PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Third Sitting

Tuesday 16 May 2023

(Morning)

CONTENTS

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

not later than

Saturday 20 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

† Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
† Henry, Darren *(Broxtowe)* (Con)
† Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
† Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 16 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

9.25 am

The Chair: I have a few preliminary announcements that Mr Speaker would like me to make. *Hansard* colleagues would be grateful if Members emailed their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent mode. Tea and coffee are not allowed during sittings.

The selection list for today's sitting, which is available in the room, shows how the selected amendments have been grouped for debate. Grouped amendments are generally on the same or a similar issue. Please note that decisions on amendments will take place not in the order in which they are debated, but in the order in which they appear on the amendment paper. The selection and grouping list shows the order of debates. Decisions on each amendment will be taken when we come to the clause to which the amendment relates.

The Member who has put their name to the lead amendment in a group will be called first. Other Members will then be free to catch my eye to speak on all or any of the amendments within that group. A Member may speak more than once in a single debate. At the end of a debate on a group of amendments, I shall again call the Member who moved the lead amendment. Before they sit down, they will need to indicate to me whether they wish to withdraw the amendment or to seek a decision. If any Member wishes to press any other amendment in a group to a vote, they will need to let me know.

Clause 1

Information relating to an identifiable living individual

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

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): It is a pleasure to serve under your chairmanship, Mr Hollobone. May I thank all hon. Members for volunteering to serve on the Committee? When I spoke on Second Reading, I expressed my enthusiastic support for the Bill—just as well, really. I did not necessarily expect to be leading on it in Committee, but I believe it is a very important Bill. It is complex and will require quite a lot of scrutiny, but it will create a framework of real benefit to the UK, by facilitating the exchange of data and allowing us to take the maximum advantage of emerging technologies. I look forward to our debates over the next few days.

Clause 1 will create a test in legislation to help organisations to understand whether the data that they are processing is personal or anonymous. This is important, because personal data is subject to data protection rules but anonymous data is not. If organisations can be confident that the data they are processing is anonymous, they will be able to use it for important activities such as research and product development without concern about the potential impact on individuals' personal data.

The new test will require data controllers considering whether data is personal or anonymous to consider two scenarios. The first is where a living individual can be identified by somebody within the data controller or processor's own organisation using reasonable means at any point at which the data is being processed, from the initial point of collection for its use and storage to its eventual deletion or onward transmission. The second scenario is where the data controller or processor knows or should reasonably know that somebody outside the organisation is likely to obtain the information and to be able to re-identify individuals from it using reasonable means. That could be a research partner or a business client with whom the data controller intends to share the data, or an outside organisation that obtains the data as a result of the data controller not putting adequate security measures in place.

What would be considered "reasonable means" in any given case takes into account, among other things, the time, effort and cost of identifying the individual, as well as the technology available during the time the processing occurs. We hope that the clarity the test provides will give organisations greater confidence about using anonymous data for a range of purposes, from marketing to medical research. I commend the clause to the Committee.

Stephanie Peacock (Barnsley East) (Lab): It is a pleasure to serve under your chairship, Mr Hollobone. I echo the Minister's thanks to everyone serving on the Bill Committee; it is indeed a privilege to be here representing His Majesty's loyal Opposition. I look forward to doing our constitutional duty as we scrutinise the Bill today and in the coming sittings.

The definition of personal data is critical, not only to this entire piece of legislation, but to the data protection regime more widely. That is because the definition of what counts as personal data sets the parameters on who will benefit from protections and safeguards set out by the legislation, and, looking at it from the other side, the various protections will not apply when data is not classed as personal. It is therefore important that the definition should be clear for both controllers and data subjects, so that everyone understands where regulations and, by extension, rights do and do not apply.

The Bill defines personal data as that where a data subject can be identified by a controller or processor, or anyone likely to obtain the information,

"by reasonable means at the time of processing".

According to the Bill, "reasonable means" take into account the time, effort, costs, technology and resources available to the person. The addition of "reasonable" to the definition has caused major concern among civil society groups, which are worried that it will introduce an element of subjectivity from the perspective of the controller when determining whether data is personal or not. Indeed, although recital 26 of the General Data Protection Regulation also refers to reasonable means—making this, in some ways, more of a formal change

than a practical one—there must still be clear parameters on how controllers or processors are to make that judgment. Without those, there may be a danger of controllers and processors avoiding the requirement to comply with rules around personal data by simply claiming they do not have the means to identify living individuals within their resources.

Has the Department undertaken an impact assessment to determine whether the definition could, first, increase subjectivity in what counts as personal data, or secondly, reduce the amount of data classified as personal data? If an assessment identifies such a risk, what steps will the Department take to mitigate that and ensure that citizens are able to exercise their rights as they can under the current definition?

Other stakeholders have raised concerns that the phrase

"at the time of the processing"

in the definition might imply that there is no continuous obligation to consider whether data is personal. Indeed, under the current definition, where personal data is

"any information that relates to an identified or identifiable living individual",

there is an implied obligation to consider whether an individual is identifiable on an ongoing basis. Rather than assessing the identifiability of a dataset at a fixed point, the controller or processor must keep the categorisation of data that it holds under careful review, taking into account technological developments, such as sophisticated new artificial intelligence or cross-referencing tools. Inserting the phrase

"at the time of the processing"

into this definition has prompted the likes of Which? to express concern that some processors may feel that they are no longer bound by this continuous obligation. That would be particularly worrying given the potential subjectivity of the new definition. If whether an individual is identifiable is based on "reasonable means", including one's resources and technology, it is perfectly feasible that, with a change of resources or technology, it could become reasonable to identify a person when once it was not.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): My hon. Friend is making an excellent speech. Does she agree that the absence of regard for the rate of technological change, particularly the rise of artificial intelligence—datasets are now being processed at phenomenal speeds—is potentially negligent on the part of the Government?

Stephanie Peacock: My hon. Friend makes an important point, which I will come to later.

In these circumstances, it is crucial that if a person is identifiable through data at any time in the future, the data is legally treated as personal so that the relevant safeguards and rights that GDPR was designed to ensure still apply.

When arguing for increased Secretary of State powers across the Bill, Ministers have frequently cited the need to future-proof the legislation. Given that, we must also consider the need to future-proof the definition of data so that technological advances do not render it useless. Does the new definition involve a continuous obligation to assess whether data is personal? Will guidance be offered to inform both controllers and data subjects on the application of this definition, so that both sides can be clear on how it will work in practice? As 5Rights has pointed out, that could avoid clogging up the regulator's time with claims about what counts as personal data in many individual cases.

Finally, when determining whether data is personal, it is also vital that controllers take into account how a determined stalker or malicious actor might find and use their data. It is therefore good to see the change made since the first iteration of the Data Protection and Digital Information Bill, to clarify that

"obtaining the information as a result of the processing"

also includes information obtained as a result of inaction by a controller or processor—for example, as the result of a failure to put in place appropriate measures to prevent or reduce the risk of hacking.

Overall, it is important that we give both controllers and data subjects clarity about which data is covered by which protections, and when. I look forward to hearing from the Minister about the concerns that have been raised, which could affect the definition's ability to allow for that clarity.

Sir John Whittingdale: I agree absolutely with the hon. Lady that the definition of personal data is central to the regime that we are putting in place. She is absolutely right that we need to be very clear and to provide organisations with clarity about what is within the definition of personal data and what is rightly considered to be anonymous. She asks whether the provision will lead to a reduction in the current level of protection. We do not believe that it will.

Clause 1 builds on the strong foundations used in GDPR recital 26 to clarify when data can be categorised as truly anonymous without creating undue risks. The aim of the provision in the Bill is to clarify when information should be considered to be personal data by including a test for identifiability in the legislation. That improved clarity will help organisations to determine when data can be considered truly anonymous and therefore pose almost no risk to the data subject.

The hon. Lady asked whether

"at the time of the processing"

extends into the future, and the answer is yes. The definition of data processing in the legislation is very broad and includes a lot of processing activities other than just the collection of data, such as alteration, retrieval, storage and disclosure by transmission, to name just a few. The phrase

"at the time of the processing"

could therefore cover a long period, depending on the nature and purpose of the processing. The test would need to be applied afresh for each new act of processing. That means that if at any point in the life cycle of processing, the data could be reasonably re-identified by someone by reasonable means, they would then not be able to legally consider to be anonymous. That includes transferring abroad to other regimes.

The clause makes it clear that a controller will have to consider the likelihood of re-identification at all stages of the processing activity. If a data controller held a dataset for several years, they would need to be mindful of the technologies available during that time that might be used to re-identify it. As the hon. Lady said, technology is advancing very fast and could well change over time from the point at which the data is first collected.

Chi Onwurah: I appreciate the Minister's clarification. He has just said that the test of identification would apply when sharing the data with another authority. However, once that has been done, the test no longer applies. Does he accept that it is possible for data to be shared that could not by this test reasonably be identified but that, over time, in a different authority, could reasonably be identified, without the data subject having any redress?

Sir John Whittingdale: If data is shared and then held by a new controller, it will be still subject to the same protections even though it has been transferred from the original. It is important that there should be the ability to continue to apply protection no matter what technology evolves over the course of time, but it will still be subject to the same protection and, of course, still be enforceable through the Information Commissioner.

Chi Onwurah: Would it be subject to the same protection if it was transferred abroad?

Sir John Whittingdale: Again, yes, it will. It will be transferred abroad only if we are satisfied that the recipient will impose the same level of protection that we regard as necessary in this country.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

MEANING OF RESEARCH AND STATISTICAL PURPOSES

Stephanie Peacock: I beg to move amendment 66, clause 2, page 4, line 8, at end insert—

"(c) do not include processing of personal data relating to children for research carried out as a commercial activity."

