PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA (USE AND ACCESS) BILL [*LORDS*]

First Sitting

Tuesday 4 March 2025

(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 8 March 2025

The Committee consisted of the following Members:

Chairs: Wera Hobhouse, † Karl Turner

† Anderson, Callum *(Buckingham and Bletchley)* (Lab)
† Aquarone, Steff *(North Norfolk)* (LD)
† Beales, Danny *(Uxbridge and South Ruislip)* (Lab)
† Bryant, Chris *(Minister for Data Protection and Telecoms)*
† Collins, Victoria *(Harpenden and Berkhamsted)* (LD)
† Dearden, Kate *(Halifax)* (Lab/Co-op)
† Entwistle, Kirith *(Bolton North East)* (Lab)
† Fortune, Peter *(Bromley and Biggin Hill)* (Con)
† Josan, Gurinder Singh *(Smethwick)* (Lab)
† Juss, Warinder *(Wolverhampton West)* (Lab)
† Kumar, Sonia *(Dudley)* (Lab)
† Macdonald, Alice *(Norwich North)* (Lab/Co-op)
† McIntyre, Alex *(Gloucester)* (Lab)
† Obese-Jecty, Ben *(Huntingdon)* (Con)
† Pearce, Jon *(High Peak)* (Lab)
† Robertson, Joe *(Isle of Wight East)* (Con)
† Spencer, Dr Ben *(Runnymede and Weybridge)* (Con)

David Weir, Kevin Candy, Sanjana Balakrishnan, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 4 March 2025

(Morning)

[Karl Turner *in the Chair*]

Data (Use and Access) Bill [*Lords*]

9.25 am

The Chair: Before we begin, I have a few preliminary reminders for the Committee. Please switch electronic devices to silent. No food or drink is permitted during sittings of the Committee, except for the water that is provided. *Hansard* colleagues would be most grateful if after having spoken Members could email their notes to hansardnotes@parliament.uk, or pass on their written speaking notes to the *Hansard* colleague in the Committee Room.

The Minister for Data Protection and Telecoms (Chris Bryant): I beg to move,

That—

1. the Committee shall (in addition to its first meeting at 9.25 am on Tuesday 4 March) meet—

(a) at 2.00 pm on Tuesday 4 March;

(b) at 11.30 am and 2.00 pm on Thursday 6 March;

(c) at 9.25 am and 2.00 pm on Tuesday 11 March;

(d) at 11.30 am and 2.00 pm on Thursday 13 March;

(e) at 9.25 am and 2.00 pm on Tuesday 18 March;

2. the proceedings shall be taken in the following order: Clauses 1 to 56; Schedule 1; Clauses 57 and 58; Schedule 2; Clauses 59 to 65; Schedule 3; Clauses 66 to 70; Schedule 4; Clause 71; Schedule 5; Clauses 72 to 80; Schedule 6; Clauses 81 to 85; Schedules 7 to 9; Clauses 86 to 103; Schedule 10; Clauses 104 to 108; Schedule 11; Clauses 109 to 112; Schedule 12; Clauses 113 to 115; Schedule 13; Clauses 116 and 117; Schedule 14; Clauses 118 to 121; Schedule 15; Clause 122; Schedule 16; Clauses 123 to 147; new Clauses; new Schedules; remaining proceedings on the Bill;

3. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 18 March.

It is a great delight to serve under your chairmanship, Mr Turner; I cannot wait to hear you tell me off repeatedly during the course of the Committee's proceedings. In the words of Julie Andrews—this is material—

"Let's start at the very beginning,
A very good place to start.
When you read you begin with A-B-C.
When you sing you begin with do-re-mi",

but when you start a Bill Committee, you start with clause 1. Basically, the programme motion says, "Let's start with clause 1 and keep on going till we come to the end." With that said, I commend the motion to the Committee.

Question put and agreed to.

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Chris Bryant.)*

The Chair: Copies of the written evidence that the Committee receives will be made available in the Committee Room and circulated to Members by email.

We now begin line-by-line consideration of the Bill. The selection list for today's sitting is available in the room. It shows how the selected amendments have been grouped for debate. Amendments grouped are generally on the same or a similar issue. The selection and grouping list shows the order of debate and decisions on each amendment are taken when we come to the clause to which the amendment relates. Decisions on new clauses will be taken once we have completed consideration of the existing clauses.

Clause 1

Customer data and business data

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

The Chair: With this it will be convenient to discuss new clause 15—*Consumer Data Right: multi-sector extension*—

"(1) The Secretary of State must, within 12 months of this Act being passed, publish a roadmap for implementing a cross-sector 'Consumer Data Right' to enable individuals and small businesses to control and share their data securely and effectively in the following sectors—

(a) energy,

(b) telecommunications,

(c) financial services, and

(d) such other sectors as regulations may specify.

(2) The roadmap under subsection (1) must set out—

(a) technical standards and data portability protocols,

(b) timelines for phased implementation in each sector,

(c) consumer protection measures, and

(d) oversight responsibilities for any designated cross-sector data regulator.

(3) In preparing the roadmap, the Secretary of State must consult relevant regulators, consumer groups, industry representatives, and any other persons the Secretary of State considers appropriate.

(4) The Secretary of State may by regulations make provision to implement the Consumer Data Right in additional sectors or extend obligations in existing ones.

(5) Regulations under this section are subject to the affirmative resolution procedure."

This new clause would require the Secretary of State to develop and publish a roadmap for extending "smart data" portability rights beyond finance to other sectors, such as energy and telecommunications.

Chris Bryant: Strictly speaking, it is a misnomer to say that we do the Bill line by line; we do it clause by clause, or grouping by grouping. The first grouping contains clause 1 and new clause 15, which was tabled by the Liberal Democrat spokesperson, the hon. Member for Harpenden and Berkhamsted.

Clauses 1 to 26 establish regulation-making powers to implement smart data schemes. I think this part of the Bill is universally accepted, or it was in a previous version of the Bill—this is at least the third version of the Bill that a House of Commons Committee has considered line by line, clause by clause or grouping by grouping. These clauses were part 3 of the old Bill, but it is none the less important that we go through each of the clauses segment by segment, because this is a newly constituted House of Commons, with different Members and political parties, and therefore we have to consider them fully.

As many hon. Members will know, smart data involves traders securely sharing data with the customer or authorised third parties at the customer's request. Those third parties may use the data to provide the customer with innovative services, including account management services or price comparisons. This has already been spectacularly successful in open banking.

Clause 1 defines the key terms and scope of part 1, which covers clauses 1 to 26. Subsection (2) defines the kinds of data to which part 1 applies: "customer data", which is information specific to a customer of a trader, and "business data", which is generic data relating to the goods, services or digital content provided by that trader. It also defines "data holder" and "trader" to clarify who may be required to provide data. That covers persons providing the goods, services or digital content, whether they are doing so themselves or through others, or processing related data.

Subsections (3) to (5) set out who is a customer of a trader. Customers can include both consumers and businesses such as companies. Subsection (6) recognises that regulations may provide for data access rather than transfer.

I commend clause 1 to the Committee and urge hon. Members to resist the temptations offered by the hon. Member for Harpenden and Berkhamsted, who tabled new clause 15. I thank her for her interest in smart data. We had a very good conversation a week ago. I am glad to be able to confirm that, following some pressure from the Liberal Democrats in the other place, the Government announced that the Department for Business and Trade intends to publish a strategy document later this year on future uses of those powers. Since the hon. Member's new clause asks for a road map and we are saying that there will be a strategy, the difference between us may just be semantic.

The strategy document will lay out the Government's plans to consult or conduct calls for evidence in a number of sectors. It is important that we implement those powers only after having properly spoken with relevant parties such as consumer groups and industry bodies in the sector. Clause 22 also requires consultation before commencement in any sector. As such, we think the best approach is to use powers in part 1 of the Bill to implement smart data schemes that fit the identified needs of the relevant sector. The strategy document will set out the Government's plans for doing so. For that reason, I ask the hon. Lady to withdraw her new clause.

Dr Ben Spencer (Runnymede and Weybridge) (Con): It is a pleasure to serve under your chairmanship, Mr Turner, and I thank all hon. Members taking part in the Committee as well as the officials. As the Minister said, this is the third iteration of this Bill and it has been extensively covered in Committee before. We rely on and thank former Members and those in the other place who worked on the Bill to get it to where it is. I am pleased that the Government are taking the Bill forward and that it is one of the early Bills in the Session.

There is much to say about the Bill that is positive, and not just because it is a reformed version of our previous two Bills. Although, ironically, the Bill does not reference the term "smart data", clause 1 brings forward smart data and smart data schemes. That will help to open up a digital revolution, which will build on the successes of open banking in other sectors. We very much support that.

