

PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DIGITAL ECONOMY BILL

Ninth Sitting

Thursday 27 October 2016

(Morning)

CONTENTS

CLAUSES 38 to 55 agreed to, some with amendments.

CLAUSE 56, as amended, under consideration when the Committee adjourned till this day at Two o'clock.

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 31 October 2016

© Parliamentary Copyright House of Commons 2016

This publication may be reproduced under the terms of the Open Parliament licence, which is published at www.parliament.uk/site-information/copyright/.

The Committee consisted of the following Members:

Chairs: MR GARY STREETER, † GRAHAM STRINGER

- | | |
|---|--|
| † Adams, Nigel (<i>Selby and Ainsty</i>) (Con) | Mann, Scott (<i>North Cornwall</i>) (Con) |
| † Brennan, Kevin (<i>Cardiff West</i>) (Lab) | † Matheson, Christian (<i>City of Chester</i>) (Lab) |
| † Davies, Mims (<i>Eastleigh</i>) (Con) | † Menzies, Mark (<i>Fylde</i>) (Con) |
| Debbonaire, Thangam (<i>Bristol West</i>) (Lab) | † Perry, Claire (<i>Devizes</i>) (Con) |
| † Foxcroft, Vicky (<i>Lewisham, Deptford</i>) (Lab) | † Skidmore, Chris (<i>Parliamentary Secretary, Cabinet Office</i>) |
| † Haigh, Louise (<i>Sheffield, Heeley</i>) (Lab) | † Stuart, Graham (<i>Beverley and Holderness</i>) (Con) |
| † Hancock, Matt (<i>Minister for Digital and Culture</i>) | † Sunak, Rishi (<i>Richmond (Yorks)</i>) (Con) |
| † Hendry, Drew (<i>Inverness, Nairn, Badenoch and Strathspey</i>) (SNP) | |
| † Huddleston, Nigel (<i>Mid Worcestershire</i>) (Con) | Marek Kubala, <i>Committee Clerk</i> |
| † Jones, Graham (<i>Hyndburn</i>) (Lab) | |
| † Kerr, Calum (<i>Berwickshire, Roxburgh and Selkirk</i>) (SNP) | † attended the Committee |

Public Bill Committee

Thursday 27 October 2016

(Morning)

[GRAHAM STRINGER *in the Chair*]

Digital Economy Bill

11.30 am

The Chair: If hon. Members wish to take off their jackets, they have the Chair's permission to do so.

Clause 38

DISCLOSURE OF INFORMATION BY CIVIL REGISTRATION
OFFICIALS

Amendment proposed (25 October): 107, in clause 38, page 36, line 12, leave out from "that" to end of subsection and insert—

- "(a) the authority or civil registration official to whom it is disclosed (the "recipient") requires the information to enable the recipient to exercise one or more of the recipient's functions and,
- (b) the data subjects whose information is being disclosed have given valid consent under data protection legislation."—(*Louise Haigh.*)

This amendment would remove bulk sharing while allowing certificates to be shared to support electronic government services.

Question again proposed, That the amendment be made.

The Chair: I remind the Committee that with this we are discussing amendment 97, in clause 38, page 36, line 15, at end insert—

"(2A) An authority or civil registration official requiring the information must specify the reasons for requiring the information to be disclosed.

(2AA) Information disclosed under this section shall not be shared with any other public or private body beyond those specified in subsection (1)."

Graham Jones (Hyndburn) (Lab): It has been a couple of days since we last met, but my hon. Friend the Member for Sheffield, Heeley made a very important point in her speech regarding where we should look for best practice. The UK is one of the Digital 5, and she brought up Estonia as a country that, when we consider big data, we should reflect on. In dealing with the Bill, we are casting our eye around to see how we can manage big data, personal information, between public bodies. She made the valid point that a fundamental question seems to run throughout the Bill and the clause: does the individual own the information or does the state own it? Because the Government have taken the view, unlike what happens in Estonia, that the state owns the information, we have a series of such clauses. We are primarily trying to find a way to balance the rights of the individual, while the state retains ownership of the information in any form, but, particularly as we move forward, in digital form; that is what I am concerned about.

Let me explain what is done in Estonia and why the Bill in years to come will probably need to be usurped by a new Bill. Estonia has transferred the ownership of data from the state to the individual. When the individual owns the data, there is no need for these complex fudges to try to find a way in which people's privacy and the integrity of data can be respected, while ownership remains with an umbrella organisation.

The criticism that I make to the Government, and my hon. Friend's point, is that a fundamental rethink or reset will have to occur at some point because of what is missing from the Bill and the clause. It talks about public bodies, but the Government do not address in this or any other clause the fact that private corporations hold enormous amounts of personal data on people and the ownership of that lies with them, not with the individual. That is why the point that she made was so pertinent. The ownership of data should lie with the individual. As a country, as a nation, we should be looking to transfer that ownership. That is why we cannot address what happens in the private sector. Absent from the Bill are any clauses or even subsections tackling data and information in the private sector. It is solely about the public sector and trying to square off those conundrums and contradictions.

The Government have missed an opportunity to empower people and to be on the side of the individual, the ordinary person, who feels disempowered by all this. They are on the side of big government and, by absence, of big corporations, which in my view is a fundamentally flawed position. That question was asked in Estonia, and it is why it reversed the answer: ownership should lie with the individual.

I can see the Parliamentary Secretary, Cabinet Office, chatting to the Minister for Digital and Culture, and he will probably provide an answer that talks about a destination, saying that if someone gets on a bus, they only get off at the end destination. We all know that when someone gets on a bus, there are many stops before the destination on the front of the bus. They do not have to go all the way. I presume the Minister will explain why the clause is correct from the Government's point of view and why my argument is flawed. He will say, "If you are going to empower the individual with data, you would need a national identification card system, as in Estonia. The empowerment of the individual must correlate with a national ID card scheme."

The Minister will make that argument, but that is like getting on a bus and only being able to get off at the final destination, with a national ID card scheme. No one is saying that. There are many bus stops we can get off at before the end. The issue is not binary, with the place we get on the bus and the place we get off. The destination is not necessarily ID cards. The principle that these are the individuals' own data should be at the heart of the Bill, and the clause does not represent that. The absence of any mention of the private sector is alarming.

Moving on, I want to touch briefly on another aspect that is missing from the Bill and should be considered. This is the Digital Economy Bill, but it is all about the public sector. There is an absence of any reference to the private sector per se. This part of the Bill deals with the digital economy and the provision of public services. Returning to the Estonia example and empowering the individual, people in Estonia can set up a business or

company in three or four minutes online. Where is the pro-business element of the Bill? It is certainly not this clause, which relates to data and information in relation to the state and public bodies. Why can individuals here not set up businesses in four minutes? Why is it not a pro-business Bill? Why does it not talk about business? Nothing in the Bill talks about being pro-business.

The clause is simply about public bodies holding big data, and in that respect, it lives in the past, not the future. I urge the Government to think about the fundamental principles and to not make the argument that the amendments would lead to an ID card system, although Estonia does have ID cards. I would have ID cards tomorrow—it is well known across the patch that I would not be on the list of soggy, wet liberals—but that does not mean that the principle that the individual owns data would lead to ID cards. It does not. I ask the Minister, with all due respect, not to suggest that I am making that argument, because I am not.

The Bill is not pro-business and is fundamentally flawed. The clause is simply about trying to manage all the conflicts and contradictions from yesterday's age. It does not deal with the future. The Government have fallen short. I emphasise the word "economy" in the Bill's title—it is not about public services, but the economy. I put that word up in bright lights. Where does the Bill talk about the economy? We are talking about public bodies and public authorities.

The Parliamentary Secretary, Cabinet Office (Chris Skidmore): That was an impressive Second Reading speech. I am here to speak to amendment 97 and 107.

Graham Jones: And stand part.

Chris Skidmore: Not necessarily; that has not been called yet. The amendments have been tabled in the name of the hon. Member for Sheffield, Heeley. She finished her speech on Tuesday, and I put on record my thanks for her impressive scrutiny of the Bill, which she has done almost single-handedly. I note that she made a weighty speech about Concentrix yesterday, so I do not know how she finds the time to sleep. I am sure that it will be noted in the Lords that we have gone through a full process of scrutiny in Committee.

The Government will ensure that citizens can access future Government digital services effectively and securely, while removing the current reliance on paper certificates. That will provide more flexibility and modernise how services are delivered.