This amendment would exempt children's data from being used for commercial purposes under the definition of scientific purposes in this clause.

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

Amendment 65, clause 2, page 4, line 21, at end insert—

"7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to "scientific research".

8. The code of practice prepared under paragraph 7 must include examples of the kinds of research purposes, fields, controllers, and ethical standards that are to be considered as being scientific, and those that are excluded from being so considered."

This amendment would require a statutory code of practice from the ICO on how the definition of scientific research in this clause is to be interpreted.

Clause stand part.

Stephanie Peacock: Fuelling safe scientific research through data will be vital to support the UK's ambition to become a science superpower. We understand that, as is the case in many areas of data protection law, lack of clarity about what counts as processing for scientific purposes causes organisations to take a risk-averse approach to conducting research. An understanding of exactly what is included would therefore give organisations confidence they need to conduct vital processing that will allow for the scientific discoveries and benefits of the future.

Unfortunately, the clause makes the same mistake as the Bill does in general by focusing on easing regulations on those who hold data, rather than looking at how data can be harnessed for the general greater good. It misses the opportunity to unlock the benefits of safely redistributing and sharing data. Indeed, none of the clauses on processing for research purposes make any attempt to explore options to incentivise controllers to share their data with independent researchers. Similarly, the Bill does not explore how the likes of data trusts or co-operatives that pool data resources in the interests of a larger group of beneficiaries or organisations could create a stronger environment for research. Instead, it leaves those who already collect and hold data to benefit from the regime by processing for their own research purposes, while those who might hope to collaborate will use alternative data sets and are no better off.

By failing to think about the safe sharing of data to fuel scientific research, the Government limit the progress the UK could make as a powerhouse of science innovation. The Bill leaves only those organisations with large amounts of data able to contribute to such progress, entrenching existing power structures and neglecting the talent held in the smaller independent organisations that would otherwise be able to conduct research for the public good.

Turning to amendment 65, it has always been written into the GDPR, in recital 159, that processing for scientific purposes should be interpreted broadly. It is therefore understandable why Ministers provided a broad definition in the Bill that allows for those conducting genuine scientific research to have absolute confidence that their processing falls under this umbrella, preventing a risk-averse environment. However, stakeholders, including Reset.tech and the Ada Lovelace Institute, have expressed worries that clause 2 goes a little too far, essentially providing a blank cheque for private companies to self-identify as conducting scientific research as a guise for processing personal information for any purpose they choose.

All that must be understood in combination with clause 9, which gives organisations an exemption from purpose limitation, allowing them to reuse data as long as it is for scientific purposes, as defined in clause 2. Indeed, though the Bill contains a few clarifications of what the definition in clause 2 includes, such as publicly and privately funded processing, commercial or non-commercial processing and processing for the likes of technological development, fundamental research, or applied research, I am keen to hear from the Minister about what specific purposes would actually be ruled out under the letter of the current definition. For example, as the Ada Lovelace Institute asked, would pseudoscientific applications, such as polygraphy or experimental AI claiming to predict an individual's religion, politics or sexuality, be categorically ruled out under the current definition?

Though it may not be the intention in the clause to enable malicious or pseudoscientific processing under the definition of science, we must ensure that the definition is not open to exploitation, or so broad that any controller could reasonably identify their processing as falling under it. Regulator guidance would be in a prime position to do that. By providing context as to what must be considered for something to be reasonably classified as scientific—for example, the purpose of the research, the

field of research, the type of controller carrying it out, or the methodological and ethical standards used—controllers using the definition legitimately will feel even more assured, and malicious processing will be explicitly excluded from the application of the definition. Amendment 65 would do nothing to stop genuinely scientific research from benefiting from the changes in this Bill and would provide further clarity around how the definition can be legitimately relied upon.

9.45 am

Turning to amendment 66, 5Rights is a leading non-governmental, non-profit charitable organisation that seeks to reimagine the digital world in a way that works for children. Like others, it has shared concerns that relaxing the legal bases on which personal data can be processed for scientific research to include privately funded research carried out by commercial entities could open the door for children's data to be exploited for commercial purposes. Clause 9 will change rules to allow processors to not inform data subjects about the reuse of their data so long as it is for scientific purposes, even if that is on a commercial basis.

Even under the existing regulatory framework, there have been plenty of examples where controllers have claimed to be using data in the best interests of young people while actually causing them harm. The development of educational technology is widely cited as the future of education, with the industry rapidly expanding because of online learning during the pandemic. However, although such technologies and services claim to be for the benefit of children, many have used children's data in irresponsible ways.

A 2022 report by Human Rights Watch reviewed 165 ed tech products endorsed by 49 Governments worldwide that were deployed in schools and colleges during the lockdowns. The study found that 89% of the products engaged in data practices that put children's rights at risk, undermined them or actively violated them. Companies monitored children without their consent or knowledge and harvested data on what they do, who they are, where they live or study and who their family and friends are to the extent that the report concluded that the only way for children to protect themselves from the invasion would be to throw their devices in the trash.

The majority of learning platforms also sent or allowed advertising technology companies to access children's data. These ad tech companies, many of which are owned by the most powerful companies in the world, can then analyse and profile children, piecing the information together with data from other public or private sources to create detailed profiles that are used to place targeted adverts or can be sold to advertisers. From that study and others like it we can clearly see that even under the current rules children's data is vulnerable to being exploited for commercial gain. It would therefore be a great mistake to make the processing of children's data for commercial purposes even less transparent than it already is.

As was the aim with the age appropriate design code, it is important that we give children a high level of privacy rights by default. Where children's data is concerned, extra safeguards must be in place to ensure that any processing that occurs is in their best interests. Amendment 66 seeks to set an example of such a safeguard in practice, providing an exemption for children's data from being defined as scientific where it is being used for commercial purposes. It will hopefully create a precedent whereby children's rights are automatically given the best protection possible.

I would like to finish by asking the Minister whether his Department has considered the impact of the new legislation on commercial scientific processing on children specifically. If so, what measures have been taken to ensure that the Bill does not put children's personal data at risk of exploitation?

Damian Collins (Folkestone and Hythe) (Con): I wish to pose a couple of questions, after two thoughtful and well-presented amendments from those on the Opposition Front Bench. With regard to children and the use of apps such as TikTok, what assurance will the Government seek to ensure that companies that process and store data abroad are abiding by the principles of our domestic legislation? I mention TikTok directly because it stores data from UK users, including children, in Singapore, and it has made clear in evidence to the Joint Committee on the Online Safety Bill that that data is accessed by engineers in China who are working on it.

We all know that when data is taken from a store and used for product development, it can be returned in its original state but a huge amount of information is gathered and inferred from it that is then in the hands of engineers and product developers working in countries such as China and under very different jurisdictions. I am interested to know what approach we would take to companies that store data in a country where we feel we have a data equivalence regime but then process the data from a third location where we do not have such a data agreement.

Sir John Whittingdale: I welcome the recognition of the importance of allowing genuine research and the benefits that can flow from it. Such research may well be dependent on using data and the clause is intended to provide clarity as to exactly how that can be done and in what circumstances.

I will address the amendments immediately. I am grateful to the hon. Member for Barnsley East for setting out her arguments and we understand her concerns. However, I think that the amendments go beyond what the clause proposes and, in addition, I do not think that there is a foundation for those concerns. As we have set out, clause 2 inserts in legislation a definition for processing for scientific research, historical research and statistical purposes. The definition of scientific research purposes is set out as

"any research that can be reasonably described as scientific"

and I am not sure that some of the examples that the hon. Lady gave would meet that definition.

The definitions inserted by the clause are based on the wording in the recitals to the UK GDPR. We are not changing the scope of these definitions, only their status in the legislation. They will already be very familiar to people using them, but setting them out in the Bill will provide more clarity and legal certainty. We have maintained a broad scope as to what is allowed to be included in scientific research, with the view that the regulator can add more nuance and context through guidance, as is currently the case. The power to require codes of practice provides a route for the Secretary of State to require the Information Commissioner to prepare any code of practice that gives guidance on good practice in processing personal data.

[Sir John Whittingdale]

There will be situations where non-statutory guidance, which can be produced without being requested under regulations made by the Secretary of State, may be more appropriate than a statutory code of practice. Examples of the types of activity that are considered scientific research and the indicative criteria that a researcher should demonstrate are best placed in non-statutory guidance produced by the Information Commissioner's Office. That will give flexibility to amend and change the examples when necessary, so I believe that the process does not change the provision. However, putting it in the legislation, rather than in the recitals, will impose stronger safeguards and make things clearer. Once the Bill has come into effect, the Government will continue to work with the ICO to update its already detailed and helpful guidance on the definition of scientific research as necessary.

Amendment 66 would prohibit the use of children's data for commercial purposes under the definition of scientific research. The definition inserted by clause 2 includes the clarification that processing for scientific research carried out as a commercial activity can be considered processing for scientific research purposes. Parts of the research community asked for that clarification in response to our consultation. It reflects the existing scope, as is already clear from the ICO's guidance, and we have seen that research by commercial bodies can have immense societal value. For instance, research into vaccines and life-saving treatments is clearly in the public interest. I entirely understand the hon. Lady's concern for children's privacy, but we think that her amendment could obstruct important research by commercial organisations, such as research into children's diseases. I think that the Information Commissioner would make it clear as to whether or not the kind of example that the hon. Lady gave would fall within the definition of research for scientific purposes.

I also entirely understand the concern expressed by my hon. Friend the Member for Folkestone and Hythe. I suspect that the question about the sharing of data internationally, particularly, perhaps, by TikTok, may recur during the course of our debates. As he knows, we would share data internationally only if we were confident that it would still be protected in the same way that it is here, which would include considering the possibility of whether or not it could then be passed on to a third country, such as China.