Victoria Collins (Harpenden and Berkhamsted) (LD): It is a pleasure to serve under your chairmanship, Mr Turner. The Liberal Democrats very much support the Bill and the move towards smart data. Every single day, millions of people in the UK unknowingly generate vast amounts of data, whether they are switching energy providers, checking their bank balance or simply browsing the internet. That is why I want to speak to new clause 15.

For the past decade, we have seen the enormous benefits of open banking, which has given customers the power to securely share their financial data with new providers. That has unlocked better deals, personalised financial data and a wave of innovation. I welcome what the Minister said about a strategy, but new clause 15 explicitly seeks to extend the benefits across multiple sectors, from energy to telecoms and beyond, giving consumers and small businesses a real say in how their data is used and the chance to benefit from that.

If Linda, a business owner in Tring, wants to switch to a cheaper energy provider or broadband deal, she faces a mountain of admin and endless calls to suppliers. She has no simple way of exporting her usage data and instantly comparing deals. But what if she did? A multi-sector consumer data right, as proposed by the new clause, would give Linda the ability to export her energy usage securely to a new provider. She could use a digital tool to automatically compare plans, switch to a greener provider and save thousands in operational costs, freeing up her focus for growing a business.

However, it is not just Linda and family businesses. New clause 15 would put real power in the hands of households struggling with the cost of living crisis—an ability to break free from restrictive contracts, find better deals and ultimately reduce bills. This is not just a radical idea: Australia has already implemented the consumer data right across finance, energy and telecoms, leading to an explosion of new services, better competition and savings for consumers. The European Union is moving in that direction, yet in the UK we have not taken that step. However, I accept what the Minister said about our strategy moving forward, which I very much welcome.

New clause 15 does not demand an overnight change. It would require the road map to be published in 12 months and to ensure that technical standards are in place and data sharing is secure and efficient. It includes a phased implementation plan to bring in new sectors gradually as well as consumer protection measures so that is done safely and fairly, with public trust at its core. This is not just about giving consumers more control over their data. It is about driving economic growth and innovation. If we get this right, we can see new fintech and comparison tools so that consumers can slash bills and switch telecom providers faster and more easily. It is about more competition, more choice and more innovation. I urge colleagues to consider the new clause, but I absolutely welcome what the Minister has said. Let us take a step forward and ensure that consumers and businesses have the rights that they deserve over their own data.

Chris Bryant: We are already committed to a strategy; I am not sure whether we need a road map for the strategy, and I would prefer us not to have such a thing in the Bill. It would also be slightly limiting, as the new clause effectively gives a list of priority areas. We want to explore quite a lot of other sectors; for instance, we might make a radical difference to the gig economy if we were to look at that sector. The hon. Lady made a good point about telecoms, although it might be specifically about smart meters. If we could turn a smart meter into an actually smart meter, which would require some telecoms work, smart data might be able to deliver cheaper bills for people. Notwithstanding the fact that I like the sentiment behind the new clause, I would resist it, so I hope the hon. Lady will not push it to a Division.

Question put and agreed to.

Clause 1 accordingly ordered to stand part of the Bill.

Clause 2

POWER TO MAKE PROVISION IN CONNECTION WITH CUSTOMER DATA

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

The Chair: With this it will be convenient to discuss clause 3 stand part.

Chris Bryant: Now we are on a winning streak. Clause 2 provides the principal authority for the relevant Secretary of State or the Treasury to establish smart data schemes in relation to customer data. The Government envisage that most smart data schemes will involve providing access to customer data. Clause 3 provides a non-exhaustive list of supplementary provisions that may be contained in regulations relating to customer data under clause 2. These include important matters such as requirements for data holders and/or third-party recipients to use specified facilities or services to ensure that smart data schemes can run effectively.

Question put and agreed to.

Clause 2 accordingly ordered to stand part of the Bill.

Clause 3 ordered to stand part of the Bill.

Clause 4

POWER TO MAKE PROVISION IN CONNECTION WITH BUSINESS DATA

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

The Chair: With this it will be convenient to discuss clause 5 stand part.

Chris Bryant: Clause 4 provides regulation-making powers that allow the relevant Secretary of State and the Treasury to require the publication of business data or the provision of business data to customers or third parties. Business data is envisaged to be contextual information provided alongside customer data, such as the price of products and services, for comparison. The Government, however, do see some uses where schemes focused on business data could be appropriate.

I should briefly say that I know there are quite a few points in the Bill where we are providing regulation-making powers. Although in general, I am not a big fan of secondary legislation, because it limits the ability of Parliament to scrutinise, it is important in an area where there is rapid technological change to provide Government Ministers with the power to enact regulations. These have already been considered by the relevant House of Lords Committee as well. The purpose of clause 5 is provide a non-exhaustive list of supplementary provisions that regulations under clause 4 can contain relating to business data. The clause largely mirrors clause 3 and contains important provisions relevant to the exercise of powers relating to business data under a smart data scheme.

Question put and agreed to.

Clause 4 accordingly ordered to stand part of the Bill.

Clause 5 ordered to stand part of the Bill.

Clause 6

DECISION-MAKERS

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

Chris Bryant: This clause applies when regulations provide for a person, referred to as a decision maker, to decide whether third-party recipients satisfy conditions allowing them to be authorised by a customer to receive customer data or to act on the customer's behalf under clause 2 or approved to receive business data under clause 4. that approach of regulating who can receive the data may not be suitable for all smart data schemes, but where it is, it will provide customers with confidence that the third parties they authorise meet approved standards. If regulations provide for a decision maker, they must also provide for the rights of those affected by decisions. These rights may include review of decisions and appeal rights to ensure transparency and accountability.

Question put and agreed to.

Clause 6 accordingly ordered to stand part of the Bill.

Clause 7

INTERFACE BODIES

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

Chris Bryant: This clause allows regulations to require the creation of interface bodies. These bodies may provide facilities and services, set standards or make related arrangements for data sharing interfaces, including application programming interfaces. Regulations may require data holders or third-party recipients to set up and fund an interface body. The role that Open Banking Ltd plays is an example of what we consider an interface body might look like under these regulations.

It is worth pointing out that the vast majority of people in this country would have no idea that smart data is what is behind their ability to have two bank accounts on one mobile phone and for the two speak to each other. There may be significant advantages for us unleashing this in other sectors as well.

Subsection (4) sets out provisions that regulations may make about the interface bodies. Among other things, regulations may confer powers on an interface body for monitoring the use of its interface, interface standards or interface arrangements. That could include powers to require the provision of documents or information subject to restrictions in clause 9, which we will come to later. Regulations may also provide procedures for complaints and enable or require interface bodies to publish or provide persons with specified documents or information relating to their functions.

Question put and agreed to.

Clause 7 accordingly ordered to stand part of the Bill.

Clause 8

ENFORCEMENT OF REGULATIONS UNDER THIS PART

Chris Bryant: I beg to move amendment 1, in clause 8, page 12, line 18, leave out "imposed by a decision-maker" and insert

"(referred to in sections 3(2) and 5(3))".

This amendment amends a reference to conditions for authorisation or approval to receive customer data or business data so as to reflect the fact that conditions will not necessarily be imposed by decision-makers.

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

Government amendments 2 to 5.

Clauses 8 and 9 stand part.

Chris Bryant: Government amendment 1 amends clause 8(5) to reflect that the conditions relating to authorisation or approval of third-party recipients will not necessarily be imposed by the decision makers who carry out the authorisation or approval. Government amendments 2, 3 and 5 amend clause 8(10) to require or allow enforcers to publish or provide documents as well as information, ensuring consistency with the powers of decision makers and interface bodies. Government amendment 4 removes unnecessary wording in subsection (10) to ensure consistency with equivalent clauses elsewhere. I commend these minor and technical amendments to the Committee.

Clause 8 enables regulations to confer powers on public bodies, known as enforcers, to monitor and enforce compliance with smart data schemes. Monitoring powers include requiring information and powers of inspection. Enforcement powers include issuing notices requiring compliance, naming and shaming non-compliance, and imposing financial penalties. Regulations may create criminal offences for falsification or similar conduct. To ensure accountability and transparency, regulations may provide for reviews of enforcers' decisions, appeal rights, and complaint procedures.

9.45 am

Clause 9 contains safeguards limiting enforcers' investigatory powers. Those require a warrant for entry to private dwellings, and restrict enforcers' use of information, safeguarding the privileges of Parliament and legal privilege, and protecting against self-incrimination, except for offences under part 1 of the Bill and perjury. The clause also prevents, subject to exceptions, written or oral statements given in investigations from being used against a person being prosecuted for an offence other than one under this part of the Bill. That reflects section 143(8) of the Data Protection Act 2018. I commend clauses 8 and 9 to the Committee.

