PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION BILL [*LORDS*]

Second Sitting

Tuesday 13 March 2018

(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 17 March 2018

The Committee consisted of the following Members:

Chairs: †David Hanson, Mr Gary Streeter

† Adams, Nigel *(Lord Commissioner of Her Majesty's Treasury)*
† Atkins, Victoria *(Parliamentary Under-Secretary of State for the Home Department)*
† Byrne, Liam *(Birmingham, Hodge Hill)* (Lab)
† Clark, Colin *(Gordon)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Haigh, Louise *(Sheffield, Heeley)* (Lab)
† Heaton-Jones, Peter *(North Devon)* (Con)
† Huddleston, Nigel *(Mid Worcestershire)* (Con)
† Jack, Mr Alister *(Dumfries and Galloway)* (Con)
† James, Margot *(Minister of State, Department for Digital, Culture, Media and Sport)*
† Jones, Darren *(Bristol North West)* (Lab)
† Lopez, Julia *(Hornchurch and Upminster)* (Con)
† McDonald, Stuart C. *(Cumbernauld, Kilsyth and Kirkintilloch East)* (SNP)
† Murray, Ian *(Edinburgh South)* (Lab)
† O'Hara, Brendan *(Argyll and Bute)* (SNP)
† Snell, Gareth *(Stoke-on-Trent Central)* (Lab/Co-op)
† Warman, Matt *(Boston and Skegness)* (Con)
† Wood, Mike *(Dudley South)* (Con)
† Zeichner, Daniel *(Cambridge)* (Lab)

Kenneth Fox, *Committee Clerk*

† **attended the Committee**

Public Bill Committee

Tuesday 13 March 2018

[Mr David Hanson *in the Chair*]

Data Protection Bill [*Lords*]

Schedule 1

Special categories of personal data and criminal convictions etc data

Amendment proposed (this day): 76, in schedule 1, page 123, line 21, at beginning insert "Except as otherwise provided,".

This amendment is consequential on Amendments 79, 82 and 90.—(Margot James.)

2 pm

Question again proposed, That the amendment be made.

The Chair: I remind the Committee that with this we are discussing Government amendments 77 to 83 and 87 to 91.

Amendment 76 agreed to.

Amendments made: 77, in schedule 1, page 124, line 24, leave out from "subject" to end of line 25.

In paragraph 8 of Schedule 1, sub-paragraph (3) contains an exception from the condition in sub-paragraph (1). This amendment would remove from the exception the requirement that the processing is carried out without the data subject's consent.

Amendment 78, in schedule 1, page 124, line 36, at end insert—

"Racial and ethnic diversity at senior levels of organisations

8A (1) This condition is met if the processing—

(a) is of personal data revealing racial or ethnic origin,

(b) is carried out as part of a process of identifying suitable individuals to hold senior positions in a particular organisation, a type of organisation or organisations generally,

(c) is necessary for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in the organisation or organisations, and

(d) can reasonably be carried out without the consent of the data subject,

subject to the exception in sub-paragraph (3).

(2) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(3) Processing does not meet the condition in sub-paragraph (1) if it is likely to cause substantial damage or substantial distress to an individual.

(4) For the purposes of this paragraph, an individual holds a senior position in an organisation if the individual—

(a) holds a position listed in sub-paragraph (5), or

(b) does not hold such a position but is a senior manager of the organisation.

(5) Those positions are—

(a) a director, secretary or other similar officer of a body corporate;

(b) a member of a limited liability partnership;

(c) a partner in a partnership within the Partnership Act 1890, a limited partnership registered under the Limited Partnerships Act 1907 or an entity of a similar character formed under the law of a country or territory outside the United Kingdom.

(6) In this paragraph, "senior manager", in relation to an organisation, means a person who plays a significant role in—

(a) the making of decisions about how the whole or a substantial part of the organisation's activities are to be managed or organised, or

(b) the actual managing or organising of the whole or a substantial part of those activities.

(7) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.".

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data for the purposes of promoting or maintaining diversity in the racial and ethnic origins of individuals who hold senior positions in organisations.

Amendment 79, in schedule 1, page 125, line 3, at end insert—

"( ) If the processing consists of the disclosure of personal data to a competent authority, or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).".

This amendment, and Amendment 80, provide that where processing falling within paragraph 9 of Part 2 of Schedule 1 (preventing or detecting unlawful acts) consists of, or is carried out in preparation for, the disclosure of personal data to a competent authority, the condition in that paragraph is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 80, in schedule 1, page 125, line 4, at end insert—

""competent authority" has the same meaning as in Part 3 of this Act (see section30).".

See the explanatory statement for Amendment 79.

Amendment 81, in schedule 1, page 125, line 16, at end insert—

"Regulatory requirements relating to unlawful acts and dishonesty etc

10A (1) This condition is met if—

(a) the processing is necessary for the purposes of complying with, or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has—

(i) committed an unlawful act, or

(ii) been involved in dishonesty, malpractice or other seriously improper conduct,

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing, and

(c) the processing is necessary for reasons of substantial public interest.

(2) In this paragraph—

"act" includes a failure to act;

"regulatory requirement" means—

(a) a requirement imposed by legislation or by a person in exercise of a function conferred by legislation, or

(b) a requirement forming part of generally accepted principles of good practice relating to a type of body or an activity.".

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data for the purposes of complying with, or assisting others to comply with, a regulatory requirement.

Amendment 82, in schedule 1, page 125, line 35, at end insert—

"( ) The condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule).".

This amendment provides that the condition in paragraph 11 of Part 2 of Schedule 1 (journalism etc in connection with unlawful acts and dishonesty etc) is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 83, in schedule 1, page 126, line 22, at end insert—

"Support for individuals with a particular disability or medical condition

13A (1) This condition is met if the processing—

(a) is carried out by a not-for-profit body which provides support to individuals with a particular disability or medical condition,

(b) is of a type of personal data falling within sub-paragraph (2) which relates to an individual falling within sub-paragraph (3),

(c) is necessary for the purposes of—

(i) raising awareness of the disability or medical condition, or

(ii) providing support to individuals falling within sub-paragraph (3) or enabling such individuals to provide support to each other,

(d) can reasonably be carried out without the consent of the data subject, and

(e) is necessary for reasons of substantial public interest.

(2) The following types of personal data fall within this sub-paragraph—

(a) personal data revealing racial or ethnic origin;

(b) genetic data or biometric data;

(c) data concerning health;

(d) personal data concerning an individual's sex life or sexual orientation.

(3) An individual falls within this sub-paragraph if the individual is or has been a member of the body mentioned in sub-paragraph (1)(a) and—

(a) has the disability or condition mentioned there, has had that disability or condition or has a significant risk of developing that disability or condition, or

(b) is a relative or carer of an individual who satisfies paragraph (a) of this sub-paragraph.

(4) For the purposes of sub-paragraph (1)(d), processing can reasonably be carried out without the consent of the data subject only where—

(a) the controller cannot reasonably be expected to obtain the consent of the data subject, and

(b) the controller is not aware of the data subject withholding consent.

(5) In this paragraph—

"carer" means an individual who provides or intends to provide care for another individual other than—

(a) under or by virtue of a contract, or

(b) as voluntary work;

"disability" has the same meaning as in the Equality Act 2010 (see section 6 of, and Schedule 1 to, that Act).

(6) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent.".*—(Margot James.)*

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data by not-for-profit bodies involved in supporting individuals with a particular disability or medical condition.

The Parliamentary Under-Secretary of State for the Home Department (Victoria Atkins): I beg to move amendment 84, in schedule 1, page 126, line 27, leave out "a reason" and insert "one of the reasons".

This amendment amends paragraph 14(1)(b) of Schedule 1 for consistency with paragraphs 18(2) and 19(2) of that Schedule.

The Chair: With this it will be convenient to discuss Government amendments 85, 86, 116 and 117.

Victoria Atkins: It is a pleasure to serve under your chairmanship, Mr Hanson. I am pleased to introduce this group of amendments, which relate to data processing for safeguarding purposes. The amendments respond to an issue raised in an amendment tabled by Lord Stevenson on Report in the Lords in December. In response to that amendment, Lord Ashton made it clear that the Government are sympathetic to the points Lord Stevenson raised and undertook to consider the matter further. Amendments 85, 116 and 117 are the result of that consideration.

I am grateful to Lord Stevenson for raising this issue, and for his contribution to what is probably the most important new measure that we intend to introduce to the Data Protection Bill. The amendments will ensure that sensitive data can be processed without consent in certain circumstances for legitimate safeguarding activities that are in the substantial public interest. We have been working across government and with stakeholders in the voluntary and private sectors to ensure that the amendments are fit for purpose and cover the safeguarding activities expected of organisations responsible for children and vulnerable adults.

The Government recognise that statutory guidance and regulator expectations place moral, if not legal, obligations on certain organisations to ensure that measures are in place to safeguard children and vulnerable adults. Amendment 85 covers processing that is necessary for protecting children and vulnerable adults from neglect or physical or mental harm. This addresses the gap in relation to expectations on, for example, sports governing bodies.

The Government have produced cross-agency and cross-governmental guidance called "Working Together to Safeguard Children", which rightly places the responsibility of safeguarding children on all relevant professionals who come into contact with children and families. For example, it creates an expectation that those volunteering at a local sports club will assess the needs of children and, importantly, will take action to protect them from abuse.

Amendment 85 permits the processing of sensitive personal data, which is necessary to safeguard children from physical, emotional, sexual and neglect-based abuse.

[Victoria Atkins]

Amendment 84 makes a consequential drafting change, while amendments 116 and 117 make an analogous change to the regimes in parts 3 and 4 of the Bill. This is aimed at putting beyond doubt a controller's ability to safeguard children and people at risk.

I thought an example might help the Committee to understand why we place such an emphasis on the amendments. An example provided by a sports governing body is that a person may make an allegation or complaint about a volunteer that prompts an investigation. Such investigations can include witness statements, which reference sensitive personal data, including ethnicity, religious or philosophical beliefs, sexual orientation and health data.

In some instances, the incident may not reach a criminal standard. In those cases, the sports body may have no legal basis for keeping the data. Keeping a record allows sports bodies to monitor any escalation in conduct and to respond appropriately. Forcing an organisation to delete this data from its records could allow individuals that we would expect to be kept away from children to remain under the radar and potentially leave children at risk.

Amendment 86 deals with a related issue where processing health data is necessary to protect an individual's economic wellbeing, where that individual has been identified as an individual at economic risk. UK banks have a number of regulatory obligations and expectations which are set out in the Financial Conduct Authority's rules and guidance. In order to meet best practice standards in relation to safeguarding vulnerable customers, banks occasionally need to record health data without the consent of the data subject.

An example was given of a bank which was contacted by a family member who was alerting the bank to an elderly customer suffering from mental health problems who was drawing large sums of money each day from their bank account and giving it away to a young drug addict whom they had befriended. The bank blocked the account while the family sought power of attorney. Again, the amendment seeks to clarify the position and give legal certainty to banks and other organisations where that sort of scenario arises or where, for example, someone suffers from dementia and family members ask banks to take steps to protect that person's financial wellbeing.

The unfortunate reality is that there still exists a great deal of uncertainty under current law about what personal data can be processed for safeguarding purposes. My brief of crime, vulnerability and safeguarding means that all too often—perhaps in the context of domestic abuse—agencies will gather, sadly, to conduct a domestic homicide review and discover that had certain pieces of information been shared more freely, perhaps more action could have been taken by the various agencies and adults and children could have been safeguarded.

These amendments are aimed at tackling these issues. We want to stop the practice whereby some organisations have withheld information from the police and other law enforcement agencies for fear of breaching data protection law and other organisations have been unclear as to whether consent to processing personal data is required in circumstances where consent would not be reasonable or appropriate. The amendments intend to address the uncertainty by providing relevant organisations with a specific processing condition for processing sensitive personal data for safeguarding purposes. I beg to move.