I hope that I can reassure the hon. Lady that emphasising the safeguards that researchers must comply with in clause 22 to protect individuals relates to all data used for these purposes, including children's data and the protections afforded to children under the UK GDPR. For those reasons, I hope that she will be willing to withdraw her amendment.

Stephanie Peacock: I am disappointed that the Minister does not accept amendment 66. Let me make a couple of brief points about amendment 65. The Minister said that he was not sure whether some of the examples I gave fitted under the definition, and that is what the amendment speaks to. I asked what specific purposes would be ruled out under the letter of the current definition, and that is still not clear, so I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 1]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 65, in clause 2, page 4, line 21, at end insert—

"7. The Commissioner must prepare a code of practice under section 124A of the Data Protection Act 2018 on the interpretation of references in this Regulation to 'scientific research'.

8. The code of practice prepared under paragraph 7 must include examples of the kinds of research purposes, fields, controllers, and ethical standards that are to be considered as being scientific, and those that are excluded from being so considered."—*(Stephanie Peacock.)*

This amendment would require a statutory code of practice from the ICO on how the definition of scientific research in this clause is to be interpreted.

The Committee divided: Ayes 6, Noes 9.

Division No. 2]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 2 ordered to stand part of the Bill.

Clause 3

CONSENT TO PROCESSING FOR THE PURPOSES OF SCIENTIFIC RESEARCH

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

The Chair: With this it will be convenient to discuss clause 4 stand part.

Sir John Whittingdale: The clause clarifies how the conditions for consent will be met in certain circumstances when processing for scientific research purposes. It clarifies an existing concept of "broad consent" that is currently found in the recitals. The measure will enable consent to

be obtained for an area of scientific research when the researcher cannot fully identify the purposes for which they are collecting the data.

Consent under UK GDPR must be for a specific purpose, but in scientific research the precise purpose may not be fully known when the data is collected. For example, the initial aim may be the study of cancer, and then later becomes the study of a particular cancer type. Currently, the UK GDPR recitals clarify that consent may be given for an area of scientific research, but as the recitals are only an interpretative aid that may not give scientists the certainty that they need. The clause will therefore add the ability to give broad consent for scientific research into the operative text of the UK GDPR, giving scientists greater certainty and confidence. The clause contains a number of safeguards to protect against misuse. That includes the requirement that seeking consent is consistent with ethical standards that are generally recognised and relevant to that area of research.

10 am

Although law enforcement agencies have the power to process personal data with the permission of the individual, there is no definition of consent in the legislation. Clause 4 again mirrors the UK GDPR definition of consent, including the conditions that must be met in order for it to be used as a lawful basis for processing. That change will address the slight risk that consent may be interpreted inconsistently with the definition used in the UK GDPR. We are taking this opportunity to make our data protection laws more consistent, by clarifying terminology for both organisations and individuals. I therefore commend the clauses to the Committee.

Stephanie Peacock: With regard to clause 3, I refer Members to my remarks on clause 2. It is sensible to clarify how controllers and processors conducting scientific research can gain consent where it is not possible to fully identify the full set of uses for that data when it is collected. However, what counts as scientific, and therefore what is covered by the clause, must be properly understood by both data subjects and controllers through proper guidance issued by the ICO.

Clause 4 is largely technical and inserts the recognised definition of consent into part 3 of the Data Protection Act 2018, for use when it is inappropriate to use one of the law enforcement purposes. I will talk about law enforcement processing in more detail when we consider clauses 16, 24 and 26, but I have no problem with the definition in clause 4 and am happy to accept it.

Sir John Whittingdale: I am grateful to the hon. Lady for her support. I agree with her on the importance of ensuring that the definition of scientific research is clear. That is something on which I have no doubt the ICO will also issue guidance.

Question put and agreed to.

Clause 3 accordingly ordered to stand part of the Bill.

Clause 4 ordered to stand part of the Bill.

Clause 5

LAWFULNESS OF PROCESSING

Stephanie Peacock: I beg to move amendment 68, in clause 5, page 6, line 37, at end insert—

"7A. The Secretary of State may not make regulations under paragraph 6 unless—

(a) following consultation with such persons as the Secretary of State considers appropriate, the Secretary of State has published an assessment of the impact of the change to be made by the regulations on the rights and freedoms of data and decision subjects (with particular reference to children),

(b) the Commissioner has reviewed the Secretary of State's statement and published a statement of the Commissioner's views on whether the change should be made, with reasons, and

(c) the Secretary of State has considered whether to proceed with the change in the light of the Commissioner's statement."

This amendment would make the Secretary of State's ability to amend the conditions in Annex 1 which define "legitimate interests" subject to a requirement for consultation with interested parties and with the Information Commissioner, who would be required to publish their views on any proposed change.

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

Amendment 67, in clause 5, page 7, line 18, at end insert—

"11. Processing may not be carried out in reliance on paragraph 1(ea) unless the controller has published a statement of—

(a) which of the conditions in Annex 1 has been met which makes the processing necessary,

(b) what processing will be carried out in reliance on that condition, or those conditions, and

(c) why that processing is proportionate to and necessary for the purpose or purposes indicated in the condition or conditions."

This amendment would require controllers to document and publish (e.g. in a privacy notice) a short statement on their reliance on a "recognised legitimate interest" for processing personal data.

Clause stand part.

Stephanie Peacock: At present, the lawful bases for processing are set out in article 6 of the UK GDPR. At least one of them must apply whenever someone processes personal data. They are consent, contract, legal obligation, vital interests, public task, and legitimate interests. That is where data is being used in ways that we would reasonably expect, there is minimal privacy impact, or there is a compelling justification for processing. Of the existing lawful bases, consent is by far the most relied upon, as it is the most clear. There have therefore been calls for the other lawful bases to be made clearer and easier to use. It is welcome to see some examples of how organisations might rely on the legitimate interests lawful ground brought on to the statute book.

At the moment, in order to qualify for using legitimate interests as grounds for lawful processing, a controller must also complete a balancing test. The balancing test is an important safeguard. As per the ICO, it requires controllers to consider the interests and fundamental rights and freedoms of the individual, and whether they override the legitimate interests that the controller has identified. That means at a minimum considering the nature of the personal data being processed, the reasonable expectations of the individual, the likely impact of processing on the individual, and whether any safeguards can be put in place to mitigate any negative impacts.

[Stephanie Peacock]

As tech.UK mentioned, the introduction of a list of legitimate interests no longer requiring that test is something many have long called for. When conducting processing relating to an emergency, for example, the outcome of a balancing test often very obviously weighs in one direction, making the decision straightforward, and the test itself an administrative task that may slow processing down. It makes sense in such instances that a considered exemption might apply.

However, given the reduction in protection and control for consumers when removing a balancing test, it is vital that a list of exemptions is limited and exhaustive, and that every item on such a list is well consulted on. It is also vital that the new lawful basis cannot be relied upon in bad faith or exploited by those who simply want to process without the burden, for reasons outside of those listed in annex 1. The Bill as it currently stands does not do enough to ensure either of those things, particularly given the Secretary of State's ability to add to the list on a whim.

I turn to amendment 67. Although it is likely not the intention for the clause to be open to exploitation, Reset.tech, among many others, has shared concerns that controllers may be able to abuse the new lawful basis of "recognised legitimate interests", stretching the listed items in annex 1 to cover some or all of their processing, and giving themselves flexibility over a wide range of processing without an explicit requirement to consider how that processing affects the rights of data and decision subjects. That is particularly concerning where controllers may be able to conflate different elements of their processing.

Reset.tech and AWO provide a theoretical case study to demonstrate that point. Let us say that there is a gig economy food delivery company that processes a range of data on workers, including minute-by-minute location data. That location data would be used primarily for performance management, but could occasionally be used in more extreme circumstances to detect crime—for example, detecting fraud by workers who are making false claims about how long they waited for an order to be ready for delivery. By exploiting the new recognised legitimate interests basis, the company could conflate its purposes of performance management and detecting crime, and justify the tracking of location data as a whole as being exempt from the balancing test, without having to record or specify exactly which processing is for the detection of crime.

Under the current regime, there remain two tests other than the balancing test that form a complete assessment of legitimate interests and help to prevent conflation of that kind. First, there is the purpose test, which requires the controller to identify which legitimate interest the company is relying upon. Secondly, there is the necessity test, which requires the controller to consider whether the processing that the company intends to conduct is necessary and proportionate to meet its purposes.

In having to conduct those tests, the food delivery company would find it much more difficult to conflate its performance management and crime prevention purposes, as it would have to identify and publicly state exactly which elements of its processing are covered by the legitimate interest purpose of crime prevention. That would make it explicit that any processing the company conducts for the purposes of performance management is not permitted under a recognised legitimate interest, meaning that a lawful basis for that processing would be required separately.

Amendment 67 therefore seeks to ensure that the benefits of the purpose and necessity tests are retained, safeguarding the recognised legitimate interests list from being used to cynically conflate purposes and being exploited more generally. In practice, that would mean that controllers relying on a purpose listed in annex 1 for processing would be required to document and publish a notice that explains exactly which processing the company is conducting under which purpose, and why it is necessary.

It is foundational to the GDPR regime that each act of processing has a purpose, so this requirement should just be formalising and publishing what controllers are already required to consider. The measure that the amendment seeks to introduce should therefore be no extra burden on those already complying in good faith, but should still act as a barrier to those attempting to abuse the new basis.

