PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

Eighth Sitting

Tuesday 23 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

Saturday 27 May 2023

The Committee consisted of the following Members:

Chairs: † Mr Philip Hollobone, Ian Paisley

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

Huw Yardley, Bradley Albrow, *Committee Clerks*

† attended the Committee

Public Bill Committee

Tuesday 23 May 2023

(Afternoon)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

Clause 100

The Information Commission

2 pm

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

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

Government amendments 44 and 45.

That schedule 13 be the Thirteenth schedule to the Bill.

Clauses 101 to 103 stand part.

The Minister for Data and Digital Infrastructure (Sir John Whittingdale): We now turn to part 5 of the Bill. Clauses 100 to 103 and schedule 13 will establish a body corporate, the Information Commission, to replace the existing regulator, the Information Commissioner, which is currently structured as a corporation sole. I should make it clear that the clauses will make no changes to the regulator's role and responsibilities; all the functions that rest with the Information Commissioner will continue to sit with the new Information Commission.

Clause 100 will establish a body corporate, the Information Commission, to replace the existing regulator, the Information Commissioner. The commission will be governed by an independent board, with chair and chief executive roles, thereby spreading the responsibilities of the Information Commissioner across a larger number of people.

Clause 101 will abolish the office of the Information Commissioner and amend the Data Protection Act 2018 accordingly. To ensure an orderly transfer of functions, the Information Commissioner's Office will not be abolished until the new body corporate, the Information Commission, is established.

Clause 102 provides for all regulatory and other functions of the Information Commissioner to be transferred to the new body corporate, the Information Commission, once it is established. The clause also provides for references to the Information Commissioner in enactments or other documents to be treated as references to the Information Commission, where appropriate, as a result of the transfer of functions to the new Information Commission.

Clause 103 will allow the Secretary of State to make a scheme for the transfer of property, rights and liabilities, including rights and liabilities relating to employment contracts, from the commissioner to the new commission. The scheme may transfer property such as IT equipment or office furniture, or transfer staff currently employed by the commissioner to the commission. The transfer scheme will be designed to ensure continuity and facilitate a seamless transition to the new Information Commission.

Schedule 13 will insert a new schedule 12A to the Data Protection Act 2018, which describes the nature, form and governance structure of the new body corporate, the Information Commission. The commission will be governed by an independent statutory board, which will consist of a chair and other non-executive members, as well as executive members including a chief executive. The new structure formalises aspects of the existing governance arrangements of the Information Commissioner's Office and brings the ICO in line with how other UK regulators, such as Ofcom and the Financial Conduct Authority, are governed. The chair of the new commission will be appointed by His Majesty by letters patent on the recommendation of the Secretary of State, as is currently the case for the commissioner.

Schedule 13 also provides for the current Information Commissioner to transfer to the role of chair of the Information Commission for the remainder of their term. I put on record the Government's intention to preserve the title of Information Commissioner in respect of the chair, in acknowledgment of the fact that the commissioner's brand is recognised and valued both domestically and internationally. Other non-executive members will be appointed by the Secretary of State, and the chief executive will be appointed by the non-executive members in consultation with the Secretary of State.

Government amendment 45 will allow the chair to appoint the first chief executive on an interim basis and for a term of up to a maximum of 24 months, which will minimise any delay in the transition from the commissioner to the new commission. As drafted, the Bill provides that the chief executive of the commission will be appointed by the non-executive members once they are in place, in consultation with the Secretary of State. The transition from the commissioner to the new Information Commission cannot take place until the board is properly constituted, with, as a minimum, a chair, another non-executive member and a chief executive in place. That requirement would be likely to cause delay to the transition, as the appointment of the non-executive members by the Secretary of State and the chief executive would need to take place consecutively.

Amendment 44 is a minor consequential amendment to paragraph 3(3)(a) of proposed new schedule 12A, making it clear that the interim chief executive is appointed as an executive member.

The amendments seek to minimise any delay in the transfer of functions to the new commission by enabling the appointment of the chief executive to take place in parallel with the appointments process for non-executive members. The appointment of the interim chief executive will be made on the basis of fair and open competition and in consultation with the Secretary of State. I commend clauses 100 to 103, schedule 13 and Government amendments 44 and 45 to the Committee.

Stephanie Peacock (Barnsley East) (Lab): It is a pleasure to serve under your chairship once again, Mr Hollobone. The clauses that restructure the Information Commissioner's Office are among those that the Opposition are pleased to welcome in the Bill.

The Information Commissioner is the UK's independent regulator for data protection and freedom of information under the Data Protection Act 2018 and the Freedom

of Information Act 2000. Under the current system, as the Minister outlined, the Information Commissioner's Office is a corporation sole, meaning that one person has overall responsibility for data protection and freedom of information, with a group of staff supporting them. However, as the use of data in our society has grown, so too has the ICO, from a team of 10 in 1984 to an organisation with more than 500 staff.

In that context, the corporation sole model is obviously not fit for purpose. Clauses 100 to 103 recognise that: they propose changes that will modernise the Information Commissioner's Office, turning it into the Information Commission by abolishing the corporation sole and replacing it with a body corporate. It is absolutely right that those changes be made, transforming the regulator into a commission with a broader set-up structure and a board of executives, among other key changes. That will bring the ICO in line with other established UK regulators such as Ofcom and the Financial Conduct Authority, reflect the fact that the ICO is not just a small commissioner's office, and ensure that it is equipped to deal with the volume of work for which it has responsibility.

It is essential that the ICO remains independent and fair. We agree that moving from an individual to a body will ensure greater integrity, although the concerns that I have raised about the impact of earlier clauses on the ICO's independence certainly remain. Overall, however, we are pleased that the Government recognise that the ICO must be brought in line with other established regulators and are making much-needed changes, which we support.

Question put and agreed to.

Clause 100 accordingly ordered to stand part of the Bill.

Schedule 13

THE INFORMATION COMMISSION

Amendments made: 44, in schedule 13, page 195, line 21, after "members" insert

"or in accordance with paragraph 23A".

This amendment is consequential on Amendment 45.

Amendment 45, in schedule 13, page 204, line 6, at end insert—

"*Transitional provision: interim chief executive*

23A (1) The first chief executive of the Commission is to be appointed by the chair of the Commission.

(2) Before making the appointment the chair must consult the Secretary of State.

(3) The appointment must be for a term of not more than 2 years.

(4) The chair may extend the term of the appointment but not so the term as extended is more than 2 years.

(5) For the term of appointment, the person appointed under sub-paragraph (1) is "the interim chief executive".

(6) Until the expiry of the term of appointment, the powers conferred on the non-executive members by paragraph 11(2) and (3) are exercisable in respect of the interim chief executive by the chair (instead of by the non-executive members).

(7) In sub-paragraphs (5) and (6), the references to the term of appointment are to the term of appointment described in sub-paragraph (3), including any extension of the term under sub-paragraph (4)."—*(Sir John Whittingdale.)*

The Bill establishes the Information Commission. This new paragraph enables the chair of the new body, in consultation with the Secretary of State, to appoint the first chief executive (as opposed to the appointment being made by non-executive members). It also enables the chair to determine the terms and conditions, pay, pensions etc relating to the appointment.

Schedule 13, as amended, agreed to.

Clauses 101 to 103 ordered to stand part of the Bill.

Clause 104

OVERSIGHT OF RETENTION AND USE OF BIOMETRIC MATERIAL

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

Sir John Whittingdale: Clause 104 will repeal the role of the Biometrics Commissioner and transfer the casework functions to the Investigatory Powers Commissioner. There is an extensive legal framework to ensure that the police can make effective use of biometrics, for example as part of an investigation to quickly and reliably identify suspects, while maintaining public trust. That includes the Police and Criminal Evidence Act 1984, which sets out detailed rules on DNA and fingerprints, and the Data Protection Act 2018, which provides an overarching framework for the processing of all personal data.

The oversight framework is complicated, however, and there are overlapping responsibilities. The Bio -metrics Commissioner currently has specific oversight responsibilities just for police use of DNA and fingerprints, while the Information Commissioner's Office regulates the use of all personal data, including biometrics, by any organisation, including the police. Clause 104 will simplify the framework by removing the overlap, leaving the ICO to provide independent oversight and transferring the casework functions to another existing body.

The casework involves extending retention periods in certain circumstances, particularly on national security grounds, and is quasi-judicial in nature. That is why clause 104 transfers those functions to the independent Investigatory Powers Commissioner, which has the necessary expertise, and avoids the conflict of interest that could occur if the functions were transferred to the ICO as regulator. Transparency in police use of biometrics is essential to retaining public trust and will continue through the annual reports of the Forensic Information Databases Service strategy board, the Investigatory Powers Commissioner and the ICO. I commend clause 104 to the Committee.

Stephanie Peacock: I will speak in more detail about my more general views on the oversight of biometrics, particularly their private use, when we come to new clauses 13, 14 and 15. However, as I look specifically at clauses 104 and 105, which seek to abolish the currently combined offices of Biometrics Commissioner and Surveillance Camera Commissioner, I would like to draw on the direct views of the Information Commissioner. In his initial response to "Data: a new direction", which proposed absorbing the functions of the Biometrics Commissioner and Surveillance Camera Commissioner into the ICO, the commissioner said that there were some functions that,

"if absorbed by the ICO, would almost certainly result in their receiving less attention".

Other functions, he said,

"simply do not fit with even a reformed data protection authority"

[Stephanie Peacock]

with there being

"far more intuitive places for them to go."

That was particularly so, he said, with biometric casework.

It is therefore pleasing that as a result of the consultation responses the Government have chosen to transfer the commissioner's biometric functions not to the ICO but to the Investigatory Powers Commissioner, acknowledging the relevant national security expertise that it can provide. However, in written evidence to this Committee, the commissioner reiterated his concern about the absorption of his office's functions, saying that work is currently being undertaken within its remit that, under the Bill's provisions, would be unaccounted for.

Given that the commissioner's concerns clearly remain, I would be pleased if the Minister provided in due course a written response to that evidence and those concerns. If not, the Government should at the very least undertake their own gap analysis to identify areas that will not be absorbed under the current provisions. It is important that this Committee and the office of the Biometrics and Surveillance Camera Commissioner can be satisfied that all the functions will be properly delegated and given the same degree of attention wherever they are carried out. Equally, it is important that those who will be expected to take on these new responsibilities are appropriately prepared to do so.

Sir John Whittingdale: I am happy to provide the further detail that the hon. Lady has requested.

Question put and agreed to.

Clause 104 accordingly ordered to stand part of the Bill.

Clause 105

OVERSIGHT OF BIOMETRICS DATABASES

Carol Monaghan (Glasgow North West) (SNP): I beg to move amendment 123, in clause 105, page 128, line 22, leave out subsections (2) and (3).

