PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Fifth Sitting

Thursday 18 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

Monday 22 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

Thursday 18 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Clause 24

National security exemption

11.30 am

Question (16 May) again proposed, That the clause stand part of the Bill.

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

Amendment 105, in clause 25, page 44, line 6, leave out "must consult the Commissioner" and insert

"must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek the approval of the Commissioner.

Clauses 25 and 26 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): When the Committee last adjourned, I had already spoken to clauses 24 to 26 and was responding to amendment 105, which was tabled by the hon. Member for Barnsley East. However, let me give a quick recap.

Clauses 24 to 26 are essentially designed to enable better joined-up working between the intelligence services and law enforcement. To that end, they will allow qualifying authorities to use part 4 of the data protection regime, but the Secretary of State will be required to issue a designation notice. We believe that enabling qualifying competent authorities to jointly process data under one regime in authorised, specific circumstances will allow better control over data in a way that is not possible under two different data protection regimes.

Amendment 105 seeks to increase the role of the Information Commissioner's Office by requiring it to judge whether the designation notice is required for the purposes of safeguarding national security. The Bill requires the Secretary of State to consult the ICO as part of the Secretary of State's decision whether to grant a notice, but it is not the function of the ICO in its capacity as a regulator to assess national security requirements. The ICO's expertise is in data protection, not in national security, and it would be inappropriate for it to decide on the latter; that decision should be reserved to the Secretary of State. We believe that clause 25 provides significant safeguards through proposed new sections 82B and 82E, which provide respectively for legal challenge and annual review of a notice. In addition, should the notice no longer be required, the Secretary of State can withdraw it. For that reason, we cannot accept the amendment.

Stephanie Peacock (Barnsley East) (Lab): I spoke to amendment 105 in our last sitting. In summary, the Bill contains a requirement to consult the commissioner. The amendment seeks to formalise some of the independent oversight of the designation notice process so that the power does not lie solely in the Secretary of State's hands. The matter of the Secretary of State's power is obviously something with which we take issue throughout the Bill. The amendment would not stop any designation notice being issued where it is genuinely necessary; it would simply add a safeguard for its approval where it is not. For that reason, I will press the amendment to a vote.

Question put and agreed to.

Clause 24 accordingly ordered to stand part of the Bill.

Clause 25

Joint processing by intelligence services and competent authorities

Amendment proposed: 105, in clause 25, page 44, line 6, leave out "must consult the Commissioner" and insert "must apply to the Commissioner for authorisation of the designation notice on the grounds that it satisfies subsection (1)(b)."—*(Stephanie Peacock.)*

This amendment seeks to increase independent oversight of designation notices by replacing the requirement to consult the Commissioner with a requirement to seek the approval of the Commissioner.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 20]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

Clause 25 ordered to stand part of the Bill.

Clause 26 ordered to stand part of the Bill.

Clause 27

Duties of the Commissioner in carrying out functions

Amendment proposed: 106, in clause 27, page 47, line 27, after "subjects", insert "decision subjects,".—*(Stephanie Peacock.)*

This amendment would require the ICO to have regard to decision subjects (see NC12) as well as data subjects as part of its obligations.

The Committee divided: Ayes 6, Noes 9.

Division No. 21]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

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

Sir John Whittingdale: We now come to the provisions in the Bill relating to the powers of the Information Commissioner. Clause 27 will introduce a new strategic framework for the Information Commissioner when carrying out his functions under data protection legislation. The framework contains a principal data protection objective and a number of general duties.

The legislation does not currently provide the commissioner with a framework of strategic objectives to help to prioritise activities and resources, evaluate performance and be held accountable by stakeholders. Instead, the commissioner is obliged to fulfil a long list of tasks and functions without a clear strategic framework to guide his work.

The clause introduces a principal objective for the commissioner, first to secure an appropriate level of protection for personal data, taking into account the interests of data subjects, controllers and others along with matters of general public interest, and secondly to promote public trust and confidence in the processing of personal data. This principal objective will replace section 2(2) of the Data Protection Act 2018.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): How does the Minister think the words

"an appropriate level of protection for personal data"

should be understood by the Information Commissioner? Is it in the light of the duties that follow, or what?

Sir John Whittingdale: Obviously that is a matter for the Information Commissioner, but that is the overriding principal objective. I am about to set out some of the other objectives that the clause will introduce, but it is made very clear that the principal objective is to ensure the appropriate level of protection. Precisely how the Information Commissioner interprets "appropriate level of protection" is a matter for him, but I think it is fairly clear what that should entail, as he himself set out in his evidence.

As I have said, clause 27 introduces new duties that the commissioner must consider where they are relevant to his work in carrying out data protection functions: the desirability of promoting innovation and competition; the importance of the prevention, investigation, detection and prosecution of criminal offences; the need to safeguard public security and national security; and, where necessary, the need to consult other regulators when considering how the ICO's work may affect economic growth, innovation and competition. There is also the statement of strategic priorities, which is introduced by clause 28. However, as I have indicated to the hon. Member for Newcastle upon Tyne Central, the commissioner will be clear that his primary focus should be to achieve the principal objective.

Clause 27 also introduces new reporting requirements for the commissioner in relation to the strategic framework. The commissioner will be required to publish a forward-looking strategy outlining how he intends to meet the new principal objective and duties, as well as pre-existing duties in the Deregulation Act 2015 and the Legislative and Regulatory Reform Act 2006.

Finally, the commissioner will be required to publish a review of what he has done to comply with the principal objective, and with the new and existing duties, in his annual report.

Carol Monaghan (Glasgow North West) (SNP): I wonder whether part of the strategy might include a list of fees that could potentially be charged for accessing data. This idea of fees seems to be quite vague in terms of amounts and levels, so it would be useful to have some more information on that.

Sir John Whittingdale: I think we will come on to some of the questions around the fees that are potentially payable, particularly by those organisations that may be required to provide more evidence, and the costs that that could entail. I will return to that subject shortly.

The new strategic framework acknowledges the breadth of the ICO's remit and its impact on other areas. We believe that it will provide clarity for the commissioner, businesses and the general public on the commissioner's objectives and duties. I therefore commend clause 27 to the Committee.

Stephanie Peacock: The importance to any data protection regime of an independent, well-functioning regulator cannot be overstated. The ICO, which is soon to be the Information Commission as a result of this Bill, is no exception to that rule. It is a crucial piece of the puzzle in our regime to uphold the information rights set out in regulation. Importantly, it works in the interests of the general public. The significance of an independent regulator is also recognised by the European Commission, which deems it essential to any adequacy agreement. The general duties of our regulator, such as those set out in this clause, are therefore vital because they form the foundations on which it operates and the principles to which it must be accountable.

Although the duties are more an indicator of overarching direction than a prescriptive list of duties, they should still aim to reflect the wide range of tasks that the regulator carries out and the values with which they do so. On the whole, the clause does this well. Indeed, the principal objective for the commissioner set out in this clause, which is

"to secure an appropriate level of protection for personal data, having regard to the interests of data subjects, controllers and others and matters of general public interest, and…to promote public trust and confidence in the processing of personal data"

is a good overarching starting point. It simply outlines the basic functions of the regulator that we should all be able to get behind, even if the Bill itself does disappointingly little to encourage the promotion of public trust in data processing.