I turn to amendment 68. As the likes of Which? have argued, any instance of removing the balancing test will inevitably enable controllers to prioritise their interests in processing over the impact on data subjects, resulting in weaker protections for data subjects and weaker consumer control. Which? research, such as that outlined in its report "Control, Alt or Delete? The future of consumer data", also shows that consumers value control over how their data is collected and used, and that they desire more transparency, rather than less, on how their data is used.

With those two things in mind—the value people place on control of their data and the degradation of that control as a result of removing the balancing test—it is vital that the power to remove the balancing test is used extremely sparingly on carefully considered, limited purposes only. Even for those purposes already included in annex 1, it is unclear exactly what impact assessment took place to ensure that the dangers of removing the test on the rights of citizens did not outweigh the positives of that removal.

It would therefore be helpful if the Minister could outline the assessment and analysis that took place before deciding the items on the list. Although it is sensible to future-proof the list and amend it as needs require, this does not necessarily mean vesting the power to do so in the Secretary of State's hands, especially when such a power is open to potential abuse. Indeed, to say that the Secretary of State must have regard to the interests and fundamental rights and freedoms of data subjects and children when making amendments to the list is simply not a robust enough protection for citizens. Our laws should not rely on the good nature of the Secretary of State; they must be comprehensive enough to protect us if Ministers begin to act in bad faith.

Further, secondary legislation simply does not offer the scrutiny that the Government claim it does, because it is rarely voted on. Even when it is, if the Government of the day have a majority, defeating such a vote is incredibly rare. For the method of changing the list to be protected from the whims of a bad faith Secretary of State who simply claims to have had regard to people's

rights, proper consultation should be undertaken by the regulator on any amendments before they are considered for parliamentary approval.

This amendment would move the responsibility for judging the impact of changes away from the Secretary of State and place it with the regulator on a yearly basis, ensuring that amendments proceed only if they are deemed, after consultation, to be in the collective societal interest. That means there will be independent assurance that any amendments are not politically or maliciously motivated. This safeguard should not be of concern to anyone prepared to act in good faith, particularly the current Secretary of State, as it would not prevent the progression in Parliament of any amendments that serve the common good. The amendment represents what genuine future-proofing in a way that retains appropriate safeguards looks like, as opposed to what ends up looking like little more than an excuse for a sweeping power grab.

Sir John Whittingdale: I welcome the hon. Lady's recognition of the value of setting out a list of legitimate interests to provide clarity, but I think she twice referred to the possibility of the Secretary of State adding to it on a whim. I do not think we would recognise that as a possibility. There is an established procedure, which I would like to go through in responding to the hon. Lady's concerns. As she knows, one of the key principles of our data protection legislation is that any processing of personal data must be lawful. Processing will be lawful where an individual has given his or her consent, or where another specified lawful ground in article 6 of the UK GDPR applies. This includes where the processing is necessary for legitimate interests pursued by the data controller, providing that those interests are not outweighed by an individual's privacy rights.

Clause 5 addresses the concerns that have been raised by some organisations about the difficulties in relying on the "legitimate interests" lawful ground, which is used mainly by commercial organisations and other non-public bodies. In order to rely on it, the data controller must identify what their interest is, show that the processing is necessary for their purposes and balance their interests against the privacy right of the data subject. If the rights of the data subject outweigh the interests of the organisation, the processing would not be lawful and the controller would need to identify a different lawful ground. Regulatory guidance strongly recommends that controllers document the outcome of their legitimate interests assessments.

As we have heard, and as the hon. Lady recognises, some organisations have struggled with the part of the legitimate interests assessment that requires them to balance their interests against the rights of individuals, and concern about getting the balancing test wrong—and about regulatory action that might follow as a result—can cause risk aversion. In the worst-case scenario, that could lead to crucial information in the interests of an individual or the public—for example, about safeguarding concerns—not being shared by third-sector and private-sector organisations. That is why we are taking steps in clause 5 and schedule 1 to remove the need to do the balancing test in relation to a narrow range of recognised legitimate activities that are carried out by non-public bodies. Those activities include processing, which is necessary for the purposes of safeguarding national security or defence; responding to emergencies; preventing crimes such as fraud or money laundering; safeguarding vulnerable individuals; and engaging with the public for the purposes of democratic engagement.

10.15 am

Amendment 68, tabled by the hon. Member for Barnsley East, would prevent the Secretary of State from using the regulation-making powers in the clause to add to the list of activities for which no balancing test is required unless she has first published an assessment of the impact of the change on the rights of individuals and formally considered any views of the Information Commissioner. The amendment is unnecessary because, as drafted, the clause already requires the Secretary of State to consider the impact of any changes to the list of the rights and freedoms of individuals and, where relevant, the need to provide children with special protection with regard to their personal data.

The regulation-making powers in the clause will also be subject to the new requirements in clause 44. They provide that any regulations made under the UK GDPR are subject to consultation with the commissioner and such other persons as the Secretary of State considers appropriate.

Damian Collins: Will my right hon. Friend confirm whether the Information Commissioner's advice will be published, either by the commissioner, the Minister or Parliament—perhaps through the relevant Select Committee?

Sir John Whittingdale: I am not sure it would necessarily be published. I want to confirm that, but I am happy to give a clear response to the Committee in due course if my hon. Friend will allow me.

As well as the advice that the Information Commissioner supplies, the proposal is also subject to the affirmative procedure, as the hon. Member for Barnsley East recognised, so Parliament could refuse to approve any additions to the list that do not respect the rights of data subjects. She suggested that it is rare for an affirmative resolution to be rejected by Parliament; nevertheless, it is part of our democratic proceedings, and every member of the Committee considering it will have the opportunity to reach their own view and vote accordingly. I hope that reassures the hon. Lady that there are already adequate safeguards in place in relation to the exercise of powers to add new activities to the list of recognised legitimate interests.

Amendment 67, which the hon. Lady also tabled, would require data controllers to publish a statement if they are relying on the new recognised legitimate interests lawful ground. The statement would have to explain what processing would be carried out in reliance on the new lawful ground and why the processing is proportionate and necessary for the intended purpose. In our view, the amendment would significantly weaken the clause. It would reintroduce something similar to the legitimate interests assessment, which, as we have heard, can unnecessarily delay some very important processing activities. In scenarios involving national security or child protection, for example, the whole point of the clause is to make sure that relevant and necessary personal data can be shared without hesitation to protect vulnerable individuals or society more generally.

I hope the hon. Lady is reassured by my response and agrees to withdraw her amendments. I commend clause 5 to the Committee.

Stephanie Peacock: We do not believe that amendment 67 would place an extra burden on those who are already complying in good faith. The idea behind it is that it will be a barrier to those attempting to abuse the new basis.

On amendment 68, we should not have laws that rely on the Secretary of State's good faith. As the Minister said, it is pretty rare for secondary legislation to be voted on, and for the Government to lose, so I do not see that as a barrier. The hon. Member for Folkestone and Hythe highlighted that although there are some protections, we do not believe that the Government protections go as far as we would like. For that reason, I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 3]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 67, in clause 5, page 7, line 18, at end insert—

"11. Processing may not be carried out in reliance on paragraph 1(ea) unless the controller has published a statement of—

(a) which of the conditions in Annex 1 has been met which makes the processing necessary,

(b) what processing will be carried out in reliance on that condition, or those conditions, and

(c) why that processing is proportionate to and necessary for the purpose or purposes indicated in the condition or conditions.*"—(Stephanie Peacock.)*

This amendment would require controllers to document and publish (e.g. in a privacy notice) a short statement on their reliance on a "recognised legitimate interest" for processing personal data.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 4]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 5 ordered to stand part of the Bill.

Schedule 1

LAWFULNESS OF PROCESSING: RECOGNISED LEGITIMATE INTERESTS

Sir John Whittingdale: I beg to move amendment 30, in schedule 1, page 137, line 28, leave out "fourth day after" and insert

"period of 30 days beginning with the day after".

Annex 1 to the UK GDPR makes provision about processing for democratic engagement purposes, including certain processing by elected representatives. This amendment increases the period for which former members of the Westminster Parliament and the devolved legislatures continue to be treated as "elected representatives" following an election. See also NC6 and Amendment 31.

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

Government amendment 31.

Government new clause 6—*Special categories of personal data: elected representatives responding to requests.*

That schedule 1 be the First schedule to the Bill.

Sir John Whittingdale: As the Committee will be aware, data protection legislation prohibits the use of "special category" data—namely, information about a person that is sensitive in nature—unless certain conditions or exemptions apply. One such exemption is where processing is necessary on grounds of substantial public interest.

Schedule 1 to the Data Protection Act 2018 sets out a number of situations where processing would be permitted on grounds of substantial public interest, subject to certain conditions and safeguards. That includes processing by elected representatives who are acting with the authority of their constituents for the purposes of progressing their casework. The current exemption applies to former Members of the Westminster and devolved Parliaments for four days after a general election—for example, if the MP has been defeated or decides to stand down. That permits them to continue to rely on the exemption for a short time after the election to conclude their parliamentary casework or hand it over to the incoming MP. In practice, however, it can take much longer than that to conclude these matters.

New clause 6 will therefore extend what is sometimes known as the four-day rule to 30 days, which will give outgoing MPs and their colleagues in the devolved Parliaments more time to conclude casework. That could include handing over live cases to the new representative, or considering what records should be retained, stored and deleted. When MPs leave office, there is an onus on them to conclude their casework in a timely manner. However, the sheer volume of their caseload, on top of the other work that needs to be done when leaving office, means that four days is just not enough to conclude all relevant business. The new clause will therefore avoid the unwelcome situation where an outgoing MP who is doing his or her best to conclude constituency casework could be acting unlawfully if they continue to process their constituents' sensitive data after the four-day time limit has elapsed. Extending the time limit to 30 days will provide a pragmatic solution to help outgoing MPs while ensuring the exemptions cannot be relied on for an indefinite period.