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

Clause stand part.

New clause 17—*Transfer of functions to the Investigatory Powers Commissioner's Office*—

"The functions of the Surveillance Camera Commissioner are transferred to the Investigatory Powers Commissioner."

Carol Monaghan: Society is witnessing an unprecedented acceleration in the capability and reach of surveillance technologies. Such an acceleration calls for protections and safeguards. Clause 105, however, does the opposite and seeks to abolish both the office of the Surveillance Camera Commissioner and its functions. The explanatory notes to the Bill state that the functions of the office of the Surveillance Camera Commissioner are duplicated and covered by the Information Commissioner's Office and its CCTV code of practice. That is not the case: the code is advisory only and is primarily concerned with data processes, not with actual surveillance.

Amendment 123 and new clause 17 would retain the functions of the Surveillance Camera Commissioner but transfer them to the Investigatory Powers Commissioner's Office, thus preserving those necessary safeguards. The IPCO already scrutinises Government activity and deals with the covert use of surveillance cameras, so dealing with overt cameras as well would be a natural extension of its function.

2.15 pm

Professor Pete Fussey of the University of Essex and Professor William Webster of the University of Stirling, who are directors of the Centre for Research into Information, Surveillance and Privacy, are considered the UK's leading experts on surveillance. They have conducted an independent review of the Bill as it relates to the functions of the Office of the Biometrics and Surveillance Camera Commissioner. Their view is that the Bill does not currently provide adequate mechanisms for the governance and oversight of surveillance cameras, including automatic number plate recognition, body-worn video, drones, facial recognition and so on, in comparison with the existing legislative arrangements under the Protection of Freedoms Act 2012.

It is important that any changes to current legislation preserve existing oversight and citizen safeguards, which are key to considering such intrusive types of technology. The Protection of Freedoms Act details provisions for the code of practice for surveillance camera systems and outlines the important functions for which the Surveillance Camera Commissioner is responsible:

"encouraging compliance with the surveillance camera code… reviewing the operation of the code, and…providing advice about the code (including changes to it or breaches of it)."

In addition to those statutory functions, Professor Fussey and Professor Webster highlight the importance of the Surveillance Camera Commissioner in relation to

"raising standards for surveillance camera developers, suppliers and users…and building legitimacy and consent for surveillance practices".

Furthermore, the commissioner reports annually to Parliament via the Home Secretary, which is an important mechanism for public trust in, and for the legitimacy of, the appropriate use of surveillance.

In his submission to the Committee, Professor Fraser Sampson, the Biometrics and Surveillance Camera Commissioner, highlights one particularly pressing role of his office at present, which relates to the procurement and use of Chinese surveillance technology. Although that role pertains to a significant national security priority, it is falling through the gaps of the Bill and has not been assigned to another office.

Clause 105 seeks to abolish the office of the Surveillance Camera Commissioner, while erasing its important functions. Considering the rapid advancement in surveillance technologies, including the concerning development and deployment of facial recognition technologies, it is more important than ever that we protect safeguards and build on them. My new clause 17 would preserve the important functions that I have outlined. The experts interviewed for Professor Fussey and Professor Webster's report supported such a change, highlighting how most of the gaps left in the Bill could be addressed if responsibility for the surveillance camera code were also moved under the IPCO.

Stephanie Peacock: Having outlined my broad concerns about clause 105 when I spoke to clause 104, I will focus briefly on the specific concern raised by the hon. Member

for Glasgow North West, which is that the Surveillance Camera Commissioner's functions will not be properly absorbed.

In evidence to the Committee, the commissioner outlined a number of non-data protection functions in relation to public space surveillance that their office currently carries out, but that, they believe, the Bill does not make provision to transfer. They cite the significant work that their office has undertaken to ensure that Government Departments are able

"to cease deploying visual surveillance systems onto sensitive sites where they are produced by companies subject to the National Intelligence Law of the People's Republic of China",

following a November 2022 instruction from the Chancellor of the Duchy of Lancaster. The commissioner says that such non-data protection work, which has received international acclaim, is not addressed in the Bill.

I am therefore hopeful that the explicit mention in amendment 123 that that the functions of the Surveillance Camera Commissioner will be transferred provides a backstop to ensure that all the commissioner's duties, including the non-data protection work, are accounted for. If the amendment is not accepted, a full-depth analysis should be conducted, as argued previously, with a full response issued to the commissioner's evidence to ensure that every one of the functions is properly and appropriately absorbed.

I understand the argument that the Surveillance Camera Commissioner's powers would be better placed with the Investigatory Powers Commissioner, rather than the ICO. Indeed, the commissioner's evidence to the Committee referenced the interim findings of an independent report it had commissioned, as the hon. Member for Glasgow North West just mentioned. The report found that most of the gaps left by the Bill could be addressed if responsibility for the surveillance camera code moved under the IPCO, harmonising the oversight of traditional and remote biometrics.

I end by pointing to a recent example that shows the value of proper oversight of the use of surveillance. Earlier this year, following a referral from my hon. Friend the Member for Bristol North West (Darren Jones), the ICO found a school in Bristol guilty of unlawfully installing covert CCTV cameras at the edge of their playing fields. Since then, the Surveillance Camera Commissioner has been responding to freedom of information requests on the matter, with more information about the incident thereby emerging as recently as yesterday. It is absolutely unacceptable that a school should be filming people without their knowledge. The Surveillance Camera Commissioner is a vital cog in the machinery of ensuring that incidents are dealt with appropriately. For such reasons, we must preserve its functions.

In short, I am in no way opposed to the simplification of oversight in surveillance or biometrics, but I hope to see it done in an entirely thorough way, so that none of the current commissioner's duties get left behind or go unseen.

Sir John Whittingdale: I am grateful to the hon. Members for Glasgow North West and for Barnsley East for the points they have made. The hon. Member for Glasgow North West, in moving the amendment, was right to say that the clause as drafted abolishes the role of the Surveillance Camera Commissioner and the surveillance camera code that the commissioner promotes compliance with. The commissioner and the code, however, are concerned only with police and local authority use in England and Wales. Effective, independent oversight of the use of surveillance camera systems is critical to public trust. There is a comprehensive legal framework for the use of such systems, but the oversight framework is complex and confusing.

The ICO regulates the processing of all personal data by all UK organisations under the Data Protection Act; that includes surveillance camera systems operated by the police and local authorities, and the ICO has issued its own video surveillance guidance. That duplication is confusing for both the operators and the public and it has resulted in multiple and sometimes inconsistent guidance documents covering similar areas. The growing reliance on surveillance from different sectors in criminal investigations, such as footage from Ring doorbells, means that it is increasingly important for all users of surveillance systems to have clear and consistent guidance. Consolidating guidance and oversight will make it easier for the police, local authorities and the public to understand. The ICO will continue to provide independent regulation of the use of surveillance camera systems by all organisations. Indeed, the chair of the National Police Data Board, who gave evidence to the Committee, said that that will significantly simplify matters and will not reduce the level of oversight and scrutiny placed upon the police.

Amendment 123, proposed by the hon. Member for Glasgow North West, would retain the role of the Surveillance Camera Commissioner and the surveillance camera code. In our view, that would simply continue the complexity and duplication with the ICO's responsibilities. Feedback that we received from our consultation showed broad support for simplifying the oversight framework, with consultees agreeing that the roles and responsibilities, in particular in relation to new technologies, were unclear.

The hon. Lady went on to talk about the oversight going beyond that of the Information Commissioner, but I point out that there is a comprehensive legal framework outside the surveillance camera code. That includes not only data protection, but equality and human rights law, to which the code cross-refers. The ICO and the Equality and Human Rights Commission will continue to regulate such activities. There are other oversight bodies for policing, including the Independent Office for Police Conduct and His Majesty's inspectorate of constabulary, as well as the College of Policing, which provide national guidance and training.

The hon. Lady also specifically mentioned the remarks of the Surveillance Camera Commissioner about Chinese surveillance cameras. I will simply point out that the responsibility for oversight, which the ICO will continue to have, is not changed in any way by the Bill. The Information Commissioner's Office continues to regulate all organisations' use of surveillance cameras, and it has issued its own video surveillance guidance.

New clause 17 would transfer the functions of the commissioner to the Investigatory Powers Commissioner. As I have already said, we believe that that would simply continue to result in oversight resting in two different places, and that is an unnecessary duplication. The Investigatory Powers Commissioner's Office oversees activities that are substantially more intrusive than those relating to overt surveillance cameras. IPCO's existing work requires it to oversee over 600 public authorities,

[Sir John Whittingdale]

as well as several powers from different pieces of legislation. That requires a high level of expertise and specialisation to ensure effective oversight.

For those reasons, we believe that the proposals in the clause to bring the oversight functions under the responsibility of the Information Commissioner's Office will not result in any reduction in oversight, but will result in the removal of duplication and greater clarity. On that basis, I am afraid that I am unable to accept the amendment, and I hope that the hon. Lady will consider withdrawing it.

Carol Monaghan: I thank the Minister for responding to my amendments. However, we have a situation where we are going from having a specialist oversight to a somewhat more generalist oversight. That cannot be good when we are talking about this fast-moving technology. I will withdraw my amendment for the moment, but I reserve the right to bring it back at a later stage. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Clause 105 ordered to stand part of the Bill.

Clause 106

OVERSIGHT OF BIOMETRICS DATABASES

Stephanie Peacock: I beg to move amendment 119, in clause 106, page 130, line 7, leave out

"which allows or confirms the unique identification of that individual".

This amendment is intended to ensure that the definition of biometric data in the Bill includes cases where that data is used for the purposes of classification (and not just unique identification).

The Chair: With this it will be convenient to discuss new clause 8—*Processing of special categories of personal data: biometric data—*

"(1) Article 9 of UK GDPR is amended as follows.

(2) In paragraph (1), after "biometric data", omit "for the purpose of uniquely identifying a natural person."

This new clause would extend the same protections that are currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including if the processing is for the purpose of classification (i.e. identification as part of a group, rather than identification as an individual).

Stephanie Peacock: Biometric data is uniquely personal. It captures our faces, fingerprints, walking style, tone of voice, expressions and all other data derived from measures of the human body. Under current UK law, biometric data is defined as

"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person".

Furthermore, biometric data counts as special category personal data only when it is used or collected for

"the purpose of uniquely identifying a natural person".

However, as the use of biometrics grows, they are not only used for identification; indeed, there is a growing set of biometric technologies used to categorise or classify people on the basis of traits thought to be statistically related or correlated, however tenuously, with particular characteristics. For instance, biometric systems have been developed that attempt to infer people's sexuality from their facial geometry, or judge criminality from pictures of people's faces. Other biometric classification systems attempt to judge people's internal emotional state or intentions from their biometrics, such as tone, voice, gait or facial expressions, known as emotion recognition. For example, employers have used facial expression and tone analysis to decide who should be selected for a job, using biometric technologies to score candidates on characteristics such as enthusiasm, willingness to learn, conscientiousness and responsibility, and personal stability.

