PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Sixth Sitting

Thursday 18 May 2023

(Afternoon)

CONTENTS

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

not later than

Monday 22 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

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

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Thursday 18 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

2 pm

Clause 47 ordered to stand part of the Bill.

Clause 48

DVS register

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

The Chair: With this it will be convenient to discuss clauses 49 to 53 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): Clauses 48 to 52 provide the Secretary of State with powers and duties relating to the governance and oversight of digital identities in the UK. Those functions will be carried out by the office for digital identities and attributes. I can tell the hon. Member for Newcastle upon Tyne Central that the office is a team of civil servants in the Department for Science, Innovation and Technology. The office will oversee certified organisations that provide trusted digital verification services, to ensure that the purpose of the legislation is being upheld as the market develops.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): I appreciate the Minister's clarification that the office will be a group of civil servants, but I do not see that set out in the Bill, in the clause that we are currently debating. Am I wrong?

Sir John Whittingdale: As the office is an internal body, within the Department, I do not think that it would necessarily be specifically identified in the legislation in that way. If there is any more information on that, I will be happy to provide it to the hon. Lady in a letter, but the office is not a separate body to the Department.

Chi Onwurah: I thank the Minister for providing greater clarification, but if the office is not a separate body, it cannot be claimed to be independent of Government, which means that the governance of digital verification services is not independent. Will he confirm that?

Sir John Whittingdale: This is a function that will operate within Government. I do not think that it is one where there is any specific need for particular independence, but as I said, I am happy to supply further details about precisely how it will operate if that is helpful to the hon. Lady.

Let me move on from the precise operation of the body. Clause 53 sets out requirements for certified digital verification service providers in relation to obtaining top-up certificates where the Secretary of State revises and republishes the DVS trust framework.

Clause 48 provides that the Secretary of State must establish and maintain a register of digital verification service providers. The register must be made publicly available. The Secretary of State is required to add a digital verification service provider to the register, provided that it has met certain requirements. To gain a place on the register, the provider must first be certified against the trust framework by an accredited conformity assessment body. Secondly, the provider must have applied to be registered in line with the Secretary of State's application requirements under clause 49. Thirdly, the provider must pay any fee set by the Secretary of State under the power in clause 50.

The United Kingdom Accreditation Service accredits conformity assessment bodies as competent to assess whether a digital verification service meets the requirements set out in the trust framework. That, of course, is an arm's length body. Assessment is by independent audits, and successful DVS providers are issued with a certificate.

The Secretary of State is prohibited from registering a provider if it has not complied with the registration requirements. An application must be rejected if it is based on a certificate that has expired, has been withdrawn by the issuing body, or is required to be ignored under clause 53 because the trust framework rules have been amended and the provider has not obtained a top-up certificate in time. The Secretary of State must also refuse to register a DVS provider if the provider was removed from the register through enforcement powers under clause 52 and reapplies for registration while still within the specified removal period.

Clause 48(7) provides definitions for "accredited conformity assessment body", "the Accreditation Regulation", "conformity assessment body" and "the UK national accreditation body".

Clause 49 makes provision for the Secretary of State to determine the form of an application for registration in the digital verification services register, the information that an application needs to contain, the documents to be provided with an application and the manner in which an application is to be submitted.

Clause 50 allows the Secretary of State to charge providers a fee on application to be registered in the DVS register. The fee amount is to be determined by the Secretary of State. The clause also allows the Secretary of State to charge already registered providers ongoing fees. The amount and timing of those fees are to be determined by the Secretary of State.

Clauses 51 and 52 confer powers and duties on the Secretary of State in relation to the removal of persons from the register. Clause 51 places a duty on the Secretary of State to remove a provider from the register if certain conditions are met. That will keep the register up to date and ensure that only providers that hold a certificate to prove that they adhere to the standards set in the framework are included in the register. Clause 52 provides a power to the Secretary of State to remove a provider

from the register if the Secretary of State is satisfied that the provider is failing to provide services in accordance with the trust framework, or if it has failed to provide the Secretary of State with information as required by a notice issued under clause 58. Clause 52 also contains safeguards in respect of the use of that power.

Clause 53 applies where the Secretary of State revises and republishes the DVS trust framework to include a new rule or to change an existing rule and specifies in the trust framework that a top-up certificate will be required to show compliance with the new rule from a specified date.

I hope that what I have set out is reasonably clear, and on that basis I ask that clauses 48 to 53 stand part of the Bill.

Stephanie Peacock (Barnsley East) (Lab): As has been mentioned, a publicly available register of trusted digital verification services is welcome; as a result, so is this set of clauses. A DVS register of this kind will improve transparency for anyone wanting to use a DVS service, as they will be able to confirm easily and freely whether the organisation that they hope to use complies with the trust framework.

However, the worth of the register relies on the worth of the trust framework, because only by getting the trust framework right will we be able to trust those that have been accredited as following it. That will mean including enough in the framework to assure the general public that their rights are protected by it. I am thinking of things such as data minimisation and dispute resolution procedures. I hope that the Department will consider embedding principles of data rights in the framework, as has been mentioned.

As with the framework, the detail of these clauses will come via secondary legislation, and careful attention must be paid to the detail of those measures when they are laid before Parliament. In principle, however, I have no problem with the provisions of the clauses. It seems sensible to enable the Secretary of State to determine a fee for registration, to remove a person from the register upon a change in circumstances, or to remove an organisation if it is failing to comply with the trust framework. Those are all functions that are essential to the register functioning well, although any fees should of course be proportionate to keep market barriers low and ensure that smaller players continue to have access. That facilitates competition and innovation.

Similarly, the idea of top-up certificates seems sensible. Members on both sides of the House have agreed at various points on the importance of future-proofing a Bill such as this, and the digital verification services framework should have space for modernisation and adaptation where necessary. Top-up certificates will allow for the removal of any organisation that is already registered but fails to comply with new rules added to the framework.

The detail of these provisions will be analysed as and when the regulations are introduced, but I will not object to the principle of an accessible and transparent register of accredited digital verification services.