Liam Byrne (Birmingham, Hodge Hill) (Lab): I rise to put on record my thanks to the Minister for listening carefully to my noble Friend Lord Stevenson. There was strong cross-party consensus on these common-sense reforms.

We all know that in our own constituencies there are extraordinary people doing extraordinary things in local groups. They are the life-blood of our communities. Many of them will be worried about the new obligations that come with the general data protection regulation and many of them will take a least-risk approach to meeting the new regulations. Putting in place some common safeguards to ensure that it is possible to keep data that allow us to spot important patterns of behaviour that can lead to appropriate investigations is very sensible and wise. These amendments will therefore be made with cross-party support.

Amendment 84 agreed to.

Amendments made: 85, in schedule 1, page 126, line 38, at end insert—

"Safeguarding of children and of individuals at risk

14A (1) This condition is met if—

(a) the processing is necessary for the purposes of—

(i) protecting an individual from neglect or physical, mental or emotional harm, or

(ii) protecting the physical, mental or emotional well-being of an individual,

(b) the individual is—

(i) aged under 18, or

(ii) aged 18 or over and at risk,

(c) the processing is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) the processing is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) For the purposes of this paragraph, an individual aged 18 or over is "at risk" if the controller has reasonable cause to suspect that the individual—

(a) has needs for care and support,

(b) is experiencing, or at risk of, neglect or physical, mental or emotional harm, and

(c) as a result of those needs is unable to protect himself or herself against the neglect or harm or the risk of it.

(4) In sub-paragraph (1)(a), the reference to the protection of an individual or of the well-being of an individual includes both protection relating to a particular individual and protection relating to a type of individual."

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data which is necessary for the protection of children or of adults at risk. See also Amendments 116 and 117.

Amendment 86, in schedule 1, page 126, line 38, at end insert—

"Safeguarding of economic well-being of certain individuals

14B (1) This condition is met if the processing—

(a) is necessary for the purposes of protecting the economic well-being of an individual at economic risk who is aged 18 or over,

(b) is of data concerning health,

(c) is carried out without the consent of the data subject for one of the reasons listed in sub-paragraph (2), and

(d) is necessary for reasons of substantial public interest.

(2) The reasons mentioned in sub-paragraph (1)(c) are—

(a) in the circumstances, consent to the processing cannot be given by the data subject;

(b) in the circumstances, the controller cannot reasonably be expected to obtain the consent of the data subject to the processing;

(c) the processing must be carried out without the consent of the data subject because obtaining the consent of the data subject would prejudice the provision of the protection mentioned in sub-paragraph (1)(a).

(3) In this paragraph, "individual at economic risk" means an individual who is less able to protect his or her economic well-being by reason of physical or mental injury, illness or disability."*—(Victoria Atkins.)*

Part 2 of Schedule 1 describes types of processing of special categories of personal data which meet the requirement in Article 9(2)(g) of the GDPR (processing necessary for reasons of substantial public interest) for a basis in UK law (see Clause 10(3)). This amendment adds to Part 2 of Schedule 1 certain processing of personal data which is necessary to protect the economic well-being of adults who are less able to protect their economic well-being by reason of a physical or mental injury, illness or disability.

Louise Haigh (Sheffield, Heeley) (Lab): I beg to move amendment 150, page 126, line 38, at end insert—

"Register of missing persons

14A This condition is met if the processing—

(a) is necessary for the establishment or maintenance of any register of missing persons, and

(b) is carried out in a manner which is consistent with any guidance which may be issued by the Secretary of State or by the Commissioner on the processing of data for the purposes of this paragraph."

It is a pleasure to serve under your chairmanship, Mr Hanson. Amendment 150 seeks to provide a similar exemption to the one that the Minister has just laid out. As my right hon. Friend the Member for Birmingham, Hodge Hill said, we completely support the principles behind this exemption to schedule 1. As the Minister made clear, too often serious case reviews or reviews after an incident of this nature, particularly in child protection cases, show clearly that if the data had been shared more effectively—often in health cases—the child could have been protected and their life might have been saved.

We tabled this amendment because of the increase in the number of missing persons and missing children over the past few years. As the shadow Police Minister, I approach this issue from a policing perspective. It is important that all data handlers fully understand their obligations and the powers that are bestowed on them. Too often, under the existing legislation, they hide behind data protection to avoid sharing data, and we fear that that tendency will become even stronger under the Bill.

Sharing data relating to missing persons is important for a number of reasons. The demand on police services from such cases has rocketed over the past few years. Police officers spend only 17% of their time responding to crime, so 83% of police time is spent responding to non-crime demand. That includes mental health call-outs, but largely it relates to missing persons. Some police forces tell me that missing persons place the greatest demand on their time.

In the west midlands, since 2015 the number of missing person incidents has doubled to nearly 13,000 cases a year. In Northumbria—one of the smallest police forces in the country—as of this minute there are 43 men and 20 women missing. For such a small police force, that is a significant number of people to be out looking for. Last year alone, such investigations cost the police service more than £600 million. One fifth of those missing persons are children in care, more than 50% are children, and a significant proportion are elderly people missing from care. Crucially, about one third are reported missing on more than one occasion. It is those individuals we seek to address with the register.

There are various reasons for the increase, one of which is certainly better police reporting. Our ageing population means that more people are in care and are going missing from care. The police have responded to that issue in various ways, including by tagging elderly individuals who go missing from care repeatedly —we have tabled amendments to explore the issues arising from that. Cuts to other public services mean that the increasing demand, which previously would have fallen elsewhere—in particular, on local authorities—is now landing on the police. We are seeing a higher tolerance of risk across the care sector, and possibly the health sector too, and a tendency to pass the buck for these issues and other vulnerabilities on to the police, who have a very low risk threshold and nowhere to pass them on.

I believe we need a review of all agencies that are involved with safeguarding to ensure that they are taking seriously their responsibilities in this regard. When the issue relates to resources, they must make the case for those resources, rather than merely pass the problem on to the police. I have heard stories about private children's care homes where staff may see that the child is outside their window or down the street, but because they are five minutes over curfew they ring the police and say that the child is missing. That passes on the responsibility, but has very serious implications for the police. It diverts resources from tackling crime and from responding to genuine cases of missing children and high-risk missing persons.

Estimates of the time associated with this activity suggest that approximately 18 hours of police time is needed for a medium-risk missing persons investigation. In 2015-16, that equated to more than 6 million investigation hours, or more than 150,000 officers occupied full time with that activity. Not being dealt with by the appropriate agency and not being responded to correctly has real implications for the individual. Going missing can be a precursor to various aspects of significant harm, such as abuse, exposure to criminal activity and mental ill-health. There are enough issues relating to police forces sharing data among themselves, let alone with other agencies. As a result, various criminal activities exploiting those weaknesses have developed. In the past, the Minister and I have discussed county lines at length, which is a criminal activity whereby organised criminal gangs exploit children. They take them, internally traffick them across the country, set them up in another vulnerable adult's

[Louise Haigh]

home and leave them to deal drugs on their behalf. That is a very profitable criminal activity, but the perpetrators have been able to evade real enforcement because of the weaknesses in data sharing and cross-agency working between police forces and agencies. The amendment will ensure that the police and all appropriate safeguarding agencies have access to the relevant data to ensure that at-risk missing people are found as quickly and safely as possible, and have their needs dealt with in the most appropriate way.

2.15 pm

I know that the Government are supportive of that idea and proposal. In their "Tackling child sexual exploitation: progress report" they recognise the need to improve the early identification of and initial response to children and young people at risk. They have committed to extend their programme of work into child safeguarding, and a key deliverable was the development of a national missing persons register. This amendment seeks to probe the Government about the establishment of that register, and about the information that it should include.

We believe—the Children's Society has made representations on this—that if designed well, key information and intelligence could be stored in one place, making the sharing of vital information about missing people in real time possible across different local areas. The information available should include previously identified risks, where people go missing from and to, and who they go missing with. Furthermore, the register should include provision for local authorities or return-home interview service providers commissioned by local authorities to input and store relevant information from those interviews, to inform risk assessment and local intelligence on missing children.

In 2016, Her Majesty's Inspectorate of Constabulary found serious inconsistencies between and within forces regarding data sharing and responding to missing children and high-risk missing adults. This issue has been highlighted by the inspectorate, and I am sure that the Minister understands the urgency of getting such a register in place. The case for the amendment is clear: it supports principles that have been outlined by the Government, and it would support our most vulnerable people and go some way towards relieving pressure on the police when responding to those high-risk missing individuals.

Victoria Atkins: I am grateful to the hon. Member for Sheffield, Heeley for affording me the opportunity to update the Committee on our progress in establishing a national register of missing persons, and to touch on the missing children and adults strategy that the Government are currently working on, which I hope will be published shortly. It will address many of the themes that the hon. Lady drew on in her speech, particularly the deliberate targeting of vulnerable children by county lines gangs, children who go missing—usually, sadly, from care homes—and the exploitation that occurs.

As the hon. Lady said, this is an important subject because each year more than 337,000 calls are made to police stations in England and Wales about missing and absent people. Happily, the vast majority are found within 24 hours, but 2% or thereabouts remain missing for more than a week. Anyone who has ever met the parents of children who go missing knows the heartache that those parents face, not just on an annual basis, but on a daily, minute-by-minute basis. They feel that pain constantly.

People who go missing are often the most vulnerable in society, and it is vital that those tasked with investigating their disappearance have the most accurate and up-to-date information available. We accept that the current technology available to frontline staff to deal with missing persons is insufficient. For example, the police national computer identifies only those currently reported as missing, while the National Crime Agency database includes only those missing for more than 72 hours. We know that the search must start the moment that a child or vulnerable person is identified as missing; we cannot wait for 72 hours. There is no national record of the history of missing persons in England and Wales.

The Government's "Tackling child sexual exploitation: progress report" published in February last year set out our commitment to deliver a national missing persons register. This will enable police officers to access up-to-date data about missing people across force boundaries and take appropriate action when they investigate missing person incidents or encounter a missing person who is away from his or her home force area. The register is being established as part of the national law enforcement data programme, which will replace the police national computer and the police national database with a new national data service. The current timetable, agreed with the police, is to launch the capability for forces to record manually missing and associated found incidents from mid-2019 with releases thereafter, including automation and establishing the ability to share controlled information beyond policing to other agencies.

In terms of the way in which the register and the scheme interplay in the Bill, the processing of the personal data held on the database will take place under either the GDPR or part 3 of the Bill. Processing of the data by the police will often be for a law enforcement purpose, including the prevention, investigation or detection of a criminal offence and any sensitive processing would fall within paragraph 3 of schedule 8, which enables processing where necessary to protect the vital interests of the data subject or another individual, or under the new safeguarding condition, which we have just debated. Where the processing is undertaken under the GDPR, the conditions in respect of protecting the vital interests of the data subject, or preventing or detecting unlawful acts, may apply. Again, the new safeguarding condition may also be applicable.

Given those provisions and the very clear timetable that the Government and police have for their programme, we are of the view that the amendment is unnecessary, but I am, of course, very appreciative that the hon. Lady has raised this in the Committee. Obviously, I will keep her informed of progress on the new register.

Louise Haigh: That is fantastic news. It is a very ambitious deadline for a police IT transformation programme. I know that South Yorkshire is going through the transformation on the CONNECT programme at the moment; it is woefully behind the timescale envisaged and over budget, as every IT transformation in the history of any Government, of any colour, has always been. I wonder, therefore, given the urgency of this issue, whether it is possible for this information to be recorded on the PNC for the time being.