Members of the Citizens' Biometrics Council convened by the Ada Lovelace Institute in 2020 to build a deeper understanding of the British public's views on biometric technologies have expressed concerns about these use cases. Members suggest that these technologies classify people according to reductive, ableist and stereotypical characteristics, harming people's wellbeing and risking characterisation in a database or data-driven systems. Further, these cases often use pseudoscientific assumptions to draw links between external features and other traits, meaning that the underlying bases of these technologies are often not valid, reliable or accurate. For example, significant evidence suggests that it is not possible accurately to infer emotion from facial expressions. Despite that, existing data protection law would not consider biometric data collected for those purposes to be special category data, and would therefore not give data subjects the highest levels of safeguards in these contexts.

2.30 pm

The Ryder review, an independent legal review commissioned by the Ada Lovelace Institute and led by Matthew Ryder KC, identified that as a potential weakness in the existing regulatory regime. Ryder argued that the use of biometrics for classification or categorisation has the potential to be just as rights-intrusive as their use for unique identification, and that similarly high safeguards should therefore apply.

The Bill is an opportunity to remedy that oversight in existing data protection legislation. The amendment and new clause would ensure that it achieves that. It would extend the same protections currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including processing for the purpose of classification.

Sir John Whittingdale: Clause 106 makes changes to the national DNA database strategy board, which provides oversight of the operation of the national DNA database, including setting policies for access and use by the police. Amendment 119 would seem to extend the power to widen the board's potential scope beyond biometrics databases for the purpose of identification, to include the purpose of classification.

The police can process data only for policing purposes. It is not clear what policing purpose there would be in being able to classify, for example, emotions or gender, even assuming it was proven to be scientifically robust, or what sort of data would be on such a database. Even if one were developed in the future, it is likely to need knowledge, skills and resources very different from what is needed to oversee a database that identifies and eliminates suspects based on biometric identification, so it would probably make sense for a different body to carry out any oversight.

New clause 8 aims to make changes in a similar way to amendment 119 in relation to the definition of biometric data for the purposes of article 9 of the GDPR. As the GDPR is not concerned with the police's use of biometric data for law enforcement purposes, the new clause would apply to organisations that are processing biometric data for general purposes. The aim seems to be to ensure that enhanced protections afforded by GDPR to biometric data used for unique identification purposes also apply to biometric data that is used for classification or categorisation purposes.

The hon. Lady referred to the Ada Lovelace Institute's comments on these provisions, and its 2022 "Countermeasures" report issued on biometric technologies, but we are not convinced that such a change is necessary. One example in the report was using algorithms to make judgments that prospective employees are bored or not paying attention, based on their facial expressions or tone of voice. Using biometric data to draw inferences about people, using algorithms or otherwise, is not as invasive as using biometric data uniquely to identify someone. For example, biometric identification could include matching facial images caught on closed circuit television to a centrally held database of known offenders.

Furthermore, using biometric data for classification or categorisation purposes is still subject to the general data protection principles in the UK GDPR. That includes ensuring that there is a lawful ground for the processing, that the processing is necessary and proportionate, and is fair and transparent to the individuals concerned. If algorithms are used to categorise and make significant decisions about people based on their biometric characteristics, including in an employment context, they will have the right to be given information about the decision, and to obtain human intervention, as a result of the measures we previously debated in clause 11.

Therefore, we do see a distinction between the use of biometric information for identification purposes and the more general classification which the hon. Lady sought to draw. Though we believe that there is sufficient safeguard already in place regarding possible use of classification by biometric data, given what I have said, I hope that she will consider withdrawing the amendment.

Stephanie Peacock: I am grateful to the Minister for his comments. We will be speaking about the private uses of biometric data later, so I beg to ask leave to withdraw my amendment.

Amendment, by leave, withdrawn.

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

Sir John Whittingdale: DNA and fingerprints are key tools in helping the police to identify and eliminate suspects quickly and accurately by comparing evidence left at crime scenes with the appropriate files on the national databases. As I previously set out, clause 106 makes changes to the National DNA Database Strategy Board. The board provides oversight of the operation of the database, including setting policies for access and use by the police.

These reforms change the scope of the board to make it clear that they should provide similar oversight of the police fingerprint database, which operates under similar rules. The change brings the legislation up to date with the board's recently published governance rules. Clause 106 also updates the name of the board to the Forensic Information Databases Strategy Board, to better reflect the broadened scope of its work. We are also taking this opportunity to simplify and future-proof oversight of national police biometric databases. While DNA and fingerprints are well established, biometrics is an area of rapid technological development, including for example the growing use of iris, face and voice recognition. Given the pace of technological change in this area and the benefits of consistent oversight, Clause 106 also includes a power for the Secretary of State to make regulations which make changes to the board's scope, for example by adding new biometric databases into the board's remit or to remove them, where a database is no longer used. Such regulations would be subject to the affirmative procedure.

For these reasons, I commend the clause to the Committee.

Stephanie Peacock: Clause 106 will primarily increase the scope of the Forensic Information Databases Strategy Board to provide oversight of the national fingerprint database. However, there are also provisions enabling the Secretary of State to add or remove a biometric database that the board oversees, using the affirmative procedure. I would therefore like to ask the Minister whether they have any plans to use these powers regarding any particular databases—or whether this is intended as a measure for future-proofing the Bill in the case of changed circumstances?

I would also like to refer hon. Members to the remarks that I have made throughout the Bill that emphasise a need for caution when transferring the ability to change regulation further into the hands of the Secretary of State alone.

Sir John Whittingdale: I would add only that this is an area where technology is moving very fast, as I referred to earlier. We think it is right to put in place this provision, to allow an extension if it becomes necessary—though I do not think we have any current plans. It is future-proofing of the Bill.

Question put and agreed to.

Clause 106 accordingly ordered to stand part of the Bill.

Clause 107

REGULATIONS

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

The Chair: With this it will be convenient to discuss clauses 108 to 114 stand part.

Sir John Whittingdale: Clause 107 will give the Secretary of State a regulation-making power to make consequential amendments to other legislation. The power enables amendments to this Bill itself where such amendments are consequential to the abolition of the Information Commissioner and his replacement by the new Information Commission. Such provision is needed because there are a number of areas where data protection legislation will need to be updated as a consequence of the Bill. This is a standard power, commonly included in Bills to ensure that wider legislation is updated where necessary as a result of new legislation. For example, references to "the Commissioner" in the Data Protection Act 2018

[Sir John Whittingdale]

will no longer be accurate, given changes to the governance structure of the Information Commissioner's Office within the Bill, so consequential amendments will be required to that Act.

Clause 108 outlines the form and procedure for making regulations under the powers in the Bill: they are to be made by statutory instrument. Where regulations in the Bill are subject to the affirmative resolution procedure, they may not be made unless a draft of the statutory instrument has been laid before Parliament and approved by a resolution of each House. That provision is needed because the Bill introduces new regulation-making powers, which are necessary to support the Bill's policy objectives. For example, powers in part 3 of the Bill replace an existing statutory framework with a new, enhanced one.

Clause 109 explains the meaning of references to "the 2018 Act" and "the UK GDPR" in the Bill. Such provision is needed to explain the meaning of those two references. Clause 110 authorises expenditure arising from the Bill. That provision is needed to confirm that Parliament will fund any expenditure incurred under the Bill by the Secretary of State, the Treasury or a Government Department. It requires a money resolution and a Ways and Means resolution, both of which were passed in the House of Commons on 17 April.

Clause 111 outlines the territorial extent of the Bill. Specifically, the clause states that the Bill extends to England and Wales, Scotland and Northern Ireland, with some exceptions. Much of the Bill, including everything on data protection, is reserved policy. In areas where the Bill legislates on devolved matters, we are working with the devolved Administrations to secure legislative consent motions. Clause 112 gives the Secretary of State a regulation-making power to bring the Bill's provisions into force. Some provisions, listed in subsection (2), come into force on the date of Royal Assent. Other provisions, listed in subsection (3), come into force two months after Royal Assent. Such provision is needed to outline when the Bill's provisions will come into force.

Clause 113 gives the Secretary of State a regulation-making power to make transitional, transitory or saving provisions that may be needed in connection with any of the Bill's provisions coming into force. For example, provision might be required to clarify that the Information Commissioner's new power to refuse to act on complaints will not apply where such complaints have already been made prior to commencement of the relevant provision. Clause 114 outlines the short title of the Bill. That provision is needed to confirm the title once the Bill has been enacted. I commend clauses 107 to 114 to the Committee.

Stephanie Peacock: The clauses set out the final technical provisions necessary in order for the Bill to be passed and enacted effectively, and for the most part are standard. I will focus briefly on clause 107, however, as a number of stakeholders including the Public Law Project have expressed concern that, as a wide Henry VIII power, it may give the Secretary of State the power to make further sweeping changes to data protection law. Can the Minister provide some assurance that the clause will allow for the creation only of further provisions that are genuinely consequential to the Bill and necessary for its proper enactment?

It is my belief that this would not have been such a concern to civil society groups had there not been multiple occasions throughout the Bill when the Secretary of State made grabs for power, concentrating the ability to make further changes to data protection legislation in their own hands. I am disappointed, though of course not surprised, that the Government have not accepted any of my amendments to help to mitigate those powers with checks and balances involving the commissioner. However, keeping the clause alone in mind, I look forward to hearing from the Minister how the powers in clause 107 will be restricted and used.

Sir John Whittingdale: We have previously debated the efficacy of the affirmative resolution procedure. I recognise that the hon. Lady is not convinced about how effective it is in terms of parliamentary scrutiny; we will beg to differ on that point. Although the power in clause 107 allows the Secretary of State to amend Acts of Parliament, I can confirm that that is just to ensure the legal clarity of the text. Without that power, data protection legislation would be harder to interpret, thereby reducing people's understanding of the legislation and their ability to rely on the law.

Question put and agreed to.

Clause 107 accordingly ordered to stand part of the Bill.

Clause 108

Regulations

2.45 pm

Amendments made: 11, in clause 108, page 131, line 2, after "Act" insert

'made by the Secretary of State, the Treasury or the Welsh Ministers'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 12, in clause 108, page 131, line 2, at end insert—

'(1A) For regulations under this Act made by the Scottish Ministers, see section 27 of the Interpretation and Legislative Reform (Scotland) Act 2010 (asp 10) (Scottish statutory instruments).'

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 13, in clause 108, page 131, line 3, after "Act" insert

'made by the Secretary of State or the Treasury'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 14, in clause 108, page 131, line 8, after "procedure" insert

'—

(a) if made by the Secretary of State or the Treasury,'.