Chi Onwurah: I thank the Minister for clarifying the role of the office for digital identities and attributes. Some of the comments I made on clause 46 are probably more applicable here, but I will not repeat them, as I am sure the Committee does not want to hear them a second time. However, I ask the Minister to clarify the process. If a company objects to not being approved for registration or says that it has followed the process set out by the Secretary of State but the Secretary of State does not agree, or if a dispute arises for whatever reason, what appeal process is there, if any, and who is responsible for resolving disputes? That is just one example of the clarity that is necessary for an office of this kind.

Will the Minister clarify the dispute resolution process and whether the office for digital identities and attributes will have a regulatory function? Given the lack of detail on the office, I am concerned about whether it will have the necessary powers and resources. How many people does the Minister envisage working for it? Will they be full-time employees of the office, or will they be job sharing with other duties in his Department?

My other questions are about something I raised earlier, to which the Minister did not refer: international co-operation and regulation. I imagine there will be instances where companies headquartered elsewhere want to offer digital verification services. Will there be compatibility issues with digital verification that is undertaken in other jurisdictions? Is there an international element to the office for digital identities and attributes?

Everyone on the Committee agrees that this is a very important area, and it will only get more important as digital verification becomes even more essential for our everyday working lives. What discussions is the Minister having with the Department for Business and Trade about the kind of market that we might expect to see in digital verification services and ensuring that it is competitive, diverse and across our country?

Sir John Whittingdale: I look forward to debating the detail of the framework with the hon. Member for Barnsley East when it comes forward, but the hon. Member for Newcastle upon Tyne Central raised a couple of specific points. As I said, the new office for digital identities and attributes will be in the Department for Science, Innovation and Technology, and it will work on a similar basis to that of the office for product safety and standards, which operates within the Department for Business and Trade.

However, I should make it clear that the office for digital identities and attributes is not a regulator, because the use of digital identities is not mandatory, so it does not have investigatory or enforcement powers. It is not our intention for it to be able to levy fines or resolve individual complaints. Further down the line, as the market develops, it may be decided that it should be housed permanently in an independent body or as an arm's length body, but that is for consideration in due course. It will start off within the Department.

I will come back to the hon. Member for Newcastle upon Tyne Central with more detail about dispute resolution. I take her point; I am not sure how often what she describes is likely to happen, but clearly it is sensible at least to take account of it.

2.15 pm

Finally, the hon. Lady asked about working internationally. Obviously, the digital economy is a global phenomenon and every country will look to establish

similar types of service, so we are extremely keen to work with other countries. We are benchmarking our own framework against those of countries that will be at different stages of their digital identity development. We will also share UK expertise with anyone who wishes to learn from the lessons that we have already gained. That will be an ongoing process, but I accept that it is important that services are developed by countries on a co-operative basis globally.

Question put and agreed to.

Clause 48 accordingly ordered to stand part of the Bill.

Clauses 49 to 53 ordered to stand part of the Bill.

Clause 54

POWER OF PUBLIC AUTHORITY TO DISCLOSE INFORMATION TO REGISTERED PERSON

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

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

Clauses 55 and 56 stand part.

Government amendments 6 and 7.

Government new clause 3—*Information disclosed by the Welsh Revenue Authority*.

Government new clause 4—*Information disclosed by Revenue Scotland.*

Sir John Whittingdale: Clause 54 creates a permissive power to enable public authorities to share information relating to an individual with registered digital verification service providers. That the power is permissive means that public authorities are not under any obligation to disclose information. The power applies only where a digital verification service provider is registered in the DVS register and the individual has requested the digital verification service from that provider. Information disclosed using the power does not breach any duty of confidentiality or other restrictions relating to the disclosure of information, but the power does not enable the disclosure of information if disclosure would breach data protection legislation. The clause also gives public authorities the power to charge fees for disclosing information.

All information held by His Majesty's Revenue and Customs is subject to particular statutory safeguards relating to confidentiality. Clause 55 establishes particular safeguards for information disclosed to registered digital verification service providers by His Majesty's Revenue and Customs under clause 54. 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 functions of HMRC.

Clause 56 obliges the Secretary of State to produce and publish a code of practice about the disclosure of information under clause 54. Public authorities must have regard to the code when disclosing information under this power. Publication of the first version of the code is subject to the affirmative resolution procedure. Publication of subsequent versions of the code is subject to the negative resolution procedure. We will work with the commissioners for HMRC to ensure that the code meets the needs of the tax system.

New clauses 3 and 4 and Government amendments 6 and 7 establish safeguards for information that reflect those already in the Bill under clause 55 for HMRC. Information held by tax authorities in Scotland and Wales—Revenue Scotland and the Welsh Revenue Authority—is subject to similar statutory safeguards relating to confidentiality. These safeguards ensure that confidence and trust in the tax system is maintained. Under these provisions, registered DVS providers may not further disclose information provided by Revenue Scotland or the Welsh Revenue Authority unless they have the consent of that revenue authority to do so. The addition of these provisions will provide an equivalent level of protection for information shared by all three tax authorities in the context of part 2 of the Bill, avoiding any disparity in the treatment of information held by different tax authorities in this context. A similar provision is not required for Northern Irish tax data, as HMRC is responsible for the collection of devolved taxes in Northern Ireland.

Stephanie Peacock: Many digital verification services will, to some extent, rely on public authorities being able to share information relating to an individual with an organisation on the DVS register. To create a permissive gateway that allows this to happen, as clause 54 does, is therefore important for the functioning of the entire DVS system, but there must be proper legal limits placed on these disclosures of information, and as ever, any disclosures involving personal data must abide by the minimisation principle, with only the information necessary to verify the person's identity or the fact about them being passed on. As such, it is pleasing to see in clause 54 the clarification of some of those legal limits, as contained in the likes of data protection legislation and the Investigatory Powers Act 2016. Similarly, clause 55 and the Government new clauses apply the necessary limits on sharing of personal data from HMRC and devolved revenue authorities under clause 54.