Victoria Atkins: I am looking at my officials and they will stop me if I am wrong, I hope. If she prefers, may I write to her? I do not think that the PNC has the capability at the moment. That is why we are having to develop this new programme, but we will write to the hon. Lady in any event. As I say, I will keep her up to date with progress. But I invite her to withdraw the amendment, please.

Louise Haigh: Given that the Minister asked so nicely, I will. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Amendments made: 87, in schedule 1, page 127, line 30, at end insert—

"( ) The reference in sub-paragraph (4)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent."

This amendment clarifies the intended effect of the safeguard in paragraph 15(4) of Schedule 1 (processing necessary for an insurance purpose).

Amendment 88, in schedule 1, page 127, line 39, at end insert—

"( ) is of data concerning health which relates to a data subject who is the parent, grandparent, great-grandparent or sibling of a member of the scheme,".

This amendment provides that the condition in paragraph 16 of Schedule 1 (occupational pension schemes) can only be relied on in connection with the processing of data concerning health relating to certain relatives of a member of the scheme.

Amendment 89, in schedule 1, page 128, line 6, at end insert—

"( ) The reference in sub-paragraph (2)(b) to a data subject withholding consent does not include a data subject merely failing to respond to a request for consent."

This amendment clarifies the intended effect of the safeguard in paragraph 16(2) of Schedule 1 (processing necessary for determinations in connection with occupational pension schemes).

Amendment 90, in schedule 1, page 131, line 14, at end insert—

"( ) If the processing consists of the disclosure of personal data to a body or association described in sub-paragraph (1)(a), or is carried out in preparation for such disclosure, the condition in sub-paragraph (1) is met even if, when the processing is carried out, the controller does not have an appropriate policy document in place (see paragraph 5 of this Schedule)."

This amendment provides that when processing consists of the disclosure of personal data to a body or association that is responsible for eliminating doping in sport, or is carried out in preparation for such disclosure, the condition in paragraph 22 of Part 2 of Schedule 1 (anti-doping in sport) is met even if the controller does not have an appropriate policy document in place when the processing is carried out.

Amendment 91, in schedule 1, page 133, line 17, leave out from "interest" to end of line 21.—*(Margot James.)*

This amendment removes provisions from paragraph 31 of Schedule 1 (extension of conditions in Part 2 of Schedule 1 referring to substantial public interest) which are unnecessary because they impose requirements which are already imposed by paragraph 5 of Schedule 1.

The Minister of State, Department for Digital, Culture, Media and Sport (Margot James): I beg to move amendment 92, page 134, line 18 [Schedule 1], leave out "on the day" and insert "when".

This amendment is consequential on Amendment 71.

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

Government amendments 107, 108, 111, 113, 114, 21, 29 to 40, 43 to 46, 118 to 121, 48, 49, 53, 55, 56, 123 to 125, 59 and 71.

Margot James: Following engagement with local government stakeholders, we have recognised that the maximum time period permitted for responses to the subject access request set out in parts 3 and 4 of the Data Protection Bill subtly differs from that permitted under the GDPR and part 2 of the Bill. That is because the GDPR and, by extension, part 2 rely on European rules for calculating time periods, whereas parts 3 and 4 implicitly rely on a more usual domestic approach. European law, which applies to requests under part 2, says that when one is considering a time period in days, the day on which the request is received is discounted from the calculation of that time period. In contrast, the usual position under UK law, which applies to requests under parts 3 and 4 of the Bill, is that that same seven-day period to respond would begin on the day on which the request was received. In a data protection context, that has the effect of providing those controllers responding to requests under parts 3 and 4 with a time period that is one day shorter in which to respond.

To provide consistency across the Bill, we have decided to include a Bill-wide provision that applies the European approach to all time periods throughout the Bill, thus ensuring consistency with the directly applicable GDPR. Having a uniform approach to time periods is particularly helpful for bodies with law enforcement functions, which will process personal data under different regimes under the Bill. Without these amendments, different time periods would apply, depending on which regime they were processing under. Ensuring consistency for calculating time periods will also assist the information commissioner with her investigatory activities and enforcement powers, for example by avoiding the confusion and potential disputes that could arise relating to her notices or requests for information.

Amendment 71 provides for a number of exemptions to the European approach where deviating from our standard approach to time periods would be inappropriate. For example, where the time period refers to the process of parliamentary approval of secondary legislation, it would clearly not be appropriate to deviate from usual parliamentary time periods. The unfortunate number of amendments in this group comes from the need to modify existing language on time periods, currently worded for compliance with the usual UK approach, so that it applies the approach of the EU rules instead. I hope that this has provided the Committee with sufficient detail on the reasons for tabling this group of amendments.

Amendment 92 agreed to.

Question proposed, That the schedule, as amended, be the First schedule to the Bill.

Liam Byrne: We had a useful debate this morning about the whys and wherefores of whether the article 8 right to privacy should be incorporated into the Bill. Although we were disappointed by the Minister's reply, what I thought was useful in the remarks she made was a general appreciation of the importance of strong data rights if the UK is to become a country with a strong environment of trust within which a world of digital trade can flourish.

I will briefly alert the Minister to a debate we want to have on Report. The reality is that we feel schedule 1 is

[Liam Byrne]

narrowly drawn. It is an opportunity that has been missed, and it is an opportunity for the Minister to come back on Report with a much more ambitious set of data rights for what will be a digital century. When we look around the world at the most advanced digital societies, we can see that a strong regime of data rights is common to them all.

I was recently in Estonia, which I hope the Minister will have a chance to visit if she has not done so already. Estonia likes to boast of its record as the world's most advanced digital society; it is a place where 99% of prescriptions are issued online, 95% of taxes are paid online and indeed a third of votes are cast online. It is a country where the free and open right to internet access is seen as an important social good, and a good example of a country that has really embraced the digital revolution and translated that ambition into a set of strong rights.

The Government are not averse to signing declaratory statements of rights that they then interpret into law. They are a signatory to the UN universal declaration of human rights and the UN convention on the rights of the child; the Human Rights Act 1998 is still in force—I have not yet heard of plans to repeal it—and of course the Equality Act 2010 was passed with cross-party support. However, those old statements of rights, which date back to 1215, were basically to correct and guard against dangerous imbalances of power. Things have moved on since 1215 and the worries that the barons had about King John. We are no longer as concerned as people were in 1215 about taking all the fish weirs out of the Thames, for example.

2.30 pm

The reality today is that we are not worried about the unchecked powers of sovereigns, but we are more and more concerned about the power of big tech companies. As of last Friday, the fearsome five data giants had a combined market capitalisation of about $2.4 trillion. They are very, very powerful players. They capture data from us and process it in a way that we do not really understand, with effects that we do not really appreciate. The Government have nodded towards that concern with the idea of setting up a digital charter, which is very much from the cones hotline school of public service reform. The problem with a digital charter is that it will contain vague commitments associated with vague frameworks, without much legislative bite. We think the Government can do much better.

Of course, that is brought into focus most sharply with regard to children. Children are not a marginal issue in this debate; they are about a third of internet users. We were grateful that the Government acquiesced in amendments moved by Baroness Kidron. She is one of the architects of the 5Rights movement, which says that children should have the right to remove content they do not want to be online anymore; the right to know who is targeting them and for what purposes; the right to safety and support, because children are often upset or abused online; the right to informed and conscious use, and the right to digital literacy. The 5Rights movement has helpfully set out those good, strong digital rights for children, but we urge the Government to build on the basic charter of digital rights in schedule 1 and go much further.

The amendments we tabled that were not selected for debate—we hope we will be able to come back to them at a later stage—include the following. One relates to the right to equality of access: every data subject should have the right to access and participate in the digital environment on equal terms, and internet access should be open and free. Another is about equality of treatment: every data subject should have the right to fair and equal treatment in the processing of his or her personal data, in a way that is encompassed by many amendments to the Bill. A third relates to security: every data subject should have the right to security and protection of their personal data and information systems, and Governments should not misuse their ability to access that information without checks and safeguards.

There should be rights to free expression through data, to privacy and to ownership of data. Every data subject should have the right to own and control their personal data and therefore should be entitled to a proportionate share of the income or other benefit derived from it. Every data subject should have the right to transparent and equal treatment in the processing of their personal data by an algorithm or an automated system. Every data subject should have the right to deploy their personal data to communicate, in pursuit of their fundamental right to freedom of association. There should be strong rights to protection online, and to remove data.

We think that a more ambitious and assertive schedule 1 could be the foundation of a strong digital Bill of Rights for the 21st century, which would go some way to creating a stronger environment of trust online. Trust is breaking down, because cyber-crime is multiplying, because public services such as the NHS have shown their vulnerability to cyber-attacks and because of the proliferation of fake news. There is wide appreciation that our children in particular are vulnerable, and I am afraid there is concern that the Government hitherto have been too reluctant to act.

Although the digital charter takes the debate on somewhat, we would encourage the Government, in the best traditions of this country and in the best tradition of our contribution to the debate about strong rights, to be more assertive and more ambitious in schedule 1 and to accommodate the amendments we will table on Report.

The Chair: To make matters clear to hon. Members and in particular those who are new to the Committee, the right hon. Member for Birmingham, Hodge Hill tabled a number of amendments—171 to 175 and 177 to 178—that were not selected because they were tabled only yesterday. We need to have several days' notice before selection can be considered. Had they been tabled earlier, we could have debated and voted on those amendments now. I have given the right hon. Gentleman leeway to widen his arguments about schedule 1, and it is up to him whether he wishes to table those amendments on Report. He is perfectly in order to do so. The debate today is on schedule 1, and the points that the right hon. Gentleman has made in relation to potential amendments are a heads-up for the future or for the Minister to respond to at this point.

Margot James: The right hon. Member for Birmingham, Hodge Hill covered a lot of important ground. He mentioned the digital charter. We are bringing forward the digital charter and we do not intend for it to be set

in stone. We recognise that this is a fast-changing environment and so it is deliberately something that will evolve over time. We both share the concerns that he expressed with regard to fake news and the rights and protections needed for children and young people who, as he says, make up a third of internet users. We will address many of the things he highlighted as part of our internet safety strategy, and I look forward to debating them further with him on Report.

To add to what we have already discussed under schedule 1, article 9 of the GDPR limits the processing of special categories of data. Those special categories are listed in article 9(1) and include personal data revealing racial or ethnic origin, health, political opinions and religious beliefs. Some of the circumstances in which article 9 says that special category data can be processed have direct effect, but others require the UK to make related provision.

Clause 10 introduces schedule 1 to the Bill, which sets out in detail how the Bill intends to use the derogations in article 9 and the derogation in article 10 relating to criminal convictions data to permit particular processing activities. To ensure that the Bill is future-proof, clause 10 includes a delegated power to update schedule 1 using secondary legislation. Many of the conditions substantively replicate existing processing conditions in the 1998 Act and hon. Members may wish to refer to annexe B to the explanatory notes for a more detailed analysis on that point.

Darren Jones: I want to make one point about schedule 1. Amendment 9, which was made this morning, allows democratic engagement to be a purpose under article 6(1)(e) of the GDPR—namely, that consent is not required for the processing of data for public interest or the exercising of official authority and the purposes of democratic engagement. I wonder whether the definitions of political parties and politicians under schedule 1 could be used to restrict that amendment, so that organisations other than political parties and politicians are not able to process data in the public interest for democratic engagement without consent. For example, if Leave.EU or Open Britain wanted to process our personal data, they ought to do so with consent, not using the same public interest for democratic engagement purposes as politicians or parties.