Amendment 97 would require registration officials and public authorities requesting information to specify reasons for requiring disclosure. In considering a request to share information under those powers, a registration official would first need to be satisfied that the recipient requires the information to enable them to exercise one or more of their functions.

In her speech on Tuesday, the hon. Lady raised some issues about the Data Protection Act 1998 and said that the Government should set out clearly that it is being honoured, particularly for registration. The hon. Member for Hyndburn talked about fundamental principles, and I can confirm that the Bill's fundamental principle is its compliance with the Data Protection Act. Data should not be disclosed if to do so would be incompatible with that Act, the Human Rights Act 1998 or part 1 of the Regulation of Investigatory Powers Act 2000.

The Data Protection Act is Magna Carta of the data world, and we want to ensure that all parts of the Bill comply with it. When disclosing information, only minimal information will be provided, in accordance with the requirements of the data recipient.

Louise Haigh (Sheffield, Heeley) (Lab): I am grateful to the Minister for his kind and polite words. If that is the case, why does the Bill contain the words "clear and compelling", rather than "necessary and proportionate", which is the term associated with the Data Protection Act?

Chris Skidmore: I have taken legal advice about that issue, which the hon. Lady raised in her previous speech, and I have been told that those words do not in any way, shape or form challenge or change the interpretation of and compliance with the Data Protection Act. We will be happy to look again at the wording and reflect on it if that gives her confidence that we are absolutely committed to ensuring that the Data Protection Act runs through the core of the Bill. Registration officials are required to be aware of the reasons for the request, so the intention behind the amendment is already achieved by the clause.

Amendment 97 seeks to prevent the onward disclosure of information by the data recipient to any other public or private body beyond the specified public authorities listed in proposed new section 19AB(1) of the Registration Service Act 1953. Disclosures under the power will be restricted to the specified public authorities listed in proposed new section 19AB(1). In addition, personal data will be shared only in accordance with the power and in adherence to the Data Protection Act, by which the recipients will also be bound. As an additional safeguard, under the code of practice, data-sharing agreements can place restrictions on onward disclosures of data, which will be adopted where appropriate.

Amendment 107 would retain the requirement for a civil registration official to be satisfied that the information was required by a recipient to fulfil one of more of their functions before disclosing data. It seeks to add a requirement that an individual must have given valid consent under data protection legislation before any disclosure of their personal data. The data protection legislation referred to is believed to be the Data Protection Act, to which these clauses are already subject. They already state that personal data must be processed fairly. In practice, it will sometimes be necessary to share information in the public interest, where it is impractical or inappropriate to seek or rely on the consent of the individual concerned, but that is already permitted under the Data Protection Act, which we are determined to ensure remains in force.

In the hon. Lady's speech on Tuesday, she talked about the uses of bulk data and asked me to give examples of where the powers will be used and where they are already used. The powers will allow registration officials to disclose birth data to other local authorities. Currently, a registrar is unable to notify another local authority if a birth takes place in their district but the child's parents reside in another. Being able to disclose data across district boundaries will assist healthcare, school and wider local authority planning. Being able to share bulk information will ensure that children are

[Chris Skidmore]

known to the local authorities in which they reside and that action can be taken to address any needs of the child or parent.

Another example relates to blue badge fraud. It is estimated that about 2.1% of blue badge fraud relates to use of a blue badge following the death of the individual to whom it belonged. The new powers will allow data to be shared with the local authorities to help reduce that fraud.

Louise Haigh: The Minister gives an important example—blue badge fraud—in which data are accessed rather than shared. The local authority will have an access point into Department for Work and Pensions data to determine whether someone is disabled, but there is absolutely no need for bulk data sharing across local authorities. That is the kind of example that we should follow in the rest of the public sector.

11.45 am

Chris Skidmore: The hon. Lady mentions legal portals through which data can be shared. The key point is that although we have specific examples of data being accessed or shared, every new data-sharing arrangement has to be established within a very specified remit. A great example of a data-sharing arrangement for registrars that is already happening is the Tell Us Once service, in which birth and death registration information is shared across local and central Government. That system has been developed by Government, is envied by the private sector and clearly demonstrates the benefit of sharing civil registration information for both citizens and Government, but the problem is that it is very limited.

We cannot move forward by having endless tiny data-sharing agreements; we need to be able to create a wider platform. For instance, to share death data, individual local authorities have to forge individual relationships. We need to ensure that that is far broader, so that local authorities and Departments can work together to help to prevent unwarranted and unwanted mail from being sent to the family of a deceased person, which can often cause a great deal of distress.

This is evolution, not revolution. We are following the Data Protection Act 1998 and the codes of practice, which the Committee will discuss, will be reviewed every year. We can now share data effectively on a bulk level but without using personal details apart from for the benefit of those it will serve: children, local authorities, planning numbers. This is absolutely the right thing to be doing.

Disclosure will take place without consent only where that is consistent with Data Protection Act rules on fair disclosure. At all times, data can be shared only with specified public authorities as defined in section 19AB of the Registration Service Act 1953. The code of practice makes it very clear that if there are any data breaches or any of those authorities do not follow the code—we will discuss the code when we consider debt measures—they can be removed from that list. With that explanation, I hope the hon. Member for Sheffield, Heeley will agree that the necessary measures are already included in the clause and will withdraw her amendment.

Louise Haigh: My hon. Friend the Member for Hyndburn made important points about the absence from the Bill of clauses dealing with the private sector. In the evidence session, we heard from the chief executive of a tech start-up in Canary Wharf who made it very clear that nothing in the Bill would help his business or others operating in the digital economy. We will certainly return to that theme. I draw my hon. Friend's attention to new clause 31, which the Committee will consider on Tuesday morning and which will require a review of data ownership across the public and private sectors.

I am grateful that the Minister has confirmed that the Government will consider a rewording of “clear and compelling”, because I think it could lead to some confusion regarding the compliance of part 5 with the Data Protection Act. It is great to hear him praise the Tell Us Once scheme, which was set up by the shadow Secretary of State for Culture, Media and Sport, my hon. Friend the Member for West Bromwich East (Mr Watson)—I will pass on the Minister's congratulations to him.

The Minister referred to a platform; will he confirm whether he is referring to a central database of citizens' civil registration information? That is a key concern. I am also glad to hear that sharing information without consent will take place only in explicitly defined circumstances, but I am still not clear why chapter 2 of part 5 will not—as our amendment 97 would—require civil registration officials to disclose why they are sharing information, as all the other chapters in part 5 require data-sharing arrangements or specified persons to do. If the Minister can explain that to me in an intervention, I will happily withdraw the amendment.

Chris Skidmore: I used the word “platform” as part of a process argument about being able to look at data in the round, rather than to suggest that there would be any centralised data collection. That is certainly not the case. For public confidence, measures in the codes of practice set out clearly that when it comes to the data-sharing measures, once data have been used for the required purpose, they are then destroyed. They are not kept on any register for any historical purpose.

Turning to the hon. Lady's second point—

The Chair: Minister, this is an intervention. I call Louise Haigh—you may intervene again, Minister.

Louise Haigh: My question stands: why is there not a requirement in this chapter of this part for the reasons for disclosure, as there is in all the other chapters? I would be grateful if the Minister intervened regarding that point.

Chris Skidmore: The registration codes of practice clearly set out that the purposes will need to be defined and that a business case will need to be made. None of that can take place until we ensure that there is a specified public function defined on the face of legislation, particularly when it comes to the code of practice that registrars will have to follow and which will be reviewed yearly. I believe that measures are in place to ensure that any data-sharing is done through a due process that is incredibly tight, restrictive and respectful of the use of individuals' data.

Louise Haigh: I am afraid I am still not satisfied with why that requirement is not on the face of the Bill as it is in other chapters, so I will press amendment 97 to a vote. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Amendment proposed: 97, in clause 38, page 36, line 15, at end insert—

“(2A) An authority or civil registration official requiring the information must specify the reasons for requiring the information to be disclosed.

(2AA) Information disclosed under this section shall not be shared with any other public or private body beyond those specified in subsection (1).”—(*Louise Haigh.*)

Question put, That the amendment be made.

The Committee divided: Ayes 7, Noes 9.

Division No. 7]

AYES

Brennan, Kevin	Jones, Graham
Foxcroft, Vicky	Kerr, Calum
Haigh, Louise	Matheson, Christian
Hendry, Drew	

NOES

Adams, Nigel	Perry, Claire
Davies, Mims	Skidmore, Chris
Hancock, rh Matt	Stuart, Graham
Huddleston, Nigel	Sunak, Rishi
Menzies, Mark	

Question accordingly negatived.