Finally, clause 56, which seeks to ensure that a code of practice is published regarding the disclosure of information under clause 54, will be a useful addition to the previous clauses and will ensure that the safety of such disclosures is properly considered in comprehensive detail. The Information Commissioner, with their expertise, will be well placed to help with this, so it is pleasing to see that they will be consulted during the process of designing this code. It is also good to see that this consultation will be able to occur swiftly—before the clause even comes into force—and that the resulting code will be laid before both Houses.

In short, although some disclosures of personal data from public authorities to organisations providing DVS are inevitable, as they are necessary for the very functioning of a verification service, careful attention should be paid to how this is done safely and legally. These clauses, alongside a well-designed framework—as already discussed—will ensure that that is the case.

Question put and agreed to.

Clause 54 accordingly ordered to stand part of the Bill.

Clauses 55 and 56 ordered to stand part of the Bill.

Clause 57

TRUST MARK FOR USE BY REGISTERED PERSONS

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

Sir John Whittingdale: Clause 57 makes provision for the Secretary of State to designate a trust mark to a DVS provider. The trust mark is essentially a kitemark that shows that the provider complies with the rules and standards set out in the trust framework, and has been certified by an approved conformity assessment body. The trust mark must be published by the Secretary of State and can only be used by registered digital verification service providers. The clause gives the Secretary of State powers to enforce that restriction in civil proceedings.

Stephanie Peacock: Trust marks are useful tools that allow organisations and the general public alike to immediately recognise whether or not a product or service has passed a certain testing standard or criterion. This is especially the case online, where due to misinformation and the prevalence of scams such as phishing, trust in online services can be lower than in the physical world.

The TrustedSite certification, for example, offers online businesses an earned certification programme that helps them to demonstrate that they are compliant with good business practices and maintain high safety standards. This is a benefit not only to the business itself, which is able to convert more users into clicks and sales, but to the users, who do not have to spend time researching each individual business and can explore pages and shop with immediate certainty. A trust mark for digital verification services would serve a similar purpose, enabling certified organisations that meet the trust framework criteria to be immediately recognisable, offering them the opportunity to be used by more people and offering the public assurance that their personal data is being handled by a verified source.

Of course, as is the case with this entire section of the Bill, the trust mark is only worth as much as the framework around it. Ministers should again think carefully about how to ensure that the framework supports the rights of the individual. Furthermore, the trust mark is useful only if people recognise it; otherwise, it cannot provide the immediate reassurance that it is supposed to. When the trust mark is established, what measures will the Department take to raise public awareness of it? In the same vein, to know the mark's value, the public must also be aware of the trust framework that the mark is measured against, so what further steps will the Department take to increase knowledge and understanding of digital verification services and frameworks? Finally, will the Department publish the details of any identified unlawful use of the trust mark, so that public faith in the reliability of the trust mark remains high?

Overall, the clause is helpful in showing that we take seriously the need to ensure that people do not use digital verification services that may mishandle their data.

Sir John Whittingdale: I am grateful to the hon. Lady for her support. I entirely take her point that a trust mark only really works if people know what it is and can look for it when seeking a DVS provider.

Regarding potential abuse, obviously that is something we will monitor and potentially publicise in due course. All I would say at this stage is that she raises valid points that I am sure we will consider as the new system is implemented.

Question put and agreed to.

Clause 57 accordingly ordered to stand part of the Bill.

Clause 58

POWER OF SECRETARY OF STATE TO REQUIRE INFORMATION

Amendments made: amendment 6, in clause 58, page 84, line 5, after "55" insert

"or (Information disclosed by the Welsh Revenue Authority)"

This amendment prevents the Secretary of State requesting a disclosure of information which would contravene the new clause inserted by NC3.

Amendment 7, in clause 58, page 84, line 5, after "55" insert

"or (Information disclosed by Revenue Scotland)"—*(Sir John Whittingdale.)*

This amendment prevents the Secretary of State requesting a disclosure of information which would contravene the new clause inserted by NC4.

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

The Chair: With this, it will be convenient to discuss clauses 58 and 59 stand part.

Sir John Whittingdale: Clauses 58 to 60 set out powers and duties conferred upon the Secretary of State in relation to the exercise of her governance and oversight functions under part 2.

Clause 58 enables the Secretary of State to issue a written notice that requires accredited conformity assessment bodies or registered DVS providers to provide information reasonably required by the Secretary of State to exercise functions under part 2. The notice must state why the information is required. It may also state what information is required, the form in which it should be provided, when it should be provided and the place to which it should be provided. Any notice given to a provider must also inform the provider that they may be removed from the DVS register if they fail to comply with the notice.

The power is subject to certain safeguards. Information does not have to be disclosed if to do so would breach clause 55 in relation to HMRC data or data protection legislation, or if disclosure is prohibited by the relevant parts of the Investigatory Powers Act 2016. Information does not need to be disclosed if doing so would reveal an offence that would expose a person to criminal proceedings. That does not apply to offences mentioned relating to false statements.

Clause 59 gives the Secretary of State the power to make regulations specifying that another person is able to exercise her functions under part 2. This clause enables us to move the governance and oversight functions of the Secretary of State to a third party if appropriate.

Chi Onwurah: I thank the Minister for giving way. Before he moves on to clause 60, can he set out, perhaps giving an example, where it might be appropriate to use

[Chi Onwurah]

the power in clause 59 to make arrangements for another person to take on these functions, or in what circumstances he envisages it being used?

Sir John Whittingdale: We are obviously at a very early stage in the development of this market. At the moment, it is felt right that oversight should rest with the Secretary of State, but it may be that as the market grows and develops there will need to be the oversight via a separate body. The clause keeps the power available to the Secretary of State to delegate the function if he or she chooses to do so.

Clause 60 requires the Secretary of State to publish an annual report on the functioning of this part. The first report must be published within 12 months of clause 47, the DVS trust framework clause, coming into force. The reports will help to ensure that the market continues to meet the needs of DVS providers, public authorities, regulators, civil society and individuals. I commend the clauses to the Committee.