Government amendments 30 and 31 will make identical changes to other parts of the Bill that rely on the same definition of "elected representative". Government amendment 30 will change the definition of "elected representative" when the term appears in schedule 1. As I mentioned when we debated the previous group of amendments, clause 5 and schedule 1 to the Bill create a new lawful ground for processing non-sensitive personal data, where the processing is necessary for a "recognised legitimate interest". The processing of personal data by elected representatives for the purposes of democratic engagement is listed as such an interest, along with other processing activities of high public importance, such as crime prevention, safeguarding children, protecting national security and responding to emergencies.

Government amendment 31 will make a similar change to the definition of "elected representative" when the term is used in clause 84. Clauses 83 and 84 give the Secretary of State the power to make regulations to exempt elected representatives from some or all of the direct marketing rules in the Privacy and Electronic Communications (EC Directive) Regulations 2003. I have no doubt that we will debate the merits of those clauses in more detail later in Committee, but for now it makes sense to ensure that there is a single definition of "elected representative" wherever it appears in the Bill. I hope the hon. Member for Barnsley East and other colleagues will agree that those are sensible suggestions and will support the amendments.

Stephanie Peacock: This set of Government provisions will increase the period for which former MPs and elected representatives in the devolved regions can use the democratic engagement purpose for processing. On the face of it, that seems like a sensible provision that allows for a transition period so that data can be deleted, processed, or moved on legally and safely after an election, and the Opposition have a huge amount of sympathy for it.

I will briefly put on record a couple of questions and concerns. The likes of the Ada Lovelace Institute have raised concerns about the inclusion of democratic engagement purposes in schedule 1. They are worried, particularly with the Cambridge Analytica scandal still fresh in people's minds, that allowing politicians and elected parties to process data for fundraising and marketing without a proper balancing test could result in personal data being abused for political gain. The decision to make processing for the purposes of democratic engagement less transparent and to remove the balancing test that measures the impact of that processing on individual rights may indicate that the Government do not share the concern about political processing. Did the Minister's Department consider the Cambridge Analytica scandal when drawing up the provisions? Further, what safeguards will be in place to ensure that all data processing done under the new democratic engagement purpose is necessary and is not abused to spread misinformation?

Sir John Whittingdale: I would only say to the hon. Lady that I have no doubt that we will consider those aspects in great detail when we get to the specific proposals in the Bill, and I shall listen with great interest to my hon. Friend the Member for Folkestone and Hythe, who played an extremely important role in uncovering what went on with Cambridge Analytica.

Damian Collins: The principle that underpinned what happened in the Cambridge Analytica scandal was the connection of Facebook profiles to the electoral register. If I understand my right hon. Friend the Minister correctly, what he is talking about would not necessarily change that situation. This could be information that the political campaign has gained anyway from a voter profile or from information that already exists in accounts it has access to on platforms such as Facebook; it would simply be attaching that, for the purposes of targeting, to people who voted in an election. The sort of personal data that Members of Parliament hold for the purposes of completing casework would not have been processed in that way. These proposals would not change in any way the ability to safeguard people's data, and companies such as Cambridge Analytica will still seek other sources of open public data to complete their work.

Sir John Whittingdale: I think my hon. Friend is right. I have no doubt that we will go into these matters in more detail when we get to those provisions. As the hon. Member for Barnsley East knows, this measure makes a very narrow change to simply extend the existing time limit within which there is protection for elected representatives to conclude casework following a general election. As we will have opportunity in due course to look at the democratic engagement exemption, I hope she will be willing to support these narrow provisions.

Stephanie Peacock: I am grateful for the Minister's reassurance, and we are happy to support them.

10.30 am

Amendment 30 agreed to.

Schedule 1, as amended, agreed to.

Clause 6

The purpose limitation

Stephanie Peacock: I beg to move amendment 69, in clause 6, page 9, leave out lines 7 to 20.

This amendment would remove the ability of the Secretary of State to amend Annex 2, so they could not make changes through secondary legislation to the way purpose limitation operates.

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

Stephanie Peacock: One of the key principles in article 5 of the EU GDPR is purpose limitation. The principle aims to ensure that personal data is collected by controllers only for specified, explicit and legitimate purposes. Generally speaking, it ensures that the data is not further processed in a manner that is incompatible with those purposes. If a controller's purposes change over time, or they want to use data for a new purpose that they did not originally anticipate, they can go ahead only if the new purpose is compatible with the original purpose, they get the individual's specific consent for the new purpose or they can point to a clear legal provision requiring or allowing the new processing in the public interest.

Specifying the reasons for obtaining data from the outset helps controllers to be accountable for their processing and helps individuals understand how their data is being used and whether they are happy with that, particularly where they are deciding whether to

[Stephanie Peacock]

provide consent. Purpose limitation exists so that it is clear why personal data is being collected and what the intention behind using it is.

In any circumstance where we water down this principle, we reduce transparency, we reduce individuals' ability to understand how their data will be used and, in doing so, we weaken assurances that people's data will be used in ways that are fair and lawful. We must therefore think clearly about what is included in clause 6 and the associated annex. Indeed, many stakeholders, from Which? to Defend Digital Me, have expressed concern that what is contained in annex 2 could seriously undermine the principle of purpose limitation.

As Reset.tech illustrates, under the current regime, if data collected for a relatively everyday purpose, such as running a small business, is requested by a second controller for the purpose of investigating crime, the small business would need to assess whether this further processing—thereby making a disclosure of the data—was compatible with its original purpose. In many cases, there will be no link between the original and secondary purposes, and there are potential negative consequences for the data subjects. As such, the further processing would be unlawful, as it would breach the principle of purpose limitation.

However, under the new regime, all it would take for the disclosure to be deemed compatible with the original purpose is the second controller stating that it requires the data for processing in the public interest. In essence, this means that, for every item listed in annex 2, there are an increased number of circumstances in which data subjects' personal information could be used for purposes outside their reasonable expectations. It seems logical, therefore, that whatever is contained in the list is absolutely necessary for the public good and is subject to the highest level of public scrutiny possible.

Instead, the clause gives the Secretary of State new Henry VIII powers to add to the new list of compatible purposes by secondary legislation whenever they wish, with no provisions made for consulting on, scrutinising or assessing the impact of such changes. It is important to remember here that secondary legislation is absolutely not a substitute for parliamentary scrutiny of primary legislation. Delegated legislation, as we have discussed, is rarely voted on, and even when it is, the Government of the day will win such a vote if they have a majority.

If there are other circumstances in which the Government think it should be lawful to carry out further processing beyond the original purpose, those should be in the Bill, rather than being left to Ministers to determine at a later date, avoiding the same level of scrutiny.

The Government's impact assessment says that clarity on the reuse of data could help to fix the market failure caused by information gaps on how purpose limitation works. Providing such clarity is something we could all get behind. However, by giving the Secretary of State sweeping powers fundamentally to change how purpose limitation operates, the clause goes far beyond increasing clarity.

Improved and updated guidance on how the new rules surrounding reusing data work would be far more fruitful in providing clarity than further deregulation in this instance. If Ministers believe there are things missing from the clause and annex, they should discuss them here and now, rather than opening the back door to making further additions afterwards, and that is what the amendment seeks to ensure.

Sir John Whittingdale: The clause sets out the conditions under which the reuse of personal data for a new purpose is permitted. As the hon. Lady has said, the clause expands on the purpose limitation principle. That key principle of data protection ensures that an individual's personal data is reused only in ways they might reasonably expect.

The current provisions in the UK GDPR on personal data reuse are difficult for controllers and individuals to navigate. That has led to uncertainty about when controllers can reuse personal data. The clause addresses the existing uncertainty around reusing personal data by setting out clearly when it is permitted. That includes when personal data is being reused for a very different purpose from that for which it was originally collected—for example, when a company might wish to disclose personal data for crime prevention.

The clause permits reuse of personal data by a controller when the new purpose is "compatible"; they get fresh consent; there is a research purpose; UK GDPR is being complied with, such as for anonymisation or pseudonymisation purposes; there is an objective in the public interest authorised by law; and certain specified objectives in the public interest set out in a limited list in schedule 2 are met. I will speak more about that when we come to the amendment and the debate on schedule 2.

The clause contains a power to add or amend conditions or remove conditions added by regulations from that list to ensure it can be kept up to date with any future developments in how personal data should be reused in the public interest. It also sets out restrictions on reusing personal data that the controller originally collected on the basis of consent.

The Government want to ensure that consent is respected to uphold transparency and maintain high data protection standards. If a person gives consent for their data to be processed for a specific purpose, that purpose should be changed without their consent only in limited situations, such as for certain public interest purposes, if it would be unreasonable to seek fresh consent. That acts as a safeguard to ensure that organisations address the possibility of seeking fresh consent before relying on any exemptions.

The restrictions around consent relate to personal data collected under paragraph 1(a) of article 6 of the UK GDPR, which came into force in May 2018. Therefore, they do not apply to personal data processed on the basis of consent prior to May 2018, when different requirements applied. By simplifying the rules on further processing, the clause will give controllers legal certainty on when they can reuse personal data and give individuals greater transparency. I support the clause standing part of the Bill.

Let me turn to amendment 69, which proposes to remove the power set out in the clause to amend the annex in schedule 2. As I have already said, schedule 2 will insert a new annex in the UK GDPR, which sets out certain specific public interest circumstances where personal data reuse is permitted. The list is strictly limited and exhaustive, so a power is needed to ensure that it is kept up to date with any future developments in how personal data is reused for important public interest purposes. That builds on an existing power in

schedule 2 to the Data Protection Act 2018, where there is already the ability to make exceptions to the purpose limitation principle via secondary legislation.