Margot James: I understand the hon. Gentleman's concerns. The GDPR requires data controls to have a legal basis laid down in law, which can take the form, for example, of a statutory power or duty, or a common-law power. Any organisation that does not have such legal basis would have to rely on one of the other processing conditions in article 6. With regard to the amendment that was agreed to this morning, we think that further restricting clause 8 might risk excluding bodies with a lawful basis for processing. However, the hon. Gentleman is free to raise the issue again on Report.

Question put and agreed to.

Schedule 1, as amended, accordingly agreed to.

Clauses 11 to 13 ordered to stand part of the Bill.

Clause 14

Automated decision-making authorised by law: safeguards

Liam Byrne: I beg to move amendment 153, in clause 14, page 7, line 30, at end insert—

"(1A) A decision that engages an individual's rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests)."

This amendment would clarify that the exemption from prohibition on taking significant decisions based solely on automated processing must apply to purely automated decisions that engage an individual's human rights.

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

Amendment 130, in clause 14, page 7, line 34, at end insert—

"(2A) A decision that engages an individual's rights under the Human Rights Act 1998 does not fall within Article 22(2)(b) of the GDPR (exception from prohibition on taking significant decisions based solely on automated processing for decisions that are authorised by law and subject to safeguards for the data subject's rights, freedoms and legitimate interests).

(2B) A decision is "based solely on automated processing" for the purposes of this section if, in relation to a data subject, there is no meaningful input by a natural person in the decision-making process."

This amendment would ensure that where human rights are engaged by automated decisions these are human decisions and provides clarification that purely administrative human approval of an automated decision does make an automated decision a 'human' one.

Amendment 133, in clause 50, page 30, line 5, at end insert ", and

(c) it does not engage the rights of the data subject under the Human Rights Act 1998."

This amendment would ensure that automated decisions should not be authorised by law if they engage an individual's human rights.

Amendment 135, in clause 96, page 56, line 8, after "law" insert

"unless the decision engages an individual's rights under the Human Rights Act 1998".

Liam Byrne: The amendments touch on what I am afraid will become an increasing part of our lives in the years to come: the questions of what decisions can be taken by algorithms; where such decisions are taken, what rights we have to some kind of safeguards, such as a good old-fashioned human being looking over the decision that is taken and the outcomes that arise; and whether we are content to acquiesce in the rule of the robots.

In a number of areas of our lives—particularly our economic and social lives—such algorithms will become more and more important. Algorithms are already used to screen job applications, for example, and to create shortlists of candidates for interview. Insurance companies use them to adjudge what premiums someone should enjoy, or whether they should be offered insurance at all. The challenge of algorithms was put best by my hon. Friend the Member for Cambridge on Second Reading: the great risk of such developments is that old injustice is hard-coded into new injustice.

That is particularly troubling when we think about the provisions and exemptions the Government have brought forward that allow the automatic processing of data in public services. Many public servants around the world are beginning to look at predictive public services and how algorithms can scan great swathes of, for example, health data and crime data, and make decisions about where police should attend, who should or should not get bail, who should be added to police

[Liam Byrne]

databases such as the gangs matrix, and how healthcare should be targeted in parts of the country or to what kinds of families. There are great risks in algorithms taking decisions in ways ungoverned by us. As parliamentarians, we have a particular duty to ensure that the appropriate safeguards are in place.

Clauses 14 and 15 allow automated processes where they are authorised by law. That creates the obligation of giving notice and what is, in effect, an ex post facto right of appeal. The Opposition's argument is somewhat different: it is better not to take decisions on the basis of automatic processing of data where those decisions affect our human rights.

They say that to err is human, but to really mess things up you need a computer. We all know from our casework, whether about the benefits or the social care system or any other kind of system that constituents might name, that sometimes the most terrible, egregious errors are made. We also know that sometimes it is very difficult for citizens to seek remedies for those problems. Very often, the reason they have come to see us in our surgeries is because, as they so often say to us, we are the last port of call and the last hope that is kicking around; if we cannot fix it, frankly, our constituent is about to give up. That is an unfortunate situation that we do not want to see multiply.

2.45 pm

The great risk with automatic processing of data and the use of algorithms, whether in the public or private sector, where there is an ex post facto right of review, is that our surgeries end up as the final court of appeal. It will then fall to us to intervene either with the company or indeed with the public agency to say, "Look, this has been really fouled up. I'm sorry, but either the data that went into the algorithm is wrong, or the conduct of the algorithm is wrong." We think it would be better if we stopped the potential for that snowballing of problems in future by stopping the ability of algorithms to take decisions where human rights are engaged.

The Minister may say that there are lots of nice safeguards in the Bill, such as that it is permitted only where it is authorised by law. Frankly, that is a hopeless safeguard, particularly when it comes to policing, because the police are authorised to do so much by law. The police can stop people, search people and put through procedures that would deny people bail. The police can add people to databases. If those decisions are taken by an algorithm, all sorts of problems will arise. We think that there should be much stronger safeguards.

Through the amendments, basically we want to try to separate the business of automatic data processing from the possibilities of automatic decision taking. It is fine for data to be processed using algorithms in a way that is automated, but not for decision taking to be automated. We want to leave unfettered the rights of businesses and the Government to process data in an automatic way, but we want fetters around the business of decision taking. It is okay to use algorithms to inform decisions but not to take decisions. The idea of a post hoc review, as many of us know from our own casework, is a nice idea that is not a reality open to many citizens in this country. There is no substitute for preventing a decision being wrong in the first place.

This debate will grow over the years to come. We hope that the Government can take the opportunity now to incorporate some fairly common-sense safeguards into the Bill, because none of us on this Committee wants old injustices to be hard-coded into new injustices. That is the risk that the Bill is running.

Brendan O'Hara (Argyll and Bute) (SNP): I will speak to amendments 130, 133 and 135, which appear in my name and that of my hon. Friend the Member for Cumbernauld, Kilsyth and Kirkintilloch East. Our amendments seek to provide protection for individuals who are subject to purely automated decision making, specifically where we believe that it could have an adverse impact on their fundamental rights. The amendments would require that where human rights are or possibly could be impacted by automated decisions, ultimately there are always human decision makers. The amendments would instil that vital protection of human rights with regard to the general processing of personal data.

The amendments seek to clarify the meaning of a decision that is based solely on automated processing, which is a decision that lacks meaningful human input. That reflects the intent of the GDPR, and provides clarification that purely administrative human approval of an automated decision does not make that decision a human one. It is simply not enough for human beings to process the information in a purely administrative fashion, but to have absolutely no oversight or accountability for the decision that they process. We strongly believe that automated decision making without human intervention should be subject to strict limitations to ensure fairness, transparency and accountability, and to safeguard against discrimination. As it stands, there are insufficient safeguards in the Bill.

As the right hon. Member for Birmingham, Hodge Hill said, we are not talking about every automated decision. We are not talking about a tech company or an online retailer that suggests alternatives that someone may like based on the last book they bought or the last song they downloaded. It is about decisions that can be made without human oversight that will or may well have long-term, serious consequences on an individual's health, financial status, employment or legal status. All too often, I fear that automated decisions involve an opaque, unaccountable process that uses algorithms that are neither as benign nor as objective as we had hoped they would be, or indeed, as we thought they were when we first encountered them.

We are particularly concerned about elements of the Bill that allow law enforcement agencies to make purely automated decisions. That is fraught with danger and at odds with the Data Protection Act 1998, as well as article 22 of the GDPR, which states:

> "The data subject shall have the right not to be subject to a decision based solely on automated processing".

Although there are provisions in the GDPR for EU member states to opt out of that, the opt-out does not apply if the data subject's rights, freedoms or legitimate interests are undermined.

I urge the Government to look again at the parts of the Bill about automated decision making, to ensure that when it is carried out, a human being will have to decide whether it is reasonable and appropriate to continue on that course. That human intervention will provide

transparency and capability, and it will ensure that the state does not infringe on an individual's freedoms—those fundamental rights of liberty and privacy—which are often subjective. Because they are subjective, they are beyond the scope of an algorithm.

There are serious human rights, accountability and transparency issues around fully automated decision making as the Bill stands. Amendment 130 says that any human involvement has to be "meaningful". We define meaningful human oversight as being significant, of consequence and purposeful. As I have said, that is far beyond the scope of an algorithm. If an individual's rights are to be scrutinised and possibly fundamentally affected, it is an issue of basic fairness that the decision is made, or at least overseen, by a sentient being. I hope the Government accept the amendments in the faith in which they were tabled.

Margot James: The amendments relate to automated decision making under the GDPR and the Bill. It is a broad category, which includes everything from trivial things such as music playlists, as mentioned by the hon. Member for Argyll and Bute, and quotes for home insurance, to the potentially more serious issues outlined by the right hon. Member for Birmingham, Hodge Hill of recruitment, healthcare and policing cases where existing prejudices could be reinforced. We are establishing a centre, the office for artificial intelligence and data ethics, and are mindful of these important issues. We certainly do not dismiss them whatsoever.

Article 22 of the GDPR provides a right not to be subject to a decision based solely on automatic processing of data that results in legal or similarly significant effects on the data subject. As is set out in article 22(2)(b), that right does not apply if the decision is authorised by law, so long as the data subject's rights, freedoms and legitimate interests are safeguarded.

The right hon. Member for Birmingham, Hodge Hill, mentioned those safeguards, but I attribute far greater meaning to them than he implied in his speech. The safeguards embed transparency, accountability and a right to request that the decision be retaken, and for the data subject to be notified should a decision be made solely through artificial intelligence.

Liam Byrne: The Minister must realise that she is risking an explosion in the number of decisions that have to be taken to Government agencies or private sector companies for review. The justice system is already under tremendous pressure. The tribunal system is already at breaking point. The idea that we overload it is pretty optimistic. On facial recognition at public events, for example, it would be possible under the provisions that she is proposing for the police to use facial recognition technology automatically to process those decisions and, through a computer, to have spot interventions ordered to police on the ground. The only way to stop that would be to have an ex post facto review, but that would be an enormous task.

Margot James: The right hon. Gentleman should be aware that just because something is possible, it does not mean that it is automatically translated into use. His example of facial recognition and what the police could do with that technology would be subject to controls within the police and to scrutiny from outside.

Louise Haigh: The case that my right hon. Friend raises is certainly not hypothetical. The Metropolitan police have been trialling facial recognition scanning at the Notting Hill carnival for the last three years with apparently no legal base and very little oversight. We will move on to those issues in the Bill. That is exactly why the amendments are crucial in holding law enforcement agencies to account.

Margot James: As the hon. Lady says, the police are trialling those things. I rest my case—they have not put them into widespread practice as yet.

Returning to the GDPR, we have translated the GDPR protections into law through the Bill. As I said, the data subject has the right to request that the decision be retaken with the involvement of a sentient individual. That will dovetail with other requirements. By contrast, the amendments are designed to prevent any automated decision-making from being undertaken under article 22(2)(b) if it engages the rights of the data subject under the Human Rights Act 1998.

Liam Byrne: Will the Minister explain to the Committee how a decision to stop and search based on an automated decision can be retaken? Once the person has been stopped and searched, how can that activity be undone?

Margot James: I am not going to get into too much detail. The hon. Member for Sheffield, Heeley mentioned an area and I said that it was just a trial. She said that facial recognition was being piloted. I do not dispute that certain things cannot be undone. Similar amendments were tabled in the other place. As my noble Friend Lord Ashton said there, they would have meant that practically all automated decisions under the relevant sections were prohibited, since it would be possible to argue that any decision based on automatic decision making at the very least engaged the data subject's right to have their private life respected under article 8 of the European convention on human rights, even if it was entirely lawful under the Act.