It is particularly welcome that the principal objective includes specific regard to

"matters of general public interest."

This should cover things like the need to consider sustainability and societal impact. However, it is a shame that that is not made explicit among the sub-objectives,

[Stephanie Peacock]

which require the commissioner to have regard to the likes of promoting innovation and safeguarding national security. That would have ingrained in our culture a desire to unlock data for the wider good, not just for the benefit of big tech. Overall, however, the responsibilities set out in the clause, and the need to report on fulfilling them, seem to reflect the task and value of the regulator fairly and accurately.

Sir John Whittingdale: I think that was slightly qualified support for the clause. Nevertheless, we welcome the support of the Opposition.

Question put and agreed to.

Clause 27 accordingly ordered to stand part of the Bill.

Clause 28

STRATEGIC PRIORITIES

11.45 am

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

Sir John Whittingdale: Clause 28 provides a power for the Secretary of State to prepare a statement of strategic priorities relating to data protection as part of the new strategic framework for the Information Commissioner. The statement will contain only the Government's data protection priorities, and the Secretary of State may choose to include both domestic and international priorities. That will enable the Government to provide a transparent statement of how their data protection priorities fit in with their wider agenda, giving the commissioner, we hope, helpful context.

Although the commissioner must take the statement into account when carrying out his functions, he is not required to act in accordance with it. That means that the statement will not be used in a way to direct what the commissioner may and may not do. Once the statement is drafted, the Secretary of State will be required to lay it before Parliament, where it will be subject to the negative resolution procedure before it can be designated. The commissioner will need to consider the statement when carrying out functions under the data protection legislation, except functions relating to a particular person, case or investigation.

Once designated, the commissioner will be required to respond to the statement, outlining how he intends to consider it in future data protection work. The commissioner will also be required to report on how he has considered the statement in his annual report. I commend the clause to the Committee.

Stephanie Peacock: Clause 28 requires that every three years the Secretary of State publish a statement of strategic priorities for the commissioner to consider, respond to, and have regard to. The statement would be subject to the negative resolution procedure in Parliament, and the commissioner would be obliged to report on what they have done to comply with it annually. Taken in good faith, I see what the clause was intended to achieve. It is, of course, important that the Government's data priorities are understood by the commissioner. It is also vital that we ensure that the regulator functions in line with the most relevant issues of the day, given the rapidly evolving landscape of technology.

A statement of strategic priorities could, in theory, allow the Government to set out their priorities on data policy in a transparent way, allowing both Ministers and the ICO to be held accountable for their relationship. However, there is and must be a line drawn between the ICO understanding the modern regulatory regime that it will be expected to uphold and political interference in the activities and priorities of the ICO. The Open Rights Group, among others, has expressed concern that the introduction of a statement of strategic priorities could cross that line, exposing the ICO to political direction, making it subject to culture wars and leaving it vulnerable to corporate capture or even corruption.

Although the degree to which those consequences would become a reality given the current strength of our regulator might be up for debate, the very concept of the Government setting out a statement of strategic priorities that must be adhered to by the commissioner at the very least sets out a need for the ICO to follow some sort of politically led direction, something that seems counterintuitive with respect to independence. As I have already argued, an independent ICO is vital not only directly, for data subjects to be sure that their rights will be implemented and for controllers to be sure of their obligations, but indirectly, as a crucial component of our EU adequacy agreement.

Even though the clause may not be intended to threaten independence, we must be extremely careful not to unintentionally embark on a slippery slope, particularly as there are other mechanisms for ensuring that the ICO keeps up with the times and has a transparent relationship with Government. In 2022, the ICO published its new strategic plan, ICO25, which sets out why its work is important, what it wants to be known for and by whom, and how it intends to achieve that by 2025. It describes the ICO's purpose, objectives and values and the shift in approach that it aims to achieve through the life of the plan, acknowledging that its work is

"complex, fast moving and ever changing."

The plan was informed by extensive stakeholder consultation and by the responsibilities that the ICO has been given by Parliament. There are therefore ways for the ICO to communicate openly with Government, Parliament and other relevant stakeholders to ensure that its direction is in keeping with the most relevant challenges and with updates to legislation and Government activity. Ministers might have been better off encouraging transparent reviews, consultations and strategies of that kind, rather than prompting any sort of interference from politicians with the ICO's priorities.

Sir John Whittingdale: We agree about the importance of the independence of the Information Commissioner, but I do not think that the statement, as we have set out, is an attempt to interfere with that. I remind the hon. Lady that in relation to the statement of strategic priorities, she asked the Information Commissioner himself:

"Do you perceive that having any impact on your organisation's ability to act independently of political direction?",

and he replied:

"No, I do not believe it will undermine our independence at all."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 6, Q3.]

Stephanie Peacock: The Minister is right to quote the evidence session, but he will perhaps also remember that in a later session Ms Irvine from the Law Society of Scotland said that she was surprised by the answer given by the Information Commissioner.

Sir John Whittingdale: Ms Irvine may have been surprised. I have to say that we were not. What the Information Commissioner said absolutely chimed with our view of the statement, so I am afraid on this occasion I will disagree with the Law Society of Scotland.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 22]

AYES

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

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 28 ordered to stand part of the Bill.

Clause 29

CODES OF PRACTICE FOR THE PROCESSING OF PERSONAL DATA

Amendment proposed: 108, in clause 29, page 53, line 11, at end insert—"(ba) decision subjects;".—*(Stephanie Peacock.)*

This amendment, together with Amendments 109 and 110, would require codes of conduct produced by the ICO to have regard to decision subjects (see NC12) as well as data subjects.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 23]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

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

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

Clause 30 stand part.

Amendment 111, in clause 31, page 56, line 30, leave out lines 30 and 31 and insert—

"(6) If the Commissioner submits a revised code under subsection (5)(b), the Secretary of State must approve the code."

This amendment seeks to limit the ability of the Secretary of State to require the Commissioner to provide a revised code to only one occasion, after which the Secretary of State must approve the revised code.

Clause 31 stand part.

Sir John Whittingdale: Given the significant number of ways in which personal data can be used, we believe that it is important that the regulator provides guidance for data controllers, particularly on complex and technical areas of the law, and that the guidance should be accessible and enable compliance with the legislation efficiently and easily. We are therefore making a number of reforms to the process by which the Information Commissioner produces statutory codes of practice.

Clause 29 is a technical measure that ensures that all statutory codes of practice issued under the Data Protection Act 2018 follow the same parliamentary procedures, have the same legal effect, and are published and kept under review by the Information Commissioner. Under sections 121 to 124 of the Data Protection Act, the commissioner is obliged to publish four statutory codes of practice: the data sharing code, the direct marketing code, the age-appropriate design code, and the data protection and journalism code. The DPA includes provisions concerning the parliamentary approval process, requirements for publication and review by the commissioner, and details of the legal effect of each of the codes. So far, the commissioner has completed the data sharing code and the age-appropriate design code.