The power in the clause also provides the possibility of narrowing a listed objective if there is evidence of any of the routes not being used appropriately. That includes limiting it, by reference, to the lawful ground of the original processing—for example, to prohibit the reuse of data that was collected on the basis of an individual's consent.

I would like to reassure the hon. Lady that this power will be used only when necessary and in the public interest. That is why the clause contains a restriction on its use; it may be used only to safeguard an objective listed in article 23 of the UK GDPR. Clause 44 of the Bill also requires that the Secretary of State must consult the commissioner, and any other persons as the Secretary of State considers appropriate, before making any regulations.

On that basis, I hope the hon. Lady will accept that the amendment is unnecessary.

Stephanie Peacock: The purpose behind our amendment —this speaks to a number of our amendments—is that we disagree with the amount of power being given to the Secretary of State. For that reason, I would like to continue with my amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 5]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Clause 6 ordered to stand part of the Bill.

Schedule 2

PURPOSE LIMITATION: PROCESSING TO BE TREATED AS COMPATIBLE WITH ORIGINAL PURPOSE

Stephanie Peacock: I beg to move amendment 71, in schedule 2, page 138, line 16, leave out "states" and insert "confirms".

This amendment would require a person who needs personal data for a purpose described in Article 6(1)(e) (a task carried out in the public interest or in the exercise of official authority vested in the controller) to confirm, and not merely to state, that they need the data for legitimate purposes.

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

Amendment 70, in schedule 2, page 139, line 30, at end insert

"levied by a public authority".

This amendment would clarify that personal data could be processed as a "legitimate interest" under this paragraph only when the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature levied by a public authority.

That schedule 2 be the Second schedule to the Bill.

Stephanie Peacock: I will begin by addressing amendment 70, which seeks only to make a wording change so that the annex cannot be misinterpreted. Paragraph 10 of annex 2 outlines that further processing is to be treated as compatible with original purposes

"where the processing is carried out for the purposes of the assessment or collection of a tax or duty or an imposition of a similar nature."

Which? has expressed concerns that that is much too vaguely worded, especially without a definition of "tax" or "duty" for the purposes of that paragraph, leaving the data open to commercial uses beyond the intention. Amendment 70 would close any potential loopholes by linking the condition to meeting a specific statutory obligation to co-operate with a public authority such as His Majesty's Revenue and Customs.

Moving on, amendment 71 would correct a similar oversight in paragraph 1 of annex 2, which was identified by the AWO and Reset.tech. Paragraph 1 aims to ensure that processing is treated as compatible with the original purpose when it is necessary for making a disclosure of personal data to another controller that needs to process that data for a task in the public interest or in the exercise of official authority and that has requested that data. However, the Bill says that processing is to be treated as compatible with the original purpose where such a request simply "states" that the other person needs the personal data for the purposes of carrying out processing that is a matter of public task. At very least, those matters should surely be actually true, rather than just stated. Amendment 71 would close that loophole, so that the request must confirm a genuine need for data in completing a task in the public interest or exercising official authority, rather than simply being a statement of need.

Beyond those amendments, I wish only to reiterate the thoughts that I expressed during the debate on clause 6. Everything contained in the annex provides for further processing that is hidden from data subjects and may not be within their reasonable expectations. The reliance on the new annex should therefore be closely monitored to ensure that it is not being exploited, or we risk compromising the purpose limitation principle altogether. Does the Department plan to monitor how the new exemptions on the reuse of data are being relied on?

10.45 am

Sir John Whittingdale: As we have already discussed with clause 6, schedule 2 inserts a new annex into the UK GDPR. It sets out certain specific public interest circumstances in which personal data reuse is permitted regardless of the purpose for which the data was originally collected—for example, when the disclosure of personal data is necessary to safeguard vulnerable individuals. Taken together, clause 6 and schedule 2 will give controllers legal certainty on when they can reuse personal data and give individuals greater transparency.

[Sir John Whittingdale]

Amendment 70 concerns taxation purposes, which are included in the list in schedule 2. I reassure the hon. Member for Barnsley East that the exemption for taxation is not new: it has been moved from schedule 2 to the Data Protection Act 2018. Indeed, the specific language in question goes back as far as 1998. We are not aware of any problems caused by that language.

The inclusion in the schedule of

"levied by a public authority"

would likely cause problems, since taxes and duties can be imposed only by law. Some must be assessed or charged by public authorities, but many become payable as a result of a person's transactions or circumstances, without any intervention needed except to enforce collection if unpaid. They are not technically levied by a public authority. That would therefore lead to uncertainty and confusion about whether processing for certain important taxation purposes would be permitted under the provision.

I hope to reassure the hon. Lady by emphasising that taxation is not included in the annex 1 list of legitimate interests. That means that anyone seeking to use the legitimate interest lawful ground for that purpose would need to carry out a balancing-of-interests test, unless they were responding to a request for information from a public authority or other body with public tasks set out in law. For those reasons, I am afraid I am unable to accept the amendment, and I hope the hon. Lady will withdraw it.

Amendment 71 relates to the first paragraph in new annex 2 to the UK GDPR, as inserted by schedule 2. The purpose of that provision is to clarify that non-public bodies can disclose personal data to other bodies in certain situations to help those bodies to deliver public interest tasks in circumstances in which personal data might have been collected for a different purpose. For example, it might be necessary for a commercial organisation to disclose personal data to a regulator on an inquiry so that that body can carry out its public functions. The provision is tightly formulated and will permit disclosure from one body to another only if the requesting organisation states that it has a public interest task, that it has an appropriate legal basis for processing the data set out in law, and that the use of the data is necessary to safeguard important public policy or other objectives listed in article 23.

I recognise that the amendment is aimed at ensuring that the requesting organisation has a genuine basis for asking for the data, but suggest that changing one verb in the clause from "state" to "confirm" will not make a significant difference. The key point is that non-public bodies will not be expected to hand over personal data on entirely spurious grounds, because of the safeguards that I described. On that basis, I hope the hon. Lady will withdraw her amendment.

Stephanie Peacock: I am reassured by what the Minister said about amendment 70 and am happy not to move it, but I am afraid he has not addressed all my concerns in respect of amendment 71, so I will press it to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 6]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Schedule 2 agreed to.

Clause 7

VEXATIOUS OR EXCESSIVE REQUESTS BY DATA SUBJECTS

Stephanie Peacock: I beg to move amendment 74, in clause 7, page 10, line 34, at end insert—

"6. Where a controller—

(a) charges a fee for dealing with a request, in accordance with paragraph 2(a), or

(b) refuses to act on a request, in accordance with paragraph 2(b)

the controller must issue a notice to the data subject explaining the reasons why they are refusing to act on the request, or charging a fee for dealing with the request, and informing the subject of their right to make a complaint to the Commissioner and of their ability to seek to enforce this right through a judicial remedy."

This amendment would oblige controllers to issue a notice to the data subject explaining the reasons why they are not complying with a request, or charging for a request, their right to make a complaint to the ICO, and their ability to seek to enforce this right through a judicial remedy.

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

Amendment 73, in clause 7, page 12, line 20, at end insert—

"(1A) When considering the resources available to the recipient for the purposes of subsection (1)(c), no account may be taken of any lack of resources which is due to a failure by the recipient to appoint staff to relevant roles where the recipient has the resources to do so."

This amendment would make it clear that, when taking into account "resources available to the controller" for deciding whether a subject access request is vexatious or excessive, this cannot include where the organisation has neglected to appoint staff, but has the finances or resources to do so.

Amendment 72, in clause 7, page 12, line 25, at end insert—

"(3) The Commissioner must prepare a code of practice under section 124A on the circumstances in which a request may be deemed vexatious or excessive.

(4) The code of practice prepared under subsection (3) must include examples of requests which may be deemed vexatious or excessive, and of requests which may be troublesome to deal with but which should not be deemed vexatious or excessive."

This amendment would require the ICO to produce a code of practice on how the terms vexatious and excessive are to be applied, with examples of the kind of requests that may be troublesome to deal with, but are neither vexatious nor excessive.

Clause stand part.

Stephanie Peacock: I will speak first to clause 7 and amendment 72. Currently, everyone has the right to ask an organisation whether or not it is using or storing their personal data and to ask for copies of that data. That is called the right of access, and exercising that right is known as making a subject access request. Stakeholders from across the spectrum, including tech companies and civil society organisations, all recognise the value of SARs in helping individuals to understand how and why their data is being used and enabling them to hold controllers to account in processing their data lawfully.

The right of access is key to transparency and often underpins people's ability to exercise their other rights as data subjects. After all, how is someone to know that their data is being used in an unlawful way, or in a way they would object to, if they are not able to ascertain whether their personal data is being held or processed by any particular organisation? For example, as the TUC highlighted in oral evidence to the Committee, the right of data subjects to make an information access request is a particularly important process for workers and their representatives, as it enables workers to gain access to personal data on them that is held by their employer and aids transparency over how algorithmic management systems operate.

It has pleased many across the board to see the Government roll back on their suggestion of introducing a nominal fee for subject access requests. However, the Bill introduces a new threshold for when controllers are able to charge a reasonable fee, or refuse a subject access request, moving from "manifestly unfounded or excessive" to "vexatious or excessive". When deciding whether a request is vexatious or excessive, the Bill requires the controller to have regard to the circumstances of the subject access request. That includes, but is not limited to, the nature of the request; the relationship between subject and controller; the resources available to the controller; the extent to which the request repeats a previous request made by the subject; how long ago any previous request was made; and whether the request overlaps with other requests made by the data subject to the controller.