3 pm

Amendment 130 also seeks to clarify what is meant by a decision

"based solely on automated processing"

to ensure that human intervention must be meaningful. We consider the amendment unnecessary, as the phrase, especially when read with recital 71 of the GDPR, already provides for this. As my noble Friend Lord Ashton stated in the other place,

"mere human presence or incidental human involvement is not sufficient"—[*Official Report, House of Lords,* 13 December 2017; Vol. 787, c. 1581.]

to change the basis of a decision. I am very happy to put that on the record once more. However, even if it were not the case, we could not go around altering definitions under the GDPR; it is not in our gift to do so.

Liam Byrne: I fear that the Minister is taking some pretty serious gambles on the application of this technology in the future. We think it is the business of this place to ensure that our citizens have strong safeguards, so we will put the amendment to a vote.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 3]

AYES

Byrne, rh Liam	Murray, Ian
Elmore, Chris	O'Hara, Brendan
Haigh, Louise	Snell, Gareth
Jones, Darren	Zeichner, Daniel
McDonald, Stuart C.	

NOES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

Question accordingly negatived.

The Chair: Does the hon. Member for Argyll and Bute wish to press amendment 130 to a Division?

Brendan O'Hara: I would like to press the amendment to a vote, or should I do that on Report?

The Chair: The hon. Gentleman can press the amendment to a vote now. If it is carried, it will be part of the Bill. If it is defeated, it will not be, and it may then be moved on Report, subject to the Speaker's discretion. If the hon. Gentleman does not press the amendment now, it may be that there is more of a likelihood of its being picked on Report, but that is a matter for the Speaker.

Brendan O'Hara: In that case, I will not press the amendment now.

Margot James: I beg to move Government amendment 10, in clause 14, page 8, line 4, leave out "21 days" and insert "1 month".

Clause 14(4)(b) provides that where a controller notifies a data subject under Clause 14(4)(a) that the controller has taken a "qualifying significant decision" in relation to the data subject based solely on automated processing, the data subject has 21 days to request the controller to reconsider or take a new decision not based solely on automated processing. This amendment extends that period to one month.

The Chair: With this it will be convenient to discuss Government amendments 11, 12, 23, 24, 27, 28, 41 and 42.

Margot James: Amendments 10, 11 and 12 relate to clause 14, which requires a data controller to notify a data subject of a decision based solely on automatic processing as soon as is reasonably practicable. The data subject may then request that the data controller reconsider such a decision and take a new decision not based solely on automated processing.

The purpose of the amendments is to bring clause 14 into alignment with the directly applicable time limits in article 12 of the GDPR, thereby ensuring that both data subjects and data controllers have easily understandable rights and obligations. Those include giving the data subject longer to request that a decision be reconsidered, requiring that the controller action the request without undue delay and permitting an extension of up to two months where necessary.

Furthermore, to ensure that there is consistency across the different regimes in the Bill—not just between the Bill and the GDPR—amendments 23, 24, 41 and 42 extend the time limit provisions for making and responding to requests in the other regimes in the Bill. That is for the simple reason that it would not be right to have a data protection framework that applies one set of time limits to one request and a different set of time limits to another.

In a similar vein, amendments 27 and 28 amend part 3 of the Bill, concerning law enforcement processing, to ensure that controllers can charge for manifestly unfounded or excessive requests for retaking a decision, as is permitted under article 12 of the law enforcement directive. To prevent abuse, amendment 28 provides that it is for the controller to be able to show that the request was manifestly unfounded or excessive.

Liam Byrne: It would be useful if the Minister could say a little more about the safeguards around the controllers charging reasonable fees for dealing with requests.

It is quite easy to envisage situations where algorithms take decisions. We have some ex post facto review; a citizen seeks to overturn the decision; the citizen thinks they are acting reasonably but the commercial interest of the company that has taken and automated the decision means that it wants to create disincentives for that rigmarole to unfold. That creates the risk of unequal access to justice in these decisions.

If the Minister is not prepared to countenance the sensible safeguards that we have proposed, she must say how she will guard against another threat to access to justice.

Margot James: The right hon. Gentleman asks a reasonable question. I did not mention that data subjects have the right of complaint to the Information Commissioner if the provisions are being abused. I also did not mention another important safeguard, which is that it is for the data controller to show that the request is manifestly unfounded or excessive. So the burden of proof is on the data controller and the data subject has the right of involving the Information Commissioner, if he or she contests the judgment taken in this context, concerning unfounded or excessive requests in the opinion of the data controller. I hope that satisfies the right hon. Gentleman.

Amendment 10 agreed to.

Amendments made: 11, in clause 14, page 8, leave out line 10 and insert "within the period described in Article 12(3) of the GDPR—"

This amendment removes provision from Clause 14(5) dealing with the time by which a controller has to respond to a data subject's request under Clause 14(4)(b) and replaces it with a requirement for the controller to respond within the time periods set out in Article 12(3) of the GDPR, which is directly applicable.

Amendment 12, in clause 14, page 8, line 16, at end insert—

'(5A) In connection with this section, a controller has the powers and obligations under Article 12 of the GDPR (transparency, procedure for extending time for acting on request, fees, manifestly unfounded or excessive requests etc) that apply in connection with Article 22 of the GDPR." *—(Margot James.)*

This amendment inserts a signpost to Article 12 of the GDPR which is directly applicable and which confers powers and places obligations on controllers to whom Clause 14 applies.

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

Clause 15

EXEMPTIONS ETC.

Margot James: I beg to move amendment 13, in clause 15, page 8, line 31, after "21" insert "and 34"

This amendment is consequential on Amendment 94.

The Chair: With this it will be convenient to discuss Government amendments 14, 93 to 106, 109, 110 and 112.

Margot James: Schedule 2 allows for particular rights or obligations contained in the GDPR to be disapplied in particular circumstances, where giving effect to that right or obligation would lead to a perverse outcome. To do that, it makes use of a number of derogations in the GDPR, including articles 6(3) and 23(1).

Amendments 93, 95 and 109 permit article 19 of the GDPR to be disapplied for the purposes in parts 1, 2 and 5 of schedule 2.

When a data controller corrects or deletes personal data following a request from a data subject, article 19 of the GDPR requires them to inform all persons to whom the personal data has been disclosed. Additionally, if requested, the data controller must inform the data subject about those persons to whom the data has been disclosed. Following the introduction of the Bill, we have had further representations from a range of stakeholders, including the banking industry, regulators and the media sector, about the problems that article 19 might create in very particular circumstances.

The amendments will ensure that, for example, where a bank may have shared personal data about one of its customers with the National Crime Agency because of a suspected fraud, it will not have to tell the data subject about that disclosure when the customer changes their address with the bank. That will ensure that the data subject is not tipped off about the suspected fraud investigation.

Several amendments in the group are designed to ensure that a valuable provision of the GDPR—article 34—does not have unintended consequences for controllers who do the right thing by seeking to prevent or detect crime, assist with the assessment or collection of tax or uncover abuses in our society. Article 34 requires data controllers to inform a data subject if there has been a data breach that is likely to result in a high risk to the rights and freedoms of an individual. In normal operation, this is an important article, which we hope will prompt a step change in the way organisations think about cyber-security.

However, article 23(1) enables member states to create laws to restrict the scope of the obligations and rights for which article 34 provides in the minority of cases where it conflicts with other important objectives of general public interest. The amendments seek to do that in the Bill. Amendment 94 responds to the concerns of the finance sector that compliance with article 34 may result in persons under investigation for financial crime being tipped off. Amendment 110 serves a similar purpose for media organisations.

Article 85(2) creates scope for member states to provide exemptions from chapter 4 of the GDPR, which includes article 34, if they are necessary to reconcile the right to the protection of personal data with the freedom of expression. The amendment intends to ensure that processing data for a special purpose that is in the public interest is not prejudiced—for example, by a controller having to notify the data subject of a breach in relation to pre-publication undercover footage. Importantly, data controllers will still be required, for the first time, to report a breach to the Information Commissioner under article 33 of the GDPR. That will ensure that she is well placed to take all the necessary steps to ensure data subjects' rights are respected, including by monitoring compliance with these new exemptions.

On the more general question of who can make use of the exemptions in schedule 2 and when, amendment 96 broadens the exemption in paragraph 7 of the schedule, which relates to the protection of members of the public. As drafted, the exemption applies to personal data processed for the purposes of discharging a function that is designed to protect members of the public against dishonesty, malpractice or incompetence by persons who carry out activities that bring them into contact with members of the public. We have identified an issue with that wording: a number of public office holders, including police staff, do not carry out activities that necessarily bring them into contact with members of the public. Amendment 96 broadens the scope of the exemption to include processing in relation to individuals who work for those organisations in a behind-the-scenes capacity.

We have also had representations from several regulators on the need to make additional provisions to protect the integrity of their activities. Amendment 97 provides the UK's Comptroller and Auditor General, and their counterpart in each of the devolved Administrations, with an exemption from certain GDPR provisions where these are likely to prejudice their statutory functions. That will prevent certain individuals who suspect they may be under scrutiny from trying to use their rights under the GDPR, such as article 15 (confirmation of processing) as a way of confirming that their data is being processed, or from using article 17 (right to erasure) and article 18 (restriction of processing) to undermine the effectiveness of an audit.

3.15 pm

Likewise, amendment 98 provides an exemption for the Bank of England from the list of GDPR provisions, where these may inhibit its ability to exercise its functions. This amendment ensures the Bank of England can continue its work as a monetary authority without undue restriction from the GDPR. Amendments 99 and 100 are technical changes, which clarify that the table in paragraph 9 of schedule 2 refers to persons rather than bodies, to reflect the legal characteristics of the listed regulators. Amendment 101 adds section 244 of the Investigatory Powers Act 2016 to the list of legislation that confers processing functions on the Information Commissioner. Section 244 requires the commissioner to audit compliance, with certain obligations imposed by part 4 of the Investigatory Powers Act. This amendment would therefore exempt the commissioner from certain provisions of the GDPR in respect of those oversight functions. Hon. Members will agree that the commissioner's powers of oversight are vital to

her being an effective regulator. This amendment will allow her to use her investigatory powers in an unrestricted manner, to ensure compliance with the rules around the retention of data.

Amendment 102 provides an exemption for the Scottish Information Commissioner. A similar provision already exists for the UK Information Commissioner. This was included to address the risk to the UK commissioner's functions under the various access to information regimes, which could be prejudiced in some circumstances if she were to comply with a full range of the data subject's rights. The Scottish commissioner has confirmed that the same rights exist when carrying out his functions under equivalent Scottish legislation. We have therefore drafted this amendment to provide the Scottish Information Commissioner with an equivalent exemption to that of the UK Information Commissioner in relation to these functions.

Amendment 104 creates protection for the Financial Conduct Authority and the Prudential Regulation Authority. Clearly such protection is necessary for the integrity of our financial services' regulatory landscape. Amendment 105 extends the exemptions in schedule 2 to the Charity Commission's functions under the Charities Act 1992, the Charities Act 2006 and the Charities Act 2011. Again, these exemptions apply only where a right or obligation would be likely to prejudice the ability to discharge a function conferred on them by statute. Amendments 106 and 112 relate to schedule 3, which provides for restrictions from certain GDPR provisions where this is necessary for health, education and social work purposes.

Paragraph 16 provides an exemption from certain GDPR provisions in relation to educational records in Northern Ireland. It currently applies only to information processed by or on behalf of the board of governors or a teacher at a grant-aided school. This amendment extends the exemption so that it includes records of information processed by or on behalf of grant-aided and independent school regardless of their governance arrangements.

Amendment 13 agreed to.

Amendment made: 14, in clause 15, page 8, line 34, after "21" insert "and 34". *—(Margot James.)*

This amendment is consequential on an amendment made in the Lords which added Article 34 of the GDPR (communication of personal data breach to the data subject) to the list of GDPR provisions that are disapplied by paragraph 11 of Schedule 2 to the Bill.

Clause 15, as amended, ordered to stand part of the Bill.