2.30 pm

Stephanie Peacock: To oversee the DVS register, it is understandable that the Secretary of State may in some cases need to require information from registered bodies to ensure that they are complying with their duties under the framework. It is good that clause 58 provides for that power, and places reasonable legal limits on it, so that disclosures of information do not disrupt legal professional privilege or other important limitations. Likewise, it is sensible that the Secretary of State be given the statutory power to delegate some oversight of the measures in this part in a paid capacity, as is ensured by clause 59.

As I have mentioned many times throughout our scrutiny of the Bill, the Secretary of State may not always have the level of expertise needed to act alone in exercising the powers given to them by such regulations. The input of those with experience and time to commit to ensuring the quality of the regulations will therefore be vital to the success of these clauses. Again, however, we will need more information about the establishment of the OfDIA and the governance of digital identities overall to be able to interpret fully both the delegated powers and the power to require information, and how they will be used. Once again, therefore, I urge transparency from the Government as those governance structures emerge.

That leads nicely to clause 60, which requires the Secretary of State to prepare and publish yearly reports on the operation of this part. A report of that nature will offer the chance to periodically review the functioning of the trust framework, register, trust mark and all other provisions contained in this part, thereby providing an opportunity to identify and rectify any recurring issues that the system may face. That is sensible for any new project, particularly one that, through its transparency, will offer accountability of the Government to the general public, who will be able to read the published reports. In short, there are no major concerns regarding any of the three clauses, though further detail on the governance of digital identities services will need proper scrutiny.

Question put and agreed to.

Clause 58 accordingly ordered to stand part of the Bill.

Clauses 59 and 60 ordered to stand part of the Bill.

Clause 61

CUSTOMER DATA AND BUSINESS DATA

Sir John Whittingdale: I beg to move amendment 46, in clause 61, page 85, line 24, after "supplied" insert "or provided".

The definition of "business data" in clause 61 refers to the supply or provision of goods, services and digital content. For consistency with that, this amendment amends an example given in the definition so that it refers to what is provided, as well as what is supplied.

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

Sir John Whittingdale: We move on to part 3 of the Bill, concerning smart data usage, which I know is of interest to a number of Members. Before I discuss the detail of clause 61 and amendment 46, I will give a brief overview of this part and the policy intention behind it. The provisions in part 3 allow the Secretary of State or the Treasury to make regulations that introduce what we term "schemes" that compel businesses to share data that they hold on customers with the customer or authorised third parties upon the customer's request, and to share or publish data that they hold about the services or products that they provide. Regulations under this part will specify what data is in scope within the parameters set out by the clauses, and how it should be shared.

The rest of the clauses in this part permit the Secretary of State or the Treasury to include in the regulations the measures that will underpin these data sharing schemes and ensure that they are subject to proper safeguards—for example, relating to the enforcement of regulations; the accreditation of third party businesses wanting to facilitate data sharing; and how these schemes can be funded through levies and charging. Regulations that introduce schemes, or significantly amend existing schemes, will be subject to prior consultation and parliamentary approval through the affirmative procedure.

The policy intention behind the clauses is to allow for the creation of new smart data schemes, building on the success of open banking in the UK. Smart data schemes establish the secure sharing of customer data and contextual information with authorised third parties on the customer's request. The third parties can then be authorised by the customer to act on their behalf. The authorised third parties can therefore provide innovative services for the customer, such as analysing spending to identify cost savings or displaying data from multiple accounts in a single portal. The clauses replace existing regulation-making powers relating to the supply of customer data in sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013; those powers are not sufficient for new smart data schemes to be effective.

Clause 61 defines the key terms and concepts for the powers in part 3. We have tabled a minor Government amendment to the clause, which I will explain. The definitions of data holder and trader in subsection (2) explain who may be required to provide data under the regulations. The definitions of customer data and business data deal with the two kinds of data that suppliers may

be required to provide. Customer data is information relating to the transactions between the customer and supplier, such as a customer's consumption of the relevant good or service and how much the customer has paid. Business data is wider contextual data relating to the goods or services supplied or provided by the relevant supplier. Business data may include standard prices, charges or tariffs and information relating to service performance. That information may allow customers to understand their customer data. Government amendment 46 clarifies that a specific example of business data—information about location—refers to the supply or provision of goods or services. It corrects a minor inconsistency in the list of examples of business data in subsection (2)(b).

Subsection (3) concerns who is a customer of the supplying trader, and who can therefore benefit from smart data. Customers may include both consumers and businesses. Subsection (4) enables customers to exercise smart data rights in relation to contracts they have already entered into, and subsection (5) allows the schemes to function through provision of access to data, as opposed to sending data as a one-off transfer.

Stephanie Peacock: The clause defines key terms in this part of the Bill, such as business data, customer data and data holder, as well as data regulations, customer and trader. These are key to the regulation-making powers on smart data in part 3, and I have no specific concerns to raise about them at this point.

I note the clarification made by the Minister in his amendment to the example given. As he outlined, that will ensure there is consistency in the definition and understanding of business data. It is good to see areas such as that being cleaned up so that the Bill can be interpreted as easily as possible, given its complexity to many. I am therefore happy to proceed with the Bill.

Damian Collins (Folkestone and Hythe) (Con): I rise to ask the Minister a specific question about the use of smart data in this way. A lot of users will be giving away data a device level, rather than just accessing individual accounts. People are just going to a particular account they are signed into and making transactions, or doing whatever they are doing in that application, on a particular device, but there will be much more gathering of data at the device level. We know that many companies—certainly some of the bigger tech companies—use their apps to gather data not just about what their users do on their particular app, but across their whole device. One of the complaints of Facebook customers is that if they seek to remove their data from Facebook and get it back, the company's policy is to give them back data only for things they have done while using its applications—Instagram, Facebook or whatever. It retains any device-level data that it has gathered, which could be quite significant, on the basis of privacy—it says that it does not know whether someone else was using the device, so it is not right to hand that data back. Companies are exploiting this anomaly to retain as much data as possible about things that people are doing across a whole range of apps, even when the customer has made a clear request for deletion.

