one of the companies closest to the Government—Equifax, which signed a joint venture agreement with the Government not too long ago—has had a huge data breach. It took at least two goes to get a full account from Equifax of exactly what had happened, despite the fact that Her Majesty's Government were its corporate partner and had employed it through the Department for Work and Pensions. All sorts of information sharing happened that never really came to light. I am not sure whether any compensation for Equifax data breaches has been paid to British citizens either.

My point is that most citizens of this country have a large amount of data banked with companies that operate from America under the protection of the first amendment. There is a growing risk that in the years to come, more of the data and information service providers based in the UK will go somewhere safer, such as Ireland, because they are worried about the future of our adequacy agreement with the European Commission. We really need to understand in detail how the Information Commissioner, who is based here, will take action on behalf of British citizens against companies in the event of data breaches. For example, how will she ensure notification within 72 hours? How will she ensure the enforcement of clause 67(4), which sets out the information that customers and citizens must be told about the problem?

This morning we debated the Government's ludicrous proposals for class action regimes, which are hopelessly inadequate and will not work in practice. We will not have many strong players in the UK who are able to take action in the courts, so we will be wholly reliant on the Information Commissioner to take action. I would therefore be grateful if the Minister reassured the Committee how the commissioner will ensure that clause 67 is enforced if the processor of the data is not on our shores.

Victoria Atkins: The right hon. Gentleman refers to companies not on these shores, about which we had a good deal of discussion this morning. Clause 67 belongs to part 3 of the Bill, which is entitled "Law enforcement processing", so I am not sure that the companies that he gives as examples would necessarily be considered under it. I suppose a part 3 controller could have a processor overseas, but that would be governed by clause 59. Enforcement action would, of course, be taken by the controller under part 3, but I am not sure that the right hon. Gentleman's examples are relevant to clause 67.

Liam Byrne: I am grateful to the Minister for that helpful clarification. Let me phrase the question differently, with different examples. The Home Office and many police forces are outsourcing many of their activities, some of which are bound to involve data collected by global organisations such as G4S. Is she reassuring us that any and all data collected and processed for law enforcement activities will be held within the boundaries of the United Kingdom and therefore subject to easy implementation of clause 67?

Victoria Atkins: The controller will be a law enforcement agency, to which part 3 will apply. I note that clause 200 provides details of the Bill's territorial application should a processor be located overseas, but under part 3 it will be law enforcement agencies that are involved.

Liam Byrne: Where G4S, for example, is employed to help with deportations, the Minister is therefore reassuring us that the data controller would never be G4S. However, if there were an activity that was clearly a law enforcement activity, such as voluntary removal, would the data controller always be in Britain and therefore subject to clause 67, even where private sector partners are used? The Minister may outsource the contract, but we want to ensure that she does not outsource the role of data controller so that a law enforcement activity here can have a data controller abroad.

Victoria Atkins: I appreciate the sentiment behind the amendment. If the Home Office outsources processing to an overseas company, any enforcement action would be taken against the Home Office as the controller. The right hon. Gentleman has raised the example of G4S in the immigration context, so I will reflect on that overnight and write to him to ensure that the answer I have provided also covers that situation.

Question put and agreed to.

Clause 67 accordingly ordered to stand part of the Bill.

Clause 68 to 71 ordered to stand part of the Bill.

Clause 72

OVERVIEW AND INTERPRETATION

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

Liam Byrne: I want to flag up an issue that we will stumble across in a couple of stand part debates: the safeguards that will be necessary for data sharing between this country and elsewhere. We will come on to the safeguards that will be necessary for the transfer of data between our intelligence agencies and foreign intelligence agencies. Within the context of this clause, which touches on the broad principle of data sharing from here and abroad, I want to rehearse one or two arguments on which Ministers should be well briefed and alert.