Schedule 2

EXEMPTIONS ETC FROM THE GDPR

Amendments made: 93, in schedule 2, page 135, line 7, at end insert—

( ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);"

This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by provisions in Part 1 of Schedule 2 to the Bill.

Amendment 94, in schedule 2, page 135, line 19, after "provisions" insert

"and Article 34(1) and (4) of the GDPR (communication of personal data breach to the data subject)" *—(Margot James.)*

This amendment adds Article 34 of the GDPR (communication of personal data breach to the data subject) to the list of GDPR provisions that are disapplied by paragraph 2(1) of Schedule 2 to the Bill (crime and taxation: general).

Liam Byrne: I beg to move amendment 156, in schedule 2, page 136, line 30, leave out paragraph 4.

This amendment would remove immigration from the exemptions from the GDPR.

We are trying to provide some careful and considered constraints on the exemptions that the Government are asking for, in particular the exemptions that Ministers seek for the purposes of immigration control.

The Bill has been drafted essentially to enable the Home Office to do two things: win cases and create a hostile environment for those who are here illegally, where it has no capacity to trace and deport individuals. In conducting its work, the Home Office draws on a wide range of private providers, from G4S to Cifas. They have a mixed record, including on data protection. The carve-out that the Government seek for immigration purposes has caused widespread concern. It has drawn concern from the other place, the Information Commissioner and the Joint Committee on Human Rights.

The Minister will try to assure us by saying there are safeguards wrapped around the exemption and that there are limits on the way it can be used, but those limits are drawn so vaguely and broadly that they are not safeguards at all. They have been drafted to apply where matters are likely to prejudice immigration control. Who gets to judge the likelihood of prejudicing immigration control is not terrifically clear. In my Home Office days, we used to call that carte blanche.

Through the powers and exemptions in the Bill, the Home Office seeks to collect data for one purpose and then use it without informed consent. Where the rubber hits the road is that, crucially, the effect will be to ensure that subject access requests are basically put beyond the scope of someone seeking information that they might be able to use either in representations that we all might make to Ministers or, more importantly, in an immigration tribunal.

I want to sound a warning note to the Minister, as I hinted on Second Reading. I was brought into the Home Office as a Minister in 2006 and, after a glorious fortnight as Minister for Police and Counter-terrorism, I was moved by my boss John Reid to become Immigration Minister, where I was asked to conduct the biggest shake-up of our immigration system for 40 years.

I created the UK Border Agency; I took UK visas out of the Foreign Office; I took Customs out of the Treasury. We created a Border Agency that could run a biometric visa programme abroad, checking fingerprints against police national computers before anyone got on a train, plane or boat to our country. We introduced much stronger controls at the border, increasing those nice new blue signs, creating smart uniforms for immigration officials, and we increased immigration policing by around £100 million a year

I said earlier that to err is human but it takes a computer really to foul things up. That is a lesson that I learned with some force during my time at the Home Office. The dedicated, fantastic officials in the Home Office and the extraordinary officers who work in what was the UK Border Agency—it has since been revised a couple of times—do an amazing job. They are dramatically

underfunded by the Treasury. They have been underfunded by the Treasury under this Government and, in my view, we did not get enough out of the Treasury in my day.

However, they are human and make mistakes. That is why we have such a complicated immigration tribunal system, where people can take their complaints to a first tier tribunal but very often need to seek a judicial review down the line. The challenge is that, if the Home Office wants to create a process and an administration for making the right decision, which can be defended in a tribunal and in a judicial review case, that process must be robust. When we streamlined the immigration tribunal system, we realised that we had to change, improve and strengthen the way that we took decisions in the Home Office because too many were made in a way that was not JR-proof. We were losing JRs and therefore denying justice to those who brought a legitimate claim against the Crown.

There were occasions when I lost cases because of information that was disclosed to the applicant through a subject access review. SARs are one of the most powerful instruments by which anybody in this country, whether a citizen or someone applying to become a citizen, or applying for a legal right to remain, can acquire information that is crucial to the delivery of justice. Many of us are incredibly sympathetic to the job that the Home Office does. Many of us will want a tougher regime in policing immigration, in particular illegal immigration, but I suspect every member of the Committee is also interested in the good conduct of justice and administrative justice. As someone who served in the Home Office for two years, I had to take some very difficult decisions, including to release subject access request information that I absolutely did not want to go into the public domain. Sometimes it was right to release that information because it helped ensure that justice was done in the courts of this land.

The Minister has some very strong safeguards in the Bill. There are strong safeguards that create exemptions for her where the interest is in crime prevention, such as, for example, illegal immigration. However, the power that the provision seeks, at which we take aim in our amendments, is a step too far and risks the most terrible injustices. It risks the courts being fouled up and our being challenged in all sorts of places, including the European Court of Human Rights in the years to come. It is an unwise provision. If I were a Home Office official, I would have tried it on—I would have tried to get it through my Minister and through the Houses of Parliament, but it is unwise and a step too far. I hope the Minister will accept the amendment and delete the provisions.

Brendan O'Hara: I will speak in favour of amendment 156. On Second Reading, I said that I would raise this matter again in Committee and I make no apologies for doing so. We regard this new exemption as extremely concerning. It permits the Government to collect and hold data for the purposes of what they describe as "effective immigration".

It also concerns me that nowhere in the Bill does there seem to be a legal definition of effective immigration control. I am worried that "effective immigration control" is highly subjective and highly politicised. It exposes individuals, weakens their rights and makes them vulnerable to whatever change in the political tide happens to come along next. This broad-ranging exemption is fundamentally unfair. It is open to abuse and runs contrary to safeguarding basic human rights. I believe that the UK's proposed immigration exemption goes much further than the scope of restrictions afforded to member states under GDPR, with all the consequences of that, which we discussed in such great detail this morning around adequacy decisions.

3.30 pm

The exemption would introduce a new and unprecedented removal of an individual's data protection rights and it is as unnecessary as it is disproportionate. Under this exemption, the Government will remove any obligation they have under data protection to inform an individual that their data has been transferred to the Home Office for immigration control purposes. That individual would not know if their data was being held or whether they were under investigation. That individual would have no right to know what data was being held by the Home Office or why. They would have no way of checking the accuracy of the information being held and therefore no way of correcting any mistakes in the information, which could then be used by the Home Office to decide whether they could live in this country or not.

Ian Murray (Edinburgh South) (Lab): The hon. Gentleman makes a powerful case against this particular exemption. He will know as well as me as a constituency Member of Parliament that one of the first things checked when someone comes to seek our advice is whether the Home Office has the correct information on an individual. Nine times out of 10, because of sheer workload, the Home Office just has it wrong. Then the visas and so on can be processed. Am I right in saying that, under this exemption, we would be unable to do that?

Brendan O'Hara: The hon. Gentleman is absolutely correct; I was just getting on to the point about the information held by the Home Office. If it cannot be checked and if it is wrong at source, it is wrong at the end of the process. As far as I can see, there are no safeguards against that. He is absolutely correct that one early error in data collection and processing becomes an irrefutable and indisputable fact by the time it reaches the Home Office. The Home Office could then base its case against an individual on that wrong information.

The hon. Gentleman is right—as constituency MPs, there is not one of us, I am sure, who is not painfully aware of wrong information being held not just by the Home Office, but by a whole range of Departments. That makes the exemption fundamentally unfair. This is an issue of basic fairness and there is little wonder it has been so loudly and roundly condemned by civil liberties groups and many in the legal profession. If we go ahead with the schedule as it stands, it fundamentally changes how we can operate and how we can help people who require our assistance.

At the moment, we have subject access requests. As matters stand, the Home Office and the subject or their legal representative have a right to access the same information, on which legal claims and challenges are based. Surely, if both sides do not have access to the same information, the fairness of any legal proceedings is inevitably compromised. Subject access requests are

[Brendan O'Hara]

often the only route through which a legal professional can make representations on very complicated issues on behalf of their client. Indeed, for clients who have been victims of domestic abuse and are fleeing an abusive partner, sometimes a subject access request is all that stands between them and a successful application to remain. This exemption will reduce legal representatives' ability to best represent their clients and it removes a fundamental tool for holding the Home Office to account when it either gets things wrong or chooses to ignore or misrepresent the facts. The exemption is fundamentally unfair and as unnecessary as it is disproportionate. I urge the Government to reconsider.

Darren Jones: I support the amendment tabled by my right hon. and hon. Friends, because there are some harsh realities about this exemption for effective immigration control, including the harsh reality that such an exemption right does not exist under the GDPR. Indeed, it is a new exemption compared with the law that exists today under the Data Protection Act 1998.

This broad, undefined exemption really must be restricted. I declare an interest. My wife is Australian and is here on a spousal visa. I therefore assume that, as a British citizen, I too could be subject to my rights being exempted for the effective control of immigration in order to understand what my wife is up to. I should declare for the record that her staying here in the UK is perfectly legitimate. This is a wide-ranging exemption that could apply to EU citizens, non-EU citizens and, as I say, British citizens who are connected with those who are subject to immigration controls.

This is not just an issue for the Home Office; there is data across various Departments that could be of use to the Home Office for the effective control of immigration. Indeed, we have been waiting for quite some time for the Government to publish the biometric strategy, setting out how they intend to use lots of biometric data across Government Departments. We have been waiting for a couple of years to see how the Government intend to do that.

My understanding is that if all the photographs held on our passports and driving licences were collated, in essence the Government would have the power to have a virtual ID card for the bulk of the adult population in this country. How on earth would that information be used for the effective control of immigration, which would potentially be applied to so many people here in the UK?

This exemption creates a derogation for many rights: the right to information, the right to access, the right to explanation, the right to erasure, the right to restriction of processing, the right to data portability, the right to object, and all the principles set out in article 5 of the GDPR. This is an enormous derogation from rights that our colleagues in Europe think are important. Again, this relates to the risk of failing to seek adequacy in our negotiations with the EU.

I seek not only to support the amendment but to ask the Minister to clarify something. If the Government do not support the amendment, how does the exemption fit within the language of article 23 of the GDPR, which states that it can only exist

"when such a restriction respects the essence of the fundamental rights"—

which we have already noticed today are being repealed by this Government—

"and freedoms and is a necessary and proportionate measure in a democratic society"?

My assertion is that this exemption goes too far and, therefore, that the amendment tabled by my right hon. and hon. Friends is perfectly sensible. I look forward to it receiving Government support.

Stuart C. McDonald (Cumbernauld, Kilsyth and Kirkintilloch East) (SNP): We have already heard three very good speeches in support of the amendment. I will not take too long to support pretty much everything that has been said so far. As a former troublesome immigration lawyer from back in the day—in fact, when the right hon. Member for Birmingham, Hodge Hill was busy making his reforms in the Department—I do not think that I could have lived it down if I had not said a few words in support of the amendment.

We must remember that the context for all this is that we have a Department—the Home Office—where, as the most recent statistics show, half of all immigration decisions that are challenged in a tribunal are overturned, which is a record high. The Home Affairs Committee has recently expressed grave concerns about the poor quality of decision making in far too many areas and the functioning of a hostile environment, for example in the area of bank checks, where there is something like a 10% error rate. We also live in a world where the creeping reach of the Home Office's information tentacles is almost being seen to put off migrants from accessing necessary public services such as health, creating a public health danger.

To provide a massive and almost unlimited exemption from many of the key protections, as has been described, is not only unjustified but counterproductive, because rather than fixing the fundamental problems with Home Office decision making, it will make them worse by hiding them from view and from scrutiny. The Home Office, not for the first time, is being pretty greedy with the powers that it seeks, because even if we take out the exemption, as this amendment proposes, the Home Office will still have plenty of scope—perhaps too much scope—to do what it wants to do. Recent immigration Acts have created myriad criminal offences in the sphere of immigration law, so the Home Office can already rely on other exemptions within the Bill where necessary. What is absolutely lacking is any explanation of why the exemption is needed. Will the Minister explain what it is about current data protection laws that has unacceptably hindered Home Office operations? I have seen no evidence of that at all.