Dr Spencer: We support technical amendments to the Bill to make sure it works properly, but I am intrigued why these amendments are necessary at such a late stage, bearing in mind the multiple layers of scrutiny that the Bill has gone through. Can he explain where he received the feedback about the necessity of the proposed changes?

Chris Bryant: As the hon. Gentleman says, these are technical changes, and sometimes we just have to go through it again and again to make sure that we have got things right. Amendment 4, for instance, was simply a matter of working out that the grammar did not really work. Sometimes, it is just a question of filleting, I am afraid, and that is what we have been doing.

Amendment 1 agreed to.

Amendments made: 2, in clause 8, page 13, line 16, after second "specified" insert "documents or".

This amendment provides that regulations may require enforcers to publish or provide documents as well as information, making the regulation-making powers in relation to enforcers consistent with the powers in relation to decision-makers and interface bodies (under clauses 6(9) and 7(4)(k)). See also Amendments 3 and 5.

Amendment 3, in clause 8, page 13, line 18, leave out "information about" and insert—

"documents or information relating to".

See the explanatory statement for Amendment 2.

Amendment 4, in clause 8, page 13, line 18, leave out—

", either generally or in relation to a particular case".

This amendment leaves out unnecessary words. Power for regulations to make provision generally or in relation to particular cases is conferred by clause 21(1)(a).

Amendment 5, in clause 8, page 13, line 20, leave out "information about" and insert—

"documents or information relating to".—*(Chris Bryant.)*

See the explanatory statement for Amendment 2.

Clause 8, as amended, ordered to stand part of the Bill.

Clause 9 ordered to stand part of the Bill.

Clause 10

FINANCIAL PENALTIES

Chris Bryant: I beg to move amendment 6, in clause 10, page 16, line 8, at end insert—

"(f) about what must or may be done with amounts paid as penalties."

This amendment confers express power to make provision about the treatment of amounts paid to enforcers as penalties, for consistency with similar powers in clauses 11(1)(b) (fees) and 12(1)(b) (levies).

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

Chris Bryant: It might more sense, in explaining the amendment, if I speak about the clause first, even though we would normally take the amendment first.

[Chris Bryant]

The clause provides safeguards on the use of financial penalties. Except where clause 16 provides otherwise for the Financial Conduct Authority, the amount of the penalty must be specified in, or determined in accordance with, the regulations. If the regulations allow an enforcer any discretion in that determination, the enforcer must publish, and have regard to, guidance. Other safeguards include an opportunity for representations before penalties are imposed, and rights of appeal to a court or tribunal. Regulations may provide for increase of the penalty in the case of late payment.

Government amendment 6, which is minor and technical for some of the same reasons I adverted to earlier, enables regulations to make provision about what is to be done with any amounts that are paid as part of clause 10. That is consistent with provisions on fee and levy receipts in clauses 11 and 12. This is another bit of tidying up of the previous version of the Bill.

Amendment 6 agreed to.

Clause 10, as amended, ordered to stand part of the Bill.

Clause 11

FEES

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

The Chair: With this it will be convenient to consider clause 12 stand part.

Chris Bryant: Clause 11 enables decision makers, interface bodies, enforcers and others to charge fees to alleviate their costs, which is obviously an important part of the Bill. It may also enable data holders to charge fees. Except where clause 15 provides otherwise for the Financial Conduct Authority, the fee amounts must be specified in, or determined in accordance with, the regulations. If the regulations allow a person to make that determination, they must publish information about the fee and how it is determined. Fees can only be charged on those directly affected by the performance of the relevant functions. That would include data holders, customers and third-party recipients. Regulations may also provide for fees to increase periodically—for instance, to cater for inflation—and for charging interest on and recovering unpaid fees.

Clause 12 enables regulations to impose a levy on data holders or third-party recipients or allow a specified public body to do so. The purpose is to meet costs incurred by bodies performing functions under the regulations and avoid costs to the taxpayer. The levy may be imposed only on persons directly affected by the performance of those functions. If the regulations allow a public authority to impose the levy, the regulations must provide how the rate of the levy and the period in which it is payable are to be determined. The public authority must also publish information about what it determines. The regulations may also make provision for charging of interest and recovery of unpaid amounts.

Question put and agreed to.

Clause 11 accordingly ordered to stand part of the Bill.

Clause 12 ordered to stand part of the Bill.

Clause 13

FINANCIAL ASSISTANCE

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

Chris Bryant: The purpose of the clause is to allow the Government to provide financial assistance where it is appropriate to do so. Although the Government expect schemes to be self-financing, as I have referred to, it is important to have statutory spending authority as a backstop where needed, and that is precisely what clause 13 provides.

Question put and agreed to.

Clause 13 accordingly ordered to stand part of the Bill.

Clause 14

THE FCA AND FINANCIAL SERVICES INTERFACES

Chris Bryant: I beg to move amendment 7, in clause 14, page 19, line 3, at end insert—

> "(ba) requiring section 2(4) actors described in the regulations to use a prescribed interface, comply with prescribed interface standards or participate in prescribed interface arrangements when taking, facilitating or doing other things in connection with relevant financial services action;".

This amendment provides that the Treasury's powers to confer rule-making powers on the Financial Conduct Authority in connection with the use of interfaces include powers relating to the use of interfaces when taking action described in clause 2(4) of the Bill (persons authorised to receive customer data taking action on behalf of customers). See also Amendment 9.

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

Government amendments 8 and 9.

Clauses 14 to 17 stand part.

Chris Bryant: Again, it might be more convenient if I speak to the clauses first and come back to the amendments, because then it is more self-explanatory, but I may need to speak at greater length here.

Open banking has revolutionised the UK retail banking sector by enhancing competition and introducing innovative services. Establishing a long-term regulatory framework for open banking will pave the way for its future growth, and this framework will rely on the FCA having the powers necessary for effective regulation and oversight. Clause 14 therefore empowers the Treasury to enable or require the FCA to set rules for interface bodies and participants in smart data schemes, ensuring compliance with essential standards. Clause 15 sets out further detail about the regulation-making powers conferred on the Treasury by clause 14.

These provisions create a clear framework for delegating rule-making powers, ensuring effective regulation, proper funding and mechanisms to address misconduct by scheme participants, with clear objectives for the FCA's oversight of smart data schemes. Regulations may enable or require the FCA to impose interface requirements relating to an interface body, as set out for the smart data powers more broadly in clause 7, and to require fees to be paid by financial services providers to cover interface body costs.

Clause 15 further provides that such regulations must impose certain requirements upon the FCA, including a requirement, so far as is reasonably possible, to exercise functions conferred by the regulations in line with specified purposes, and a requirement that the FCA must have regard to specified matters when exercising such functions. Additionally, regulations under clause 15 may empower or require the FCA to impose requirements on individuals or organisations to review their conduct, to take corrective action and to make redress for loss or damage suffered by others as a result of their conduct.

Clause 16 covers the Treasury's ability to make regulations enabling the FCA to impose financial penalties and levies. The regulations may require or enable the FCA to set the amount or method for calculating penalties for breaches of FCA interface rules. The regulations must require the FCA to set out its penalties policy, and may specify matters that such a policy must include. Additionally, the Treasury may impose itself, or provide for the FCA to impose, a levy on data holders or third-party recipients of financial services data under the scheme to cover its regulatory costs, with the funds being used as specified in the regulations. Only those capable of being directly impacted should be subject to the levy.

Penalties and levies are a necessary part of smart data schemes, including in financial services, to allow the FCA to penalise non-compliance and recover the costs of its regulatory activities. The clause ensures that any penalties or levies are subject to proportionate controls.

Clause 17 gives the Treasury the power to amend section 98 of the Financial Services (Banking Reform) Act 2013 through regulations. This will allow the Treasury to update the definitions of the FCA's responsibilities and objectives in that section, so they can include new functions or objectives given to the FCA by regulations made under part 1 of this Bill. That will ensure that the FCA's new duties fit into the existing system for co-ordinating payment system regulators, helping maintain a consistent approach across the financial sector. Regulations made under the clause will be subject to the affirmative procedure.

We have tabled Government amendments 7 to 9 to ensure that the Treasury may delegate to the FCA powers to set rules for action initiation, as well as data sharing. We think this is vital to ensure that open banking continues to work properly and is in line with the policy as set out elsewhere.

Dr Spencer: I apologise, Mr Turner: I misspoke earlier with regard to our position on the Government amendments. Rather than offering positive support, I meant to say that we will not oppose the technical amendments.

What does the FCA think about these amendments? Has the Department consulted the FCA?