Section 128 of the Act permits the Secretary of State to make regulations requiring the Information Commissioner to prepare other codes that give guidance as to good practice in the processing of personal data. Those powers have not yet been used, but may be useful in the future. However, due to the current drafting of the provisions, any codes required by regulations made by the Secretary of State and issued by the commissioner would not be subject to the same formal parliamentary approval process or review requirements as the codes issued under sections 121 to 124. In addition, they do not have the same legal effect, and courts and tribunals would not be required to take a relevant provision of the code into account when determining a relevant question. Clearly, it is not appropriate to have two different standards of statutory codes of practice. To address that, clause 29 replaces the original section 128 with new section 124A, so that codes required in regulations made by the Secretary of State follow a similar procedure to codes issued under sections 121 to 124.

New section 124A provides the Secretary of State with the power to make regulations requiring the commissioner to produce codes of practice giving guidance as to good practice in the processing of personal data. Before preparing any code, the commissioner must consult the Secretary of State and other interested parties such as trade associations, data subjects and groups representing data subjects. That is similar to the consultation requirements for the existing codes. The parliamentary approval processes and requirements for the ICO to keep existing codes under review are also extended to

[Sir John Whittingdale]

any new codes required by the Secretary of State. The amendment also ensures that those codes requested by the Secretary of State have the same legal effect as those set out on the face of the DPA.

Clauses 30 and 31 introduce reforms to the process by which the commissioner develops statutory codes of practice for data protection. They require the commissioner to undertake and publish impact assessments, consult with a panel of experts during the development of a code, and submit the final version of a code to the Secretary of State for approval. Those processes will apply to the four statutory codes that the commissioner is already required to produce and to any new statutory codes on the processing of personal data that the commissioner is required to prepare under regulation made by the Secretary of State.

The commissioner will be required to set up and consult a panel of experts when drafting a statutory code. That panel will be made up of relevant stakeholders and, although the commissioner will have discretion over its membership, he or she will be required to explain how the panel was chosen. The panel will consider a draft of a statutory code and submit a report of its recommendations to the commissioner. The commissioner will be required to publish the panel's response to the code and, if he chooses not to follow a recommendation, the reasons must also be published.

Clause 30 also requires the commissioner to publish impact assessments setting out who will be affected by the new or amended code and the impact it will have on them. While the commissioner currently carries out impact assessments when developing codes of practice, we believe that there are advantages to formalising an approach on the face of the legislation to ensure consistency.

Given the importance of the statutory codes, we believe it is important that there is a further degree of democratic accountability within the process. Therefore, clause 31 requires the commissioner to submit the final version of a statutory code to the Secretary of State for approval.

On that basis, I commend the relevant clauses to the Committee, but I am aware that the hon. Member for Barnsley East wishes to propose an amendment.

Stephanie Peacock: I turn first to clauses 29 and 30. Codes of practice will become increasingly important as the remit of the ICO expands and modernises. As such, it is important that the codes are developed in a way that is conducive to the product being as effective and useful as possible.

Although the ICO already carries out impact assessments for new codes of practice, that is only done as best practice and currently does not have any statutory underpinning. It is therefore pleasing to see clauses that will require consistency and high standards when developing new codes, ensuring that the resulting products are as comprehensive and helpful as possible. It is welcome, for example, to see that experts will be consulted in the process of developing these codes, including Government officials, trade associations and data subjects. It is also good to see that the commissioner will be required to publish a statement relating to the establishment of the expert panel, including how and why members were selected.

12 noon

Given recent scandals that have shown that appointments to positions of power can be vulnerable, it is good practice to have transparency on the credentials of the panel, and how each of them came to be in such a position. That transparency is also reflected in the requirement for the commissioner to publish an explanation in any case where the panel's recommendations are not accepted. That will ensure that proper consideration must be taken of the panel's input, and it makes the commissioner accountable to the public.

I turn to clause 31 and amendment 111. Given the transparent and comprehensive statutory procedure set out in clause 30 to ensure that codes of practice are developed in conjunction with officials, industry and data subjects, and informed by expertise, the addition of the clause seems somewhat counterintuitive. Indeed, having already passed through the rigorous and transparent procedure, the clause allows codes of practice to be subject to endless interference from the Secretary of State, who—no matter their level of expertise or their intention—would be able to veto the codes, and send them back to the commissioner with recommendations for changes as many times as they wanted or needed to.

That level of interference from a politically appointed and motivated Minister in the product of an independent regulator has caused a lot of concern across a range of stakeholders. Indeed, almost every civil society group and trade association I engaged with in the run up to the Committee has raised concerns that the procedure could threaten the independence of the ICO altogether. That was also reflected in the consultation responses to the proposal in "Data: a new direction," in which the Government admitted that a majority of people disagreed, citing concerns about the risk to independence.

This matters—not just inherently, but for public trust in the entire system of data protection. Any interpretation or potential that the independence of the commissioner is being downgraded could have a knock-on impact on the public's ability to trust in its functions and, in turn, their ability to exercise their rights. Furthermore, it matters for the maintenance of our adequacy agreement with the EU, as such agreements rely heavily on the existence of a truly independent and functioning regulator.

I will again cite the figures from the Government's own impact assessment, in which it is acknowledged that losing the agreement could cost up to £460 million as a one-off and £410 million every year afterwards. That is based on a direct reduction in UK-EU trade, and it may be even larger when accounting for onward supply chains with trade with third countries. It is therefore a concern for not just those most interested in data rights—though their input is, of course, crucial—but every single business that relies on EU adequacy and all of us who live in the economy that benefits from it.

To try to counteract concerns over the process, the Secretary of State will be required to publish their rationale for approving or not approving a code. Though the principle of transparency is always welcome, it is unfortunately not enough in this instance to justify any compromise—perceived or otherwise—to the independence of the ICO. Furthermore, there are no stated limits on the reasons that a Secretary of State might be able to refuse a code, even if they are made in bad faith or under severe misguidance, meaning that further harms may occur as a result of the changes. Given the scale of

the risks I have outlined, I am keen to hear from the Minister what the real benefit of the clause is. What value is there in the Secretary of State being able to endlessly interfere with an expertly formed code that they themselves have requested?

Amendment 111 recognises that there may be a very limited set of circumstances in which the Secretary of State may wish to comment on a code and correct an oversight or major misinterpretation of the law. Indeed, the Government say in their consultation response that the measure is intended as a "final safeguard". However, such instances should take only one round of amendments to resolve. The amendment would therefore accommodate one statement from the Secretary of State but give the regulator the ultimate say on its contents, ensuring that there is no risk of its independence being at stake. Anything more than that would put data rights, independence, and potentially adequacy at risk.

Sir John Whittingdale: I welcome the support of the Opposition for many of the principles contained in the clauses. I turn to amendment 111, tabled by the hon. Lady. As the clause originally sets out, once the commissioner is issued the final version of the code, the Secretary of State decides whether to approve it. If they do approve the code, it will be laid before Parliament for final approval. If they do not, they are required to publish their reasons.