Another concern is that it is not just the Home Office that will benefit from this exemption but other organisations that are involved in immigration control, such as G4S in its operation of detention centres. There is no justification for that, but there are serious risks, harms and injustices that might be created by the proposed exemption.

As we have heard, subject access requests are regularly a crucial part of representing a migrant caught up in the immigration system. They can be used to establish statuses that have not been communicated or have been lost. They can be used to establish other crucial facts that have not been known to that individual or their representatives. They can, of course, be absolutely crucial in establishing that the Home Office has made errors, as all too many hon. Members will have experienced.

Members of the Committee have been provided with a host of examples by the Law Society, the Bar Council, the Immigration Law Practitioners' Association and others. Those are real-life examples occurring day in, day out. Quite simply, the failure to allow those individuals access to data protection rights is not only a denial of those rights but a denial of access to justice altogether. This part of the Bill desperately needs reconsideration by the Government.

Victoria Atkins: I feel I should defend all the hardworking people both in the Home Office and Border Force who do their best to do their jobs, day in, day out, to ensure that we have an effective, fair and proportionate immigration system. They have come under a bit of an attack in this debate.

Ian Murray: I do not think anybody on the Committee would disagree with the statement that the staff work incredibly hard. Would it not be a show of solidarity with those staff to give them the resources they require to do the job properly?

Victoria Atkins: The hon. Gentleman is starting the debate in very sparky form.

Ian Murray: You started it.

Victoria Atkins: I didn't start it. The point is that, when people talk obliquely about the Home Office, it is people working in the Home Office who have to make these decisions day in, day out and who have to apply the law and do their best. I think we need to bear that in mind when we are talking about the Home Office system and how bad it is.

The provision relating to data processing for the purposes of immigration control in paragraph 4 of schedule 2 has been the subject of much debate. I would like to address some of the misunderstandings that have clearly arisen during the course of the Bill around both the purpose and scope of the provision. I hope I can persuade the Committee that this is a necessary and proportionate measure to protect the integrity of our immigration system.

Mr Alister Jack (Dumfries and Galloway) (Con): Opposition Members have expressed concern, which I would like to emphasise, that this exemption is too wide. Can the Minister provide an assurance that that is not the case?

Victoria Atkins: Very much so. I will take it slowly because it is complicated and I want to ensure that the points raised today have been addressed. First, I was asked who decides the definition of effective immigration control in the schedule. That is an established term of art. It is used, for example, in the Immigration Act 2014. The Freedom of Information Act 2000 uses a similar term, namely

"the operation of the immigration controls".

In the context of the schedule, we have adopted a wraparound term such as that, rather than set out a detailed list of specific immigration-related functions to which the exemption might be applied. Given the undoubted complexity of immigration legislation, there is a danger that any such list would be incomplete and would need to be regularly reviewed and updated. The term is either the precise term or similar to those already in law, such as in the Freedom of Information Act, which has been law for 18 years.

The hon. Member for Argyll and Bute seems concerned that once the Home Office system has accessed some of this information, it is lost forever and will not be revealed to the person whom it concerns. I will give case examples later, but I reassure him that the way in which we describe this exemption in the Home Office is that it is a pause on two of the data protection principles. Once the pause is lifted, because the end has been achieved—the person has been found or whatever—all those rights kick back in again, and they are able to make requests for the information that the hon. Gentleman set out. We see it as a pause, not as a long-standing and permanent exemption. It is just for the precise circumstances of enabling the immigration system and its protections.

3.45 pm

Liam Byrne: The Under-Secretary of State will know better than anybody that there are very tight time limits over the windows within which people can ask for entry clearance officer reviews or reconsideration, either by an immigration official or, in extremis, by the Minister. How long will the pause last, and can she guarantee the Committee today that the pause will never jeopardise the kick-in of time limits on an appeal or a reconsideration decision?

Victoria Atkins: The reason for the pause is—I will give case studies of this—to enable the immigration system to operate. If someone has gone missing, requests for data will be required to find that person. Once that person is found, and there is no longer a need to apply the exemption, it will be lifted.

Liam Byrne: That is not an answer to my question. I am asking for a guarantee to the Committee this afternoon that the pause will never jeopardise somebody's ability to submit a valid request for a reconsideration or an appeal with the information that they need within the time windows set out by Home Office regulations—yes or no.

Victoria Atkins: I am asked whether this will have an impact on someone's application, either at appeal or reconsideration. Of course, information is obtained so that a person can be brought in. As I say, I will make it clear with case studies, so perhaps I can answer the right hon. Gentleman in more detail when I give such an example, but the purpose of this is generally to find a person. When the need, as set out under the exemption, no longer exists, the rights kick back in again. This relates only to the first two data protection principles under the GDPR. Again, I will go into more detail in a moment, but this is not the permanent exemption from rights as perhaps has been feared by some; it is simply to enable the process to work. Once a person has been brought into the immigration system, all the protections of the immigration system remain.

Stuart C. McDonald: The circumstances that the Minister describes for using the exemption are much narrower than the way the exemption is actually drawn. It seems to me that if that is the only way in which the Home Office wants to use the exemption, it could frame it in a much narrower way and possibly gain cross-party support.

Victoria Atkins: I will move on to the case studies in a moment, as I have given way several times. First, I will lay out the titles, then I will come on to article 23. Again, our analysis is that the provision fits within one of the exemptions in article 23. That is precisely the reason that we have drawn it in this way.

We very much welcome the enhanced rights and protections for data subjects afforded by the GDPR. The authors of the GDPR accepted that at times those rights need to be qualified in the general public interest, whether to protect national security, the prevention and detection of crime, the economic interests of the country or, in this case, the maintenance of an effective system of immigration control. Accordingly, a number of articles of the GDPR make express provision for such exemptions, including article 23(1)(e), which enables restrictions to be placed on certain rights of data subjects. Given the extension of data subjects' rights under the GDPR, it is necessary to include in the Bill an explicit targeted but proportionate exemption in the immigration context.

The exemption would apply to the processing of personal data by the Home Office for the purposes of

"the maintenance of effective immigration control, or…the investigation or detection of activities that would undermine the maintenance of effective immigration control".

It would also apply to other public authorities required or authorised to share information with the Department for either of those specific purposes.

Let me be clear on what paragraph 4 of schedule 2 does not do. It categorically does not set aside the whole of the GDPR for all processing of personal data for all immigration purposes. It makes it clear that the exemption applies only to certain GDPR articles. The articles that the exemption applies to are set out in paragraph 4(2) of schedule 2. They relate to various rights of data subjects provided for in chapter 3 of the GDPR, such as the rights to information and access to personal data, and to two of the data protection principles—namely the first one, which relates to fair and transparent processes, and the purpose limitation, which is the second one.

Liam Byrne: As I understand it, the derogations that are sought effectively remove the right to information in article 13; the right to information where data is obtained from a third party in article 14; the right of subjects' access in article 15; the right to erasure in article 17; the right to restriction of processing in article 18; the right to object in article 21(1); the principle of lawful, fair and transparent processing in article 5; the principle of purpose limitation in article 5(1)(b); and the data protection principles in article 5 of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability to the extent that they correspond to the rights above. That is a pretty broad set of rights to be cast out.

Victoria Atkins: Those are not the data protection principles. If one continues to read on to paragraph 4(2)(b) of schedule 2, it sets out the two data protection principles that I have just highlighted. The provisions set out in sub-paragraph (2)(a) relate to the data protection principles of fair and transparent processing and the purpose limitation. As I say, this is not a permanent removal. This is, as we describe it, a pause. There is not a free hand to invoke the permitted exception as a matter of routine.

All of the data protection principles, including those relating to data minimisation, accuracy, storage limitation and integrity and confidentiality, will continue to apply to everyone. So, too, will all the obligations on data controllers and processors, all the safeguards around cross-border transfers, and all the oversight and enforcement powers of the Information Commissioner. The latter is particularly relevant here, as it is open to any data subject affected by the provisions in paragraph 4 of schedule 2 to make a complaint to the Information Commissioner that the commissioner is then under a duty to investigate. Again, I hope that that addresses some of the concerns that the hon. Member for Argyll and Bute raised.

Contrary to the impression that has perhaps been given or understood, paragraph 4 does not give the Home Office a free hand to invoke the permitted exceptions as a matter of routine. The Bill is clear that the exceptions may be applied only to the extent that the application of the rights of data subjects, or the two relevant data protection principles, would be likely to prejudice

"the maintenance of effective immigration control, or…the investigation or detection of activities that would undermine the maintenance of effective immigration control".

That is an important caveat.

Liam Byrne: The Minister will know that in paragraph 2(1)(a) we already have a set of exemptions that relate to the prevention or detection of a crime, including, presumably, all of the crimes that fall into the bucket of organising or perpetrating illegal immigration. Despite constant pressing during the debate in the other place and here, we have not yet had a clear answer as to why additional powers and exemptions are needed, over and above the powers expressly granted and agreed in paragraph 2(1)(a).

Victoria Atkins: I am grateful to the right hon. Gentleman for raising that issue, because it allows me to get to the nub of how we approach the immigration system. We do not see the immigration system as some form of criminality or as only being open to the principles of criminal law. He will know that we deal with immigration in both the civil law and criminal law contexts. The exemption he has raised in terms of paragraph 2 of the schedule deals with the criminal law context, but we must also address those instances where the matter is perhaps for civil law.

We know that in the vast majority of immigration cases, people are dealt with through immigration tribunals or through civil law. They are not dealt with through criminal law. That is the point; we must please keep open the ability to deal with people through the civil law system, rather than rushing immediately to criminalise them. If, for example, they have overstayed, sometimes it is appropriate for the criminal law to become involved, but a great number of times it is for the civil law to be applied to deal with that person's case either by way of civil penalty or by finding an arrangement whereby they can be given discretion to leave or the right to remain. We have the exemption in paragraph 4 so that we do not just focus on the criminal aspects that there may be in some immigration cases. We must ensure that we also focus on the much wider and much more widely used civil law context.

It is important to recognise that the exemptions will not and cannot be targeted at whole classes of vulnerable individuals, be they victims of domestic abuse or human

trafficking, undocumented children or asylum seekers. The enhanced data rights afforded by the GDPR will benefit all those who are here lawfully in the United Kingdom, including EU citizens. The relevant rights will be restricted only on a case-by-case basis where there is evidence that the prejudice I have mentioned is likely to occur.

Peter Heaton-Jones (North Devon) (Con): The Minister specifically mentioned EU citizens. There have been concerns that the exemption will impact those EU nationals who are already here and who, as we have already heard, are contributing hugely to the UK. Can she assure us that the exemption is not targeted at them?

Victoria Atkins: Absolutely. The exemption will not be enacted on the basis of nationality. It is enacted on a case-by-case basis to uphold the integrity of the immigration system. There will be no question of EU nationals being in any way targeted by it. Indeed, we know the great effect that EU nationals and other people from other countries have had in this country, and we certainly would not be looking to target them on the basis of nationality.

Darren Jones: Is it not right to say that EU citizens will be part of the immigration system? They will be immigrants with immigration rights as part of the Brexit process. These rules could therefore apply to them, could they not? Secondly—

Victoria Atkins: I will answer the first one—yes. The hon. Gentleman asked whether EU citizens would be targeted. Once we leave the European Union, we will have our own immigration policy. There will clearly be no distinction between EU and non-EU, because everyone will be outside of the UK, if I may put it that way, very inelegantly.