Amendment made: 119, in clause 38, page 37, line 35, at end insert—

“() The code of practice must be consistent with the code of practice issued under section 52B (data-sharing code) of the Data Protection Act 1998 (as altered or replaced from time to time).”—(*Chris Skidmore.*)

This amendment requires a code of practice issued under section 19AC of the Registration Service Act 1953 by the Registrar General and relating to the disclosure of information under section 19AA of that Act to be consistent with the data-sharing code of practice issued by the Information Commissioner under the Data Protection Act 1998.

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

Chris Skidmore: The clause amends the Registration Service Act 1953 to introduce new flexible data-sharing powers that allow registration officials to share data from birth, death, marriage and civil partnership records with public authorities for the purpose of fulfilling their functions. That will provide more flexibility and modernise how Government services are delivered.

Being able to share registration data will bring many benefits, for example, in combating housing tenancy fraud. The National Fraud Authority estimates that housing tenancy fraud—for example, a tenant dies and someone else continues to live in the property when they have no right to—costs local authorities around £845 million each year. Being able to provide death data to local authorities will assist in reducing that kind of fraud. The sharing of data will provide benefits for the public in a number of different ways, including the removal of barriers when accessing Government services. It will pave the way for citizens to access Government services more conveniently, efficiently and securely, for example by removing the current reliance on paper certificates to access services.

Data will continue to be protected in accordance with data protection principles, and a number of safeguards will be put in place. Registration officials will be able to share data with only specified public authorities, as defined in new section 19AB—which also includes a power for the Minister to make regulations to add, modify or remove a reference to a public body, thereby providing reassurance that the data will only be disclosed in a targeted way to the Departments listed. As set out in paragraph 58 of the code of practice, the Registrar General has a responsibility to review the code annually, which will involve the national panel for registration. As an additional safeguard, such regulations will be made under the affirmative procedure, requiring the approval of both Houses.

All data sharing will be underpinned by a statutory code of practice, as set out in section 19AC. As I have said, when revising the code the Registrar General will have an obligation to consult the Minister, the Information Commissioner and other relevant parties. The code of practice will act as a safeguard by explaining how discretionary data-sharing powers should be used. The code will require data-sharing agreements to be drawn up, which will include safeguards on things such as how data will be used and stored and for how long they are to be retained, and forbidding data to be cross-linked in any way.

Question put and agreed to.

Clause 38, as amended, accordingly ordered to stand part of the Bill.

Clause 39

CONSEQUENTIAL PROVISION

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

Louise Haigh: Several questions relating to the clause remain unanswered because we were cantering through on Tuesday afternoon. Will the Minister confirm, and give examples of, what the powers in this part of the Bill will exclude? Will he give some guidance on how officials are meant to determine where the line is for what is and is not included? Will there be more guidance issued for non-public sector authorities that will come under the legislation? Will he assure us that the codes, in their next iteration, will provide further guidance on how officials should deal with conflicts of interest when sharing data, how they should identify any unintended risks from disclosing data to organisations, and how sponsoring public authorities should assess whether their systems and procedures are appropriate for the secure handling of data? I would also be grateful if the Minister confirmed what lessons have been learned from the recent National Audit Office report that found more than 9,000 data incidents in the past year alone, and how the Government are improving their data processes to address those issues.

Will the Minister assure us that nothing in the Bill will undermine patient confidentiality? I am aware that the British Medical Association has written to him but has not had a response. The BMA is unclear about whether the scope of the Bill includes the disclosure of personal health and social care information, which would significantly weaken existing protections for confidential

[*Louise Haigh*]

data. Will the well established rules that already protect such confidential information continue to apply, and will he assure us that these powers will not override common law in this vital area?

Finally, on a significant area that has not yet been addressed, do the Government intend to implement the EU's general data protection regulation? If they do, why is the Bill not compliant with it?

Chris Skidmore: On the European directive, which is to be introduced in May 2018, the codes will be revised and will reflect that. That is why the flexibility we have from the codes not being written into the Bill is so important—so that we can deal with instances in which there will be change in the future. They will be updated to reflect that change in May 2018.

Civil registration officers—public servants who want to share data for the benefit of the public—are not trying to do anything that would compromise those whom they serve. In the code of practice, paragraph 47 states that privacy impact assessments will be put in place to ensure that there will be compliance with data protection obligations and that they meet individual expectations of privacy. All Departments entering into data-sharing arrangements under the powers must comply with privacy impact assessments and publish the findings. We want to ensure transparency so that members of the public understand why it is necessary for those data to be shared.

An application to share data is not simply a permissive path by which new data-sharing arrangements can be established without going through due process and regard. In the fairness and transparency section of the data code of practice, there are many questions that must be addressed in order to establish the data-sharing arrangements. They are clearly laid out.

12 noon

Louise Haigh: The Minister says that civil registration officials will be required to publish their findings. What exactly will they be required to publish, under either the code or the measures in the clause?

Chris Skidmore: Paragraphs 47 and 49 of the civil registration data-sharing code of practice clearly state:

“All government departments entering into data sharing arrangements under these powers must conduct a Privacy Impact Assessment and to publish its findings. The Information Commissioner's Conducting Privacy Impact Assessments code of practice provides guidance on a range of issues in respect of these assessments, including the benefits of conducting privacy impact assessments and practical guidance on the process required to carry one out...Registration officials entering into new data sharing arrangements should refer to the following guidance issued by the Information Commissioner on Privacy Impact Assessments which includes screening questions...to determine whether a Privacy Impact Assessment is required.”

On health care data, the Government are considering Dame Fiona Caldicott's recommendations. The consultation closed on 7 September, and I confirm that the Bill's powers will not be used in relation to health and care data before we have completed that process.

Louise Haigh: The Bill explicitly says that health and social care information should be excluded, but there are concerns that it is drafted so widely that it could be used for that, and I think that the Minister has just confirmed it. He is saying that it is wide enough that should the Government decide on the basis of Dame Fiona's review that they want to share health and social care information, the Bill will enable it. Is that the case?

Chris Skidmore: The Government will respond to the National Data Guardian's review. It will not have an impact on the Bill at this stage. The Department of Health recently concluded a public consultation and is considering how to implement her recommendations. As it will take time to make the changes and demonstrate that the public have confidence in them, it would be inappropriate for the Government to seek new information sharing powers in respect of health and care data at this time. I note that we will come to health and care data when we debate a later group of amendments on research, and I hope to provide more information when we do.

Question put and agreed to.

Clause 39 accordingly ordered to stand part of the Bill.

Clause 40

DISCLOSURE OF INFORMATION TO REDUCE DEBT OWED TO THE PUBLIC SECTOR

Louise Haigh: I beg to move amendment 190, in clause 40, page 39, line 21, leave out “have regard, in particular, to” and insert “must comply with”.

The Chair: With this it will be convenient to discuss the following: amendment 191, in clause 44, page 42, line 8, leave out “have regard to” and insert “comply with”.

Amendment 192, in clause 52, page 49, line 8, leave out “have regard to” and insert “comply with”.

Amendment 193, in clause 60, page 55, line 20, leave out “have regard to” and insert “comply with”.

Amendment 194, in clause 67, page 66, line 15, leave out “have regard to” and insert “comply with”.

Amendment 198, in clause 82, page 80, line 18, at end insert

“and only after the codes of practice required under sections 35, 44, 52 and 60 have been approved by a resolution of each House of Parliament.”

New clause 35—*Public register of data disclosures*—

(1) No disclosure by a public authority under Part 5 shall be lawful unless detailed by an entry in a public register.

(2) Any entry made in a public register under subsection (1) shall be disclosed to another person only for the purposes set out in this Part.

(3) Each entry in the register must contain, or include information on—

- (a) the uniform resource locator of the entry,
- (b) the purpose of the disclosure,
- (c) the specific data to be disclosed,
- (d) the data controllers and data processors involved in the sharing of the data,
- (e) any exchange of letters between the data controllers on the disclosure,

(f) any other information deemed relevant.

(4) In this section, “uniform resource locator” means a standardised naming convention for entries made in a public register.

Louise Haigh: These are further amendments tabled by my hon. Friend the Member for Cardiff West and me to make the codes of practice, on which officials have obviously worked so hard and which were developed in consultation with the Information Commissioner, legally binding. With your permission, Mr Stringer, I will come to specific issues about the data-sharing measures and fraud during debate on clause stand part.

I appreciate what the Minister said about sanctions being enforced on those authorities that do not have regard to the code of practice, but it says on the front page of the code:

“The contents of this Code are not legally binding”;

it merely

“recommends good practice to follow when exercising the powers set out in the Bill.”