Chris Bryant: I am not sure whether we have specifically—I am looking to my left for inspiration. I am getting vague inspiration, although it is remarkably non-productive. If the hon. Member would like to intervene for a little longer, perhaps I will be able to be more inspired.

Dr Spencer: I thank the Minister for giving way. I appreciate that it is a technical question and I hope he is able to give a response. Equally, I appreciate that he may have to write to me in due course. I see that there are papers coming his way.

Chris Bryant: To quote Richard II, methinks I am a prophet new inspired. Yes, this is all based on a consultation with the FCA. The FCA is content with us proceeding in this direction. I hope that, on that basis, the shadow Minister—I am trying to differentiate between his not opposing and supporting, but I think on the whole in Parliament, if you are not against us, you are for us. I think in this measure he is for us.

10 am

Amendment 7 agreed to.

Amendments made: 8, in clause 14, page 19, line 14, leave out "or (b)" and insert ", (b) or (ba)".

This amendment is consequential on Amendment 7.

Amendment 9, in clause 14, page 20, line 11, at end insert—

"'relevant financial services action' means action described in section 2(4) taken in relation to services or digital content provided or supplied by a financial services provider;

'section 2(4) actor' means—

(a) a person who, in reliance on regulations under subsection (4) of section 2, takes action described in that subsection;

(b) a data holder or other person who facilitates or does other things in connection with such action."—*(Chris Bryant.)*

This amendment defines terms used in the paragraph inserted by Amendment 7.

Clause 14, as amended, ordered to stand part of the Bill.

Clauses 15 to 17 ordered to stand part of the Bill.

Clause 18

LIABILITY IN DAMAGES

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

Chris Bryant: The clause will ensure that public authorities given powers under part 1 are not liable in damages for their acts or omissions in exercising their functions. That mirrors the exemption from liability for the Financial Conduct Authority under the Financial Services and Markets Act 2000, and allows public authorities to carry out their functions effectively. However, regulations cannot remove liability for things done in bad faith or which are unlawful under the Human Rights Act 1998.

Question put and agreed to.

Clause 18 accordingly ordered to stand part of the Bill.

Clause 19

DUTY TO REVIEW REGULATIONS

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

Chris Bryant: I know all Members of the Committee were wondering, "When are we going to review all of these provisions?" Fortunately, we have reached a clause that requires review of the regulations at least at five-yearly intervals. The Government recognise the importance of ongoing scrutiny of regulations. As part of a review, the regulation maker must consider whether the regulations remain appropriate—which seems rather basic, but anyway. The findings of the review will be published in a report laid before Parliament. This will uphold our commitment to transparency in the creation and maintenance of future regulations.

Question put and agreed to.

Clause 19 accordingly ordered to stand part of the Bill.

Clause 20

RESTRICTIONS ON PROCESSING AND DATA PROTECTION

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

The Chair: With this it will be convenient to discuss clauses 21 to 24 stand part.

Chris Bryant: Clause 20 allows regulations to provide that the processing of information they require does not breach obligations of confidence or other restrictions on processing information. However, regulations cannot compel businesses to breach data protection legislation. This mirrors the approach taken towards pensions dashboards in the Pensions Act 2004.

Clause 21 outlines further provisions that regulations may contain. Those include references to published standards and technical requirements, and the conferral of functions. The clause allows the part 1 powers to be used flexibly and tailored for their purpose. It also prevents regulations from enabling a person to set the maximum amounts of fines, financial penalties or fees, which adds to the safeguards in clauses 10 and 11. Finally, the clause stipulates when regulations can amend primary legislation to support consumer redress.

Clause 22 ensures that the regulations are properly scrutinised and requires that certain regulations be subject to affirmative parliamentary scrutiny. Those include regulations that introduce smart data schemes or make them more onerous, contain enforcement provisions and impose fees or a levy, as well as regulations under the financial services sector clauses. The clause also requires appropriate consultation before the regulations are made.

Clause 23 clarifies that part 1 powers may be used to amend existing subordinate legislation dealing with equivalent subject matter, rather than creating stand-alone regulations. This provision could be used to amend existing data-sharing requirements such as open banking provisions in the Payment Services Regulations 2017.

Clause 24 repeals sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013, which part 1 of the Bill replaces. The powers in the 2013 Act are no longer adequate to enable the introduction of effective smart data schemes. That was recognised in the previous iterations of this Bill under a previous Government, and we agree.

Question put and agreed to.

Clause 20 accordingly ordered to stand part of the Bill.

Clauses 21 to 24 ordered to stand part of the Bill.

Clause 25

OTHER DEFINED TERMS

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

The Chair: With this it will be convenient to discuss clause 26 stand part.

Chris Bryant: I thought that this discussion might take a little longer. Much as I am tempted to dally on clauses 25 and 26, clause 25 basically defines various terms used in part 1 of the Bill, and clause 26 provides an index of terms used in part 1, including those defined in clause 25, so I do not think my heart is in the business of doing so. Without further ado, I urge that clauses 25 and 26 stand part of the Bill.

Question put and agreed to.

Clause 25 accordingly ordered to stand part of the Bill.

Clause 26 ordered to stand part of the Bill.

Clause 27

INTRODUCTORY

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

The Chair: With this it will be convenient to discuss new clause 9—*Right to use non-digital verification services*—

"(1) This section applies when an organisation—

(a) requires an individual to use a verification service; and

(b) uses a digital verification service for that purpose.

(2) Where it is reasonably practicable for an organisation to offer a non-digital method of verification, the organisation must—

(a) make a non-digital alternative method of verification available to any individual required to use a verification service; and

(b) provide information about digital and non-digital methods of verification to those individuals before verification is required."

This new clause would create a duty upon organisations to support digital inclusion by offering non-digital verification services where practicable.

Chris Bryant: Part 2 of the Bill is about digital verification services. Those are obviously a very important part of the Bill; they lay out how we want to move into a new era and they are essential to many businesses being able to deliver their services effectively. They are also important to the Government being able to deliver some of the things we hope for—in terms of greater productivity in the delivery of services—and, frankly, to turning Government-provided services into services that feel as intuitively available and accessible as those provided by the private sector.

Clause 27 defines digital verification services and sets out the scope of provision in part 2, which runs from clauses 27 to 55, to help secure their reliability. New clause 9, which we will hear about in a few moments, has been tabled by the hon. Member for North Norfolk. It would require organisations to offer non-digital

verification services where practicable. The provision would change the voluntary nature of part 2 by imposing new obligations on businesses.

I fully support the idea of digital inclusion, which is why as the digital inclusion Minister I introduced our first action plan last week; we are the first Government to bring one forward in 10 years. However, we believe that the new clause is unnecessary because we are already prioritising digital inclusion. The office for digital identities and attributes will monitor the inclusivity of certified services, and include findings in the annual report that must be published under clause 53, which we will come to later.

In addition, there are already legislative protections in the Equality Act 2010 for protected groups. If in future the Government find evidence suggesting that regulatory intervention is appropriate to ensure that individuals have equal access to services across the economy, then we will consider appropriate intervention. I reassure the House that digital inclusion is a high priority for the Government, which is why we have set up the digital inclusion and skills unit within the Department for Science, Innovation and Technology, and why just last week we published the digital inclusion action plan, setting out the first five immediate steps we are taking towards our ambition of delivering digital inclusion for everyone across the UK, regardless of their circumstances.

We want to be able to deliver as many services digitally as possible, in a way that is fully accessible to people. However, we also accept that many people are not engaged in the digital world, and that there must also be provision for them. For those reasons, I hope the hon. Member for North Norfolk feels comfortable not pressing his new clause to a vote.

Dr Spencer: Digital verification services are important, and will make a big change when rolled out as part of this legislation. The provision is entirely right, particularly on the proportionality of data disclosure. Reading through some of the various reports and briefings we have received, the example used is of someone going into a nightclub: why should a scanned copy of their driving licence be consumed and contained by whoever the data holder is, when all they need to do is prove their age? These services will open the door to allow the proportionate disclosure of data. There is a both a data assurance component and a section on privacy, so we are glad that the Government are taking these measures forward.

I sympathise with the intention of new clause 9, in the name of the hon. Member for North Norfolk, which is to make sure that we do everything we can to support people who are digitally excluded. That ensures that people are not locked out and that there is a degree of reciprocity, so that as we digitalise more, the opportunity remains for people to access non-digital base services. I am not sure about the scope of the binding duty in the provision and about how the duties on small providers, as opposed to a duty on public service providers, play out politically. I think those are different things. Nevertheless, I support the sentiment of the new clause.