The amendment would place a limit on that, so that the Secretary of State would be able to reject the final version of the code only once. If the code is revised by the commissioner in the light of the comments of the Secretary of State and resubmitted, under the amendment the Secretary of State would have to lay the code in Parliament for final approval. Although I understand the concern behind the amendment, we do not believe it to be justified. I understand that the hon. Lady does not want a code to be rejected multiple times, but we regard this as a final safeguard and it will be fully transparent. We are absolutely committed to maintaining the commissioner's independence, but we think it also important that the Government have the opportunity to give a view before the code is laid before Parliament and for Parliament to give final approval. The amendment would unduly limit the Government's ability to provide as necessary that further degree of democratic accountability.

The hon. Lady referred to the importance of maintaining adequacy, which we have already touched on. I fully share her view on its importance to the wider functioning of the economy, but when she raised the matter with the Information Commissioner he did not believe that it posed any risk. Indeed, he went on to point out:

"A failure of the Secretary of State to table and issue a proposed code would not affect the way in which the commissioner discharges his or her enforcement functions. We would still be able to investigate matters and find them in breach, regardless of whether that finding was consistent with the Secretary of State's view of the law."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 6-7, Q4.]

On that basis, we think that there should be the ongoing ability for the Secretary of State—and, through the Secretary of State, Parliament—to approve the final version of the code, but we do not feel that this interferes with the Information Commissioner's ability to carry out his functions, nor does it represent any view as to our adequacy agreement.

Stephanie Peacock: The problem is that the Government are operating on the basis that everyone is acting in good faith, and although I am sure that the Minister and the current Secretary of State are doing so, we do not know what the future holds. It was incredibly encouraging that throughout the evidence sessions a number of witnesses said they did not feel that adequacy was at threat. That is welcome and reassuring, but only the EU Commission can give us adequacy. I am afraid the Minister simply has not done enough to alleviate my concerns about the independence of the ICO. I understand that the Minister disagrees with the Law Society of Scotland, but the full quote was:

"The ICO is tasked with producing statutory codes of conduct, which are incredibly useful for my clients and for anyone working in this sector. The fact that the Secretary of State can, in effect, overrule these is concerning, and it must be seen as a limit on the Information Commissioner's independence."—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 74, Q156.]

As such, I will push my amendment to a vote.

Question put and agreed to.

Clause 29 accordingly ordered to stand part of the Bill.

Clause 30 ordered to stand part of the Bill.

Clause 31

CODES OF PRACTICE: APPROVAL BY THE SECRETARY OF STATE

Amendment proposed: 111, in clause 31, page 56, line 30, leave out lines 30 and 31 and insert—

"(6) If the Commissioner submits a revised code under subsection (5)(b), the Secretary of State must approve the code."—*(Stephanie Peacock.)*

This amendment seeks to limit the ability of the Secretary of State to require the Commissioner to provide a revised code to only one occasion, after which the Secretary of State must approve the revised code.

Question put, That the amendment be made.

The Committee divided: Ayes 6, Noes 9.

Division No. 24]

AYES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

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

The Committee divided: Ayes 9, Noes 6.

Division No. 25]

AYES

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

NOES

Huq, Dr Rupa	Onwurah, Chi
Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

Question accordingly agreed to.

Clause 31 ordered to stand part of the Bill.

Clause 32

VEXATIOUS OR EXCESSIVE REQUESTS MADE TO THE COMMISSIONER

Amendments made: 40, in clause 32, page 57, line 16, leave out paragraphs (a) and (b) insert—

"(a) for the heading substitute "Vexatious or excessive requests",

(b) before subsection (1) insert—

"(A1) This section makes provision about cases in which a request made to the Commissioner, to which the Commissioner is required or authorised to respond under the data protection legislation, is vexatious or excessive (see section 204A).",

(ba) in subsection (1) omit the words from the beginning to "excessive,",

(bb) after subsection (1) insert—

"(1A) In subsection (1)—

(a) the reference in paragraph (a) to charging a reasonable fee is, in a case in which section 134 is relevant, a reference to doing so under that section, and

(b) paragraph (b) is not to be read as implying anything about whether the Commissioner may refuse to act on requests that are neither vexatious nor excessive.","

This amendment adds further amendments of section 135 of the Data Protection Act 2018 to clause 32 to make clear that the Information Commissioner may refuse to deal with a vexatious or excessive request made by any person.

Amendment 41, in clause 32, page 57, line 21, after "(3)" insert "—

"(i) for "(1)" substitute "(A1)", and

(ii)".—*(Sir John Whittingdale.)*

This amendment is consequential on Amendment 40.

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

Sir John Whittingdale: Taking advantage of your invitation, Mr Hollobone, I shall speak only briefly. The UK's data protection framework allows a data subject or data protection officer to make a request to the Information Commissioner for information concerning the exercise of their data protection rights. The commissioner is expected to respond to a data subject or data protection officer and make no charge in the majority of cases, but the commissioner can refuse to respond or charge a reasonable fee for a response to a request when it is "manifestly unfounded or excessive". Clause 7 changes the "manifestly unfounded or excessive" threshold for all requests from data subjects across the UK data protection framework to "vexatious or excessive". Clause 32 replicates that language, inserting the same new threshold into section 135 of the Data Protection Act 2018, to ensure that the Information Commissioner's exemption is consistent across the legislation. I urge the Committee to agree to the clause.

Stephanie Peacock: The new threshold contained in the clause has been discussed in debates under clause 7, and I refer hon. Members to my remarks in those debates, as many of the same concerns apply. The guidance that will be needed to interpret the terms "vexatious" and "excessive" should be no less applicable to the Information Commissioner, whose co-operation with data subjects and transparency should be exemplary, not least because the functioning of the regulator inherently sets an example for other organisations on how the rules should be followed.

Question put and agreed to.

Clause 32, as amended, accordingly ordered to stand part of the Bill.

Clause 33

ANALYSIS OF PERFORMANCE

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

Sir John Whittingdale: Clause 33 introduces the requirement for the Information Commissioner to prepare and publish an analysis of their performance, using key performance indicators. The regulator will be required to publish that analysis at least annually. The commissioner will have the discretion to decide which factors effectively measure their performance.

Improving the commissioner's monitoring and reporting mechanisms will strengthen their accountability to Parliament, organisations and the public, who have an interest in the commissioner's effectiveness. Performance measurement will also have benefits for the commissioner, including by supporting their work of measuring progress towards their objectives and ensuring that resources are prioritised in the right areas. I urge that clause 33 stand part of the Bill.

Stephanie Peacock: I welcome the clause, as did the majority of respondents who supported the proposal in the "Data: a new direction" consultation. As recognised by the Government's response to their consultation, respondents felt the proposal would allow for the performance of the ICO to be assessed publicly and provide evidence of how the ICO is meeting its statutory obligations. We should do all we can to promote accountability, transparency and public awareness of the obligations and performance of the ICO. The clause allows for just that.

Question put and agreed to.

Clause 33 accordingly ordered to stand part of the Bill.

Clause 34

POWER OF THE COMMISSIONER TO REQUIRE DOCUMENTS

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

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

Clauses 35 to 38 stand part.

Government amendment 47.

Clause 42 stand part.

12.15 pm

Sir John Whittingdale: This is a slightly chunkier set of clauses and amendments, so I will not be as brief as in the last two debates.