I will be grateful if the Minister can say something about that. If he cannot do so now, will he write to me or say something in the future? When considering the way that these regulations work, particularly in the era of smart data when it will be far more likely that data is gathered across multiple applications, it should be clear what rights customers have to have all that data deleted if they request it.

Sir John Whittingdale: I share my hon. Friend's general view. Customers can authorise that their data be shared through devices with other providers, so they should equally have the right to take back that data if they so wish. He invites me to come back to him with greater detail on that point, and we would be very happy to do so.

Amendment 46 agreed to.

Clause 61, as amended, ordered to stand part of the Bill.

Clause 62

Power to make provision in connection with customer data

Stephanie Peacock: I beg to move amendment 112, in clause 62, page 87, line 2, at end insert—

"(3A) The Secretary of State or the Treasury may only make regulations under this section if—

(a) the Secretary of State or the Treasury has conducted an assessment of the impact the regulations may have on customers, businesses, or industry,

(b) the assessment mentioned in paragraph (a) has been published, and

(c) the assessment concludes that the regulations achieve their objective without imposing disproportionate, untargeted or unnecessary cost on customers or businesses."

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

Amendment 113, in clause 62, page 87, line 12, at end insert—

"(5) The Secretary of State or the Treasury may invite a relevant sectoral regulator to contribute to, or to conduct, any impact assessment conducted in order to enable the Secretary of State or the Treasury to fulfil their obligation under subsection (4)."

This amendment would allow the Secretary of State or the Treasury to enable a relevant sectoral regulator to contribute to, or conduct, any impact assessments on smart data regulations.

Amendment 114, in clause 62, page 87, line 12, at end insert—

"(5) The Secretary of State or the Treasury must consult representatives of the relevant business or industry sector to inform their decision whether to make regulations under this section."

This amendment would require the Secretary of State or the Treasury to consult representatives of the relevant business or industry sector before making smart data regulations.

Amendment 115, in clause 62, page 87, line 12, at end insert—

"(5) Within six months of the passage of this Act, the Secretary of State must—

(a) publish a target date for the coming into force of the first regulations under this section, and

(b) make arrangements for the completion of an assessment of the impact of those regulations."

This amendment would require Government to identify a target for a first smart data scheme within 6 months, and make arrangements for an impact assessment for these regulations.

Stephanie Peacock: Of all the provisions in the Bill, the ones on smart data are those that I am most excited about and pleased to welcome. The potential of introducing smart data schemes is immense: they can bring greater choice to consumers, enable innovation, increase competition and result in the delivery of better products and services. I will address amendments 112 and 113, but I look forward to the opportunity to speak in support of this part more widely.

Most of the detail on how and where smart regimes will be regulated in practice through this Bill will follow in secondary legislation and regulation. That is deliberate and welcome, as it ensures that smart data schemes are built around the realities of the sectors to which they apply. Given that they cannot be included on the face of the Bill, however, it is important that the regulations are prepared in the way that any good data-related law is. There must be a committee of consultation to ensure that the outcome works effectively for consumers and businesses, with the appropriate data protection safeguards.

Indeed, there may be certain sectors in which the costs simply outweigh the benefits of introducing such a regime. Sky believes that there is currently no evidence that a smart data scheme in the communications sector would bring clear and tangible additional benefits to customers. Ofcom consulted on the proposal in 2020 and came to a similar conclusion. Sky argues that the communications sector already has

"a very high bar for supporting consumers to use data to find the best deal for them. For example, in 2020 Ofcom introduced End of Contract Notifications",

which tell customers when their current contract is ending and what they could save by signing up to another deal. Sky says that Ofcom is

"also in the process of introducing One Touch Switching for fixed broadband which will make it easier for customers to move between providers who operate on different networks".

As BT identifies, smart data initiatives require significant time and investment to implement. The Government's impact assessment estimates that the implementation cost for the telecoms sector for a smart data initiative could be anywhere between £610 million and £732 million. That is not to say that the cost outweighs the potential benefits for all industries, including telecoms, but it is important that the Government weigh that up before making any regulations, particularly given that large costs be passed on to consumers, or that there may be less investment in other areas. In the telecoms industry, it could lead to a reduction in investment in full-fibre broadband and 5G. It is imperative, therefore, to ensure that all costs remain targeted, proportionate and necessary to bring about an overall benefit that outweighs the costs. An impact assessment would provide assurance that this has been taken into consideration before any new schemes are introduced.

When conducting such an assessment, sectoral regulators, which can provide expert insight into the impact of smart data in any particular industry, will be well placed to assess the costs and benefits in the detail needed. That is something the Government themselves recognise, as they have placed a requirement in the Bill to consult those regulators. The amendments I propose would strengthen that commitment, allowing relevant sectoral regulators the opportunity, where appropriate, to be formally involved in the process of conducting an impact assessment.

2.45 pm

Moving to amendment 114, smart data initiatives are incredibly complex to run, let alone implement in the first place. As BT argues, for example, a working regime will require steps to guarantee the security, interoperability, quality, intelligibility and comparability of sensitive data across different industry actors. For that to come to fruition, Government must work to establish a collaborative relationship with sectoral regulators and industry. Only then will they be able to work together to co-create a functioning smart scheme that provides solutions that actually benefit consumers. Inserting a requirement to consult industry when conducting an impact assessment would allow that kind of collaboration to be built into the process from the very beginning, giving them a meaningful say on how their industry might be impacted and what the potential challenges of implementation might be. If the Minister does not intend to accept the amendment, will he tell us what steps will his Department take to foster collaborative relationships between Government, regulators and industry before making regulations for any smart data schemes?

Turning to amendment 115, although we must be cautious to ensure that smart data is being implemented where it is actually beneficial—hence the requirement to conduct impact assessments—if the UK is to be a frontrunner in capitalising on the possibilities of smart data, we must act quickly. At the moment, however, although this part lays the foundations for the Secretary of State to regulate for a smart data regime, there is no obligation on them to do so, or even to explore the option of doing so. The amendment would ensure that this opportunity does not get forgotten within the busy day-to-day operations of the Department by ensuring that a target for a data scheme is identified within six months.