Steff Aquarone (North Norfolk) (LD): It is a pleasure to serve under your chairship, Mr Turner. Don't get me wrong: there are huge opportunities to improve the seamlessness of services for all users, regardless of whether they access those services digitally or not. Through new clause 9, I want to establish a right for those who do not wish to or cannot use digital identification within the verification framework that the Bill creates. The amendment was also tabled in Committee in the other place by the noble Lord Clement-Jones, and I am pleased to bring it before this House, too.

10.15 am

I am proud to represent the constituency with the oldest age demographic in the country; I think I have more nonagenarians in my constituency than any other MP. However, the data tells us that it is highly likely I also represent one of the communities with the most digital exclusion. Ofcom says that 18% of those aged over 65 do not have internet access. There will be people in the same circumstances in all our constituencies. The stats show that a similar number of people on low incomes do not have access to the internet, and in North Norfolk, even some of those who do will have a slow and unreliable connection.

Obviously, I want to see a widening of internet access and widespread digital upskilling, and the Minister is right to mention the importance of digital inclusion, but there will always be circumstances where that simply is not feasible for some people. As Age UK said recently:

"It will never be possible to get everyone online."

That reality has been accepted in my community, where people make sure that information or important documents are available in a diverse range of forms that suit everyone. Currently, the Bill does not ensure a similar equality of access to verification and identification. As Liberal Democrats, we believe in equality of access and freedom of choice for all. As it stands, without an enshrined right to non-digital identification, the Bill does not provide that.

Digital verification might not be possible for someone for a wide range of highly valid reasons. They might not be able to access the internet. They might not have the skills or confidence to part safely with important personal data using digital means. They might have concerns about privacy, security, anonymity or the potential for mass surveillance. They might simply not want to, and citizens should not be dictated to about how they can go about doing something so fundamental as proving who they are—our existence as individuals within the systems of the state and beyond.

I have heard concerns from veterans about these proposals. The veterans ID card is held by many of the ex-service personnel I am proud to represent, and the proposals might mean these individuals handing over highly sensitive information about their service and tours of duty to acquire this digital ID. The security of that information has huge ramifications for the safety and security of our veterans. Rightly, many might prefer to use traditional methods in order to retain full control of that information.

I looked over what the Minister's colleague in the Lords said when my Lib Dem colleague tabled the new clause, and I was disappointed with the approach she indicated the Government were taking, which the Minister has repeated today. The Minister in the Lords said:

"the Government will take action in the future if evidence emerges that people are being excluded".—[*Official Report, House of Lords,* 3 December 2024; Vol. 841, c. GC372.]

I can tell the Minister now that people will be excluded. We do not need to wait for the inevitable to happen to legislate against it—we can do it right away and prevent us all from returning here in a matter of months or years to pass new legislation to fix the problem that was always coming down the tracks.

I note with even greater interest that those on the Labour Front Bench were rather more open to the idea when they were in opposition. When the matter was raised as part of the Data Protection and Digital Information Bill, the Minister seemed more open to the concerns raised in the Lords from across the Benches about the right to non-digital verification. I hope some of that openness might return if we pass this new clause.

I hope the Minister will consider accepting our new clause, which would provide reassurance to the many who are worried about the potential limitations that a digital verification system could place on them. Their concerns are very real and valid, and I know that many of my constituents in North Norfolk and many constituents of all members of the Committee will be hoping to hear reassurances that go beyond what we have heard from the Minister so far and that their rights will be protected in the Bill.

Chris Bryant: I note the comments from the shadow Minister, and I am grateful for them.

There is a fundamental flaw in the argument from the hon. Member for North Norfolk that this new clause was tabled in the House of Lords, because what he means is that it was lost in the House of Lords—the House of Lords did not bring it to us. There is a second flaw in the argument, which is that it seems to presume that people will be required to use a digital verification service. That is not true. People will be able to use non-digital systems if they want to in every circumstance. That is an essential part of being able to take forward digital verification services. It may be that a growing number of people begin to find them more useful, reliable and trustworthy than carrying around a set of papers. I am sure that many of us have gone through the tedious process of renting a car—having to turn up with copies of the previous three months of bills sent to your house, and all that. They have to be printed out, of course, and not provided in digital form, and so on. In the end, therefore, this measure will be transformational for the vast majority of people, but that does not mean that we should exclude people.

Where the hon. Member for North Norfolk is absolutely right is that there are many different patterns of digital exclusion. One, which I am very conscious of from my own constituency in south Wales, is physical digital exclusion. Many people in the south Wales valleys simply do not have the physical digital connections, a mobile phone or whatever it may be, to be able to transact their business. The second is the simple issue of poverty. Social tariffs do not even touch the edge for lots of families, because it is yet another bill. Even another £10 or £15 bill a month is one that has to compete with whether they have fresh food on the table for the kids. Another level where people might be excluded relates to age, at the top end and at the bottom end. The hon. Member mentioned nonagenarians, but he could go down to 60-year-olds and find people who simply do not want to use open banking or any kind of digital system, do not have a smartphone and have absolutely no intention of getting one, or, for that matter, do not have any kind of broadband connection to their home. I understand that fully, and that is why the Bill is written as it is, so that it is permissive and not mandatory.

That is an important reason why—although I have listened to the arguments that the hon. Member for North Norfolk has repeated from Big Brother Watch—I am determined to do everything we possibly can to tackle each and every one of the issues of digital exclusion. I have not even referred to skills—people might have some form of disability, might have simply never acquired or wanted to acquire digital skills, or might find using a screen particularly difficult for whatever set of reasons. We want to tackle every single form of digital exclusion, but I do not think that this is the place to do so. We will not be able to tackle digital exclusion by putting an additional measure in the Bill, and that is why, if the hon. Member wants to push this to a vote, I will still resist his new clause. I commend the clause as drafted to the Committee.

Victoria Collins: The Minister says that the proposal for digital verification services is not mandatory, so a non-digital version will be available for people to use. May I check what the guarantees are? We have seen this with card payments and even the banks—in Harpenden, we lost all our banks, apart from Nationwide. A very big team campaigned to get a banking hub, because a lot of people said, "You can either go online or drive many miles to get to a bank." I want to understand what guarantees are in place to secure that non-digital version.

Chris Bryant: It is simply that there is no requirement for people to use a digital verification service to be able to secure the service that they want. Obviously, that is a key part of how local government or Government have to deliver their services. They have to think not only about the people who can use digital services, but about those who cannot, for all the reasons that we have laid out.

The hon. Member for Harpenden and Berkhamsted is absolutely right about banks, and it is not just in Harpenden; I do not have a bank in my constituency. I have seen them go one after another after another. We have a banking hub, but even it has had to move. That provides all sorts of difficulties for people who do not want to do their banking in any way other than physically going into a bank. That is why both our Government many years ago, then the Conservative Government for years, were trying to encourage people to use the post office as an alternative means of doing their banking.

That is the pattern that we will have to adopt. Government will always have to be aware. While we may want all the productivity gains and the added security that digital verification services can provide, none the less we need to ensure that others are provided for. That is all provided for in the Bill, and I would say adequately, although the hon. Member may disagree with me. Yet again, I am still resisting any amendment and urge that the clause stand part of the Bill.

Victoria Collins: I thank the Minister for his reply, and I do understand. I will leave what happens with new clause 9 to my hon. Friend the Member for North

Norfolk, but it is important to state that we have seen a pattern, as my hon. Friend mentioned, of rights being taken away when we know that people cannot access services, and then the problem being solved after it was created. We need to think about a way to secure non-digital services, whether in respect of public services and council tax, our banks, or whatever it is. The Government need to think about how we can protect those services, whether through this Bill or something else, to ensure that those who are excluded can still access a non-digital version of services.

Chris Bryant: Even without inspiration, I agree with everything the hon. Lady said. I would add the fact that to park a car in lots of places in the country now we have to go online using a smartphone. When I was in Cardiff recently, the sign said "Go to the app", but it did not say which app. What frustrates me is that every local authority in the land seems to have adopted a different app, so if we park in more than one local authority area, we have to download app after app, upload all our card details and all the rest of it.

I hope to God that one of the things smart data might be able to solve is the issue of different apps for parking, because the car does not change, we do not change and our banking details do not change; the only thing that changes is our location. To achieve that, though, we must also address the issue of digital exclusion. Lots of areas simply do not have a download speed of 5 megabits per second for mobile coverage, even though Ofcom probably suggests that there is 99% coverage in all areas from all four operators. My problem is that the new clause tries to correct many deficiencies in society, none of which has anything to do with digital verification services.

Steff Aquarone: I am well aware of the Minister's frustration with mobile parking apps and I sympathise. Likewise, there is the frustration of having to take two separate bits of physical ID to a bank branch on two separate occasions to get a simple credit card approved. However, I cannot agree with the Minister's accusation that new clause 9 tries to solve the entire universe. I remind him of what we have seen in practice when rights to alternatives are not enshrined. The reality is that if the rights to non-digital identification and verification are not enshrined in the Bill, the options and competitiveness of the options for those who do not or are unwilling to use digital verification will reduce.