Clause 34 is a clarificatory amendment to the Information Commissioner's powers in section 142 of the Data Protection Act to require information. Its purpose is to clarify the commissioner's existing powers to put it beyond doubt that the commissioner can require specific documents as well as information when using the information notice power. Subsections (3) to (7) of the clause make consequential amendments to references to information notices elsewhere in the Data Protection Act.

Clause 35 makes provision for the Information Commissioner to require a data controller or processor to commission a report from an approved person on a specified matter when exercising the power under section 146 of the Data Protection Act to issue an assessment notice. The aim of the power is to ensure that the regulator can access information necessary to its investigations.

In the event of a data breach, the commissioner is heavily dependent on the information that the organisation provides. If it fails to share information—for example, because it lacks the capability to provide it—that can limit the commissioner's ability to conduct a thorough investigation. Of course, if the organisation is able to provide the necessary information, it is not expected that the power would be used. The commissioner is required to act proportionately, so we expect that the power would be used only in a small minority of investigations, likely to be those that are particularly complex and technical in nature.

Clause 36 grants the Information Commissioner the power to require a person to attend an interview and answer questions when investigating a suspected failure to comply with data protection legislation. At the moment, the Information Commissioner can only interview people who attend voluntarily, which means there is a heavy reliance on documentary evidence. Sometimes that is ambiguous or incomplete and can lead to uncertainty. The ability to require a person to attend an interview will help to explain an organisation's practices or evidence submitted, and circumvent a protracted and potentially fruitless series of back-and-forth communication via information notices. The power is based on existing comparable powers for the Financial Conduct Authority and the Competition and Markets Authority.

Clause 37 amends the provisions for the Information Commissioner to impose penalties set out in the Data Protection Act. It will allow the commissioner more time, where needed, to issue a final penalty notice after issuing a notice of intent. At the moment the Act requires the commissioner to issue a notice of intent to issue a penalty notice; the commissioner then has up to six months to issue the penalty notice unless an extension is agreed. That can prove difficult in some cases—for instance, if the organisation under investigation submits new evidence that affects the case at a late stage, or when the legal representations are particularly complex. The clause allows the regulator more time to issue a final penalty notice after issuing a notice of intent, where that is needed. That will benefit business, as it means the commissioner can give organisations more time to prepare their representations, and will result in better outcomes by ensuring that the commissioner has sufficient time to assess representations and draw his conclusions.

Clause 38 introduces the requirement for the Information Commissioner to produce and publish an annual report on regulatory activity. The report will include the commissioner's investigatory activity and how the regulator has exercised its enforcement powers. That will lead to greater transparency of the commissioner's regulatory activity.

Clauses 34 to 37, as I said, make changes to the Data Protection Act 2018 in respect of the Information Commissioner's enforcement powers. Consequential on clauses 35 and 36, clause 42 makes changes to the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016, known as the EITSET regulations. The EITSET regulations extend and modify the Information Commissioner's enforcement powers to apply to its role as the supervisory body for trust service providers under the UK regulations on electronic identification and trust services for electronic transactions, known as the UK eIDAS. Clause 42 amends the EITSET regulations to ensure that the new enforcement powers introduced by clauses 34 to 37 are available to the Information Commissioner for the purposes of regulating trust service providers.

The new powers will help to ensure that the Information Commissioner is able to access the evidence needed to inform investigations. The powers will result in more informed investigations and, we believe, better outcomes. Clause 42 ensures that the Information Commissioner will continue to be able to act as an effective supervisory body for trust service providers established in the UK.

Government amendment 47 amends schedule 2 to the EITSET regulations. The amendment 2 is consequential to the amendment of section 155(3)(c) of the Data Protection Act made by schedule 4 to the Bill. The amendment to schedule 2 will remove the reference to consultation under section 65 of the Data Protection Act when section 155 is applied. It is necessary to remove reference to section 65 of the Data Protection Act when section 155 is applied with modification under schedule 2, as consultation requirements under that section are not relevant to the regulation of trust service providers under the UK eIDAS.

I hope that that is helpful to Members in explaining the merits of our approach to ensuring that the Information Commissioner has the right enforcement tools at its disposal and continues to be an effective and transparent regulator. I commend the clauses and Government amendment 47 to the Committee.

Stephanie Peacock: I will speak to each of the relevant clauses in turn. On clause 34, I am satisfied that the clarification that the Information Commissioner can require documents as well as information is necessary and will be of use to the regulator. I am pleased therefore pleased to accept the clause as drafted and to move on to the other clauses in this part.

Clause 35 provides for the commissioner to require an approved person to prepare a report on a specified matter, as well as to provide statutory guidance on, first, the factors it considers when deciding to require such a report and, secondly, the factors it considers when determining whom the approved person might be. That

[Stephanie Peacock]

power to commission technical reports is one that the vast majority of respondents to the "Data: a new direction" consultation supported, as they felt it would lead to better informed ICO investigations. Any measures that help the ICO to carry out its duties rigorously and to better effect, while ensuring that relevant safeguards apply, are measures that I believe Members across the Committee will want to support.

In the consultation, however, the power was originally framed to commission a "technical report", implying that it would be limited to particularly complex and technical investigations where there is significant risk of harm or detriment to data subjects. Although the commissioner is required to produce guidance on the circumstances in which a report might be required, I would still like clarification from the Minister of why such a limit was not included in the Bill as drafted. Does he expect it to be covered by the guidance produced by the ICO? Such a clarification is necessary not because we are against clause 35 in principle, just in acknowledgement that ICO's powers—indeed, enforcement powers generally—must always be proportionate to the task at hand.

Furthermore, some stakeholders have said that it is unclear whether privilege will attach to reports required by the ICO and whether they may be disclosable to third parties who request copies of them. Greater clarity about how the power will operate in practice would therefore be appreciated.

Turning to clause 36, it is a core function of the ICO to monitor and enforce the UK's data protection legislation and rules, providing accountability against the activities of all controllers, processors and individuals. To fulfil that function, the ICO may have to conduct an investigation to establish a body of evidence and determine whether someone has failed to comply with the legislation. The Government's consultation document said that the ICO sometimes faces problems engaging organisations in those investigations, despite their having a duty to co-operate fully, especially in relation to interviews, as many people are nervous of negative consequences in their life or career if they participate in one. However, interviews are a crucial tool for investigations, as not all the relevant evidence will be available in written form. Indeed, that may become even more the case after the passing of this Bill, due to the reduced requirements to keep records, conduct data protection impact assessments and assign data protection officers—all of which contribute to a larger pool of documentation tracking data processing.

Clause 36, which will explicitly allow the ICO to compel witnesses to comply with interviews as part of an investigation, will, where necessary, ensure that as much relevant evidence as possible is obtained to inform the ICO's judgment. That is something that we absolutely welcome. It is also welcome to see the safeguards that will be put in place under this clause, including the right not to self-incriminate and exemptions from giving answers that would infringe legal professional privilege or parliamentary privilege. That will ensure that the investigatory powers of the ICO stay proportionate to the issues at hand. In short, clause 36 is one that I am happy to support. After all, what is the purpose of us ensuring that data protection legislation is fit for purpose here today if the ICO is unable to actually determine whether anyone is complying?