This amendment is consequential on Amendments 8 and 10 and NC5.

Amendment 15, in clause 108, page 131, line 9, at end insert—

'(b) if made by the Scottish Ministers, the regulations are subject to the negative procedure (see section 28 of the Interpretation and Legislative Reform (Scotland) Act 2010 (asp 10));

(c) if made by the Welsh Ministers, the statutory instrument containing the regulations is subject to annulment in pursuance of a resolution of Senedd Cymru.'

This amendment is consequential on Amendments 8 and 10 and NC5. It makes provision about the meaning of the negative resolution procedure in connection with regulations made by Scottish Ministers or Welsh Ministers.

Amendment 16, in clause 108, page 131, line 10, after "Act" insert

'made by the Secretary of State or the Treasury'.—*(Sir John Whittingdale.)*

This amendment is consequential on Amendments 8 and 10 and NC5.

Clause 108, as amended, ordered to stand part of the Bill.

Clauses 109 to 114 ordered to stand part of the Bill.

New Clause 1

GENERAL PROCESSING AND CODES OF CONDUCT

'In Article 41 of the UK GDPR (monitoring of approved codes of conduct)—

(a) in paragraph 4, omit the words from ', including suspension' to the end, and

(b) after that paragraph insert—

"4A. If the action taken by a body under paragraph 4 consists of suspending or excluding a controller or processor from the code, the body must inform the Commissioner, giving reasons for taking that action."'.—*(Sir John Whittingdale.)*

This new clause clarifies that bodies accredited under Article 41 of the UK GDPR to monitor compliance with codes of conduct under Article 40 are only required to notify the Information Commissioner if they suspend or exclude a person from a code.

Brought up, read the First and Second time, and added to the Bill.

New Clause 2

CODES OF CONDUCT

'(1) The PEC Regulations are amended as follows.

(2) After regulation 32 insert—

"**Codes of conduct**

32A.—(1) The Commissioner must encourage representative bodies to produce codes of conduct intended to contribute to compliance with these Regulations.

(2) Under paragraph (1), the Commissioner must encourage representative bodies to produce codes which take account of, among other things, the specific features of different sectors.

(3) A code of conduct described in paragraph (1) may, for example, make provision with regard to—

(a) rights and obligations under these Regulations;

(b) out-of-court proceedings and other dispute resolution procedures for resolving disputes arising in connection with these Regulations.

(4) The Commissioner must encourage representative bodies to submit codes of conduct described in paragraph (1) to the Commissioner in draft.

(5) Where a representative body does so, the Commissioner must—

(a) provide the representative body with an opinion on whether the code correctly reflects the requirements of these Regulations,

(b) decide whether to approve the code, and

(c) if the code is approved, register and publish the code.

(6) The Commissioner may only approve a code if, among other things—

(a) the code contains a mechanism for monitoring whether persons who undertake to apply the code comply with its provisions, and

(b) in relation to persons other than public bodies, the mechanism involves monitoring by a body which is accredited for that purpose by the Commissioner under regulation 32B.

(7) In relation to amendments of a code of conduct that is for the time being approved under this regulation—

(a) paragraphs (4) and (5) apply as they apply in relation to a code, and

(b) the requirements in paragraph (6) must be satisfied by the code as amended.

(8) A code of conduct described in paragraph (1) may be contained in the same document as a code of conduct described in Article 40 of the UK GDPR (and a provision contained in such a document may be a provision of both codes).

(9) In this regulation—

'public body' has the meaning given in section 7 of the Data Protection Act 2018 (for the purposes of the UK GDPR);

'representative body' means an association or other body representing categories of—

(a) communications providers, or

(b) other persons engaged in activities regulated by these Regulations;

'the UK GDPR' has the meaning given in section 3(10) of the Data Protection Act 2018.

Accreditation of bodies monitoring compliance with codes of conduct

32B.—(1) The Commissioner may, in accordance with this regulation, accredit a body for the purpose of monitoring whether persons other than public bodies comply with a code of conduct described in regulation 32A(1).

(2) The Commissioner may accredit a body only where the Commissioner is satisfied that the body has—

(a) demonstrated its independence,

(b) demonstrated that it has an appropriate level of expertise in relation to the subject matter of the code,

(c) established procedures which allow it—

(i) to assess a person's eligibility to apply the code,

(ii) to monitor compliance with the code, and

(iii) to review the operation of the code periodically,

(d) established procedures and structures to handle complaints about infringements of the code or about the manner in which the code has been, or is being, implemented by a person,

(e) made arrangements to publish information about the procedures and structures described in sub-paragraph (d), and

(f) demonstrated that it does not have a conflict of interest.

(3) The Commissioner must prepare and publish guidance about how the Commissioner proposes to take decisions about accreditation under this regulation.

(4) A body accredited under this regulation in relation to a code must take appropriate action where a person infringes the code.

(5) If the action taken by a body under paragraph (4) consists of suspending or excluding a person from the code, the body must inform the Commissioner, giving reasons for taking that action.

(6) The Commissioner must revoke the accreditation of a body under this regulation if the Commissioner considers that the body—

(a) no longer meets the requirements for accreditation, or

(b) has failed, or is failing, to comply with paragraph (4) or (5).

(7) In this regulation, 'public body' has the same meaning as in regulation 32A.

Effect of codes of conduct

32C. Adherence to a code of conduct approved under regulation 32A may be used by a person as a means of demonstrating compliance with these Regulations.'

(3) In regulation 33 (technical advice to the Commissioner)—

(a) omit ', in connection with his enforcement functions,' and

(b) at the end insert 'where the request is made in connection with—

(a) the Commissioner's enforcement functions, or

(b) the Commissioner's functions under regulation 32A or 32B (codes of conduct).'

(4) In Schedule 1 (Information Commissioner's enforcement powers) (inserted by Schedule 10 to this Act), in paragraph 18(b)(ii) (maximum amount of penalty), for 'or 24' substitute ', 24 or 32B(4) or (5)".'.—*(Sir John Whittingdale.)*

This new clause inserts provision requiring the Information Commissioner to encourage representative bodies to prepare codes of conduct relating to compliance with the PEC Regulations and makes provision about the content of such codes.

Brought up, read the First and Second time, and added to the Bill.

New Clause 3

Information disclosed by the Welsh Revenue Authority

'(1) This section applies where the Welsh Revenue Authority discloses personal information to a person under section 54 for the purpose of enabling the person to provide digital verification services for an individual.

(2) The person must not further disclose the information otherwise than for the purpose of providing digital verification services for the individual, except with the consent of the Welsh Revenue Authority.

(3) Any other person who receives the information, whether directly or indirectly from the person to whom the Welsh Revenue Authority discloses the information, must not further disclose the information, except with the consent of the Welsh Revenue Authority.

(4) A person who discloses information in contravention of subsection (2) or (3) commits an offence.

(5) It is a defence for a person charged with an offence under subsection (4) to prove that the person reasonably believed—

(a) that the disclosure was lawful, or

(b) that the information had already lawfully been made available to the public.

(6) A person who commits an offence under subsection (4) is liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both);

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or a fine not exceeding the statutory maximum (or both);

(c) on summary conviction in Northern Ireland, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum (or both);

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both).

(7) In this section,

"personal information" means information relating to a person whose identity—

(a) is specified in the information, or

(b) can be deduced from it.'.—*(Sir John Whittingdale.)*

If the Welsh Revenue Authority discloses information under clause 54, this new clause prevents further disclosure of that information without the consent of the Welsh Revenue Authority.

Brought up, read the First and Second time, and added to the Bill.

New Clause 4

Information disclosed by Revenue Scotland

'(1) This section applies where Revenue Scotland discloses personal information to a person under section 54 for the purpose of enabling the person to provide digital verification services for an individual.

(2) The person must not further disclose the information otherwise than for the purpose of providing digital verification services for the individual, except with the consent of Revenue Scotland.

(3) Any other person who receives the information, whether directly or indirectly from the person to whom Revenue Scotland discloses the information, must not further disclose the information, except with the consent of Revenue Scotland.

(4) A person who discloses information in contravention of subsection (2) or (3) commits an offence.

(5) It is a defence for a person charged with an offence under subsection (4) to prove that the person reasonably believed—

(a) that the disclosure was lawful, or

(b) that the information had already lawfully been made available to the public.

(6) A person who commits an offence under subsection (4) is liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both);

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or a fine not exceeding the statutory maximum (or both);

(c) on summary conviction in Northern Ireland, to imprisonment for a term not exceeding 6 months or a fine not exceeding the statutory maximum (or both);

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or a fine (or both).

(7) In this section,

"personal information" means information relating to a person whose identity—

(a) is specified in the information, or

(b) can be deduced from it.'.—*(Sir John Whittingdale.)*

If Revenue Scotland discloses information under clause 54, this new clause prevents further disclosure of that information without the consent of Revenue Scotland.

Brought up, read the First and Second time, and added to the Bill.

New Clause 5

Meaning of "appropriate national authority"

'(1) In section 93, "appropriate national authority" means the Secretary of State, subject as follows.

(2) The Scottish Ministers are also an appropriate national authority in relation to regulations under section 93 which contain only provision which would be within the legislative competence of the Scottish Parliament if contained in an Act of that Parliament.

(3) The Welsh Ministers are also an appropriate national authority in relation to regulations under section 93 which contain only provision which would be within the legislative competence of Senedd Cymru if contained in an Act of the Senedd (ignoring any requirement for the consent of a Minister of the Crown).

(4) The consent of a Minister of the Crown is required before any provision is made by the Welsh Ministers in regulations under section 93 so far as that provision, if contained in an Act of Senedd Cymru, would require the consent of a Minister of the Crown.

(5) In Schedule 7B to the Government of Wales Act 2006 (general restrictions on legislative competence of Senedd Cymru), in paragraph 11(6)(b) (exceptions to restrictions relating to Ministers of the Crown)—

(a) omit the "or" at the end of sub-paragraph (viii), and

(b) after sub-paragraph (ix) insert "; or

(x) section 93 of the Data Protection and Digital Information Act 2023."

(6) In this section, "Minister of the Crown" has the same meaning as in the Ministers of the Crown Act 1975.'—*(Sir John Whittingdale.)*

This new clause makes provision about the exercise of the regulation-making power conferred by clause 93 on the Secretary of State, Scottish Ministers and Welsh Ministers. See also Amendments 8, 9 and 10.

Brought up, read the First and Second time, and added to the Bill.