Chris Bryant: The thing is, it is already enshrined in law under the Equality Act 2010. That is perfectly adequate for the purposes of the Bill—it protects all the characteristics that the hon. Gentleman referred to, including age—so I urge him not to pursue his new clause.

Question put and agreed to.

Clause 27 accordingly ordered to stand part of the Bill.

Clause 28

DVS TRUST FRAMEWORK

Chris Bryant: I beg to move amendment 10, in clause 28, page 30, line 32, leave out subsections (3) and (4).

This amendment removes subsections which were inserted at Report stage in the Lords.

The Chair: With this it will be convenient to discuss Government amendment 11.

Chris Bryant: We will be talking about clauses 28 to 31, but now I will speak to Government amendment 10 to clause 28, along with Government amendment 11. Several Members may wish to speak to this issue.

Government amendment 10 removes subsections (3) and (4) of clause 28, which were added on Report in the House of Lords. The subsections require the Secretary of State, when preparing the digital verification service trust framework, to assess whether certain listed public authorities reliably verify personal data. This seems very dry, but it is a clear and specific issue. The trust framework provides rules for digital verification services, not rules for how public authorities process data. Data protection legislation already requires public authorities to ensure that any personal data they process is accurate and, where necessary, kept up to date. As such, the Government cannot proceed with the change introduced in the Lords as it would duplicate existing legislation and bring in matters that are out of scope of the trust framework.

10.30 am

Government amendment 11 removes subsection (6), which was inserted to clause 45 on Report in the Lords. The subsection states that public authorities must not disclose personal data under the clause unless it

"is clearly defined and accompanied by metadata, and"

the public authority can confirm that the information is accurate,

"has not been changed or tampered"

with, or the public authority can attest it has been changed lawfully and was accurate at the time of the change.

The Government would like to remove the changes made in the Lords for two reasons. First, they have the potential to cut across rights granted under the Equality Act and the Gender Recognition Act 2004. They also place the Secretary of State in a position where he is unable to confirm that the provision is compatible with the European convention on human rights—the sentence at the front of the Bill. Secondly, the changes sought to require public authorities to release more information than may be needed for the purposes of a digital verification check, and were therefore at odds with the data-minimisation principle in existing data protection legislation.

A key benefit of choosing to use a digital identity is that only the specific information required about a data subject is shared for each separate digital verification check. The changes made in the Lords would prevent the privacy benefits associated with using a digital identity from being realised. For instance, if the changes remain in the Bill, and someone goes to rent a car and is asked whether they are male or female, the data verification process would have to verify whether they had at any point in their life changed their gender. That would effectively out every trans person in the country whenever they went to buy a house, rent a car, rent a house, rent a flat or anything like that. We think that is completely disproportionate and an unnecessary invasion of privacy.

Of course, it is absolutely right that public authorities, where appropriate, have that information, but that is not the purpose of a digital verification system. The

Government are already acting to develop data standards on key entities and their attributes, to ensure that the way in which data is organised, stored and shared is consistent among public authorities. That work is being led by the Data Standards Authority, with input from the Home Office, HMRC, the Office for National Statistics, NHS England, the Department for Education, the Ministry of Justice, the Local Government Association and the Police Digital Service. That co-ordinated approach will ensure that this important work is approached holistically.

The Chair: Before I call the shadow Minister, I want to clarify that amendment 11 is in this group, but a decision on it will be taken when we get to clause 45.

Dr Spencer: Amendments 10 and 11 seek to remove certain provisions that were introduced in Committee in the other place. I thank Sex Matters for its work, but also many people in this policy area who have tried to focus on the importance of data accuracy and validity when it is used.

I hope we all agree that it is important that data, when it is collected—in fact it is a principle of data collection and maintenance—is accurate and correct and that there is no point holding or using data if it is incorrect. Biased data is worse than no data at all. Therefore, I do not understand—especially given the extra use of the data that will come as part of digital verification services—why the Minister and the Government are not keen on the provision to stipulate that public bodies that hold sensitive data should be certain of its accuracy, particularly when the data is going to be passed on and used as part of digital verification services. I am confused by the resistance to ensuring that the data is correct, particularly when we anticipate that it will be used as part of a far bigger spectrum. It will be consumed by a digital verification service in which it is not routine to go back and look at the original paper records. The only dataset to be relied on will be some Oracle Excel spreadsheet or whatever database is used by public authorities.

This debate has become more acute with regard to the importance of sex data. It is critical that sex data is available to protect public spaces and to be used in scientific research to allocate someone's sex as part of medicine and healthcare. I speak as a former doctor, and I guess I should declare an interest in that I am married to a doctor. The use of sex data is critical in medical screening programmes, such as cervical screening and prostate screening, to understand and interpret investigations. It is critical that the data is accurate; otherwise, there is a danger that research will not be appropriate or will produce bad results, and there is also a potential degree of medical harm. It is critical that we get sex data correct when it is being used.

I do not agree with the argument that requiring the disclosure of sex data is either disproportionate or somehow a breach of the European convention on human rights. The whole point of digital verification services is proportionate disclosure. In fact, we have heard speeches from both sides of the Committee about proportionate disclosure, and limiting the amount of personal data that is passed on as part of a digital verification service.

My challenge is, quite simply, that if somebody is collecting sex data as part of a verification system, why are they doing so? If they do not need to know what someone's sex is, it should not be collected. Digital verification services allow people to choose their proportionate disclosure. There will be times when sex data is required for renting a property—that example has been used before—because people may want to rent properties in single-sex accommodation. I may argue that is a proportionate disclosure. If it is a standard rental property in another situation, it is probably a non-proportionate disclosure. Another argument has been made that it is needed to triangulate data to verify ID. Again, that does not seem to work, because the whole point of a digital verification service is to allow someone to have a digital ID framework and use different points to verify.

The perversity of this debate is that these schemes and their proportionate disclosure protect people's identities. They protect people from non-disproportionate disclosure. We need to make sure that the data we are using is accurate and correct, and that it says what we want it to say when someone is inquiring about somebody's sex. If somebody is asking for sex data but they do not need it, people should be able to say no, which the existing provisions allow for.

Chris Bryant: No, they don't.

Dr Spencer: What is the point of politics if we do not have a debate? We strongly disagree with the interpretation that the provisions are somehow incompatible with ECHR rights. They totally support people's privacy rights under article 8 regarding proportionate disclosures. If somebody needs to have someone's sex data, they need sex data. They do not need gender data. The provisions allow for it, and if somebody does not need sex data, they should not be collecting it in the first place.

Joe Robertson (Isle of Wight East) (Con): It is an honour to serve under your chairmanship, Mr Turner.

Further to the comments made by my hon. Friend the Member for Runnymede and Weybridge, does the Minister at least accept that the Bill poses a risk of entrenching inaccurate data relating to sex through public bodies using DVS systems? Notwithstanding his views on the Lords amendments, could he address that point? What steps will the Government take to ensure the reliability of sex data to ensure protection, such as of women using female-only spaces? What will the Minister do to ensure that inaccurate data entrenched by the Bill will not pose a risk to people in those situations and others? I am thinking, of course, of services available in healthcare, but that is by no means the only example.

Chris Bryant: I need to make it absolutely clear, for a start, that the element of clause 45 that we are removing—subsection (6)—makes no reference to sex or gender at all. The words do not appear on the face of the Bill at all. Subsection (6) refers to accuracy and inaccuracy, but it says

"the public authority is able to attest that it…has been corrected through a lawfully made correction,"

and that is obviously aiming at a particular form of lawfully made correction.

Public authorities are already bound in law by data protection legislation—this goes to the point that the hon. Member for Isle of Wight East just made—to ensure that the personal data they process is accurate

and, importantly, that it is accurate for the purpose for which it is being processed, and that it is kept up to date where necessary. In essence, what the noble Lords' amendments to the Bill did was say that we should also be keeping, in every instance, a history of what the data had been. That, I think, is problematic.

The hon. Member is absolutely right about wanting to preserve women-only spaces, which is why public authorities are required to process information that is accurate for the purpose for which it is being processed. In the delivery of healthcare, for instance, when it comes to health screening for transgender and non-binary individuals, the Department of Health and Social Care has comprehensive guidance that sets out the NHS default adult screening programmes that are available in England and lays out who is invited. In England, it is up to GPs to ensure that, as part of processing gender change, the individual is correctly registered for relevant screenings in relation to their sex.