That absolutely does not mean that any regulations themselves will have to be made, but it would encourage the Government to actually act on this part and to state an intention to explore the potential of smart data within a certain sector. Arrangements could be made to conduct a proper impact assessment to analyse whether this would be beneficial. There will be no real benefit from this part if it is left unused. It is vital that we capture the moment and enable smart data where it can boost our economy and the consumer experience.

Sir John Whittingdale: I assure the hon. Lady that I and, no doubt, the whole Committee share her excitement about the potential offered by smart data, and I have sympathy for the intention behind her amendments. However, taking each one in turn, we feel amendment 112 is unnecessary because the requirements are already set by the better regulation framework, the Small Business, Enterprise and Employment Act 2015 and, indeed, these clauses. Departments will conduct an impact assessment in line with the better regulation framework and Green Book guidance when setting up a new smart data scheme, and must demonstrate consideration of their requirements under the Equality Act 2010. That will address the proportionality, targeting and necessity of the scheme.

Moreover, the clauses require the Government to consider the effect of the regulations on matters including customers, businesses and competition. An impact assessment would be an effective approach to

meeting those requirements. However, there is a risk that prescribing exactly how a Department should approach the requirements could unnecessarily constrain the policymaking process.

I turn to amendment 113. Clause 74(5) already requires the Secretary of State or the Treasury to consult with relevant sector regulators as they consider appropriate. As part of the process, sector regulators may be asked to contribute to the development of regulatory impact assessments, so we do not believe the amendment is necessary.

On amendment 114, we absolutely share the view of the importance of Government consulting businesses before making regulations. That is why, under clause 74(6), the Secretary of State or the Treasury must, when introducing a smart data scheme, consult such persons as are likely to be affected by the regulations and such sectoral regulators as they consider appropriate. Those persons will include businesses relevant to the envisaged scheme.

On amendment 115, we absolutely share the ambition to grab whatever opportunities smart data offers. In particular, I draw the hon. Lady's attention to the commitments made last month by the Economic Secretary to the Treasury, who set out the Treasury's plans to use the smart data powers to provide open banking with a sustainable regulatory framework, while the Under-Secretary of State for Business and Trade, my hon. Friend the Member for Thirsk and Malton (Kevin Hollinrake), chaired the inaugural meeting of the Smart Data Council last month. That council has been established to support and co-ordinate the development of smart data schemes in a timely manner.

With respect to having a deadline for schemes, we should recognise that implementation of the regulations requires careful consideration. The hon. Member for Barnsley East clearly recognises the importance of consultation and of properly considering the impacts of any new scheme. We are committed to that, and there is a risk that a statutory deadline for making the regulations would jeopardise our due diligence. I assure her that all her concerns are ones that we share, so I hope that she will accept that the amendments are unnecessary.

Stephanie Peacock: I am grateful to the Minister for those assurances. I am reassured by his comments, and I am happy to beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

The Chair: With this it will be convenient to discuss clause 63 stand part.

Sir John Whittingdale: Clause 62 provides the principal regulation-making power to establish smart data schemes in relation to customer data. The clause enables the Secretary of State or the Treasury to make regulations that require data holders to provide customer data either directly to a customer, or to a person they have authorised, at their request. Subsection (3) of the clause also allows for an authorised person who receives the customer data, to exercise the customer's rights in relation to their data on their behalf. We call that "action initiation".

An illustrative example could be in open banking, where customers can give authorised third parties access to their data to compare the consumer's current bank account with similar offers, or to group the contracts within a household together for parents or guardians to better manage children's accounts. Subsection (3) could allow the authorised third party to update the customer's contact details across the associated accounts, for example if an email address changes.

Clause 63 outlines the provisions that smart data scheme regulations may contain when relating to customer data. The clause establishes much of the critical framework that smart data schemes will be built on. On that basis, I commend clauses 62 and 63 to the Committee.

Stephanie Peacock: As previously mentioned, and with the caveats that I expressed when I was discussing my amendments, I am extremely pleased to be able to welcome this part of the Bill. In essence, clauses 62 and 63 enable regulations that will allow for customer data to be provided to a third party on request. I will take the opportunity to highlight why that is the case by looking at some of the benefits that smart data can provide.

Since 2018, open banking—by far the most well known and advanced version of smart data in operation—has demonstrated what smart data can deliver over and over again. For the wider economy, the benefits have been remarkable, with the total value to the UK economy now amounting to more than £4.1 billion, according to Coadec, the Coalition for a Digital Economy. Consumers' experience of banking has been revolutionised if they have consented of their own accord to have third-party applications access their financial data.

Indeed, a whole host of money management tools and apps can now harness people's financial data to create personalised recommendations based on their spending habits, including how to budget or save. During a cost of living crisis, some of those tools have been extremely valuable in helping people to manage new bills and outgoings. Furthermore, online retailers can now connect directly to someone's bank so that, rather than spending the time filling in their card details each time they make a purchase, an individual can approve the transaction via their online banking system.

It is important to reiterate that open banking is based on consent, so consumers participate only if they feel it is right for them. As it happens, millions of people have capitalised on the benefits. More than seven million consumers and 50% of small and medium-sized enterprises have used open banking services to gain a holistic view of their finances, to support applications for credit and to pay securely, quickly and cheaply.

Though open banking has brought great success for both consumers and the wider economy, it is also important that the Government learn lessons from its implementation. We must pay close attention to how the introduction of open banking has impacted both the industry and consumers and ensure that any takeaways are factored in when considering an expansion of smart data into new industries.

Further, given that the Government clearly recognise the value of open data, as shown by this section of the Bill, it is a shame that the Bill does not go further in exploring the possibilities of opening datasets in other

[Stephanie Peacock]

settings. Labour has explicitly set out to do that in its industrial strategy. For example, we have identified that better, more open datasets on jobs could help us to understand where skills shortages are, allowing jobseekers, training providers and Government to better fill those gaps.