Stakeholders such as the TUC, the Public Law Project and Which? have expressed concerns that, as currently drafted, the terms that make up the new threshold are too subjective and could be open to abuse by controllers who may define any request they do not want to answer as vexatious or excessive. Currently, all there is in the Bill to guide controllers on how to apply the threshold is a non-exhaustive list of considerations; as I raised on Second Reading, if that list is non-exhaustive, what explicit protections will be in place to stop the application of terms such as "vexatious" and "excessive" being stretched and manipulated by controllers who simply do not want to fulfil the requests they do not like?

There are concerns that without further guidance even the considerations listed could be interpreted selfishly by controllers who lack a desire to complete a request. For example, given that many subject access requests come from applicants who are suspicious of how their data is being used, or have cause to believe their data is being misused, there is a high likelihood that the relationship any given applicant has with the controller has previously involved some level of friction and, perhaps, anger. The Bill prompts controllers to consider their relationship with a data subject when determining whether their request is vexatious; what is to stop a controller simply marking any data subject who has shared suspicions as "angry and vexatious", thereby giving them grounds to refuse a genuine request?

Without clarity on how both the new threshold and the considerations apply, the ability of data subjects to raise a legal complaint about why their request was categorised as vexatious and excessive will be severely impeded. As AWO pointed out in oral evidence, that kind of legal dispute over a subject access request may be only the first stage of court proceedings for an individual, with a further legal case on the contents of the subject access request potentially coming afterwards. There simply should not be such a long timescale and set of legal proceedings in order for a person to exercise their fundamental data rights. Even the Information Commissioner himself, despite saying that he was clear on how the phrases "vexatious" and "excessive" should be applied, mentioned to the Committee that it was right to point out that such phrases were open to numerous interpretations.

The ICO is in a great position to provide clear statutory guidance on the application of the terms, with specific examples of when they do and do not apply, so that only truly bad-natured requests that are designed to exploit the system can be rejected or charged for. Such guidance would provide clarity on the ways in which a request might be considered troublesome but neither vexatious nor excessive. That way, controllers can be sure that they have dismissed, or charged for, only requests that genuinely pass the threshold, and data subjects can be assured that they will still be able to freely access information on how their data is being used, should they genuinely need or want it.

On amendment 73, one consideration that the Bill suggests controllers rely on when deciding whether a request is vexatious or excessive is the "resources available" to them. I assume that consideration is designed to operate in relation to the "excessive" threshold and the ability to charge. For example, when a subject access request would require work far beyond the means of the controller in question, the controller would be able to charge for providing the information needed, to ensure that they do not experience a genuine crisis of resources as a result of the request. However, the Bill does not explicitly express that, meaning the consideration in its vague form could be applied in circumstances beyond that design.

Indeed, if a controller neglected to appoint an appropriate number of staff to the responsibility of responding to subject access requests, despite having the finances and resources to do so, they could manipulate the consideration to say that any request they did not like was excessive, as a result of the limited resources available to respond. As is the case across many parts of the Bill, we cannot have legislation that simply assumes that people will act in good faith; we must instead have legislation that explicitly protects against bad-faith interpretations. The amendment would ensure just that by clarifying that a controller cannot claim that a request is excessive simply because they have neglected to arrange their resources in such a way that makes responding to the request possible.

On amendment 74, as is the case with the definition of personal data in clause 1, where the onus is placed on controllers to decide whether a living individual could

[Stephanie Peacock]

reasonably be identified in any dataset, clause 7 again places the power—this time to decide whether a request is vexatious or excessive—in the hands of the controller.

As the ICO notes, transparency around the use of data is fundamentally linked to fairness, and is about being

"clear, open and honest with people from the start about who you are, and how and why you use their personal data".

If a controller decides, then, that due to a request being vexatious or excessive they cannot provide transparency on how they are processing an individual's data at that time, the very least they could do, in the interests of upholding fairness, is to provide transparency on their justification for classifying a request in that way. The amendment would allow for just that, by requiring controllers to issue a notice to the data subject explaining the grounds on which their request has been deemed vexatious or excessive and informing them of their rights to make a complaint or seek legal redress.

In oral evidence, the Public Law Project described the Bill's lack of a requirement for controllers to notify subjects as to why their request has been rejected as a decision that creates an "information asymmetry". That is particularly concerning given that it is often exactly that kind of information that is needed to access the other rights and safeguards outlined in the Bill and across GDPR. A commitment to transparency, as the amendment would ensure, would not only give data subjects clarity on why their request had been rejected or required payment, but provide accountability for controllers who rely on the clause, and thereby a deterrent from misusing it to reject any requests that they dislike. For controllers, the workload of issuing such notices should surely be less than that of processing a request that is genuinely vexatious and excessive, ensuring that the provision does not counterbalance the benefits brought to controllers through the clause.

Sir John Whittingdale: Let me start by recognising the importance of of subject access requests. I am aware that some have interpreted the change in the wording for grounds of refusal as a weakening. We do not believe that is the case.

On amendment 72, in our view the new "vexatious or excessive" language in the Bill gives greater clarity than there has previously been. The Government have set out parameters and examples in the Bill that outline how the term "vexatious" should be interpreted within a personal data protection context, to ensure that controllers understand.

11 am

The power to request codes of practice exists in the legislation and should be relied on to request any new codes. That power provides a route for the Secretary of State to require the Information Commissioner to prepare any code of practice that gives guidance on good practice in the processing of personal data. However, there will be situations where non-statutory guidance, which can be produced without being requested under regulations made by the Secretary of State, may be more appropriate than a statutory code of practice.

Examples of when a request may or may not be vexatious or excessive are best placed in non-statutory guidance produced by the ICO, as that will provide the flexibility to amend and change those examples whenever necessary. A wider code of practice on subject access requests may be a useful tool to create clarity. However, the Government want to work with the ICO to set out the scope of any code, in consultation with affected stakeholders, before using the power to request it.

Amendment 73 focuses on the new parameters for controllers to consider when determining whether a request is vexatious or excessive. The parameters include

"resources available to the controller",

thereby emphasising the importance of proportionality when considering whether a request is vexatious or excessive.

Damian Collins: Does my right hon. Friend agree that the provisions will be helpful and important for organisations that gather data about public persons, and particularly oligarchs, who are very adept at using subject access requests to bombard and overwhelm a journalist or a small investigatory team that is doing important work looking into their business activities?

Sir John Whittingdale: I completely agree with my hon. Friend. That is an issue that both he and I regard as very serious, and is perhaps another example of the kind of legal tactic that SLAPPs—strategic lawsuits against public participation—represent, whereby oligarchs can frustrate genuine journalism or investigation. He is absolutely right to emphasise that.

It is important to highlight that controllers can already consider resource when refusing or charging a reasonable fee for a request. The Government do not wish to change that situation. Current ICO guidance sets out that controllers can consider resources as a factor when determining if a request is excessive.

The new parameters are not intended to be reasons for refusal. The Government expect that the new parameters will be considered individually as well as in relation to one another, and a controller should consider which parameters may be relevant when deciding how to respond to a request. For example, when the resource impact of responding would be minimal even if a large amount of information was requested—such as for a large organisation—that should be taken into account. Additionally, the current rights of appeal allow a data subject to contest a refusal and ultimately raise a complaint with the ICO. Those rights will not change with regard to individual rights requests.

Amendment 74 proposes adding more detail on the obligations of a controller who refuses or charges for a request from a data subject. The current legislation sets out that any request from a data subject, including subject access requests, is to be responded to. The Government are retaining that approach and controllers will be expected to demonstrate why the provision applies each time it is relied on. The current ICO guidance sets out those obligations on controllers and the Government do not plan to suggest a move away from that approach.

The clause also states that it is for the controller to show that a request is vexatious or excessive in circumstances where that might be in doubt. Thus, the Government believe that the existing legislation provides the necessary protections. Following the passage of the

Bill, the Government will work with the ICO to update guidance on subject access requests, which we believe plays an important role and is the best way to achieve the intended effect of the amendments. For those reasons, I will not accept this group of amendments; I hope that the hon. Member for Barnsley East will be willing to withdraw them.

I turn to clause 7 itself. As I said, the UK's data protection framework sets out key data subject rights, including the right of access—the right for a person to obtain a copy of their personal data. A subject access request is used when an individual requests their personal data from an organisation. The Government absolutely recognise the importance of the right of access and do not want to restrict that right for reasonable requests.

The existing legislation enables organisations to refuse or charge a reasonable fee for a request when they deem it to be "manifestly unfounded or excessive". Some organisations, however, struggle to rely on that in cases where it may be appropriate to do so, which as a consequence impacts their ability to respond to reasonable requests.

The clause changes the legislation to allow controllers to refuse or charge a reasonable fee for a request that is "vexatious or excessive". The clause adds parameters for controllers to consider when relying on the "vexatious or excessive" exemption, such as the nature of the request and the relationship between the data subject and the controller. The clause also includes examples of the types of request that may be vexatious, such as those intended to cause distress, those not made in good faith or those that are an abuse of process.

We believe that the changes will give organisations much-needed clarity over when they can refuse or charge a reasonable fee for a request. That will ensure that controllers can focus on responding to reasonable requests, as well as other important data and organisational needs. I commend the clause to the Committee.