I simply do not buy this argument that we need to make this provision in relation to all digital verification services. Although it is of course right that, in the delivery of prison services or in the health service, or in so many other areas, simple common sense should apply in relation to female-only spaces and wanting to make sure that women are safe, I do not think that this Bill on digital verification services benefits from the introduction of a measure that would effectively mean that in the provision of every digital verification service—whether in regard to the provision of some sensitive service or not—you should make this provision. That is why we tabled amendments 10 and 11, and I urge all hon. Members to support them.

Victoria Collins: The Liberal Democrats support the Government amendments. As the Minister highlighted, the amendments are about proportionality in digital verification services. For Liberal Democrats, it is about the balance between trust and helping to protect privacy, as well as getting the data needed to make our society better. We believe that the original proposal had the proportionality right, so we will support the Government's amendment.

Question put, That the amendment be made.

The Committee divided: Ayes 13, Noes 4.

Division No. 1]

AYES

Anderson, Callum	Josan, Gurinder Singh
Aquarone, Steff	Juss, Warinder
Beales, Danny	Kumar, Sonia
Bryant, Chris	Macdonald, Alice
Collins, Victoria	McIntyre, Alex
Dearden, Kate	Pearce, Jon
Entwistle, Kirith	

NOES

Fortune, Peter	Robertson, Joe
Obese-Jecty, Ben	Spencer, Dr Ben

Question accordingly agreed to.

Amendment 10 agreed to.

10.45 am

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

The Chair: With this it will be convenient to discuss clauses 29 to 31 stand part.

Chris Bryant: Clause 28 requires the Secretary of State to prepare and publish the digital verification service framework, which will set out rules for the provision of digital verification services for providers that want to be certified and appear on a Government register. The rules will draw on existing technical requirements, standards and best practice, and guidance and legislation. They will help organisations to provide services in a trusted and consistent way, and enable inter-operability and increasing public confidence.

The clause allows the Secretary of State to revise and republish the trust framework as the market evolves. The requirement to consult the Information Commissioner and others whom the Secretary of State considers appropriate will ensure the trust framework's development is informed by industry expertise and the wider regulatory environment.

Clause 29 allows the Secretary of State to prepare and publish supplementary codes. The codes will be relevant to sectors that require rules to cater for their specific requirements around identity checks, supplementary to those in the DVS trust framework. For example, additional rules are needed when proving someone's right to work in the UK. By working with those operating in such sectors, the Secretary of State can identify market and user needs for these codes, and that will help to encourage digital identity adoption across the wider economy. The requirement for the Secretary of State to consult the Information Commissioner and others as appropriate when preparing a supplementary code should also ensure that those needs are taken into account in its development.

Clause 30 allows the Secretary of State to withdraw a published supplementary code if, for example, it is no longer required or is outdated. The Secretary of State will need to publish his determination to withdraw a supplementary code and allow at least 28 days before its withdrawal.

Clause 31 requires the Secretary of State to carry out a review of the digital verification service trust framework and any published supplementary code at least every 12 months. When doing so, the Secretary of State should consult the Information Commissioner and anyone he or she considers appropriate. This review will ensure that the body of rules governing digital verification services keeps up to date with the digital identity market, and is fit for purpose as that market evolves.

Question put and agreed to.

Clause 28, as amended, accordingly ordered to stand part of the Bill.

Clauses 29 to 31 ordered to stand part of the Bill.

Clause 32

DVS REGISTER

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

The Chair: With this it will be convenient to discuss clauses 33 to 38 stand part.

Chris Bryant: These clauses are all about the digital verification service register. Clause 32 requires the Secretary of State to establish and maintain a publicly available register of digital verification service providers, which is called the digital verification service register. This duty will ensure that people can look up which digital verification service providers have met the requirements to join the register, making it easier for people to know which providers can be trusted and to realise the benefits of this technology with confidence.

Subject to limited powers of refusal in clause 34, clause 33 requires the Secretary of State to register a digital verification service provider if it applies to appear on the register and if it holds a certificate from an accredited conformity assessment body confirming its digital verification service is compliant with the digital verification service trust framework. In practice, this means that in applying to join the register, a provider must have its service certified against the trust framework by a body that has been independently accredited by the UK Accreditation Service. The digital verification service provider must also have made an application in accordance with requirements made by determination under clause 39 and paid any relevant fee, as set out in clause 39. This provides confidence to users and businesses that only those digital verification services that meet these conditions will appear on the digital verification service register.

Clause 34 grants the Secretary of State the power to refuse applications to the digital verification service register in two circumstances: first, where he considers it necessary to do so in the interests of national security or, secondly, where he is satisfied that the provider is not compliant with the trust framework. Before a refusal, he must provide written notice of his intention, informing the provider of his reasons and of the opportunity to make representations. He need not share reasons on national security grounds where to do so would be contrary to those interests. Those powers will act as a backstop, allowing the Secretary of State to stop bad actors—I always worry about that term, thinking about actors who have appeared in movies that I have not liked—entering the system in circumstances where, for example, he has intelligence that conformity assessment bodies do not. That should increase confidence that registered DVS providers are trustworthy and secure.

Clause 35 allows registered digital verification service providers to have multiple certified services listed in the digital verification services register. The provider must apply for the Secretary of State to amend its register entry to accommodate this. This is largely a technical provision to ensure that the register can operate appropriately and seamlessly when providers offer more than one service that is certified against the trust framework.

Clause 36 provides for a registered provider to apply to the Secretary of State to add a supplementary note to their entry in the register if its service is certified against the supplementary code, its application complies with any requirements set out in a determination under clause 38, and it has paid any required fee. Supplementary notes will make it easy for people and businesses to see which registered digital verification services are certified against the rules of the supplementary code, so that they can find a trusted service that meets their needs.

In the same way that clause 35 allows registered digital verification service providers to have multiple certified services listed in the register, clause 37 allows providers with multiple services certified against the supplementary code to have that information suitably noted in the register. The digital verification service provider must apply to the Secretary of State to have its supplementary note amended to accommodate this. This technical requirement ensures that the register can operate appropriately and seamlessly when DVS providers offer more than one service that is certified against both the trust framework and a supplementary code.

Finally, clause 38 makes provision for the Secretary of State to determine the form of applications to the register and supplementary notes, the information that needs to be contained in the application, the documents to be provided and the manner in which is to be submitted. He must publish this determination, which will ensure that the requirements are clear for digital verification service providers who wish to make an application. For the same reason, if he revises the determination at a later time, this must also be published.

Question put and agreed to.

Clause 32 accordingly ordered to stand part of the Bill.

Clauses 33 to 38 ordered to stand part of the Bill.

Clause 39

FEES FOR APPLICATIONS FOR REGISTRATION, SUPPLEMENTARY NOTES, ETC

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

Chris Bryant: The clause provides for the Secretary of State to make regulations regarding the payment of fees for applications to the register and applications for supplementary notes. The regulations will be subject to the negative procedure. The fees can be set at a level higher than the administrative costs of determining applications or those associated with the DVS providers' ongoing registration in the DVS register. This is to help ensure that fees may cover the total operating costs relating to governance, which includes functions such as publishing an annual report and keeping the trust framework up to date.

The Government amended clause 39 from the original Bill that was introduced prior to the general election in response to a recommendation from the Delegated Powers and Regulatory Reform Committee so that these fees are set by regulations instead of determination. This ensures that any fees the Secretary of State may wish to charge for these applications are subject to parliamentary scrutiny.

Question put and agreed to.

Clause 39 accordingly ordered to stand part of the Bill.

Clause 40

DUTY TO REMOVE PERSON FROM THE DVS REGISTER

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

The Chair: With this it will be convenient to discuss clauses 41 to 44 stand part.

Chris Bryant: Clause 40 requires the Secretary of State to remove a digital verification service provider from the digital verification service register in the following circumstances: when that provider asks to be removed; if it stops providing all services for which it is registered; or if it no longer holds a certificate for at least one of these services. This duty ensures that the Secretary of State acts to uphold the digital verification service register in these circumstances to uphold trust and confidence in it.

Clause 41 allows the Secretary of State to remove a digital verification service provider from the digital verification service register if it is not compliant with the trust framework or a supplementary code; if it fails to provide information in response to a clause 51 written notice; or if removal is necessary in the interests of national security. Before removal, the Secretary of State must provide written notice informing the provider of reasons for removal and the opportunity to make representations. Reasons need not be given where this would be contrary to national security interests. These powers will help ensure that the register lists only certified services and that the Secretary of State can act to remove services where necessary, providing confidence in its accuracy.