The provisions in clauses 62 and 63 to create new regimes of smart data are therefore welcome, but the Bill unfortunately remains a missed opportunity to fully capitalise on the opportunities of open, secure data flows.

Question put and agreed to.

Clause 62 accordingly ordered to stand part of the Bill.

Clause 63 ordered to stand part of the Bill.

Clause 64

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 consider clause 65 stand part.

Sir John Whittingdale: Clause 64 provides the principal regulation-making power for the creation of smart data schemes relating to business data. Regulations created through this clause allow for business data to be provided to the customer of a trader or a third-party recipient. Business data may also be published to be more widely available.

These regulations relating to business data will increase the transparency around the pricing of goods and services, which will increase competition and benefit both consumers and smaller businesses. To give just one example, the Competition and Markets Authority recently highlighted the potential of an open data scheme that compared the prices of fuel at roadside stations, increasing competition and better informing consumers. It is that kind of market intervention that the powers provide for.

Clause 65 outlines provisions that regulations relating to business data may contain. Those provisions are non-exhaustive. The clause largely mirrors clause 63, extending the same protections and benefits to schemes that make use of businesses data exclusively or in tandem with customer data. The clause differs from clause 63 in subsection (2), where an additional consideration is made as to who may make a request for business data. As action initiation relates only to an authorised person exercising a customer's rights relating to their data, clause 65 does not include the references to that that are made in subsections (7) and (8) of clause 63.

Stephanie Peacock: The measures in these clauses largely mirror 62 and 63, but they refer to business data rather than customer data. I therefore refer back to my comments on clause 62 and 63 and the benefits that new regulations such as these might be able to provide. Those remarks provide context as to why I am pleased to support these measures, which will allow the making of regulations that require data holders to share business data with third parties.

However, I would like clarification from the Minister on one point. The explanatory notes explain that the powers will likely be used together with those in clauses 62 and 63, but it would be good to hear confirmation from the Minister on whether there may be circumstances in which the Department envisages using the powers regarding business data distinctly. If there are, will he share examples of those circumstances? It would be good for both industry and Members of this House to have insight into how these clauses, and the regulatory powers they provide, will actually be used.

Sir John Whittingdale: I think it is probably sensible if I come back to the hon. Lady on that point. I am sure we would be happy to provide examples if there are ones that we can identify.

Question put and agreed to.

Clause 64 accordingly ordered to stand part of the Bill.

Clause 65 ordered to stand part of the Bill.

Clause 66

DECISION-MAKERS

3 pm

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

The Chair: With this it will be convenient to discuss Clauses 67 to 72 stand part.

Sir John Whittingdale: Clauses 66 to 72 contain a number of provisions that will allow smart data regulations to function effectively. They are provisions on decision makers who approve and monitor third parties that can access the data, provisions on enforcement of the regulations and provisions on the funding of smart data schemes. It is probably sensible that I go through each one in more detail.

Clause 66 relates to the appointment of persons or accrediting bodies referred to as decision makers. The decision makers may approve the third parties that can access customer and business data, and act on behalf of customers. The decision makers may also revoke or suspend their accreditation, if that is necessary. An accreditation regime provides certainty about the expected governance, security and conduct requirements for businesses that can access data. Customers can be confident their chosen third party meets an appropriate standard. Clause 66 allows the decision maker to monitor compliance with authorisation conditions, subject to safeguards in clause 68.

Clause 67 enables regulations to confer powers of enforcement on a public body. The public body will be the enforcer, responsible for acting upon any breaches of the regulations. We envisage that the enforcer for a smart data scheme is likely to be an existing sectoral regulator, such as the Financial Conduct Authority in open banking. While the clause envisages civil enforcement of the regulations, subsection (6) allows for criminal offences in the case of falsification of information or

evidence. Under subsections (3) and (10), the regulations may confer powers of investigation on the enforcer. That may include powers to require the provision of information and powers of entry, search and seizure. Those powers are subject to statutory restrictions in clause 68.

Clause 68 contains provisions limiting the investigatory powers given to enforcers. The primary restriction is that regulations may not require a person to give an enforcer information that would infringe the privileges of Parliament or undermine confidentiality, legal privilege and, subject to the exceptions in subsection (7), privilege against self-incrimination. Subsection (8) prevents any written or oral statement given in response to a request for information in the course of an investigation from being used as evidence against the person being prosecuted for an offence, other than that created by the data regulations.

Clause 69 contains provisions relating to financial penalties and the relevant safeguards. It sets out what regulations must provide for if enabling the use of financial penalties. Subsection (2) requires that the amount of a financial penalty is specified in, or determined in accordance with, the regulations. For example, the regulations may set a maximum financial penalty that an enforcer can impose and they may specify the methodology to be used to determine a specific financial penalty.

Clause 70 enables actors in smart data schemes to require the payment of fees. The circumstances and conditions of the fee charging process will be specified in the regulations. The purpose of the clause, along with clause 71, is to seek to ensure that the costs of smart data schemes, and of bodies exercising functions under them, can be met by the relevant sector.

It is intended that fees may be charged by accrediting bodies and enforcers. For example, regulations could specify that an accrediting body may charge third parties to cover the cost of an accreditation process and ongoing monitoring. Enforcers may also be able to charge to cover or contribute to the cost of any relevant enforcement activities. The regulations may provide for payment of fees only by persons who are directly affected by the performance of duties, or exercise of powers, under the regulations. That includes data holders, customers and those accessing customer and business data.

Clause 71 will enable the regulations to impose a levy on data holders or allow a specified public body to do so. That is to allow arrangements similar to those in section 38 of the Communications Act 2003, which enables the fixing of charges by Ofcom. Together with the provision on fees, the purpose of the levy is to meet all or part of the costs incurred by enforcers and accrediting bodies, or persons acting on their behalf. The intention is to ensure that expenses can be met without incurring a cost to the taxpayer. Levies may be imposed only in respect of data holders that appear to be capable of being directly affected by the exercise of the functions.