Stephanie Peacock: I appreciate that, as the Minister said, the Government do not intend the new terms to be grounds for refusal, but his remarks do not reassure me that that will not be the case. Furthermore, as I said on moving the amendment, stakeholders such as the TUC, Public Law and Which? have all expressed concern that, as drafted, those terms are too subjective. I will press the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 7]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 73, in clause 7, page 12, line 20, at end insert—

"(1A) When considering the resources available to the recipient for the purposes of subsection (1)(c), no account may be taken of any lack of resources which is due to a failure by the recipient to appoint staff to relevant roles where the recipient has the resources to do so."—*(Stephanie Peacock.)*

This amendment would make it clear that, when taking into account "resources available to the controller" for deciding whether a subject access request is vexatious or excessive, this cannot include where the organisation has neglected to appoint staff, but has the finances or resources to do so.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 8]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

Amendment proposed: 72, in clause 7, page 12, line 25, at end insert—

"(3) The Commissioner must prepare a code of practice under section 124A on the circumstances in which a request may be deemed vexatious or excessive.

(4) The code of practice prepared under subsection (3) must include examples of requests which may be deemed vexatious or excessive, and of requests which may be troublesome to deal with but which should not be deemed vexatious or excessive."—*(Stephanie Peacock.)*

This amendment would require the ICO to produce a code of practice on how the terms vexatious and excessive are to be applied, with examples of the kind of requests that may be troublesome to deal with, but are neither vexatious nor excessive.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 9]

AYES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

Question accordingly negatived.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 10]

AYES

Bristow, Paul	Hunt, Jane
Collins, Damian	Richards, Nicola
Double, Steve	Simmonds, David
Eastwood, Mark	Whittingdale, rh Sir John
Henry, Darren	

NOES

Amesbury, Mike	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 7 ordered to stand part of the Bill.

Clause 8

TIME LIMITS FOR RESPONDING TO REQUESTS BY DATA SUBJECTS

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

Sir John Whittingdale: Clause 8 makes changes to the time requirements to which an organisation must adhere when responding to a subject access request. Currently, organisations must respond to a subject access request within a set period; in the majority of cases, that is one month from receipt of the request. This clause enables organisations to "stop the clock" on the response time when an organisation is unable to respond without further information or clarification from an individual. For example, when the controller has information on multiple data subjects with the same name, they may require further information to help to differentiate the data subject's information from others'. Organisations must have a legitimate reason to pause the response time; once confirmation is received from the data subject, the original time obligations resume.

The clause will also enable organisations to extend the period permitted for law enforcement and the intelligence services to respond to complex requests by two further months in certain circumstances. This replicates the existing provisions applicable to processing requests under the UK GDPR. Currently, all subject access requests received under the law enforcement and intelligence services regimes must be actioned within one month, irrespective of the complexity or number of requests received from an individual. Consequently, complex or confusing requests can disproportionately burden public bodies operating under those regimes, creating resource pressures.

Clause 8 will rectify the disparity currently existing between processing regimes and put law enforcement and intelligence services organisations on an equal footing to UK GDPR organisations. That will also provide a consistent framework for organisations operating under more than one regime at the same time. The clause also brings clarity on how best to respond to a confusing or complex request, ensuring that organisations do not lose time while seeking this clarification and can instead focus on responding to a request. On that basis, I urge that clause 8 stand part of the Bill.

11.15 am

Stephanie Peacock: I expressed my thoughts on the value and importance of subject access requests when we debated clause 7, and most of the same views remain pertinent here. Clause 8 allows for subject access requests to be extended where the nature of the request is complex, or due to volume. Some civil society groups, including Reset.tech, have expressed concern that that could mean that requests are unduly delayed for months, reflecting concern that they could be disregarded altogether, which was discussed when we debated clause 7. With that in mind, can the Minister tell us what protections will be in place to ensure that data controllers do not abuse the new ability to extend subject access requests, particularly by using the excuse that it is a large amount of data, in order to delay requests that they simply do not wish to respond to?

The clause provides some clarity on clause 7 by demonstrating that just because a request is lengthy or comes in combination with many others, it is not necessarily excessive as the clause gives controllers the option to extend the timeframe for dealing with requests that are high in volume. Of course, we do not want to unnecessarily delay requests, but allowing controllers to manage their load within a reasonable extended timeframe can act as a safeguard against their automatically relying on the "excessive" threshold. With that in mind, I am happy for the clause to stand part. However, I reiterate that my comments on clause 7 should be referred to.

Sir John Whittingdale: May I briefly respond to the hon. Lady's comments? I assure her that controllers will not be able to stop the clock for all subject access requests—only for those where they reasonably require further information to be able to proceed with responding. Once that information has been received from a data subject, the clock resumes and the controller must proceed with responding to the request within the applicable time period, which is usually one month from when the controller receives the request information. A data subject who has provided the requested information would also be able to complain to a controller, and ultimately to the Information Commissioner's Office, if they feel that their request has not been processed within the appropriate time. I hope the hon. Lady will be assured that there are safeguards to ensure that this power is not abused.

Question put and agreed to.

Clause 8 accordingly ordered to stand part of the Bill.

Clause 9

INFORMATION TO BE PROVIDED TO DATA SUBJECTS

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

The Chair: With this it will be convenient to discuss clause 10 stand part.

Sir John Whittingdale: Clause 9 provides researchers, archivists and those processing personal data for statistical purposes with a new exemption from providing certain information to individuals when they are reusing datasets for a different purpose, which will help to ensure that important research can continue unimpeded. The new exemption will apply when the data was collected directly from the individual, and can be used only when providing the additional information would involve a disproportionate

effort. There is already an exemption from this requirement where the personal data was collected from a different source.

The clause also adds a non-exhaustive list of examples of factors that may constitute a disproportionate effort. This list is added to both the new exemption in article 13 and the existing exemption found in article 14. Articles 13 and 14 of the UK GDPR set out the information that must be provided to data subjects at the point of data collection: article 13 covers circumstances where data is directly collected from data subjects, and article 14 covers circumstances where personal data is collected indirectly—for example, via another organisation. The information that controllers must provide to individuals includes details such as the identity and contact details of the controller, the purposes of the processing and the lawful basis for processing the data.

Given the long-term nature of research, it is not always possible to meaningfully recontact individuals. Therefore, applying a disproportionate effort exemption addresses the specific problem of researchers wishing to reuse data collected directly from an individual. The exemption will help ensure that important research can continue unimpeded. The clause also makes some minor changes to article 14. Those do not amend the scope of the exemption or affect its operation, but make it easier to understand.

I now turn to clause 10, which introduces an exemption relating to legally professionally privileged data into the law enforcement regime, mirroring the existing exemptions under the UK GDPR and the intelligence services regime. As a fundamental principle of our legal system, legal professional privilege protects confidential communications between professional legal advisers and their clients. The existing exemption in the UK GDPR restricts an individual's right to access personal data that is being processed or held by an organisation, and to receive certain information about that processing.

However, in the absence of an explicit exemption, organisations processing data under the law enforcement regime, for a law enforcement purpose rather than under the UK GDPR, must rely on ad hoc restrictions in the Data Protection Act. Those require them to evaluate and justify its use on a case-by-case basis, even where legal professional privilege is clearly applicable. The new exemption will make it simpler for organisations that process data for a law enforcement purpose to exempt legally privileged information, avoiding the need to justify the use of alternative exemptions. It will also clarify when such information can be withheld from the individual.

Hon. Members might wonder why an exemption for legal professional privilege was not included under the law enforcement regime of the Data Protection Act in the first place. The reason is that we faithfully transposed the EU law enforcement directive, which did not contain such an exemption. Following our exit from the EU, we are taking this opportunity to align better the UK GDPR and the law enforcement regime, thereby simplifying the obligations for organisations and clarifying the rules for individuals.

Stephanie Peacock: The impact of clause 9 and the concerns around it should primarily be understood in relation to the definition contained in clause 2, so I refer hon. Members to my remarks in the debate on clause 2. I also refer them to my remarks on purpose limitation in clause 6. To reiterate both in combination, I should say that purpose limitation exists so that it is clear why personal data is being collected, and what the intention is behind its use. That means that people's data should not largely be reused in ways not initially collected for, unless a new legal basis is obtained.

It is understandable that, where genuine scientific, historical and statistical research is occurring, and there is disproportionate effort to provide the information required to data subjects, there may be a need for exemption and to reuse data without informing the subject. However, that must be done only where strictly necessary. We must be clear that, unless there are proper boundaries to the definition of scientific data, this could be interpreted far too loosely.

I am concerned that, without amendment to clause 2, clause 9 could extend the problem of scientific research being used as a guise for using people's personal data in malicious or pseudoscientific ways. Will the Minister tell us what protections will be in place to ensure that people's data is not reused on scientific grounds for something that they would otherwise have objected to?

On clause 10, I will speak more broadly on law enforcement processing later in the Bill, but it is good to have clarity on the legal professional privilege exemptions. I have no further comments at this stage.

Carol Monaghan (Glasgow North West) (SNP): What we are basically doing is changing the rights of individuals, who would previously have known when their data was used for a purpose other than that for which it was collected. The terms

"scientific or historical research, the purposes of archiving in the public interest or statistical purposes"

are very vague, and, according to the Public Law Project, open to wide interpretation. Scientific research is defined as "any research that can reasonably described as scientific, whether publicly or privately funded".

I ask the Minister: what protections are in place to ensure that private companies are not given, through this clause, a carte blanche to use personal data for the purpose of developing new products, without the need to inform the data subject?

Sir John Whittingdale: These clauses relate to one of the fundamental purposes of the Bill, which is to facilitate genuine scientific research—obviously, that carries with it huge potential benefits in the areas of tackling disease or other scientific advances. We debated the definition of scientific research earlier in relation to clause 2. We believe that the definition is clear. In this particular case, the use of historical data can be very valuable. It is simply impractical for some organisations to reobtain consent when they may not even know where original data subjects are now located.

The Chair: Order. I apologise to the Minister. He can resume his remarks at 2 o'clock, when we meet again in this room but, it being 11.25 am, the Committee is now adjourned.

11.25 am

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

Adjourned till this day at Two o'clock.