Clause 42 requires the Secretary of State to remove a service from the digital verification service register if the digital verification service provider requests removal; if it ceases to provide one or more of those services, but not all of them; or if it no longer holds a certificate for all those services. Similar to clause 41, these duties provide confidence to people and businesses that the digital verification service register can be trusted as an accurate source of information. Whereas clauses 40 and 41 cover removal of a digital verification service provider as a whole, the clause 42 duty enables the Secretary of State to remove one or more services, should a digital verification service provider have more than one service registered and one or more, but not all, those services no longer meet the digital verification service register's conditions.

Clause 43 requires the Secretary of State to remove a supplementary note from the digital verification service register if the digital verification service provider requests its removal; if it ceases to provide all the services to which the note relates; if it no longer holds a certificate for at least one of those services; or if the supplementary code to which the note relates has been withdrawn. This is a technical requirement to ensure that changes in certification and provision of multiple services in accordance with supplementary codes are accurately reflected for digital verification service providers, upholding confidence that the digital verification service register can be trusted as an accurate source of information.

11 am

Clause 44 requires the Secretary of State to remove a registered service from a digital verification service provider's supplementary note if the provider requests it; if they cease to provide one or more of the services recorded on the note, but not all; or if they no longer hold a certificate for all the services included in the note. This, too, is a technical requirement to ensure that changes in certification and the provision of multiple services in accordance with supplementary codes are accurately reflected for digital verification service providers, upholding confidence that the digital verification service register can be trusted as an accurate source of information.

Question put and agreed to.

Clause 40 accordingly ordered to stand part of the Bill.

Clauses 41 to 44 ordered to stand part of the Bill.

Clause 45

POWER OF PUBLIC AUTHORITY TO DISCLOSE INFORMATION TO REGISTERED PERSON

Amendment proposed: 11, in clause 45, page 43, line 12, leave out subsection (6).—*(Chris Bryant.)*

This amendment removes a subsection which was inserted at Report stage in the Lords.

Question put, That the amendment be made.

The Committee divided: Ayes 12, Noes 4.

Division No. 2]

AYES

Anderson, Callum	Josan, Gurinder Singh
Aquarone, Steff	Juss, Warinder
Beales, Danny	Kumar, Sonia
Bryant, Chris	Macdonald, Alice
Dearden, Kate	McIntyre, Alex
Entwistle, Kirith	Pearce, Jon

NOES

Fortune, Peter	Robertson, Joe
Obese-Jecty, Ben	Spencer, Dr Ben

Question accordingly agreed to.

Amendment 11 agreed to.

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

Chris Bryant: The clause creates a permissive information gateway. This will enable public authorities to share information relating to an individual with registered digital verification services, when requested by the individual. The gateway enables digital identity checks to be made against public authority data, thereby increasing the trustworthiness of identity and eligibility checks across the economy.

Clause 45 also makes it clear that the power does not authorise disclosure of information that would breach the data protection legislation or the Investigatory Powers Act 2016. However, disclosure of information under the clause would not breach any obligations of confidence owed by the public authority or any other restrictions on the disclosure of the information. The clause also enables public authorities to charge a fee for the disclosure of information under the clause.

Dr Spencer: I am not going to rehash the previous debates. Clearly, the Committee has made its decision, no matter how disappointing that is. I just wanted to pick up the Minister's previous point about the use of common sense in arbitration decisions when it comes to access to protected same-sex spaces. I fully support using common sense, but how does that play out in a situation where somebody has gone through a digital verification service that has used data that is held by a

[Dr Ben Spencer]

local authority, but that has been changed at a later date—that is, in effect, gender data? How will that be resolved?

Chris Bryant: I think that I will have to write to the hon. Gentleman. We have agreed the amendment, so that is slightly rehashing the debate. I am happy to write to him and he will have that before we come back for Thursday's Committee sitting.

Question put and agreed to.

Clause 45, as amended, accordingly ordered to stand part of the Bill.

Clause 46

INFORMATION DISCLOSED BY THE REVENUE AND CUSTOMS

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

The Chair: With this it will be convenient to consider clauses 47 and 48 stand part.

Chris Bryant: Clauses 46, 47 and 48 relate to His Majesty's Revenue and Customs, the Welsh Revenue Authority and Revenue Scotland respectively. The clauses provide additional safeguards to any information disclosed through the information gateway by these bodies. They place restrictions on onward sharing and create offences for the wrongful disclosure of such data, thereby creating appropriate protection for tax data shared through the gateway. A similar provision is not required for Northern Irish tax data, as HMRC is responsible for the collection of devolved taxes in Northern Ireland. The Government will not commence measures to enable the disclosure of information held by HMRC until the commissioners for HMRC are satisfied that the technology and processes for information sharing uphold the particular safeguards relating to taxpayer confidentiality, and therefore allow information sharing by HMRC to occur without adverse effect on the tax system or any other function of HMRC.

Question put and agreed to.

Clause 46 accordingly ordered to stand part of the Bill.

Clauses 47 and 48 ordered to stand part of the Bill.

Clause 49

CODE OF PRACTICE ABOUT THE DISCLOSURE OF INFORMATION

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

Chris Bryant: I am sure Members were wondering when we were going to get to a code of practice, and this is the clause that introduces it. Clause 49 requires the Secretary of State to prepare and publish a code of practice for the disclosure of information under the information gateway created in clause 45. The code of practice will provide guidance and best practice for such disclosure, including what information should be shared, who it should be shared with and how to share it securely.

In preparing and revising the code, the Secretary of State must consult with the Information Commissioner, devolved Governments and other appropriate persons. The code will be laid before Parliament before it is finalised. The first version of the code will be subject to the affirmative procedure and subsequent versions to the negative procedure, allowing proper parliamentary scrutiny.

Dr Spencer: Will the code of practice include information on the proportionate disclosure of data through the DVS scheme?

Chris Bryant: Yes.

Question put and agreed to.

Clause 49 accordingly ordered to stand part of the Bill.

Clause 50

TRUST MARK FOR USE BY REGISTERED PERSONS

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

Chris Bryant: This clause enables the Secretary of State to designate a trust mark to be used only by registered providers of digital verification services. This will help users to identify those digital verification service providers that have been assessed as reliable and trustworthy. The clause gives the Secretary of State the power to bring civil proceedings against unauthorised use of the trust mark. The trust mark has now been registered as a trademark in the UK, so the Secretary of State will also be able to take appropriate legal action against misuse under trademark law.

Question put and agreed to.

Clause 50 accordingly ordered to stand part of the Bill.

Clause 51

POWER OF SECRETARY OF STATE TO REQUIRE INFORMATION

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

Chris Bryant: Clause 51 enables the Secretary of State to issue written notices to accredited conformity assessment bodies and registered digital verification service providers, requesting information that he may reasonably require to exercise his functions under part 2 of the Bill. That could include information on inclusion, fraud or other statistical information to assist the Secretary of State in carrying out his duties under this part of the Bill.

The notice must state why the information is required and may specify or describe particular information, together with the form in which it must be provided, the time within which it must be provided and where it must be provided. The clause also sets out circumstances where disclosure would not be required—for example, where it would contravene the data protection legislation.

Non-compliance with the clause by registered providers may result in removal from the digital verification services register.

Question put and agreed to.

Clause 51 accordingly ordered to stand part of the Bill.

Clause 52

ARRANGEMENTS FOR THIRD PARTY TO EXERCISE FUNCTIONS

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

The Chair: With this it will be convenient to consider clauses 53 and 54 stand part.

Chris Bryant: I am conscious that we are steaming towards the end of part 2 of the Bill. It is 11.10 am, and we could go on until 11.30 am, but it might be convenient for Members if we were to end a little earlier and then move on to parts 3 and 4 this afternoon. That would be a matter for the Whips, and I do not like to tell a Whip what to do.

Clause 52 allows the Secretary of State to make regulations for his functions to be exercised by a third party. Such delegation may be made for any function of the Secretary of State under part 2 of the Bill, except for his regulation-making powers. The delegation may also provide for payments to be made and received from the third party to whom functions are delegated.

This clause gives the Secretary of State the flexibility to adapt to the governance needs of the digital identity market as it grows. Governance functions will initially sit within the Department for Science, Innovation and Technology, and future plans to delegate any function in part 2 of the Bill will be carefully considered and subject to parliamentary scrutiny under the affirmative procedure.

Clause 53 requires the Secretary of State to prepare and publish reports on the operation of part 2 of the Bill at least every 12 months, with the first report due 12 months after the commencement of clause 28, which concerns the publication of the digital verification services trust framework. These reports will be published on gov.uk. This publication will strengthen transparency in the Government's digital identity programme and boost trust in the market.

Clause 54 is an index of terms defined or explained in part 2 of the Bill. It sets out the subsection numbers where definitions and explanations can be found.

Ordered, That the debate be now adjourned.—*(Kate Dearden.)*

11.12 am

Adjourned till this day at Two o'clock.