That is not really a strong enough message to send to officials and all those involved in data-sharing arrangements. I would be interested to hear examples from the Minister of when it would be considered reasonable not to follow the code, as I assume that that is why he does not want to build it into primary legislation. I know that he will tell me that his real reason is that he wants to future-proof the codes. That is all well and good, but the Bill is already outdated. One witness wrote to us in evidence:

“Part 5 seems to imply an approach to ‘data sharing’ modelled on the era of filing cabinets and photocopiers when—quite literally—the only way to make data available to others was to send them a duplicate physical copy. Modern technology has already rendered the need for such literal ‘data sharing’ obsolete: data can now be used without copying it to others and without compromising security and privacy.”

Furthermore, data sharing is not defined, either legally or technically, in the Bill or in the codes of practice. Does data sharing mean data duplication—copying and distribution—or does it mean data access, or alternatives such as attribute exchange or claim confirmation? These are all quite different things, with their own very distinct risk profiles, and in the absence of any definition, the term “data sharing” is ambiguous at best and potentially damaging in terms of citizens’ trust, cyber-security and data protection. Let me give an example: there is a significant difference between, and different security risk associated with, distributing personal information to third parties, granting them controlled and audited one-time access for the purpose of a specific transaction, or simply confirming that a person is in debt or is or is not eligible for a particular benefit, without revealing any of their detailed personal data.

What is more, there is no reference in the clause to identity and how officials, citizens, or organisations, or even devices and sensors, will be able to prove who they are and their entitlement to access specific personal data. Without this, it is impossible to share data securely, since it will not be possible to know with whom data are being shared and whether they are an appropriate person or organisation to have access to those data. Security audits, of who has accessed which data, when and why, require a trusted identity framework to ensure that details of who has been granted access to data are

accurately recorded. Presumably, it will also be mandatory to implement good practice security measures, such as protecting monitoring, preventing in real time inappropriate attempts at data access, and flagging such attempts, to enable immediate mitigating action to be taken.

As I said on Tuesday, all these details are moot, as are the codes of practice and indeed the Information Commissioner Office’s excellent code of practice, if the existence and detail of data sharing is not known about to be challenged; hence the need for a register, as set out in new clause 35. That is why we have tabled our amendments and we would like the Minister to give serious consideration to the inclusion of these important principles and safeguards in the Bill. We are not talking about detailed regulations, we are certainly not talking about holding back technological advances, and we are not talking about the “dead hand of Whitehall”, as the Minister said on Tuesday. We are talking about vital principles that should be in primary legislation, alongside any new powers to share information. The most important of those principles is transparency, which is exactly what new clause 35 speaks to. It would require public authorities to enter in a public register all data disclosures across Government.

The Minister did not know the detail of the audits that are mentioned in the codes of practice. We really need more detail on those audits, as it may well satisfy us in our request for this register. Will all data-sharing agreements be kept in a single place in each Department, updated as data are shared and disclosed across Government, with Government agencies and with non-public sector organisations? Will these additional agencies keep similar audits and—crucially—will those audits be publicly available? Also, will the audits include the purpose of the disclosure, the specific data to be disclosed, how the data were transferred, how the data are stored and for how long, how the data are deleted at the end of that time frame, what data controllers and processors are involved in the sharing of that data, and any other restrictions on the use of further disclosure of that data?

If we have, in a single place, data-sharing amendments, as this amendment would establish, the public can see and trust how their data are being used and for what purpose. They can understand why they are getting a letter from Concentrix about Her Majesty’s Revenue and Customs, or why they have been targeted for a warm home scheme, and—crucially—they can correct or add to any information on themselves that is wrongly held.

Drew Hendry (Inverness, Nairn, Badenoch and Strathspey) (SNP): Does the hon. Lady agree that, if there is an opportunity to access a proactive notification service that indicates to the member of public that their data are being used and for what purpose, that should be included in any future consideration of this matter?

Louise Haigh: I completely agree, and I believe that the gov.uk Notify service would be an excellent means by which to go about that. I hope that the Minister will consider it.

Graham Jones: My hon. Friend is making a valid point, which I referenced in my point about getting on the bus and the destination. She is suggesting that individuals have rights to own their information; there

[Graham Jones]

is a register that they could accept. This is the journey that we have to make. It is about empowering the individual. My hon. Friend is making a powerful point. I am pleased that the Opposition are making this point, because it needs to be made. The future will be about individual ownership of information. I hope that my hon. Friend prosecutes the argument as well as she can.

Louise Haigh: The point is vital and it is the point that was made earlier in our proceedings. Unless we get this right at this stage, it will become a scandal that the Government will then have to deal with and it will hold back progress on sharing data, as we saw with the care.data scandal. We do not want to see the Government embroiled in another scandal like that and we hope that they heed our warnings in order to avoid one in the future.

The objective behind the register is that it could be considered an amnesty for all existing data-sharing projects, with the disclosure assisting understanding of the problem and improving public trust. Let us not kid ourselves that the Bill covers the only data sharing that happens across Government. In a recent interview with *Computer Weekly*, the new director of the Government Digital Service, Kevin Cunningham, said:

“The real work is going on in”

places such as “Leeds and Manchester”—I would disagree with him on that point for a start, because we are not fans of Leeds in Sheffield—

“as well as London. We need to be part of that. The example I use is where DWP now runs a whole set of disability benefits. It would be incredibly helpful if DWP had selected and consensual access to some of”—

those people’s—

“medical data. Right now, NHS Digital and DWP are having that conversation in Leeds and we’re not in the conversation. Why wouldn’t GDS be in a conversation like that? If we’re going to be, we’ve got to be in Leeds—we can’t do that from here.”

We know that that conversation is happening between the DWP and the NHS—despite assurances that sharing of health and social care information is not happening across Government—only because a random official mentioned it in a random interview, so I ask this question again: does the Minister have an audit of data-sharing agreements and arrangements across Government, or is it the case, as I fear it is, that not only do the public not know which data are shared across Government, for what purpose and how they are stored, but Ministers do not know either?

Calum Kerr (Berwickshire, Roxburgh and Selkirk) (SNP): The hon. Lady is making an excellent point. What this cuts back to is the underlying theme of transparency. Rather than the Government acting in a paternal way—“We’ll do what is best for the citizens”—they should be transparent and make it clear to citizens why and where data are being used.

Louise Haigh: That is exactly the kind of attitude that underpins these elements of the Bill: “Trust us. We’ll sort it out. Give us your data. No problem. We’re going to share them freely and fairly.” The Government may well do. The problem is that the public do not have that

trust in them. As I said on Tuesday, this is not a party political point. The previous Labour Government were not up to scratch in handling data either. This is not a party political attack at all. It is a genuine attempt to get these proposals in the best shape possible, to aid Government digitisation and deliver efficient public services.

Just as the Government give taxpayers a summary of how their tax money has been spent so they should give citizens information on how they have used data on them. If there is transparency through a register, there can be an informed conversation about whether a data disclosure will solve the problems that it claims to. There has been data sharing to prevent fraud for decades and a complete absence of audited and accurate results from that work. Arguing that current data sharing has not prevented fraud and so there should be more data sharing equates to doing the same thing over and again and expecting a different result.

The amendment is vital to restore and build on public trust in the Government handling of data. It is not in my nature to call on my constituents to trust this Government, but if they enacted the amendment, I absolutely would. I would be able to tell my constituents in good faith that they were right to trust their data to this or any future Government, because they and the data community could see exactly how and why their data were being used and exert some control over it. If the Government do not heed this lesson now, I am afraid that they will learn the hard way when things go the way of care.data or worse, as they inevitably will.

12.15 pm

Chris Skidmore: I thank the hon. Lady for her speech, and I appreciate the caution with which she approaches the subject. We have been determined that our definition of data sharing should be in the ICO’s code of practice, and we have adopted that definition in our own draft code. We will comply with ICO’s best practice, which of course means keeping careful records of all data-sharing agreements. We already keep registers of data sharing by Department, and they are FOI-able. We need to take public confidence with us. We will not allow data to be shared with a public authority that does not have appropriate systems in place.

To reassure those whom the hon. Lady seeks to assure that their data can be shared without any compromise to individual security, I will take a journey through the data sharing code of practice. When we come to establish some of the fraud elements, it will be an incremental process. Debt and fraud data-sharing pilots will be set up, and the UK Government are establishing a review group to oversee UK-wide and England-only data sharing under the fraud and debt powers. The review will be responsible for collating the evidence that will inform the Minister’s review of the operations powers as required under the Bill after three years. Devolved Administrations will establish their own Government structure for the oversight of data-sharing arrangements within their respective devolved territories.