On clause 37, it seems entirely reasonable that the ICO may require more than the standard six months to issue a penalty notice in particularly complex investigations. Of course, it remains important that the operations of the ICO are not allowed to slow unduly in cases where a penalty can be issued in the usual timeframe, but where the subject matter is particularly complicated, it makes sense to allow the ICO an extension to enable the investigation to be concluded in the proper, typically comprehensive manner. Indeed, complex investigations may be more common as we adjust to the new data legislation and a rapidly evolving technological landscape. By conducting the investigations properly and paying due attention to particularly technical issues, new precedents can be set that will speed up the regulator's processes on the whole. Clause 37 is therefore welcomed by us, as it was by the majority of respondents to the Government's consultation.

Turning to clause 38, as we have said multiple times throughout the progress of this Bill and in Committee, transparency and data protection should go hand in hand. Requiring the ICO to publish information each year on the investigations it has undertaken and the powers it has used will embed a further level of transparency into the regulatory system. Transparency breeds accountability, and requiring the regulator to publish information on the powers it is using will encourage such powers to be used proportionately and appropriately. Publishing an annual report with that information should also give us a better idea of how effectively the new regulatory regime is working. For example, a high volume of cases on a recurring issue could indicate a problem within the framework that needs addressing. Overall, it is welcome that Parliament and the public should be privy to information about how the ICO is discharging its regulatory functions. As a result, I am pleased to support clause 38.

Finally, the amendments to clause 42 are of a consequential nature, and I am happy to proceed without asking any further questions about them.

Sir John Whittingdale: I am most grateful to the hon. Lady for welcoming the vast majority of the provisions within these clauses. She did express some concern about the breadth of the powers available to the Information Commissioner, but I point out that they are subject to a number of safeguards defining how they can be used. The commissioner is required to publish how he will exercise his powers, and that will provide organisations with clarity on the circumstances in which they are to be used.

As the hon. Lady will be aware, like other regulators, the Information Commissioner is subject to the duty under the Legislative and Regulatory Reform Act to exercise their functions

"in a way which is transparent, accountable, proportionate and consistent",

and,

"targeted only at cases in which action is needed."

There will also be a right of appeal, which is consistent with the commissioner's existing powers. On that basis, I hope that the hon. Lady is reassured.

Question put agreed to.

Clause 34 accordingly ordered to stand part of the Bill.

Clauses 35 to 38 ordered to stand part of the Bill.

Clause 39

COMPLAINTS TO CONTROLLERS

12.30 pm

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

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

Clauses 40 and 41 stand part.

That schedule 8 be the Eighth schedule to the Bill.

Sir John Whittingdale: These three clauses, together with schedule 8, streamline and clarify complaint routes for data subjects by making the respective rights and responsibilities of data controllers and data subjects clear in legislation. The measures will reduce the volume of premature complaints to the Information Commissioner, and give an opportunity to controllers to resolve complaints before they are escalated to the regulator.

Clause 39 enables data subjects to complain to a data controller if they believe that there has been an infringement of their data protection rights, and creates a duty for data controllers to facilitate the making of complaints by taking appropriate steps, such as providing a complaints form. The requirement will encourage better conversations and more dialogue between data subjects and data controllers. It will formalise best practice, and align with the standard procedures of other ombudsman services, which require complainants to seek to resolve an issue with the relevant organisation before escalation. The clause also introduces a regulation-making power for the Secretary of State to require controllers to notify the Information Commissioner of the number of complaints made to them in circumstances specified in the regulations.

Clause 40 provides the Information Commissioner with a new power to refuse to act on certain data protection complaints if certain conditions are met, specifically if the complaint has not been made to the relevant controller; the controller has not finished handling the complaint and less than 45 days have elapsed since it was made; or the complaint is considered vexatious or excessive, as defined in the Bill. For example, that could be the case with a complaint that repeats a previous complaint made by the data subject to the commissioner. The power is in addition to the discretion that the commissioner can already exercise to "take appropriate steps" to respond to a complaint and investigate it "to the extent appropriate." The clause requires the Information Commissioner to publish guidance about how it will respond to complaints and exercise its power to refuse to act on complaints. Finally, the clause also outlines the process for appeals if the commissioner refuses to act on a data protection complaint.

Clause 41 introduces schedule 8, which contains miscellaneous minor and consequential amendments to the UK General Data Protection Regulation and the Data Protection Act relating to complaints by data subjects.

Schedule 8 makes consequential amendments to the UK GDPR and the DPA relating to complaints by data subjects, which will ensure consistency across data protection legislation in relation to the changes to the complaints framework under clauses 39 and 40.

Stephanie Peacock: I will focus most of my remarks on the group on clauses 39 and 40, as clause 41 and schedule 8 contain mostly consequential provisions, as the Minister outlined.

There are two major sections to the clauses. First, they require a complainant to issue their complaint to the controller directly, through allowing the commissioner to refuse to process their complaint otherwise. Secondly, they require the commissioner to refuse any complaint that is vexatious or excessive. I will speak to both in turn.

As the ICO grows and its remit expands, given the rapidly growing use of data in our society, it makes sense that its resources should be focused where they are most needed. Indeed, when giving evidence to the Committee, the Information Commissioner and Paul Arnold of the ICO stated that their current duty to investigate all complaints is creating a burden on their resources. Therefore, the proposal to require that complainants reach out to their data controller first, before contacting the ICO, seems to make sense, as it will allow the regulator to move away from handling low-level complaints, or complaints that are under way but not yet resolved. Instead, it would be able to refocus resources into handling complaints that have been mishandled or that offer a serious threat to data rights and public trust in data use.

Though that may be seen by some businesses and controllers as shifting an extra requirement on to them, the move should be viewed overall as a positive one, as it will require controllers to have clear processes in place for handling complaints and hopefully incentivise against conducting the kind of unlawful processing that prompts complaints in the first place. Indeed, the ICO already encourages that type of best practice, with complainants often encouraged to speak directly with the relevant data controller first before seeking help from the regulator. The clause would therefore simply formalise the arrangement, providing clarity on three levels. First, it would ensure that data subjects are clear on their right to complain directly to the controller. Secondly, it would ensure that controllers are clear on their duty to respond to such complaints. Finally, the ICO would be certain of its ability to refuse a request if the complainant refuses to comply with that model.

Although it is vital that the ICO is able to modernise and direct efforts where they are most needed, it is also vital that a healthy relationship is kept between the public—as data and decision subjects—and the ICO. The public must feel that the commissioner is there to support them in exercising their rights or seeking redress where necessary, not least because lodging a complaint can already be a difficult and distressing process. Indeed, even the commissioner himself said, when he first assumed his role, that he wanted to

"make it easy for people to access remedies if things go wrong."

As such, it is pleasing to see safeguards built into the clause that ensure a complainant can still escalate their complaint to the ICO, and appeal any refusal from the commissioner to a tribunal.

Data rights groups, such as the Open Rights Group, hold much more serious concerns about the ability to refuse vexatious and excessive requests. Indeed, they worry that the new power will allow the ICO to ignore widespread and systemic abuses of data rights. As was the case with subject access requests, the difference between a complaint made in anger—which is quite likely, given that the complainant believes they have suffered an abuse

[Stephanie Peacock]

of their rights—and a vexatious one must be clearly distinguished. The ICO should not be able to reject complaints of data abuses simply because the complainant acts in ways caused by distress.