New Clause 6

SPECIAL CATEGORIES OF PERSONAL DATA: ELECTED REPRESENTATIVES RESPONDING TO REQUESTS

'In paragraph 23 of Schedule 1 to the 2018 Act (special categories of personal data: elected representatives responding to requests), in sub-paragraph (4), for "fourth day after" substitute "period of 30 days beginning with the day after".'.—*(Sir John Whittingdale.)*

Schedule 1 to the Data Protection Act 2018 includes provision about certain processing of special categories of personal data by elected representatives. This new clause increases the period for which former members of the Westminster Parliament and the devolved legislatures continue to be treated as "elected representatives" following an election. See also Amendments 30 and 31.

Brought up, read the First and Second time, and added to the Bill.

New Clause 7

PRE-COMMENCEMENT CONSULTATION

'(1) A requirement to consult under section 83 may be satisfied by consultation before, as well as by consultation after, that section comes into force.

(2) A requirement to consult under a provision inserted into the PEC Regulations by any of sections 79 to 86 may be satisfied by consultation before, as well as by consultation after, the provision inserting that provision comes into force.'.—*(Sir John Whittingdale.)*

This new clause provides that requirements imposed by the Bill to consult under or in connection with the PEC Regulations can be satisfied by consultation which takes place before the relevant provision of the Bill comes into force.

Brought up, read the First and Second time, and added to the Bill.

New Clause 8

PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA: BIOMETRIC DATA

'(1) Article 9 of UK GDPR is amended as follows.

(2) In paragraph (1), after "biometric data", omit "for the purpose of uniquely identifying a natural person."'.—*(Stephanie Peacock.)*

This new clause would extend the same protections that are currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data, including if the processing is for the purpose of classification (i.e. identification as part of a group, rather than identification as an individual).

Brought up, and read the First time.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 28]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

New Clause 9

TRANSPARENCY IN USE OF ALGORITHMIC TOOLS

'(1) The Secretary of State must by regulations make provision requiring Government departments, public authorities and Government contractors using algorithmic tools to process personal data to use the UK Algorithmic Transparency Standard.

(2) The UK Algorithmic Transparency Standard ("the Standard") is the standard published by the Central Digital and Data Office and Centre for Data Ethics and Innovation as part of the Government's National Data Strategy.

(3) Regulations under subsection (1) must require the publication of the information required by the Standard.

(4) Regulations under subsection (1) may provide for exemptions to the requirement for publication where necessary—

(a) to avoid obstructing an official or legal inquiry, investigation or procedure,

(b) to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties,

(c) to protect public security, or

(d) to safeguard national security.'—*(Stephanie Peacock.)*

This new clause puts legislative obligation on public bodies using personal data to use the UK Algorithmic Transparency Standard.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

In order for the public to have trust in algorithmic decision making, particularly where used by the Government, they must be able to understand how and when it is being used as a basic minimum. That is something that the Government themselves previously recognised by including a proposal to make transparency reporting on the use of algorithms in decision making for public sector bodies compulsory in their "Data: a new direction" consultation. Indeed, the Government have already made good progress on bringing together a framework that will make that reporting possible. The algorithmic transparency recording standard they have built provides a decent, standardised way of recording and sharing information about how the public sector uses algorithmic tools. There is also full guidance to accompany the standard, giving public sector bodies a clear understanding of how to complete transparency reports, as well as a compilation of pilot reports that have already been published, providing a bank of examples.

However, despite that and the majority of consultation respondents agreeing with the proposed compulsory reporting for public sector bodies—citing benefits of increased trust, accountability and accessibility for the public—the Government chose not to go ahead with the legislative change. Relying on self-regulation in the early stages of the scheme is understandable, but having conducted successful pilots, from the Cabinet Office to West Midlands police, it is unclear why the Government now choose not to commit to the very standard they created. This is a clear missed opportunity, with the standard running the risk of failing altogether if there is no legislative requirement to use it.

As the use of such algorithms grows, particularly considering further changes contained in clause 11, transparency around Government use of big data and automated decision-making tools will only increase in importance and value—people have a right to know how they are being governed. As the Public Law Project argues, transparency also has a consequential value;

[Stephanie Peacock]

it facilitates democratic consensus building about the appropriate use of new technologies, and it allows for full accountability when things go wrong.

Currently, in place of that accountability, the Public Law Project has put together its own register called "Tracking Automated Government", or TAG. Using mostly freedom of information requests, the register tracks the use of 42 algorithmic tools and rates their transparency. Of the 42, just one ranked as having high transparency. Among those with low transparency are asylum estates analysis, used to help the Home Office decide where asylum interviews should take place, given the geographical distribution of asylum seekers across the asylum estate; the general matching service and fraud referral and intervention management system, used as part of the efforts of the Department for Work and Pensions to combat benefit fraud and error—for example, by identifying claimants who may potentially have undisclosed capital or other income; and housing management systems, such as that in Wigan Metropolitan Borough Council, which uses a points-based system to prioritise social housing waiting lists.

We all want to see Government modernising and using new technology to increase efficiency and outcomes, but if an algorithmic tool impacts our asylum applications, our benefits system and the ability of people to gain housing, the people affected by those decisions deserve at the very least to know how they are being made. If the public sector sets the right example, private companies may choose to follow in the future, helping to improve transparency even further. The framework is ready to go and the benefits are clear; the amendment would simply make progress certain by bringing it forward as part of the legislative agenda. It is time that we gave people the confidence in public use of algorithms that they deserve.

Sir John Whittingdale: I thank the hon. Member for Barnsley East for moving new clause 9. We completely share her wish to ensure that Government and public authorities provide transparency in the way they use algorithmic tools that process personal data, especially when they are used to make decisions affecting members of the public.

The Government have made it our priority to ensure that transparency is being provided through the publication of the algorithmic transparency recording standard. That has been developed to assist public sector organisations in documenting and communicating their use of algorithms in decision making that impacts members of the public. The focus of the standard is to provide explanations of the decisions taken using automated processing of data by an algorithmic system, rather than all data processing.

The standard has been endorsed by the Government's Data Standards Authority, which recommends the standards, guidance and other resources that Government Departments should follow when working on data projects. Publishing the standard fulfils commitments made in both the national data strategy 2020 and the national artificial intelligence strategy. Since its publication, the standard has been piloted with a variety of public sector organisations across the UK, and the published records can be openly accessed via gov.uk. It is currently being rolled out more widely across the public sector.

Although the Government have made it a priority to advance work on algorithmic transparency, the algorithmic transparency recording standard is still a maturing standard that is being progressively promoted and adopted. It is evolving alongside policy thinking and Government understanding of the complexities, scope and risks around its use. We believe that enshrining the standard into law at this point of maturity could hinder the ability to ensure that it remains relevant in a rapidly developing technology field.

Therefore, although the Government sympathise with the intention behind the new clause, we believe it is best to continue with the current roll-out across the public sector. We remain committed to advancing algorithmic transparency, but we do not intend to take forward legislative change at this time. For that reason, I am unable to accept the new clause as proposed by the Opposition.

Stephanie Peacock: I am grateful to the Minister, but I am still confused about why, having developed the standard, the Government are not keen to put it into practice and into law. He just said that he wants to keep it relevant; he could use some of the secondary legislation that he is particularly keen on if he accepted the new clause. As I outlined, this issue has real-life consequences, whether for housing, asylum or benefits. In my constituency, many young people were affected by the exam algorithm scandal. For those reasons, I would like to push the new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 29]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

New Clause 10

PROVISION ABOUT REPRESENTATION OF DATA SUBJECTS

'(1) Section 190 of the Data Protection Act 2018 is amended as follows.

(2) In subsection (1), leave out "After the report under section 189(1) is laid before Parliament, the Secretary of State may" and insert "The Secretary of State must, within three months of the passage of the Data Protection and Digital Information Act 2023,".'—*(Stephanie Peacock.)*

This new clause would require the Secretary of State to exercise powers under s190 DPA2018 to allow organisations to raise data breach complaints on behalf of data subjects generally, in the absence of a particular subject who wishes to bring forward a claim about misuse of their own personal data.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

Overall, the aim of the GDPR is to ensure the effective and complete protection of data subjects. That protection cannot be considered effective or complete if people cannot seek justice, remedy and repair if an organisation processes personal data unlawfully. Therefore, there must be suitable methods of redress for all data and decision subjects in any suitable data protection regime. Bringing any kind of legal case is not something people take lightly. Cases can be lengthy, costly and, in many lower-level cases, seem disproportionate to the loss suffered or remedy available. That is no different in cases surrounding the misuse of personal data.

As the law stands, article 80(1) of the EU GDPR has been implemented in the UK, meaning a data subject has the right to mandate a not-for-profit body or organisation to lodge a complaint on their behalf. That means, for example, a charity can help an individual to bring forward a case where they have been materially impacted by a data breach. Such provisions help to ensure that those who have suffered an infringement can be supported in lodging a claim, and are not disincentivised by a lack of understanding, resources or cost. However, the UK has not yet adopted article 80(2), which goes one step further, allowing those same organisations to lodge a complaint independently of a data subject's mandate.

3 pm

Currently, where there has been a macro-level infringement, non-profit organisations have no right to lodge a complaint on behalf of the wide group of people impacted, unless an individual evidences the specific impact of the breach or infringement on them. If one individual is prepared to launch a case, an organisation can help: where many individuals are affected, if no one in particular has the evidence or resources to bring an individual case, that same organisation would not be able to lodge a complaint, even though the negative impact of such an infringement could be much larger, could have arisen by design and could have far-reaching consequences.

Organisations that champion the rights of consumers, such as Which?, Reset and 5Rights, strongly argue that an effective data protection redress framework requires a collective redress mechanism. They say that that would aid in creating an environment where data subjects have confidence in the way that organisations use their data and can be assured that processes are in place to protect their data rights if something goes wrong domestically or internationally.

Indeed, individual rights are not enough. In modern data processing, our data is used to make decisions about us individually and it is pooled together to analyse trends and predict behaviours across a whole population. In those cases where data is processed as a collective, producing collective outcomes, the people and communities impacted in turn deserve to have collective representations made on their behalf. That is particularly so in the workplace, where unions and other representative organisations can recognise the collective dimensions of data but do not currently have the access to act formally on their members' behalf. As the TUC recognises, that only increases the asymmetry between the power of employers to collect and use data relating to their workers and the inability of employees to control that data in return. The great strength of feeling about the lack of protections for workers in this Bill was demonstrated by the App Drivers and Couriers Union's "Kill the Data Bill" protest that took place on 18 May outside the Department for Science, Innovation and Technology building.

Introducing article 80(2) would help to deliver something positive for workers and deliver better accountability for all. However, in their call for evidence on implementing the article, the Government said that they believe that

"there is insufficient evidence of systemic failings in the current regime"

to warrant its introduction. That is despite the ICO itself being cited in the response as being broadly supportive of the intention of article 80(2). The regulator, it said,

"recognised that opt-out proceedings have the potential both to contribute to the protection of the rights of data subjects who may not be aware of the potential breaches of their data protection rights, and to raise awareness and understanding of data rights and data misuse."