Following that, a request to initiate a pilot under the debt and fraud powers must be sent to the appropriate review groups in the territory, accompanied by a business case. The business case must detail its operational period, the nature of the fraud and debt recovery being addressed,

the purpose of the data share and how its effectiveness will be measured. Absolutely rock-solid requirements need to be put in place. For instance, the public service delivery debt and fraud powers require a number of documents to be produced as part of the case for a pilot.

Those documents will be a business case for the data-sharing arrangement, which can be collated by all the organisations involved; data-sharing agreements; and a security plan. Furthermore, as part of any formal data-sharing agreements with public authorities that grant access to information, security plans should include storage arrangements to ensure that information is stored in a robust, proportionate and rigorously tested manner and assurances that only people who have a genuine business need—

Graham Jones: The Minister is making an argument to which I would extend my previous comments. He is arguing that there will be security because we will have a data repository—it will inevitably be a single data repository—with secure firewalls around it. However, the architectural principle for which he is arguing is that all data will be kept in one place. From a security perspective, that is the most dangerous way to store data. To return to why Estonia leads the world, there is a distribution—

The Chair: Order. That is an intervention. I am quite happy if the hon. Gentleman wants to catch my eye, but interventions should be short. I have been very lenient with that one.

Chris Skidmore: To return to the security angle, we must have assurances that only people with a genuine business need to see the personal information involved in a data-sharing arrangement will have access to it; confirmation of who will notify in the event of any security breach; and procedures in place to investigate the cause of any security breach. Paragraph 104 of the code suggests:

“You should ensure that data no longer required is destroyed promptly and rendered irrecoverable. The same will apply to data derived or produced from the original data, except where section 33 of the DPA applies (in relation to data processed for research purposes).”

At all times, we want to ensure that public confidence is taken forward with the pilots. They will be put in place only once all the boxes have been ticked. Paragraph 108 of the code states:

“You should make it easy for citizens to access data sharing arrangements and provide information so that the general public can understand what information is being shared and for what purposes. You should communicate key findings or the benefits to citizens derived from data sharing arrangements to the general public to support a better public dialogue on the use of public data.”

Security is not discretionary. Amendment 190 would not reinforce that requirement. It is not a question of compliance with systems in place. Instead, there must be adequate systems in place and Ministers must have regard to those systems to ensure they meet the essential security specifications that the Government demand.

Amendments 191 to 194 concern the codes of practice and present a similar discussion to the one we had about using “have regard to” or “compliance to”. The

powers cover a range of public authorities in devolved areas, and we want to ensure flexibility in how powers will be operated, so that we can learn from what works and adapt the code as necessary. If bodies fail to adhere to the code, the Minister will make regulations to remove their ability to share information under the power as set out in paragraph 11 of the code of practice.

As I mentioned, the requirement to have regard to the code of practice does not mean that officials have discretion to disregard the code at will. They will be expected to follow the code or they will lose their ability to share data. There could be exceptional reasons why it is reasonable to depart from the requirements of the code. To fix a rigid straitjacket creates a system of bureaucracy where officials must follow processes that run contrary to logic. This is standard drafting language adopted for the above reasons in the Immigration Act 2016, the Children and Families Act 2014 and the Protection of Freedoms Act 2012, to name a few recent pieces of legislation.

Louise Haigh: It is welcome to hear how detailed and extensive these audits will be. If they are subject to the Freedom of Information Act 2000, will the Minister consider proactively publishing them anyway, so that we can be assured that they are all kept in one place and that data sharing happens only in accordance with data-sharing arrangements that are in the public domain?

Chris Skidmore: When we set up new data-sharing arrangements, we must remember that the ICO and the devolved Administrations must be consulted and that the powers must go before Parliament again. We will have further scrutiny when considering the regulations under the affirmative procedure for secondary legislation.

Louise Haigh: Given that the arrangements have to go through all the obstacles that the Minister has just outlined, I do not understand why not then include them in a central register, so that they are all in one place. We could then be confident that not just those cases in the Bill but all data sharing across the Government is made public and people can have confidence in how and why their data are being used and shared.

Chris Skidmore: The hon. Lady refers to new clause 35, so I would now like to address that and take her points on board. This is about informing the public about what information is being shared by public authorities and for what reason.

The Bill’s provisions already include a number of commitments to transparency and proportionality, which I have already discussed in disclosing information by public authorities. There is a consistent requirement to uphold the Data Protection Act, including its privacy principles that govern the secure, fair and transparent processing of information.

We require the publishing of privacy impact assessments and privacy notices as set out in paragraph 82 of the code of practice. The research power requires the UK Statistics Authority, as the accrediting body, to maintain and publish a register of all persons and organisations it has accredited, and they can be removed under clause 61(5), which mandates that a withdrawal of accreditation will take place if there has been a failure to have regard to the code of practice.

[Chris Skidmore]

The requirements of the new clause would inevitably create a new set of administrative burdens, which in turn would carry significant cost implications. It is not clear how the uniform resource locator referred to would be agreed upon, or what assessment has been made of the administrative changes that may be required across the public sector. The requirement might have an unintended consequence. For example, it is possible that including information on the specific data to be disclosed would raise difficult questions about whether the public register would interfere with the duty of confidentiality or breach the provisions of the Data Protection Act. Some of the new powers—in particular, the research provisions—would involve the sharing of non-identifying information, so it is not clear how citizens would understand from a register which datasets contain information relating to them or any particular group of reasons.

The key purpose of the new powers is to simplify the legal landscape to enable public authorities to do their job more effectively and deliver better outcomes for the citizen. The new clause, however well intentioned—I respect the hon. Lady's point—risks working against that purpose and I therefore invite her to withdraw it.

Louise Haigh: The Opposition drafted the amendments and I accept that they may not be perfect, but the principle behind the idea of a data register is impossible to argue with. If the Minister claims that these audits will be done thoroughly and that they will be subject to the Freedom of Information Act anyway, I see no reason why they should not be proactively published, so that the public and Opposition Members can have full confidence that everything in the codes of practice, which are not statutory, is being properly adhered to.

Christian Matheson (City of Chester) (Lab): Does my hon. Friend concur that a proactive publication might be a lot more cost-effective than chasing after hundreds or, indeed, thousands of FOI requests?

Louise Haigh: Absolutely. This is where the Government often miss a trick: the interrelationship between FOI and open data could drive significant efficiencies across the Government and provide citizens and the data community with valuable data, including data that are valuable to the digital economy. I appreciate that our amendment might not be perfectly drafted, but I hope that the Minister will give serious consideration to the proactive publication of these audits and of all data-sharing arrangements across the Government.

Drew Hendry: There are existing mechanisms across Europe whereby information can be given to the public proactively. Does the hon. Lady agree that the public should not have to go through the process of making an FOI request—they should not have to go through all that hassle—to get the information that pertains to them and their lives?

Louise Haigh: Exactly. The data belong to them; that is exactly right. They should not have to jump over legalistic hurdles to find out how and why the Government are using data that should belong to them, and the Bill completely turns the view that they should not have to

do so on its head. I take the Minister's point about the amendment not being properly drafted. We will go away and redraft it and we will absolutely return to this issue on Report. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

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

Louise Haigh: As I have already set out, the Opposition broadly support the objectives outlined in the clause, but, as we have said on several occasions, those objectives must be set within strict safeguards to enable the better management of services.

Indeed, the open data policy process, which has been referenced several times, was a practical and commendable way in which to establish key principles for data to be handled, and to seek the views of industry experts. It is just a shame that it was completely ignored.

Polls show that the public consistently approve of the better use of data across Departments to help to improve customer service; nobody could really dispute that. However, our concerns are not related to the broader principle but to the practicality of these measures.

As we heard in the evidence we received, if these new powers are used appropriately in the management of debt, they could help put a stop to aggressive, uncoordinated approaches from Government agencies to debt. There is little doubt that debt collection for central Government Departments leaves a lot to be desired. Vulnerable citizens facing multiple hardships are being pursued in a way that is to the detriment of the overall policy of reducing debt.

Citizens Advice said in its evidence to the Committee that there has been a big growth in demand for help with debt, as policies such as the bedroom tax and complex tax credit arrangements are pushing people, through no fault of their own, into debt. The Government's haphazard approach often compounds matters and creates perverse outcomes, whereby thousands of individuals who are claiming exactly what they should be claiming are targeted in profiling exercises, which amount to nothing short of a mass Government-sponsored phishing exercise. Such an exercise has no place in necessary Government efforts to reduce error.