As the response of the Government to their consultation reveals, only about half of respondents agreed with the proposal to set out criteria by which the ICO can decide not to investigate a complaint. The safeguard to appeal any refusal from the commissioner is therefore crucial in ensuring that there is a clear pathway for data subjects and decision subjects to dispute the decision of the ICO. It is also right that they should be informed of that safeguard, as well as told why their complaint has been refused, and given the opportunity to complain again with a more complete picture of information.

Overall, the clauses seems to strike the right balance between ensuring safeguards for data and decision subjects while helping the ICO to modernise. However, terms such as "vexatious" and "excessive" must be clearly defined to ensure that the ICO is able to exercise this new power of refusal proportionately and sensibly.

Carol Monaghan: I am looking for some clarification from the Minister. Under clause 39, it says:

"A controller must facilitate the making of complaints…such as providing a complaint form which can be completed electronically and by other means."

Can the Minister clarify whether every data controller will have to provide an electronic means of making a complaint? For many small data controllers, which would include many of us in the room, providing an electronic means of complaint might require additional expertise and cost that they may not have. If it said, "and/or by other means", which would allow a data controller to provide a paper copy, that might provide a little more reassurance to data controllers.

Sir John Whittingdale: Let me address the point of the hon. Member for Glasgow North West first. The intention of the clause is to ensure that complainants go first to the data controller, and the data controller makes available a process whereby complaints can be considered. I certainly fully understand the concern of the hon. Lady that it should not prove burdensome, particularly for small firms, and I do not believe that it would necessarily require an electronic means to do so. If that is not the case, I will tell her, but it seems to me that the sensible approach would be for data controllers to have a process that the Information Commissioner will accept is available to complainants first, before a complaint is possibly escalated to the next stage.

With regard to the point of the hon. Member for Barnsley East, we have debated previously the change in the threshold to "vexatious" and "excessive", and we may continue to disagree on that matter.

Question put and agreed to.

Clause 39 accordingly ordered to stand part of the Bill.

Clauses 40 and 41 ordered to stand part of the Bill.

Schedule 8 agreed to.

Clause 42

CONSEQUENTIAL AMENDMENTS TO THE EITSET REGULATIONS

Amendment made: 47, Clause 42, page 72, line 12, at end insert—

"(7A) In paragraph 13 (modification of section 155 (penalty notices)), in sub-paragraph (3)(c), for "for "data subjects"" there were substituted "for the words from "data subjects" to the end".".—*(Sir John Whittingdale.)*

This amendment inserts an amendment of Schedule 2 to the EITSET Regulations which is consequential on the amendment of section 155(3)(c) of the Data Protection Act 2018 by Schedule 4 to the Bill.

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

Clause 43

PROTECTION OF PROHIBITIONS, RESTRICTIONS AND DATA SUBJECT'S RIGHTS

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

Sir John Whittingdale: Clause 43 is a technical measure that creates a presumption that our data protection laws should not be overridden by future laws that relate to the processing of personal data, but it respects parliamentary sovereignty by ensuring that Parliament can depart from this presumption in particular cases if it deems it appropriate to do so. For example, if new legislation permitted or required an organisation to share personal data with another for a particular purpose, the default position in the absence of any specific indication to the contrary would be that the data protection legislation would apply to the new arrangement.

Damian Collins (Folkestone and Hythe) (Con): Will my right hon. Friend confirm that the provision will also apply with trade agreements? Certainly in the early stages of the negotiations for a UK-US trade agreement, the United States Government sought to include various provisions relating to tech policy. In such a scenario, would this legislation take precedence above anything written into a trade agreement?

Sir John Whittingdale: That would certainly be my interpretation. I do not see that a trade agreement could possibly overturn an Act of Parliament unless Parliament specifically sets out that it intends that that should be the case. This is a general protection, essentially saying that in all future cases data protection legislation applies unless Parliament specifically indicates that that should not be the case.

Until now, ensuring that any new data protection measures are read consistently with the data protection legislation has relied either on inclusion of express provision to that effect in new data processing measures, or on general rules of interpretation. There are risks to that situation. Including relevant provisions in each and every new data processing provision is onerous and could be inadvertently omitted. General rules of interpretation can be open to different interpretations by courts, particularly in the light of legal challenges following our exit from the European Union. This can create the potential for legal uncertainty and as a result could lead to a less effective and comprehensive data protection legislative framework.

Clause 43 creates a presumption that any future legislation permitting the processing of personal data will be subject to the key requirements of the UK's data protection legislation unless clear provisions are made to the contrary. This is a technical but necessary measure and I commend it to the Committee.

Stephanie Peacock: I understand that the clause contains legal clarifications relating to the interaction of data protection laws with other laws. On that basis, I am happy to proceed.

Question put and agreed to.

Clause 43 accordingly ordered to stand part of the Bill.

Clause 44

REGULATIONS UNDER THE UK GDPR

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

Sir John Whittingdale: The clause outlines the process and procedure for making regulations under powers in the UK GDPR. Such provision is needed because the Bill introduces regulation-making powers into the GDPR. There is an equivalent provision in section 182 of the Data Protection Act. Among other things, the clause makes it clear that, before making regulations, the Secretary of State must consult the Information Commissioner and such other persons as they consider appropriate, other than when the made affirmative procedure applies. In such cases, the regulations can be made before Parliament has considered them, but cannot remain as law unless approved by Parliament within a 120-day period.

12.45 pm

Clause 45 introduces schedule 9, which contains a number of minor amendments to the GDPR and the Data Protection Act. Schedule 9 makes it clear that the requirements for lawful processing in articles 6 and 9 of the GDPR are cumulative. It makes technical amendments to the definition of good practice in section 124 of the Data Protection Act and other minor amendments to the Act to clarify that, in calculating the 40-day parliamentary period permitted for any objection or rejection of documents laid before Parliament, such period does not include any whole days within a period when Parliament is dissolved or prorogued, or when both Houses of Parliament are adjourned for more than four days. The amendments are minor but will improve the legal clarity of the text.

Question put and agreed to

Clause 44 accordingly ordered to stand part of the Bill.

Clause 45 ordered to stand part of the Bill.

Schedule 9 agreed to.

Clause 46

INTRODUCTORY

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

The Chair: With this it will be convenient to discuss clause 47 stand part.

Sir John Whittingdale: I am sure that the Committee will be pleased to learn that we have now completed part 1 of the Bill. [HON. MEMBERS: "Hear, hear!"]

Clause 46 provides an overview of the provisions in part 2 that are aimed at securing the reliability of digital verification services through a trust framework, a public register, an information gateway and a trust mark.

Clause 47 will require the Secretary of State to prepare and publish the digital verification services trust framework, a set of rules, principles, policies, procedures and standards that an organisation that wishes to become a certified and registered digital verification service provider must follow. The Secretary of State must consult the Information Commissioner and other appropriate persons when preparing the trust framework; that consultation requirement can be satisfied ahead of the clause coming into force. The Secretary of State must review the trust framework every 12 months and must consult the Information Commissioner and other appropriate persons when carrying out the review. I commend both clauses to the Committee.