Of course, there must be space to debate valid concerns around the measures. For example, some business groups expressed worries in the call for evidence that the article could increase litigation costs and insurance premiums during a period of economic uncertainty. However, non-profits, such as those that would be operating under the article, are restricted by their own lack of resources in times of uncertainty, and by their mandates. As such, they are likely to consider claims or other action only in limited circumstances where there is high merit. Such a change is therefore not likely to open the floodgates for unnecessary legal cases, or to give rise to a compensation culture, but will simply allow for cases to take place when they are necessary.

There are also valid concerns that a so called opt-out model could actually cut individuals out of the process if a legal claim is pursued without their knowledge, which would run counter to the principles of transparency. However, that could easily be resolved by ensuring that appropriate safeguards were in place so that any proceedings under article 80(2) are well publicised and give individuals the opportunity to opt out at their choice.

Systemic failings should not be needed to realise that collective redress, at a time when the impacts of data are indeed collective, is a fundamental part of being able to properly exercise one's data rights. New clause 10 acknowledges that and simply seeks to ensure that, as the use of large-scale data grows, communities and groups of people will have collective rights that reflect those that an individual has. Only then can our protection laws be considered effective and complete.

Sir John Whittingdale: I am grateful to the hon. Lady for setting out the purposes of the new clause. As she has described, it aims to require the Secretary of State to use regulation-making powers under section 190 of the Data Protection Act to implement article 80(2) of the UK GDPR. It would enable non-profit organisations with an expertise in data protection law to make complaints to the Information Commissioner and/or take legal action against data controllers without the specific authorisation of the individuals who have been affected by data breaches. Relevant non-profit organisations can already take such actions on behalf of individuals who have specifically authorised them to do so under provisions in article 80(1) of the UK GDPR.

[Sir John Whittingdale]

In effect, the amendment would replace the current discretionary powers in section 190 of the Data Protection Act with a duty for the Secretary of State to legislate to bring those provisions into force soon after the Bill has received Royal Assent. Such an amendment would be undesirable for a number of reasons. First, as required under section 189 of the Data Protection Act, we have already consulted and reported to Parliament on proposals of that nature, and we concluded that there was not a strong enough case for introducing new legislation.

Although the Government's report acknowledged that some groups in society might find it difficult to complain to the ICO or bring legal proceedings of their own accord, it pointed out that the regulator can and does investigate complaints raised by civil society groups even when they are not made on behalf of named individuals. Big Brother Watch's recent complaints about the use of live facial recognition technology in certain shops in the south of England is an example of that.

Secondly, the response concluded that giving non-profit organisations the right to bring compensation claims against data controllers on behalf of individuals who had not authorised them to do so could prompt the growth of US-style lawsuits on behalf of thousands or even millions of customers at a time. In the event of a successful claim, each individual affected by the alleged breach could be eligible for a very small payout, but the consequences for the businesses could be hugely damaging, particularly in cases that involved little tangible harm to individuals.

Some organisations could be forced out of business or prompted to increase prices to recoup costs. The increase in litigation costs could also increase insurance premiums. A hardening in the insurance market could affect all data controllers, including those with a good record of compliance. For those reasons, we do not believe that it is right to extend the requirement on the Secretary of State to allow individuals to bring actions without the consent of those affected. On that basis, I ask the hon. Lady to withdraw the motion.

Stephanie Peacock: Data is increasingly used to make decisions about us as a collective, so it is important that GDPR gives us collective rights to reflect that, rather than the system being designed only for individuals to seek redress. For those reasons, I will press my new clause to a vote.

Question put, That the clause be read a Second time.

The Committee divided: Ayes 4, Noes 9.

Division No. 30]

AYES

Long Bailey, Rebecca	Peacock, Stephanie
Monaghan, Carol	Wakeford, Christian

NOES

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

Question accordingly negatived.

New Clause 11

PRIVACY ENHANCING TECHNOLOGIES

'(1) Within six months of the passage of this Act, the Secretary of State must publish and lay before Parliament a report on the potential impact of privacy enhancing technologies on the use and protection of personal data.

(2) "Privacy enhancing technologies" are software and hardware systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'—*(Stephanie Peacock.)*

This new clause would require the Secretary of State to publish a report on the potential impact of Privacy Enhancing Technologies.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

Privacy enhancing technologies are technologies and techniques that can help organisations to share and use people's data responsibly, lawfully and securely. They work most often by minimising the amount of data used, maximising data security—for example by encrypting or anonymising personal information—or empowering individuals. One of the best-known examples of a PET is synthetic data: data that is modelled to reproduce the statistical properties of a real dataset when taken as a whole. That type of data could allow third-party researchers or processors to analyse the statistical outcomes of the data without having access to the original set of personal data, or any information about identifiable living individuals.

Another example of PETs are those that minimise the amount of personal data that is shared without affecting the data's utility. Federated learning, for example, allows for the training of an algorithm across multiple devices or datasets held on servers, so if an organisation wants to train a machine-learning model but has limited training data available, they can send the model to a remote dataset for training. The model will then return having benefited from those datasets, while the sensitive data itself is not exchanged or ever put in the hands of those in ownership of the algorithm. The use of PETs therefore does not necessarily exclude data from being defined as personal or falling within the remit of GDPR. They can, however, help to minimise the risk that arises from personal data breaches and provide an increased level of security.

The Government have positioned the Bill as one that seeks to strengthen the data rights of citizens while catalysing innovation. PETs could and should have been a natural area for the Bill to explore, because not only can such devices help controllers demonstrate an approach based on data protection by design and default, but they can open the door for new ways of collaborating, innovating and researching with data. The Royal Society has researched the role that PETs can play in data governance and collaboration in immense detail, with its findings contained in its 2023 report, which is more than 100 pages long. One of the report's key recommendations was that the Government should develop a national PET strategy to promote their responsible use as tools for advancing scientific research, increasing security and offering new partnership possibilities, both domestically and across borders.

It is vital to acknowledge that working with PETs involves risks that must be considered. Some may not be robust enough against attacks because they are in the

early stages of development, while others might require a significant amount of expertise to operate, without which their use may be counterproductive. It is therefore important to be clear that the amendment would not jump ahead and endorse any particular technology or device before it was ready. Instead, it would enshrine the European Union Agency for Cybersecurity definition of PETs in UK law and prompt the Government to issue a report on how that growing area of technology might play a role in data processing and data regulation in future.

That could include identifying the opportunities that PETs could provide while also looking at the threats and potential harms involved in using the technologies without significant expertise or technological readiness. Indeed, in their consultation response, the Government even mentioned they were keen to explore opportunities around smart data, while promoting understanding that they should not be seen as a substitute for reducing privacy risks on an organisational level. The report, and the advancing of the amendment, would allow the Government that exploration, indicating a positive acknowledgment of the potentially growing role that PETs might play in data processing and opening the door for further research in the area.

Even by their name, privacy enhancing technologies reflect exactly what the Bill should be doing: looking to the future to encourage innovation in tech and then using such innovation to protect citizens in return. I hope hon. Members will see those technologies' potential value and the importance of analysing any harms, and look to place the requirement to analyse PETs on the statute book.

Sir John Whittingdale: We absolutely agree with the Opposition about the importance of privacy enhancing technologies, which I will call PETs, since I spoke on them recently and was told that was the best abbreviation—it is certainly easier. We wish to see their use by organisations to help ensure compliance with data protection principles and we seek to encourage that. As part of our work under the national data strategy, we are already exploring the macro-impacts of PETs and how they can unlock data across the economy.

The ICO has recently published its draft guidance on anonymisation, pseudonymisation and PETs, which explains the benefits and different types of PETs currently available, as well as how they can help organisations comply with data protection law. In addition, the Centre for Data Ethics and Innovation has published an adoption guide to aid decision making around the use of PETs in data-driven projects. It has also successfully completed delivery of UK-US prize challenges to drive innovation in PETs that reinforce democratic values. Indeed, I was delighted to meet some of the participants in those prize challenges at the Royal Society yesterday and hear a little more about some of their remarkable innovations.

As the hon. Lady mentioned, the Royal Society has published reports on how PETs can maximise the benefit and reduce the harms associated with data use. Adding a definition of PETs to the legislation and requiring the Government to publish a report six months after Royal Assent is unlikely to have many advantages over the approach that the ICO, the CDEI and others are taking to develop a better understanding in the area. Furthermore, many PETs are still in the very early stages of their deployment and use, and have not been widely adopted across the UK or globally. A statutory definition could quickly become outdated. Publishing a comprehensive report on the potential impacts of PETs, which advocated the use of one technology or another, could even distort a developing market, and lead to unintended negative impacts on the development of what are promising technologies. For that reason, I ask the hon. Lady to withdraw the new clause.

3.15 pm

Stephanie Peacock: I am grateful to the Minister for his clarification on the pronunciation of the acronym. I acknowledge the points he made. I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

New Clause 13

Oversight of biometric technology use by the Information Commission

'(1) The Information Commission must establish a Biometrics Office.

(2) The Biometrics Office is to consist of a committee of three commissioners with relevant expertise, appointed by the Commission.

(3) The functions of the Biometrics Office are—

(a) to establish and maintain a public register of relevant entities engaged in processing biometric data;

(b) to oversee and review the biometrics use of relevant entities;

(c) to produce a Code of Practice for the use of biometric technology by registered parties, which must include—

(i) compulsory standards of accuracy and reliability for biometric technologies,

(ii) a requirement for the proportionality of biometrics use to be assessed prior to use and annually thereafter, and a procedure for such assessment, and

(iii) a procedure for individual complaints about the use of biometrics by registered parties;

(d) to receive and publish annual reports from all relevant entities, which must include the relevant entity's proportionality assessment of their biometrics use;

(e) to enforce registration and reporting by the issuing of enforcement notices and, where necessary, the imposition of fines for non-compliance with the registration and reporting requirements;

(f) to ensure lawfulness of biometrics use by relevant entities, including issuing compliance and abatement notices where necessary.

(4) The Secretary of State may by regulations add to the responsibilities of the Biometrics Office.

(5) Regulations made under subsection (4) are subject to the affirmative resolution procedure.

(6) For the purposes of this Part—

"biometric data" has the meaning given by section 106 of this Act (see subsection 13);

"relevant entity" means any organisation or body corporate (whether public or private) which processes biometric data, other than where the biometric processing undertaken by the organisation or body corporate is otherwise overseen by the Investigatory Powers Commissioner, because it is—

(a) for the purposes of making or renewing a national security determination as defined by s.20(2) Protection of Freedoms Act 2012; or

(b) for the purposes set out in s.20(6) Protection of Freedoms Act 2012.'.—*(Stephanie Peacock.)*

This new clause, together with NC14 and NC15, are intended to form a new Part of the Bill which creates a mechanism for the Information Commission to oversee biometric technology use by private parties.