Shocking research by the charity StepChange has found that these aggressive debt collection methods have resulted in Government Departments having the dubious accolade of being second, behind bailiffs and ahead of mobile phone companies, in the list of those organisations that are considered most likely to treat debtors unfairly.

Again, there is little doubt that the Government's move to help Departments to better share necessary information on debt could help reduce the uncoordinated approach that currently harms debtors. However, there are two problems. First, as we have heard, the Government's debt collection process is flawed and suffers from a lack of trust; and, secondly, the clause will furnish the Government with an extension of their power in matching data, yet this year alone the Government have demonstrated an abysmal failure to match their powers to their responsibility to the users of their services. That leaves public trust hanging by a thread.

12.30 pm

The Minister mentioned Concentrix earlier—an outsourcer I am particularly obsessed with, and an example of how data matching can go wrong and how the safeguards surrounding the match can be completely ineffective. The Government used credit reference data and data from the electoral roll to target tax credit claimants for error and fraud. Individuals were accused of cohabiting, and their benefits were withdrawn as a result. One 19-year-old girl was accused of failing to declare that she had a 74-year-old partner, even though the man was dead. One of my constituents had her tax credits stopped while she was in a coma, and another young woman went without her benefits because Concentrix assumed that living in a Joseph Rowntree Housing Trust property meant she was shackled up with a 19th-century philanthropist.

I noticed earlier this week that HMRC is up for *Civil Service World's Analysis and Use of Evidence* award. If HMRC is the best the civil service currently has to offer in the use of data, we should be seriously concerned about giving it any more powers. As well as failing the hard-working vulnerable people HMRC is supposed to serve, that contract failed on an incredible scale. Concentrix breached its performance standards on more than 120 occasions in less than a year, 90% of mandatory reconsiderations were found to be successful, thousands of people had their tax credits arbitrarily withdrawn, causing severe financial hardship, and letters containing the details of individuals' claims and why they need to prove they are entitled to tax credits were addressed to the wrong people. Those breaches of data security demonstrate the high stakes involved for the Government with these data-sharing powers.

Although HMRC has done the right thing in announcing that it will not renew that contract, we need to investigate how that happened in the first place and ensure it never happens again. The Government cannot repeatedly get this wrong when chasing error and fraud in the tax credit system and the other areas that these clauses address. There is absolutely nothing to prevent them from employing another private sector contractor, tasking it with relentlessly chasing down cash and enabling it to match data from across central Government Departments with publicly available information and build a picture of individuals and who to target.

Subsection (3)(a) seems to allow for such profiling, which could have a range of unintended and severe consequences. It gives the authority the power to take action not only to collect debt but to identify it. That important distinction extends the power of the Crown. If hon. Members think that is a hypothetical concern, they should take a look at the contract between Concentrix and HMRC, which is not a unique contract in the public sector. Under the section entitled “data analytics and matching requirements”, it says,

“The authority requires that the contractor, as part of the error and fraud compliance service, provide and apply a data matching and analytics solution to enhance the Authority's own risk and profiling capability”.

The Minister said that the codes will be updated if the GDPR is followed in May 2018, but the Bill will be statutorily non-compliant with the GDPR, which explicitly bans the use of data for profiling.

The contract with Concentrix clearly failed, and the firm was not fit to conduct checks of that kind, but that raises chilling questions about the further extension of

data-sharing powers and what can be legally provided to private companies to pursue people legitimately claiming housing benefit, child tax credits or any other benefit. The codes of practice and the legislation are very clear that personal information should be used only for the purpose for which it was disclosed, but if that purpose is so broad a power, that gives no comfort to those of us who think that their sensitive data could be used to target them.

The draft regulations provide that the Home Office, the Lord Chancellor, the Justice Department and other Crown authorities can share information for the purpose of tackling error and fraud. It would help if the Government assured us that the data will be shared only when debt has already been identified to speed up the process. The Government should rule out the type of profiling conducted by Concentrix, which led to the targeting of individuals based on erroneous data. If the power is extended to give companies such as Concentrix access to data from not only HMRC but other Government Departments and local authorities, they could build up such a picture.

However, it is clearly not only private sector outsourcing that is of concern—the public sector has shown itself to have serious flaws in the management of personal information and in debt collection. In recent years, cuts to departmental budgets and staff numbers and increasing demands from citizens for online public services have changed the way Government collect, store and manage information. The many drivers for that change include successive IT and digital strategies since 2010. We need to ensure that the Government as a whole improve their data-sharing practices. That is why we will come back to our amendment, which would make reporting a data breach to the Information Commissioner mandatory if it has met a number of conditions. We simply cannot have personal data being breached and the Information Commissioner and the individual not being informed if it is serious.

We are broadly in favour of the power set out in the clause, but we have serious concerns about its use, even within the bounds of the purpose for which it is disclosed. We are concerned that the power will be used to identify debt, as the Bill clearly states, and we would be grateful for reassurance from the Minister.

Chris Skidmore: Good debt management is a key part of achieving the Government's fiscal policy objectives. Clause 40 provides a permissive power that will enable information to be shared for the purposes of identifying, collecting, or taking administrative or legal action as a result of debt owed to the Government. With more than £24 billion of debt owed to the Government, the problem is clearly significant.

Public authorities need to work together more intelligently to ensure that more efficient management of debt occurs. We believe that the new power will assist in achieving that. By enabling the efficient sharing of information to allow appropriate bodies to draw on a wider source of relevant data, informed decisions can be made about a customer's circumstances and their ability to pay. Sharing information across organisational boundaries will help the Government to understand the scale of the issues individuals are facing, and where vulnerable customers are identified, they can be given appropriate support and advice.

Citizens Advice stated:

[Chris Skidmore]

“This new power is an opportunity to advance the fairness and professionalisation agenda in government debt collection... Sharing data between debt collecting departments will create improved opportunities for better treatment of people in vulnerable situations, and must be matched with fairer and more effective dispute resolution processes.”

The Government agree with that and have worked with non-fee paying debt advice agencies to develop fairness principles to accompany the power, which are included in annex A of the code of practice.

It is important to dwell on the principles that organisations will adhere to, which state:

“Pilots operating under the new data sharing power should aim to use relevant data to help to differentiate between: A customer who cannot pay their debt because of vulnerability or hardship...; A customer who is in a position to pay their debts but who may need additional support; and A customer who has the means to pay their debt, but chooses not to pay - so public authorities, and private bodies acting on their behalf, can assess which interventions could best be used to recover the debt”, and that:

“Pilots must be conscious of the impact debt collection practices have on vulnerable customers and customers in hardship”.

The principles go on to cover:

“Using relevant sources of data and information to make informed decisions about a customer’s individual circumstances and their ability to pay.”

That process could include:

“An assessment of income versus expenditure to create a tailored and affordable repayment plan based on in work and out of work considerations, including the ability to take irregular income into account; and consideration of the need for breathing space to seek advice, or forbearance, in cases of vulnerability and hardship... Where a vulnerable customer is identified, they should be given appropriate support and advice, which may include signposting to non-fee paying debt advice agencies.”

Louise Haigh: I would be grateful if the Minister confirmed that those pilots and the powers enabled in the Bill will apply only to individuals already identified as being in debt, and that they will not seek to profile individuals who may or may not be in debt.

Chris Skidmore: Yes, I can confirm that. Moving forward, I reassure the Committee that we will continue to work closely with Citizens Advice and StepChange to look at fairness in Government debt management processes. Only HMRC and DWP have full reciprocal debt data-sharing gateways in place, under the Welfare Reform Act 2012. This power will help level the playing field for specified public authorities by providing a straightforward power to share data for clearly outlined purposes. Current data-sharing arrangements are time-consuming and complex to set up, and significantly limit the ability of public authorities to share debt data. This power will help facilitate better cross-Government collaboration that will help drive innovation to improve debt management. The clause will provide a clear power for specified public authorities to share data for those purposes, and will remove the existing complications and ambiguities over what can and cannot be shared and by whom.

Christian Matheson: The Minister may have just clarified the point I was seeking to tease out of him. The problems that my hon. Friend the Member for Sheffield, Heeley described show that, far from helping people

with debt, the agencies acting on behalf of the Government have created debt that did not exist previously by misusing Government data. The Minister may have just assured us that that will not be the case. If the Minister is really concerned about reducing Government debt, perhaps the Government should have not chopped in half the number of HMRC tax inspectors and instead gone after the people who owe the Government tax.