Stephanie Peacock: Clause 46 defines digital verification services. Central to the definition, and to the framing of the debate on part 2, is the clarification that they are

"services that are provided at the request of an individual".

That is a crucial distinction: digital verification services and the kinds of digital identity that they enable are not the same as any kind of Government-backed digital ID card, let alone a compulsory one. As we will discuss, it is important that any such services are properly regulated and can be relied on. However, the clause seems to set out a sensible definition that clarifies that all such services operate at individual request and are entirely separate from universal or compulsory digital identities.

I will speak in more depth about clause 47. As we move towards an increasingly digitally focused society, it makes absolute sense that someone should be able, at their own choice, to prove their identity online as well as in the physical world. Providing for a trusted set of digital verification services would facilitate just that, allowing people to prove with security and ease who they are for purposes including opening a bank account or moving house, akin to using physical equivalents like a passport or a proof of address such as a utility bill. It is therefore understandable that the Government, building on their existing UK digital identity and attributes trust framework, want to legislate so that the full framework can be brought into law when it is ready.

In evidence to the Committee, Keith Rosser highlighted the benefits that a digital verification service could bring, using his industry of work and employment as a live case study. He said:

"The biggest impact so far has been on the speed at which employers are able to hire staff"—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 52, Q112.]

In a study of 70,000 hires, the digital identity route took an average time of three minutes and 30 seconds, saving about a week compared with having to meet with an employer in person to provide physical documents. That has benefits not only to the individuals, who can start work a week earlier, but to the wider economy, since the same people will start contributing to taxation and their local economy a week earlier too.

Secondly, Keith identified that digital verification could open up remote jobs to people living in areas where employment opportunities are harder to come by. In theory, someone living in my constituency of Barnsley East could be hired in a role that would previously have been available only in London, thanks to their ability to prove who they are without ever having to meet their employer in person.

[Stephanie Peacock]

In the light of those benefits, as well as the potential reduction in fraud from cutting down on the usability of fake documents, in principle it seems only logical to support a framework that would allow trusted digital verification services to flourish. However, the key is to ensure that the framework breeds the trust necessary to make it work. In response to the digital identity call for evidence in 2019, the Government identified that a proportion of respondents were concerned about their privacy when it came to digital verification, saying that without assurances on privacy protections it would be hard to build trust in those systems. It is therefore curious that the Government have not accompanied their framework with any principles to ensure that services are designed and implemented around user needs and that they reflect important privacy and data protection principles.

Can the Minister say why the Government have not considered placing the nine identity assurance principles on the statute book, for example, to be considered when legislating for any framework? Those principles were developed by the Government's own privacy and consumer advisory group back in 2014; they include ensuring that identity assurance can take place only where consent, transparency, multiplicity of choice, data minimisation and dispute resolution procedures are in place. That would give people the reassurance to trust that the framework is in keeping with their needs and rights, as well as those of industry.

Furthermore, can the Minister explain whether the Government intend to ensure that digital verification will not be the only option in any circumstance, making it mandatory? As Big Brother Watch points out, digital identity is not a practical or desired option, particularly for vulnerable or marginalised groups. Elderly people may not be familiar with such technology, while others might be priced out of it, especially given the recent rise in the cost of broadband and mobile bills attached to inflation. Although we must embrace the opportunities that technology can provide in identity verification, there must also be the ability to opt out and use offline methods of identification where needed, or we will risk leaving people out of participating in key activities such as jobseeking.

Finally, I look forward to hearing more about the governance of digital verification services and the framework. The Bill does not provide a statutory basis for the new office for digital identities and attributes, and there is therefore no established body for the functions related to the framework. It is important that when the new office is established, there is good communication from Government about its powers, duties, functions and funding model. After all, the framework and the principles it supports are only as strong as their enforcement.

Overall, I do not wish to stand in the way of this part of the Bill, with the caveat that I am keen to hear from the Minister on privacy protections, on the creation of the new office and on ensuring that digital verification is the beginning of a new way of verifying one's identity, not the end of any physical verification options.

Chi Onwurah: It is a pleasure to follow my hon. Friend the Member for Barnsley East. I have some general comments, which I intend to make now, on the digital verification services framework introduced and set out in clause 46. I also have some specific comments on subsequent clauses; I will follow your guidance, Mr Hollobone, if it is your view that my comments relate to other clauses and should be made at a later point.

Like my hon. Friend, I recognise the importance of digital verification services and the many steps that the Government are taking to support them, but I am concerned about the lack of coherence between the steps set out in the Bill and other initiatives, consultations and activities elsewhere in Government.

As my hon. Friend said, the Government propose to establish an office for digital identities and attributes, which I understand is not a regulator as such. It would be good to have clarity on the position, as there is no discussion in the Bill of the duties of the new office or any kind of mechanisms for oversight or appeal. What is the relationship between the office for digital identities and attributes and this legislation? The industry has repeatedly called for clarity on the issue. I think we can all agree that a robust and effective regulatory framework is important, particularly as the Bill confers broad information-gathering powers on the Secretary of State. Will the Minister set out his vision and tell us how he sees the services being regulated, what the governance model will be, how the office—which will sit, as I understand it, in the Department for Science, Innovation and Technology—will relate to this legislation, and whether it will be independent of Government?

Will the Minister also help us to understand the relationship between the digital verification services set out in the Bill and other initiatives across Government on digital identity, such as the Government Digital Service's One Login service, which we understand will be operated across Government services, and the initiatives of the Home Office's fraud strategy? Is there a relationship between them, or are they separate initiatives? If they are separate, might that be confusing for the sector? I am sure the Minister will agree that we in the UK are fortunate to have world leaders in digital verification, including iProov, Yoti and Onfido. I hope the Minister agrees that for those organisations to continue their world-leading role, they need clarification and understanding of the direction of Government and how this legislation relates to that direction.

Finally, I hope the Minister will agree that digital identity is a global business. Will he say a few words about how he has worked with, or is working with, other countries to ensure that the digital verification services model set out in this legislation is complementary to other services and interoperable as appropriate, and that it builds on the learnings of other digital verification services?

Sir John Whittingdale: I am grateful to the hon. Member for Barnsley East for setting out the Opposition's general support for the principle of moving towards the facilitation of digital verification services. She set out some of the benefits that such services can provide, and I completely echo her points on that score. I reiterate the central point that none of this is mandatory: people can choose to use digital verification services, but there is no intention to make them compulsory.

The trust framework has been set out with a wide number of principles and standards, to which privacy is central. The hon. Member for Barnsley East is right that that will be necessary to obtain trust from people seeking to use the services. She and the hon. Member for Newcastle upon Tyne Central have both set out detailed questions about the operation of the new office and the work alongside other Government Departments. I would like to respond to their points but, given that we are about to break, we could accept the general principle of this clause and then discuss them, no doubt in greater detail, in the debate on subsequent clauses. Will the Committee accept this clause with the assurance that we will address a lot of the issues just raised as we come to subsequent clauses in this part of the Bill?

Question put and agreed to.

Clause 46 accordingly ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned. —*(Steve Double.)*

1 pm

Adjourned till this day at Two o'clock.