Brought up, and read the First time.

Stephanie Peacock: I beg to move, That the clause be read a Second time.

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

New clause 14—*Requirement to register with the Information Commission—*

'(1) Any relevant entity intending to process biometric data for purposes other than those contained in section 20(2) and section 20(6) of the Protection of Freedoms Act 2012 must register with the Information Commission prior to the deployment of the biometric technology.

(2) An application for registration must include an explanation of the intended biometrics use, including an assessment of its proportionality and its extent.

(3) All relevant entities must provide an annual report to the Biometrics Office addressing their processing of biometric data in the preceding year and their intended processing of biometrics in the following year .

(4) Each annual report must contain a proportionality assessment of the relevant entity's processing of biometric data in the preceding year and intended processing of biometric data in the following year.

(5) Any relevant entity which processes biometric data without having registered with the Information Commission, or without providing annual reports to the Biometrics Office, is liable to an unlimited fine imposed by the Information Commission.'

See explanatory statement to NC13.

New clause 15—*Private biometrics use prior to entry into force of the Act—*

'Any relevant entity engaged in processing biometric data other than for the purposes contained in section 20(2) and section 20(6) of the Protection of Freedoms Act 2012 prior to the entry into force of this Part must register with the Information Commission in accordance with section *[Requirement to register with the Information Commission*] within six months of the date of entry into force of this Part; and subsection (5) of that section does not apply to such an entity during that period.'

See explanatory statement to NC13. This new clause would provide a transitional period of six months for entities which were already engaged in the processing of biometric data to register with the Commission.

Stephanie Peacock: A wider range of biometric data is now being collected than ever before. From data on the way we walk and talk to the facial expressions we make, biometric data is now being collected and used in a wide range of situations for many distinct purposes. Great attention has rightly been paid to police use of facial recognition technology to identify individuals, for example at football matches or protests. Indeed, to date, much of the regulatory attention has focused on those use cases, which are overseen by the Investigatory Powers Commissioner. However, the use of biometric technologies extends far beyond those examples, and there has been a proliferation of biometrics designed by private organisations to be used across day-to-day life—not just in policing.

We unlock smartphones with our faces or fingerprints, and companies have proposed using facial expression analysis to detect whether students are paying attention in online classes. Employers have used facial expression and tone analysis to decide who should be selected for a job—as was already mentioned in reference to new clause 8. As the proliferation of biometric technologies occurs, a number of issues have been raised about their impact on people and society. Indeed, if people's identities can be detected by both public and private actors at any given point, there is potential for it to significantly infringe on someone's privacy to move through the world with freedom of expression, association and assembly. Similarly, if people's traits, characteristics or abilities can be automatically assessed on the basis of biometrics, often without a scientific basis, it may affect free expression and the development of personality.

Public attitudes research carried out by the Ada Lovelace Institute shows that the British public recognise the potential benefits of tools such as facial recognition in certain circumstances—for example, smartphone locking systems and in airports—but often reject their use in others. Large majorities are opposed to the use of facial recognition in shops, schools and on public transport, as well as by human resources departments in recruitment. In all cases, the public expect the use of biometrics to be accompanied by safeguards and limitations, such as appropriate transparency and accountability measures.

Members of the citizens' biometrics council, convened by the Ada Lovelace Institute in 2020 and made up of 50 members of the public, expressed the view that biometric technologies as currently used are lacking in transparency and accountability. In particular, safeguards are uneven across sectors. Private use of biometrics are not currently subject to the same level of regulatory oversight or due process as is afforded within the criminal justice system, despite also having the potential to create changes of life-affecting significance. As a result, one member of the council memorably asked:

"If the technology companies break their promises…what will the implications be? Who's going to hold them to account?"

It is with those issues in mind that experts and legal opinion seem all to come to the same consistent conclusion that, at the moment, there is not a sufficient legal framework in place to manage the unique issues that the private proliferation of biometrics use raises. An independent legal review, commissioned by the Ada Lovelace Institute and led by Matthew Ryder KC, found that current governance structures and accountability mechanisms for biometrics are fragmented, unclear and ineffective. Similar findings have been made by the Biometrics and Surveillance Camera Commissioner, and Select Committees in this House and in the other place.

The Government, however, have not yet acted on delivering a legal framework to govern the use of biometric technology by private corporations, meaning that the Bill is a missed opportunity. New clause 13 therefore seeks to move towards the creation of that framework, providing for the Information Commission to oversee the use of biometric technology by private parties, and ensure accountability around it. I hope that the Committee see the value of this oversight and what it could provide and will support the new clause.

Sir John Whittingdale: New clause 13 would require the Information Commission to establish a new separate statutory biometrics office with responsibility for the oversight and regulation of biometric data and technology. However, the Information Commissioner already has responsibility for monitoring and enforcing the processing of biometric data, as it falls within the definition of personal data. Under the Bill, the new body corporate—the

Information Commission—will continue to monitor and enforce the processing of all personal data under the data protection legislation, including biometric data. Indeed, with its new independent board and governance structure, the commission will enjoy greater diversity in skills and decision making, ensuring that the regulator has the right blend of skills and expertise at the very top of the organisation.

Furthermore, the Bill allows the new Information Commission to establish committees, which may include specialists from outside the organisation with key skills and expertise in specialist areas. As such, the Government are of the firm view that the Information Commission is best placed to provide regulatory oversight of biometric data, rather than delegating responsibility and functions to a separate office. The creation of a new body would likely cause confusion for those seeking redress, by creating novel complaints processes for biometric-related complaints, as set out in new clause 13(3)(c)(iii). It would also complicate regulatory oversight and decision making by providing the new office with powers to impose fines, as per subsection (2)(e). For those reasons, I encourage the hon. Lady to withdraw her new clause.

New clauses 14 and 15 would require non-law enforcement bodies that process biometric data about individuals to register with the Information Commissioner before the processing begins. Where the processing started prior to passage of the Bill, the organisation would need to register within six months of commencement. As part of the registration process, the organisation would have to explain the intended effect of the processing and provide annual updates to the Information Commissioner's Office on current and future processing activities. Organisations that fail to comply with these requirements would be subject to an unlimited fine.

I appreciate that the new clauses aim to make sure that organisations will give careful thought to the necessity and proportionality of their processing activities, and to improve regulatory oversight, but they could have significant unintended consequences. As the hon. Lady will be aware, there are many everyday uses of biometrics data, such as using a thumbprint to access a phone, laptop or other connected device. Such services would always ask for the user's explicit consent and make alternatives such as passwords available to customers who would prefer not to part with their biometric data.

If every organisation that launched a new product had to register with the Information Commissioner to explain its intentions and complete annual reports, that could place significant and unnecessary new burdens on businesses and undermine the aims of the Bill. Where the use of biometric data is more intrusive, perhaps involving surveillance technology to identify specific individuals, the processing will already be subject to the heightened safeguards in article 9 of the UK GDPR. The processing would need to be necessary and proportionate on the grounds of substantial public interest.

The Bill will also require organisations to designate a senior responsible individual to manage privacy risks, act as a contact point for the regulator, undertake risk assessments and keep records in relation to high-risk processing activities. It would be open to the regulator to request to see these documents if members of the public expressed concern about the use of the technology.

I hope my response has helped to address the issues the hon. Lady was concerned about, and I would respectfully ask her to not to press these new clauses.

Stephanie Peacock: It does indeed provide reassurance. On that basis, I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

The Chair: We now come to the big moment for the hon. Member for Loughborough. Weeks of anticipation are now at an end. I call her to move new clause 16.

New Clause 16

PROCESSING OF DATA IN RELATION TO A CASE-FILE PREPARED BY THE POLICE SERVICE FOR SUBMISSION TO THE CROWN PROSECUTION SERVICE FOR A CHARGING DECISION

'(1) The 2018 Act is amended in accordance with subsection (2).

(2) In the 2018 Act, after section 40 insert—

"**40A Processing of data in relation to a case-file prepared by the police service for submission to the Crown Prosecution Service for a charging decision**

(1) This section applies to a set of processing operations consisting of the preparation of a case-file by the police service for submission to the Crown Prosecution Service for a charging decision, the making of a charging decision by the Crown Prosecution Service, and the return of the case-file by the Crown Prosecution Service to the police service after a charging decision has been made.

(2) The police service is not obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in preparing a case-file for submission to the Crown Prosecution Service for a charging decision.

(3) The Crown Prosecution Service is not obliged to comply with the first data protection principle except insofar as that principle requires processing to be fair, or the third data protection principle, in making a charging decision on a case-file submitted for that purpose by the police service.

(4) If the Crown Prosecution Service decides that a charge will not be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service it must take all steps reasonably required to destroy and delete all copies of the case-file in its possession.

(5) If the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service it must return the case-file to the police service and take all steps reasonably required to destroy and delete all copies of the case-file in its possession.

(6) Where the Crown Prosecution Service decides that a charge will be pursued when it makes a charging decision on a case-file submitted for that purpose by the police service and returns the case-file to the police service under subsection (5), the police service must comply with the first data protection principle and the third data protection principle in relation to any subsequent processing of the data contained in the case-file.

(7) For the purposes of this section—

(a) The police service means—

(i) constabulary maintained by virtue of an enactment, or

(ii) subject to section 126 of the Criminal Justice and Public Order Act 1994 (prison staff not to be regarded as in police service), any other service whose members have the powers or privileges of a constable.

(b) The preparation of, or preparing, a case-file by the police service for submission to the Crown Prosecution Service for a charging decision includes the submission of the file.

(c) A case-file includes all information obtained by the police service for the purpose of preparing a case-file for submission to the Crown Prosecution Service for a charging decision."' —*(Jane Hunt.)*

This new clause adjusts Section 40 of the Data Protection Act 2018 to exempt the police service and the Crown Prosecution Service from the first and third data protection principles contained within the 2018 Act so that they can share unredacted data with one another when making a charging decision.

Brought up, and read the First time.

Jane Hunt (Loughborough) (Con): I beg to move, That the clause be read a Second time.

It is a pleasure to speak before you today, Mr Hollobone, and to move my new clause. I recently met members of the Leicestershire Police Federation, who informed me of its concerns regarding part 3 of the Data Protection Act 2018, which imposes unnecessary and burdensome redaction obligations on the police and taking them away from the frontline. I thank the Police Federation for providing me with the information I am going to discuss and for drafting the new clause I have tabled.

Part 3 of the 2018 Act implemented the law enforcement directive and made provision for data processing by competent authorities, including police forces and the Crown Prosecution Service, for "law enforcement purposes".