Question put and agreed to.

Clause 40 accordingly ordered to stand part of the Bill.

Clause 41

FURTHER PROVISIONS ABOUT POWER IN SECTION 40

Amendments made: 120, in clause 41, page 40, line 5, at end insert—

“(ba) for the prevention or detection of crime or the prevention of anti-social behaviour,”

This amendment and amendment 123 create a further exception to the bar on using information disclosed under Chapter 3 of Part 5 of the Bill for a purpose other than that for which it was disclosed. The amendments allow use for the prevention or detection of crime or the prevention of anti-social behaviour.

Amendment 121, in clause 41, page 40, line 6, leave out

“(whether or not in the United Kingdom)”.

This amendment removes the provision stating that a criminal investigation for the purposes of clause 41(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to a criminal investigation covers an investigation overseas in any event.

Amendment 122, in clause 41, page 40, line 8, leave out

“and whether or not in the United Kingdom”.

This amendment removes the provision stating that legal proceedings for the purposes of clause 41 may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to legal proceedings covers proceedings overseas in any event.

Amendment 123, in clause 41, page 40, line 11, at end insert—

“() In subsection (2)(ba) “anti-social behaviour” has the same meaning as in Part 1 of the Anti-social Behaviour, Crime and Policing Act 2014 (see section 2 of that Act).”—(*Chris Skidmore.*)

See the explanatory statement for amendment 120.

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

Clause 42

CONFIDENTIALITY OF PERSONAL INFORMATION

Amendments made: 124, in clause 42, page 41, line 4, at end insert—

“(da) for the prevention or detection of crime or the prevention of anti-social behaviour,”

This amendment and amendment 127 create a further exception to the bar on the further disclosure of information disclosed under Chapter 3 of Part 5 of the Bill, allowing disclosure for the prevention or detection of crime or the prevention of anti-social behaviour.

Amendment 125, in clause 42, page 41, line 5, leave out

“(whether or not in the United Kingdom)”.

This amendment removes the provision stating that a criminal investigation for the purposes of clause 42(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to a criminal investigation covers an investigation overseas in any event.

Amendment 126, in clause 42, page 41, line 8, leave out

“and whether or not in the United Kingdom”.

This amendment removes the provision stating that legal proceedings for the purposes of clause 42(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to legal proceedings covers proceedings overseas in any event.

Amendment 127, in clause 42, page 41, line 12, at end insert—

() In subsection (2)(da) “anti-social behaviour” has the same meaning as in Part 1 of the Anti-social Behaviour, Crime and Policing Act 2014 (see section 2 of that Act).”

See the explanatory statement for amendment 124.

Amendment 128, in clause 42, page 41, line 13, leave out subsections (3) and (4) insert—

() A person commits an offence if—

- (a) the person discloses personal information in contravention of subsection (1), and
- (b) at the time that the person makes the disclosure, the person knows that the disclosure contravenes that subsection or is reckless as to whether the disclosure does so.” —(*Chris Skidmore.*)

This amendment applies to the disclosure of personal information in contravention of subsection (1) of clause 42. It has the effect that it is an offence to do so only if the person knows that the disclosure contravenes that subsection or is reckless as to whether it does so.

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

Clause 43 ordered to stand part of the Bill.

Clause 44

CODE OF PRACTICE

Amendment made: 129, in clause 44, page 42, line 7, at end insert—

() The code of practice must be consistent with the code of practice issued under section 52B (data-sharing code) of the Data Protection Act 1998 (as altered or replaced from time to time).”—(*Chris Skidmore.*)

This amendment requires a code of practice issued under clause 44 by the relevant Minister and relating to the disclosure of information under clause 40 to be consistent with the data-sharing code of practice issued by the Information Commissioner under the Data Protection Act 1998.

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

Louise Haigh: In evidence, Citizens Advice told us that an estimated £1 in every £5 of debt in this country is debt to the Government. It found that its clients can suffer detriment when public bodies have overly aggressive, unco-ordinated and inconsistent approaches to debt collection. There is also fairly substantial evidence that central Government debt collection lags behind the high standards expected of other creditors, including water companies, council tax collection departments, banks and private debt collectors.

I ask the Minister to consider extending the common standard financial statement to set affordable payments, as the energy, water, banking and commercial debt collection sectors do. That is demonstrated by research from StepChange, which found that in terms of debt collection, those facing severe financial difficulty were likely to rate the DWP and local authorities only just behind bailiffs as those most likely to treat them unfairly.

12.45 pm

We know there has been a big growth in demand for help with debts from Government. Hard-pressed households feel public sector creditors are behaving worse than private companies and even payday lenders. That is a serious indictment of the lack of binding standards that apply to Government bodies chasing

outstanding debt. I am pleased to note that the chief executive of HMRC has just announced that it will not be outsourcing anything ever again in relation to tax credits, following the Concentrix debate. We very much welcome that.

I would be grateful if the Minister confirmed, when he has received advice from his colleagues, whether the Government will update the standards relating to public debt collection, so that they are in line with the private sector.

Chris Skidmore: The Government have started work to look into the common financial statement and standard financial statement alongside non-fee-paying debt advice agencies. That work is in its infancy, but the evidence will help us to decide whether the CFS/SFS could have benefits for Government. Until that work is completed, the Government cannot commit fully to adopt the CFS/SFS.

Louise Haigh: Will the Minister give a timeframe for when that work will be completed and when we will have a statement from the Government?

Chris Skidmore: It is not possible for me to give a timeframe in a Bill Committee discussing clause stand part. I suggest that I write to the hon. Lady, setting out those details in due course.

Government debt is clearly different from private sector debt. It is not contractual. The Government provide a wide range of services to citizens, such as the NHS and education system, and targeted support for those who meet the eligibility requirements to receive benefits. In return, citizens are required to pay taxes and repay any benefit in tax credit overpayments or fines that have been imposed for criminal activity. That revenue helps to fund vital services. The Government aim to ensure that customers are treated fairly. We encourage customers to engage early, so that they can agree on an affordable and sustainable repayment plan that takes individual circumstances into account. We understand that if poor debt collection practice occurs, that can cause distress.

The clause requires in particular that the code of practice must be issued by the Minister. It sets out more detail about how the power will operate and the disclosure and use of data. All specified public authorities and other bodies disclosing or using information under the power must have regard to the code of practice, which sets out in detail best practice of how the data-sharing power should be used. That includes what data should be shared, how data will be protected, issues around privacy and confidentiality and, significantly, the set of fairness principles that I talked about, which must be considered when exercising the power in clause 40. With that in mind, and the fact I have discussed extensively how the codes of practice will help protect the most vulnerable in society, I hope the clause will stand part of the Bill.

Louise Haigh: I am grateful to the Minister for the commitment to write to me. It would be welcome if he could write to all members of the Committee. That shows how committed he is to improving the detail of the clause.

Question put and agreed to.

Clause 44, as amended, accordingly ordered to stand part of the Bill.

Clause 45

DUTY TO REVIEW OPERATION OF CHAPTER

Chris Skidmore: I rise to speak to amendment 130, in clause 45, page 43, line 10, at end insert—

‘() The relevant Minister may only make regulations under subsection (5)—

- (a) in a case where the regulations include provision relating to Scotland, with the consent of the Scottish Ministers;
- (b) in a case where the regulations include provision relating to Wales, with the consent of the Welsh Ministers;
- (c) in a case where the regulations include provision relating to Northern Ireland, with the consent of the Department of Finance in Northern Ireland.”

This amendment requires the relevant Minister to obtain the consent of the Scottish Ministers, Welsh Ministers or Department of Finance before making regulations which, following a review under clause 45, amend or repeal Chapter 3 of Part 5 and make provision relating to Scotland, Wales or Northern Ireland respectively.

The Chair: With this it will be convenient to discuss Government amendment 141.

Chris Skidmore: It is envisaged that information-sharing powers will enable sharing arrangements to be set, but they may take place solely within a devolved territory or involving data relating to devolved matters. The amendments intend to require the consent of Scottish Ministers, Welsh Ministers and the Department of Finance in Northern Ireland before making any regulations to amend or repeal the provisions that relate to those territories. Regrettably, we have found technical flaws with the amendments, so we will reconsider this issue and return to it at a later stage.

Louise Haigh: I would be grateful if the Minister confirmed what technical issues there are with the amendments.

Chris Skidmore: There are a number of technical issues in these amendments, and we are determined to consult thoroughly with the devolved Administrations and the relevant offices. We will do so in due course. We will return to that later in the Bill.