Our intelligence agencies do an extraordinary job in keeping this country safe, which sometimes involves the acquisition and use of data that results in the loss of life. All Committee members will be familiar with the drone strike that killed Reyaad Khan and Ruhul Amin, and many of us will have heard the Prime Minister's assurances in the Liaison Committee about the robust legal process that was gone through to ensure that the strike was both proportionate and legal.

The challenge—the public policy issue that arises under chapter 5 of the Bill—is that there is a number of new risks. First, there is the legal risk flagged up by the Court of Appeal in 2013, when justices said that it was not clear that UK personnel will be immune from criminal liability for their involvement in a programme that involves the transfer of intelligence from an intelligence service here to an American partner and where that American partner uses that information to conduct drone strikes that involve the loss of life. Confidence levels differ, but we in the Committee are pretty confident about the legal safeguards around those kinds of operations in this country. We can be less sure about the safeguards that some of our partners around the world have in place. The Court of Appeal has expressed its view, which was reinforced in 2016 by the Joint Committee on Human Rights. The Committee echoed the finding that "front-line personnel…should be entitled to more legal certainty" than they have today.

This section of the Bill gives us the opportunity to ensure that our intelligence services are equipped with a much more robust framework than they have today, to ensure that they are not subject to the risks flagged by the Court of Appeal or by the Joint Committee on Human Rights.

4.15 pm

We have shared intelligence with our partners, particularly in the Five Eyes network, for many moons. We have great specialism in that area. We have a number of RAF bases in this country and abroad with particularly important capabilities, and our facility in Cheltenham is pretty much the best in the world. We have to confront the challenge that the governance of some of our Five Eyes partners is perhaps not as cautious as the leadership of those countries was in the past. Since the election of President Trump, there has been a dramatic increase in the United States' drone programme.

We need to face up to the challenge—not duck, ignore, or pretend it is not there—that we want to preserve the legal safeguards that ensure that our intelligence services can do their job. We want to ensure that there are good, strong, robust arrangements for sharing intelligence with our partners.

We do not want to jeopardise our intelligence services or the information sharing agreements because of the misuse of intelligence by our partners abroad. That is particularly important when our partners abroad are deploying legal force in countries such as Syria, northern Iraq and, increasingly, Yemen, where the number of drone strikes has increased by 288% in recent years.

On this clause, it is appropriate to say that we want to have a good debate about what the safeguards need to look like to ensure good and safe intelligence sharing between our agencies. We hope the Government will be open-minded and will acknowledge our objective. The life of our intelligence services is complicated enough without having to question whether what they are doing is legally viable and whether it will be subject to legal challenge in the future. I hope we can reflect on that correctly, because we are not entirely sure that the safeguards in the Bill are robust enough.

Victoria Atkins: We are still on part 3, which deals with law enforcement processing. It does not relate to processing by security services. We will come to that when we debate amendment 159 to clause 109, so I reserve the right to respond to those observations on that amendment in due course.

The Chair: There is no amendment before the Committee. We are on clause 72. The right hon. Member for Birmingham, Hodge Hill made some comments, which I did not rule out of order. The Minister has indicated that she will respond to the wider issue of concerns about drones and national security at a later date. That is a matter for her. If the right hon. Gentleman is happy with that, and if the Minister is content, I will put the question that the clause stand part of the Bill.

Question put and agreed to.

Clause 72 accordingly ordered to stand part of the Bill.

Clauses 73 to 86 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned.—*(Nigel Adams.)*

4.21 pm

Adjourned till Tuesday 20 March at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

DPB 25 Open Rights Group and the3million
DPB 26 defenddigitalme
DPB 27 Reprieve
DPB 28 Association of British Insurers (ABI)
DPB 29 Associated Newspapers
DPB 30 European Justice Forum
DPB 31 Press Recognition Panel
DPB 32 Which?
DPB 33 Open Rights Group and Chris Pounder
DPB 34 Baylis Media Ltd
DPB 35 Personal Investment Management & Financial Advice Association (PIMFA)
DPB 36 Robin Makin
DPB 37 Robin Makin (Chapter 3 of Part 4)