Although recital (4) to the law enforcement directive emphasised that the

"free flow of personal data between competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences…should be facilitated while ensuring a high level of protection of personal data,"

part 3 of the 2018 Act contains no provision at all to facilitate the free flow of personal data between the police and the CPS. Instead, it imposes burdensome obligations on the police, requiring them to redact personal data from information transferred to the CPS. Those obligations are only delaying and obstructing the expeditious progress of the criminal justice system and were not even mandated by the law enforcement directive.

The problem has arisen due to chapter 2 of part 3 of the 2018 Act, which sets out six data protection principles that, as I have mentioned, apply to data processing by competent authorities for law enforcement purposes. Section 35(1) states:

"The first data protection principle is that the processing of personal data for any of the law enforcement purposes must be lawful and fair."

Section 35(2) states:

"The processing of personal data for any of the law enforcement purposes is lawful only if and to the extent that it is based on law and either—

(a) the data subject has given consent to the processing for that purpose, or

(b) the processing is necessary for the performance of a task carried out for that purpose by a competent authority."

The Police Federation has said that it is very unlikely that section 35(2)(a) will apply in this context. It has also said that, in the case of section 35(2)(b), the test of whether the processing is "necessary" is exacting, requiring a competent authority to apply its mind to the proportionality of processing specific items of personal data for the particular law enforcement purpose in question. Under sections 35(3) to (5), where the processing is "sensitive processing", an even more rigorous test applies, requiring among other things that the processing is "strictly necessary" for the law enforcement purpose in question. Section 37 goes on to state:

"The third data protection principle is that personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed."

For the purposes of the 2018 Act, the CPS and each police force are separate competent authorities and separate data controllers. Therefore, as set out in section 34(3), the CPS and each police force must comply with the data protection principles. A transfer of information by a police force to the CPS amounts to the processing of personal data.

The tests of "necessary" and "strictly necessary" under the first data protection principle and the third data protection principle require a competent authority to identify and consider each and every item of personal data contained within information that it is intending to process, and to consider whether it is necessary for that item of personal data to be processed in the manner intended.

The Police Federation has explained that, when the police prepare a case file for submission to the CPS for a charging decision, the practical effect is that they have to spend huge amounts of time and resources on doing so. They go through the information that has been gathered by investigating officers in order to identify every single item of personal data contained in that information; decide whether it is necessary—or, in many cases, strictly necessary—for the CPS to consider each item of personal data when making its charging decision; and redact every item of personal data that does not meet that test.

3.30 pm

Furthermore, the National Police Chiefs' Council and the CPS have produced detailed guidance on the redaction process, which emphasises that the 2018 Act is a legal requirement and that the police and CPS do not have any special relationship that negates the need to redact and protect personal information. The combination of the requirements of the guidance and of the Act represents a huge amount of administrative work for police officers, resulting in hours of preparing appropriate redactions.

Picture the scene: an incident occurs, and 10 police officers go to it. As they arrive, they all turn on their body-worn cams. They speak to different people and view different backgrounds with the cameras. They gather all sorts of different data, CCTV footage, Ring footage—just name it—and have to redact each in real time afterwards. It can take weeks to deal with just one incident. That burden was highlighted in the 2022 annual review of disclosure by the Attorney General's Office, which recorded:

"We have heard evidence, from all members of the justice system but especially the police, that redaction of material for disclosure is placing a significant pressure on resources"

and that one police force had invested £1 million in a disclosure specialist team solely to deal with redaction.

Furthermore, inevitably, such work is carried out by relatively junior officers who have no particular expertise in data protection, and much of it may never even be

used by the CPS if the matter is not charged or the defendant pleads guilty before trial. Nationally, about 25% of cases that are submitted to the CPS are not charged. A significant proportion of that time and money could therefore be saved if the redaction of personal data by the police occurred after, rather than before, a charging decision had been made by the CPS.

That is exactly what my new clause would ensure happened. It inserts a proposed new section into the 2018 Act to exempt the police service and the CPS from complying with the first data protection principle—except in so far as that principle requires processing to be fair—or with the third data protection principle when preparing a case file for submission to the CPS for a charging decision, thereby facilitating the free flow of personal data between the police and the CPS. Where the CPS decides to charge, the case file would be returned to the police to carry out the redaction exercise before there is any risk of the file being disclosed to any person or body other than the CPS. In the 25% of cases where the CPS decides not to charge, the unredacted file would simply be deleted by the CPS.

My new clause would have no obvious disadvantages, as the security of the personal data would not be compromised and the necessary redactions would still be undertaken once a charging decision had been made. Furthermore, there are already provisions in the Bill designed to reduce the burden that part 3 of the 2018 Act imposes on law enforcement bodies. For example, as previously discussed, clause 16 will reduce the burden of the logging obligation in section 62 of the 2018 Act. The impact of those other provisions would be greatly enhanced if my new clause were also included in the Bill.

It is crucial that we do everything we can to ease the administrative burdens on police officers, so that we can free up thousands of policing hours and get police back on to the frontline, supporting communities and tackling crime. My new clause would go a long way to achieving that by facilitating the free flow of personal data between the police and the CPS, which would speed up the criminal justice process and reduce the burden on the taxpayer.

I hope not to have to press the new clause to a vote, and that the Minister will provide some encouragement that the issue will be resolved during progress of the Bill.

Stephanie Peacock: New clause 16 would amend section 40 of the Data Protection Act 2018, allowing police services to share unredacted data with the Crown Prosecution Service when it is making a charging decision. I am incredibly sympathetic to the aim that the hon. Member for Loughborough has set out, which is to get the police fighting crime on the frontline as much as possible. In oral evidence, Aimee Reed, director of data at the Metropolitan police, said that if the police could share information redacted before charging decisions were made, it would be "of considerable benefit". She said that that would

"enable better and easier charging decisions"

and

"reduce the current burden on officers"—[*Official Report, Data Protection and Digital Information (No. 2) Public Bill Committee,* 10 May 2023; c. 58, Q126.]

That would allow them to focus their time on other things. It is therefore good to see that concept being explored in a new clause.

To determine the value of the change, we would like to see a full impact assessment of the potential risks and harms associated with it. I hope that that could be conducted with the intention of weighing the change against the actual cost of the current burden that police face in redacting data. Without such an assessment, it is hard to determine whether the benefit to the police would be proportionate to the impact or harms that might occur as a result of the change, particularly for the subjects of data involved. That is not to say that any change would not be beneficial, but perhaps more detail could be explored with regard to the proposal.

As I believe that this is the final time that I will speak in this Committee, may I say a few words of thanks?

The Chair: I think that you should wait for the next Question.

Stephanie Peacock: Okay, I will wait for the next Question. Thank you for your guidance, Mr Hollobone.

Sir John Whittingdale: I thank my hon. Friend the Member for Loughborough, who has been assiduous in pursuing her point and has set out very clearly the purpose of her new clause. We share her wish to reduce unnecessary burdens on the police as much as possible. The new clause seeks to achieve that in relation to the preparation by police officers of pre-charge files, which is an issue that the National Police Chiefs' Council has raised with the Home Office, as I think she knows.

This is a serious matter for our police forces, which estimate that about four hours is spent redacting a typical case file. They argue that reducing that burden would enable officers to spend more time on frontline policing. We completely understand the frustration that many officers feel about having to spend a huge amount of time on what they see as unnecessary redaction. I can assure my hon. Friend that the Home Office is working with partners in the criminal justice system to find ways of safely reducing the redaction burden while maintaining public trust. It is important that we give them the time to do so.

We need to resolve the issue through an evidence-based solution that will ensure that the right amount of redaction is done at the right point in the process, so as to reduce any delays while maintaining victim and witness confidence in the process. I assure my hon. Friend that her point is very well taken on board and the Government are looking at how we can achieve her objective as quickly as possible, but I hope she will accept that, at this point, it would be sensible to withdraw her new clause.

Jane Hunt: I thank the Minister greatly for what he has said, and for the time and effort that is being put in by several Departments to draw attention to the issue and bring it to a conclusion. I am happy that some progress has been made and, although I reserve my right to bring back the new clause at a later date, I beg to ask leave to withdraw the motion.

Clause, by leave, withdrawn.

The Chair: Hon. Members will be disappointed to hear that we have reached the final Question that I must put to the Committee.

Question proposed, That the Chair do report the Bill, as amended, to the House.

Stephanie Peacock: It has been a real pleasure to represent His Majesty's loyal Opposition in the scrutiny of the Bill. I thank the Minister for his courteous manner, all members of the Committee for their time, the Clerks for their work and the many stakeholders who have contributed their time, input and views. I conclude by thanking Anna Clingan, my senior researcher, who has done a remarkable amount of work to prepare for our scrutiny of this incredibly complex Bill. Finally, I thank you, Mr Hollobone, for the way in which you have chaired the Committee.

Sir John Whittingdale: May I join the hon. Lady in expressing thanks to you, Mr Hollobone, and to Mr Paisley for chairing the Bill Committee so efficiently and getting us to this point ahead of schedule? I thank all members of the Committee for their participation: we have been involved in what will be seen to be a very important piece of legislation.

I am very grateful to the Opposition for their support in principle for many of the objectives of the Bill. It is absolutely right that the Opposition scrutinise the detail, and the hon. Member for Barnsley East and her colleagues have done so very effectively. I am pleased that we have reached this point with the Bill so far unamended, but obviously we will be considering it further on Report.

I thank all my hon. Friends for attending the Committee and for their contributions, particularly saying "Aye" at the appropriate moments, which has allowed us to get to this point. I also thank the officials in the Department for Science, Innovation and Technology. I picked up this baton on day two of my new role covering the maternity leave of my hon. Friend the Member for Hornchurch and Upminster (Julia Lopez); I did so with some trepidation, but the officials have made my task considerably easier and I am hugely indebted to them.

I thank everybody for allowing us to get this point. I look forward to further debate on Report, in due course.

The Chair: May I thank all hon. Members for their forbearance during the passage of the Bill and thank all the officers of the House for their diligence and attention to duty? My one remaining humble observation is that if the day ever comes when a facial recognition algorithm is attached to the cameras in the main Chamber to assess whether Members are bored or not paying attention, we will all be in very big trouble.

Question put and agreed to.

Bill, as amended, accordingly to be reported.

3.41 pm

Committee rose.

Written evidence reported to the House

DPDIB33 Jonathan Sellors MBE, Legal Counsel and Company Secretary, UK Biobank (supplementary submission)

DPDIB34 Marie Curie

DPDIB35 techUK (supplementary submission)

DPDIB36 Information and Records Management Society

DPDIB37 Aviva

DPDIB38 Equality and Human Rights Commission

DPDIB39 TransUnion International UK Limited

DPDIB40 British Medical Association