Kevin Brennan (Cardiff West) (Lab): It is unusual for the Government to introduce amendments and then find technical problems with them. That is obviously what has happened and it is very unfortunate. Given that we were expecting to debate the amendments at this point, can the Minister give us an indication of when he will bring back non-defective amendments—or whether, indeed, he intends to bring any further amendments in this area?

Chris Skidmore: When it comes to the point of process that the hon. Gentleman mentions, we intend to return to this further into the Bill. The particular issue that arose with the amendments as currently drafted is that the need for consent needs to apply correctly only to devolved matters. We found that the amendments do not reflect that, which is why we wish to withdraw them today.

Kevin Brennan: It would be helpful if that were to happen during the Commons stage of the Bill, rather than in the Lords, so that this House has an opportunity, at least on Report, to consider this aspect.

Chris Skidmore: I note the hon. Gentleman’s concerns and will reflect on them. I cannot give any further information at this moment. We hope to ensure that the amendments, when later drafted, will reflect the Government’s desire to listen carefully to all devolved nations and ensure that this applies across the UK.

The Chair: The amendment is not moved.

Clause 45 ordered to stand part of the Bill.

Clauses 46 to 48 ordered to stand part of the Bill.

Clause 49

FURTHER PROVISIONS ABOUT POWER IN SECTION 48

Amendments made: 131, in clause 49, page 46, line 43, at end insert—

“(ba) for the prevention or detection of crime or the prevention of anti-social behaviour,”

This amendment and amendment 134 create a further exception to the bar on using information disclosed under Chapter 4 of Part 5 of the Bill for a purpose other than that for which it was disclosed. The amendments allows use for the prevention or detection of crime or the prevention of anti-social behaviour.

Amendment 132, in clause 49, page 46, line 44, leave out “(whether or not in the United Kingdom)”

This amendment removes the provision stating that a criminal investigation for the purposes of clause 49(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to a criminal investigation covers an investigation overseas in any event.

Amendment 133, in clause 49, page 46, line 46, leave out “and whether or not in the United Kingdom”

This amendment removes the provision stating that legal proceedings for the purposes of clause 49(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to legal proceedings covers proceedings overseas in any event.

Amendment 134, in clause 49, page 47, line 6, at end insert—

‘() In subsection (2)(ba) “anti-social behaviour” has the same meaning as in Part 1 of the Anti-social Behaviour, Crime and Policing Act 2014 (see section 2 of that Act).”—(*Chris Skidmore.*)

See the explanatory statement for amendment 131.

Clause 49, as amended, ordered to stand part of the Bill.

Clause 50

CONFIDENTIALITY OF PERSONAL INFORMATION

Amendments made: 135, in clause 50, page 47, line 44, at end insert—

“(da) for the prevention or detection of crime or the prevention of anti-social behaviour,”

This amendment and amendment 138 create a further exception to the bar on the further disclosure of information disclosed under Chapter 4 of Part 5 of the Bill, allowing disclosure for the prevention or detection of crime or the prevention of anti-social behaviour.

Amendment 136, in clause 50, page 48, line 1, leave out “(whether or not in the United Kingdom)”

This amendment removes the provision stating that a criminal investigation for the purposes of clause 50(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to a criminal investigation covers an investigation overseas in any event.

Amendment 137, in clause 50, page 48, line 4, leave out “and whether or not in the United Kingdom”

This amendment removes the provision stating that legal proceedings for the purposes of clause 50(2) may be within or outside the United Kingdom. This is for consistency and on the basis that a reference to legal proceedings covers proceedings overseas in any event.

Amendment 138, in clause 50, page 48, line 11, at end insert—

“() In subsection (2)(da) “anti-social behaviour” has the same meaning as in Part 1 of the Anti-social Behaviour, Crime and Policing Act 2014 (see section 2 of that Act).”

See the explanatory statement for amendment 135.

Amendment 139, in clause 50, page 48, line 12, leave out subsections (3) and (4) insert—

“() A person commits an offence if—

- (a) the person discloses personal information in contravention of subsection (1), and
- (b) at the time that the person makes the disclosure, the person knows that the disclosure contravenes that subsection or is reckless as to whether the disclosure does so.”—(*Chris Skidmore.*)

This amendment applies to the disclosure of personal information in contravention of subsection (1) of clause 50. It has the effect that it is an offence to do so only if the person knows that the disclosure contravenes that subsection or is reckless as to whether it does so.—

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

Clause 51 ordered to stand part of the Bill.

Clause 52

INFORMATION DISCLOSED BY THE REVENUE AND CUSTOMS

Amendment made: 140, in clause 52, page 49, line 7, at end insert—

“() The code of practice must be consistent with the code of practice issued under section 52B (data-sharing code) of the Data Protection Act 1998 (as altered or replaced from time to time).”—(*Chris Skidmore.*)

This amendment requires a code of practice issued under clause 52 by the relevant Minister and relating to the disclosure of information under clause 48 to be consistent with the data-sharing code of practice issued by the Information Commissioner under the Data Protection Act 1998.

Clause 52, as amended, ordered to stand part of the Bill.

Clauses 53 to 55 ordered to stand part of the Bill.

Clause 56

DISCLOSURE OF INFORMATION FOR RESEARCH PURPOSES

Chris Skidmore: I beg to move amendment 142, in clause 56, page 52, line 23, at end insert—

“(3A) For the purposes of the first condition the information may be processed by—

- (a) the public authority,
- (b) a person other than the public authority, or
- (c) both the public authority and a person other than the public authority,

(subject to the following provisions of this Part).

(3B) Personal information may be disclosed for the purpose of processing it for disclosure under subsection (1)—

- (a) by a public authority to a person involved in processing the information for that purpose;
- (b) by one such person to another such person.”

This amendment and amendments 143, 144, 146 to 149, 151 to 153, 159, 160 and 162 to 166 relate to the processing of information for disclosure under clause 56 so as to remove identifying features. They make it clear that a person other than the public authority which is the source of the information may be involved in processing that information.

The Chair: With this it will be convenient to discuss Government amendments 143 to 153, 159, 160 and 162 to 170.

Chris Skidmore: The amendments apply to the research power. Together they provide clarity on the conditions that must be met when information provided by public authorities for research purposes is processed, as set out in clause 56. They also require public authorities to obtain accreditation to process personal information with that power, and they provide further clarity on the exclusion of health and adult social care information in clauses 56 and 63.

Personal information must not be disclosed to researchers under the power unless it is first processed in a way that protects the privacy of all data subjects. Those involved in the processing of information must be accredited as part of the conditions under this power. Processing may be carried out by the public authority that holds the data concerned, a different public authority, or specialist persons or organisations outside the public sector, including those providing secure access facilities and other functions, those commonly referred to as trusted third parties, or a combination of the two.

These amendments have been tabled to ensure that the position is reflected accurately in clause 56 and to ensure that it is clear that each accredited processor can disclose information to other accredited processors as required. In addition, they clarify that a person involved in the processing of information other than the public authority holding the information can disclose the de-identified information to researchers.

As drafted, the Bill does not require public authorities to be accredited or to process data for disclosure to researchers. On reflection, the Government recognise the importance of ensuring that all bodies involved in processing information are subject to the same level of accountability and scrutiny. The amendments will enable the UK Statistics Authority, as the accrediting body, to enforce a consistent approach to best practice for handling information.

Finally, it is important that the exclusion of health and adult social care data is defined in a way that is accurate and transparent. As drafted, the research clauses could be interpreted as excluding from the power public authorities that are primarily health and adult social care providers, but which provide some health-related services. That could mean that, contrary to the intention of the Bill, public authorities, including local authorities that provide a range of services, are at risk of being barred from sharing data relating to their functions because they provide some health and social care-related services.

The amendments will clarify that public authorities whose sole function is to provide health and/or adult social care services will be excluded from the power. They also clarify that public authorities that provide

[Chris Skidmore]

health and/or adult social care services as part of a range of services can share information, including health and adult social care data.

Louise Haigh: I very much welcome the amendments. Has the Minister considered the Information Commissioner's recommendation to have an additional offence for re-identifying anonymised personal information, as in the Australian model? I otherwise support the amendments.

Chris Skidmore: We are obviously working closely with the Information Commissioner. We will consider all her recommendations in due course, but I cannot comment on that at this moment in time.

Amendment 142 agreed to.

1.1 pm

Ordered, That further consideration be now adjourned.
—(Graham Stuart.)

Adjourned till this day at Two o'clock.