Clause 72 provides statutory authority for the Secretary of State or the Treasury to give financial assistance, including to accrediting bodies or enforcers. Subsection (2) provides that the assistance may be given on terms and conditions that are deemed appropriate by the regulation maker. Financial assistance is defined to include both actual or contingent assistance, such as a grant, loan, guarantee or indemnity. It does not include the purchase of shares. I commend clauses 66 to 72 to the Committee.

Stephanie Peacock: Clauses 66 to 72 provide for decision makers and enforcers to help with the operation and regulation of new smart data regimes. As was the case with the digital verification services, where I agreed that there was a need for the Secretary of State to have limited powers to ensure compliance with the trust framework, powers will be needed to ensure that any regulations made under this part of the Bill are followed. The introduction in clause 67 of enforcers—public bodies that will, by creating fines, penalties and notices of compliance, ensure that organisations follow regulations made under part 3—is therefore welcome.

As ever, it is pleasing to see that the relevant restrictions on the powers of enforcers are laid out in clause 68, to ensure that they cannot infringe upon other, more fundamental rights. It is also right, as is ensured by clause 69, that there are safeguards on the financial penalties that an enforcer is able to issue. Guidance on the amount of any penalties, as well as a formalised process for issuing notices and allowing for appeal, will provide uniformity across the board so that every enforcer acts proportionately and consistently.

Decision makers allowed for by clause 66 will be important, too, in conjunction with enforcers. They will ensure there is sufficient oversight of the organisations that are enabled to have access to customer or business data through any particular smart data regimes. Clauses 70, 71 and 72, which finance the activities of decision makers and enforcers, follow the trend of sensible provisions that will be required if we are to have confidence that regulations made under this part of the Bill will be adhered to. In short, the measures under this grouping are largely practical, and they are necessary to support clauses 62 to 65.

Question put and agreed to.

Clause 66 accordingly ordered to stand part of the Bill.

Clauses 67 to 72 ordered to stand part of the Bill.

Clause 73

CONFIDENTIALITY AND DATA PROTECTION

Question proposed, That the clause stand part of the Bill

The Chair: With this it will be convenient to discuss clauses 74 to 77 stand part.

Sir John Whittingdale: Clauses 73 to 77 relate to confidentiality and data protection; various provisions connected with making the regulations, including consultation, parliamentary scrutiny and a duty to conduct periodic reviews of regulations; and the repeal of the existing regulation-making powers that these clauses replace.

Clause 73(1) allows the regulations to provide that there are no contravening obligations of confidence or other restrictions on the processing of information. Subsection (2) ensures that the regulations do not require or authorise processing that would contravene the data protection legislation. The provisions are in line with

[Sir John Whittingdale]

the approach taken towards pension dashboards, which are electronic communications services that allow individuals to access information about their pensions.

Clause 74(1) allows the regulation-making powers to be used flexibly. Subsection (1)(f) allows regulations to make provision by reference to specifications or technical requirements. That is essential to allow for effective and safe access to customer data, for instance the rapid updating of IT and security requirements, and it mirrors the powers enacted in relation to pensions dashboards, which I have mentioned. Clause 74(2) provides for limited circumstances in which it may be necessary for regulations to modify primary legislation to allow the regulations to function effectively. For instance, it may be necessary to extend a statutory alternative dispute resolution scheme in a specific sector to cover the activities of a smart data scheme.

Clause 74(3) states that affirmative parliamentary scrutiny will apply to the first regulations made under clauses 62 or 64; that is, affirmative scrutiny will apply to regulations that introduce a scheme. Affirmative parliamentary scrutiny will also be required where primary legislation is modified, where regulations make requirements more onerous for data holders and where the regulations confer monitoring or enforcement functions or make provisions for fees or a levy. Under clause 74(5), prior to making regulations that will be subject to affirmative scrutiny, the Secretary of State or the Treasury must consult persons who are likely to be affected by the regulations, and relevant sectoral regulators, as they consider appropriate.

The Government recognise the importance of enabling the ongoing scrutiny of future regulations, so clause 75 requires the regulation maker to review the regulations at least at five-yearly intervals. Clause 76 repeals the regulation-making powers in sections 89 to 91 of the Enterprise and Regulatory Reform Act 2013, which are no longer adequate to enable the introduction of effective smart data schemes. Those sections are replaced by the clauses in part 3 of the Bill. Clause 77 defines, or refers to definitions of, terms used in part 3 and is essential to the functioning and clarity of part 3. I commend the clauses to the Committee.

Stephanie Peacock: Many of the clauses in this grouping are supplementary to the provisions that we have already discussed, or they provide clarification as to which regulations under part 3 are subject to parliamentary scrutiny. I have no further comments to add on the clauses, other than to welcome them as fundamental to the wider part. However, I specifically welcome clause 75, which requires that the regulations made under this part be periodically reviewed at least every five years.

I hope that such regulations will be under constant review on an informal basis to assess how well they are working, but it is good to see a formal mechanism to ensure that that is the case over the long term. It would have been good, in fact, to see more such provisions throughout the Bill, to ensure that regulations that are made under it work as intended. Overall, I hope it is clear that I am very supportive of this part's enabling of smart data regimes. I look forward to it coming into force and unlocking the innovation and consumer benefits that such schemes will provide.

Question put and agreed to.

Clause 73 accordingly ordered to stand part of the Bill.

Clause 74 to 77 ordered to stand part of the Bill.

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

3.14 pm

Adjourned till Tuesday 23 May at twenty-five minutes past Nine o'clock.

Written evidence reported to the House

DPDIB29 Connected by Data (supplementary submission)

DPDIB30 Reset

DPDIB31 Professor David Erdos, Professor of Law and the Open Society, Co-Director, Centre for Intellectual Property and Information Law, Faculty of Law, University of Cambridge

DPDIB32 Kent & Medway Health and Care Strategic Information Governance Network