Darren Jones: But they would still be subject to the right to exempt them from their data protection rights. I welcome the Minister's comments on the time-limited nature of the intention of using the rules, but can she point me to the section of the Bill that defines that time limit, because I am struggling to find it?

Victoria Atkins: If I may, I will come back to that point in a moment. In the case of subject access requests, each request would need to be considered on its own merits. For example, we could not limit the information given to visa applicants on how their personal data would be processed as part of that application. Rather, the restrictions would be applied only where there was a real likelihood of prejudice to immigration controls as a result of disclosing the information concerned.

4 pm

It is equally important to shed light on another concern that has been voiced. Some of the briefing that has been circulated suggests that the Bill creates new information sharing gateways. That is simply not the case. As I have indicated, schedule 2 sets out certain exceptions from GDPR. It does not of itself create new powers to share data between data controllers. However, where personal data is shared between controllers for the limited immigration purposes specified in paragraph 4, it means that the data subject does not need to be notified, if to do so would be prejudicial to the maintenance of effective immigration control.

It may assist the Committee if I explain the kind of information that it may be necessary to withhold from data subjects. The classes of information that the Home Office may wish to withhold include a description of the data held, our data sources, the purposes for which that data is being processed, and the details of the recipients to whom the data has been disclosed. There will be circumstances in which the disclosure to a data subject of such information could afford him or her the opportunity to circumvent our immigration controls. A couple of examples will serve to illustrate where the disclosure of such information may have precisely that adverse effect.

In the case of a suspected overstayer, if we had to disclose, in response to a subject access request, what we are doing to track their whereabouts with a view to effecting administrative removal—that is the difference from the paragraph 2 point that the right hon. Member for Birmingham, Hodge Hill highlighted—evidently, that would tip them off, and thus undermine such enforcement action.

Liam Byrne: If someone has overstayed, they have committed a crime. Therefore, paragraph 2(1)(a) absolutely bites. We are seeking to prevent that crime. Someone who has overstayed their visa has committed a crime. It is kind of as simple as that.

Victoria Atkins: In that scenario, we may well effect their removal administratively. It does not mean that it is going through the criminal courts.

By way of a second example, take a case where the Home Office is considering an application for an extension of leave to remain in the UK. It may be that we have evidence that the applicant has provided false information to support his or her claim. In such cases, we may need to contact third parties to substantiate the veracity of the information provided in support of the application. If we are then obliged to inform the claimant that we are taking such steps, they may abscond and evade detection.

Liam Byrne: If someone has submitted false information in support of an application to the Government, and signed it, as they must, that is called fraud. That is also a crime, and is covered by paragraph 2(1)(a).

Victoria Atkins: I take the right hon. Gentleman's point, particularly in relation to the overstayer, but as the purpose of processing personal data in many immigration areas is not generally the pursuit of criminal enforcement action, it is not clear that it would be appropriate in all cases to rely on crime-related exemptions, where the real prejudice lies in our ability to take administrative enforcement action. It may well be that in some cases a crime has been committed, but that will not always be the case.

Criminal sanctions are not always the correct and proportionate response to people who are in the UK without lawful authority. It is often better to use administrative means to remove such a person and prevent re-entry, rather than to deploy the fully panoply of the criminal justice system, which is designed to rehabilitate members of our communities. As the purpose

[Victoria Atkins]

of processing personal data in such cases is not generally the pursuit of a prosecution, it is not clear that we could, in all cases, rely on that exemption relating to crime.

Stuart C. McDonald: So far we have had some hypothetical examples about what might happen in the future, but given that we have a data protection regime in place already, it would be useful to know whether the Minister can give us examples of situations that have arisen in which the Home Office has been hindered by the current data protection regime. We have not heard anything like that so far.

Victoria Atkins: If I may, I will continue with my speech, because I have more information to give. Perhaps at the end I can deal with the hon. Gentleman's point.

Liam Byrne: I just want to dissolve one confusion in the Minister's remarks. The nature of the Home Office response, whether it is a prosecution through a civil court, a civil sanction or a civil whatever else, does not affect the nature of the offence that is committed. The Home Office has a range of sanctions and choices in responding to an offence, but that does not stop the offence being an offence. The offence is still a crime, and is therefore covered by paragraph 2(1)(a).

Victoria Atkins: The right hon. Gentleman is assuming that each and every immigration case that will be covered by these provisions necessitates the commission of a crime.

Liam Byrne: We are preventing crime.

Victoria Atkins: I would not make that assumption. The vast majority of immigration cases are dealt with in a civil context.

Darren Jones: Will the Minister give way?

Victoria Atkins: No, forgive me. I have been very generous with interventions. I am going to make some progress, and then no doubt others will intervene on me in due course.

I turn to the charge that the exemption has no basis in EU law. Article 23 of the GDPR allows member states to restrict the application of certain provisions of the regulation to safeguard important objectives of general public interest. Immigration control constitutes one such objective. We see immigration as an important matter of public interest, and the GDPR allows member states to exempt rights where that is the case. We are not alone in our belief that immigration is an important matter of general public interest. The Irish Government clearly stated that in their own Data Protection Bill. Clause 54 of the Irish Bill gives powers to make regulations restricting certain rights and obligations under the GDPR to safeguard important objectives of general public interest. The list of such objectives in the Bill includes matter relating to immigration.

Opposition Members have talked about their concerns about the fact that these provisions may be covered by paragraph 2 of the schedule. I want to reflect on the outcome of the debate on this provision in the House of Lords, which contains many noble Lords who are extremely learned in the law, have much experience of campaigning on immigration rights and so on. We listened very carefully to the concerns raised at Lords Committee stage, and as a result the Government tabled amendments at Lords Report stage to narrow the scope of the exemption so that it no longer covers the right to rectification and data portability. In response to those amendments, Lord Kennedy of Southwark said:

"The amendments tabled by the Government provide important clarification on what is exempt, limit the power in Bill and seek to address the concerns highlighted during the previous debate and today…I am happy to support their amendments."—[*Official Report, House of Lords,* 13 December 2017; Vol. 787, c. 1590.]

Furthermore, in a Division on a Liberal Democrat amendment to strike out the immigration exemption, the official Opposition abstained. I wonder what has changed between their abstaining on that amendment and accepting that the Government's amendments were sufficient, and today. Nothing has changed since the Bill left the Lords, so perhaps the right hon. Member for Birmingham, Hodge Hill can help us with why their position has changed.

I hope I have been able to satisfy the Committee that this provision is necessary and important.

Gareth Snell (Stoke-on-Trent Central) (Lab/Co-op): It is a pleasure to serve under your chairmanship, Mr Hanson. Will the Minister give a tangible example, as she has done in other cases, of where an immigration case may require exemption under paragraph 4—in other words, a case in which a crime has not been committed and therefore would not be covered under paragraph 2(2)? The cases she has mentioned so far would, on the face of it, be covered by paragraph 2(2), because a criminal act had taken place or was about to take place.

Victoria Atkins: There may be occasions when there is a person we have lost track of whose status is irregular. If we know they have a child, we will seek from the Department for Education assistance to find the whereabouts of the child. That child has not committed a criminal offence, so I would be very concerned to ensure that the Home Office, Border Force or whoever else acted lawfully when seeking that data in order to enable them to find the parent or whoever is the responsible adult, as part of the immigration system.

Louise Haigh: In that example, would the exemption not be covered under the safeguarding exemption, as brought by the Government amendment to schedule 1?

Victoria Atkins: I have to say, that had not occurred to me as an obvious—

Louise Haigh: A missing child?

Victoria Atkins: No—the child is not missing, but the parent is; so we seek advice from the Department for Education about where the child is. It may be that cleverer lawyers than me in the Home Office will find an exemption for that, but the point of this exemption of paragraph 4 is to cover the lawfulness of the Home Office in seeking such information in order to find parents or responsible adults who may have responsibility, and either to regularise their stay or to remove them.

I encourage the right hon. Member for Birmingham, Hodge Hill to withdraw his amendment, as we believe that it is not the wholesale disapplication of data subjects'

rights, and it is a targeted provision wholly in accordance with the discretion afforded to member states by the GDPR and is vital to maintaining the integrity and effectiveness of our immigration system.

Liam Byrne: Anyone who was not alarmed by this provision certainly will leave this Committee Room thoroughly alarmed by the Minister's explanations.

First, we were invited to believe that we could safeguard due process and the rights of newcomers to this country by suspending those rights and pursuing people through civil court. We were then asked to believe that the Home Office's ambition to deal with these cases with civil response rendered inoperable the powers set out in paragraph 2(1)(a), confusing the response from the Home Office and the nature of the offence committed up front. Then, we were invited to believe that this was not a permanent provision—even though that safeguard is not written into the Bill—but a temporary provision. What is not clear is when those temporary provisions would be activated and, crucially, when they would be suspended.

Victoria Atkins *rose—*

Liam Byrne: I am happy to give way in a moment. Most of us here who have done our fair share of immigration cases—I have done several thousand over the last 14 years—know that on some occasions, the Home Office interpretation of time is somewhat different from a broadly understood interpretation of time. I have cases in which a judge has ordered the issue of a visa, and six months later we are still chasing the Home Office for the issue of the visa. I will not be alone in offering these examples.

Perhaps when the Minister intervenes, she could set out what "temporary" means, where it is defined and where are the limits, and she still has not answered my question whether she will guarantee that the implementation of this pause will not jeopardise someone's ability to submit either a request for an entry clearance officer review or an appeal within the legally binding time windows set out in Home Office regulations.

Victoria Atkins: The key to this is the purpose for which we are processing the data. Even if there are criminal sanctions, that does not mean that we are processing for that purpose, particularly where we are not likely to pursue a prosecution. The primary purpose is often immigration control—that does not fit under paragraph 2 as he has described it—rather than enforcing the criminal justice system. That is the point. It is for the purpose of processing the data. The crime-related provisions in the Bill refer to the importance of identifying the purposes of the processing. Where the primary purpose is immigration related, it is not clear that we could rely on the crime-related exemptions. That is why paragraph 4 is in the schedule.

Liam Byrne: I am really sorry to have to say this, but that is utter nonsense. The idea that the Home Office will seek to regularise someone's immigration status by denying them access to information that might support their case is, frankly, fanciful.

This is not a new debate; we last had it in 1983. The Home Office tried to sketch this exemption into legislation then, it failed, and we should not allow the exemption to go into the Bill, especially given that all the explanations we have heard this afternoon are about cases where paragraph 2(1)(a), or the safeguarding provisions drafted by the Government, would provide the necessary exemptions and safeguards in the contingencies that the Minister is concerned about.

4.15 pm

Darren Jones: I feel for the Under-Secretary, because she is on a bit of a sticky wicket given the Government's drafting, but does my right hon. Friend agree that it is concerning that I asked twice to be pointed to specifics—I asked first how the pause is drafted in the Bill, and secondly where the word "immigration" appears under article 23 of the GDPR—but on neither occasion was I was pointed to them? We ought also to draw the Committee's attention to the report on the Bill by the Joint Committee on Human Rights, which states:

"The GDPR does not expressly provide for immigration control as a legitimate ground for exemption."

Liam Byrne: My hon. Friend is bang on the money, but perhaps the Under-Secretary can enlighten us.

Victoria Atkins: All rights are reinstated once the risk to prejudice is removed. The wording is in line 35 of paragraph 4:

"to the extent that the application of those provisions would be likely to prejudice any of the matters mentioned in paragraphs (a) and (b)."

To reassure the hon. Member for Bristol North West, that is the end point.

Liam Byrne: I am grateful to the Under-Secretary for clarifying a point that was not at issue. No one is concerned about what rights kick back in at the end of a process. We are worried about how long the process will last, who will govern it, what rights newcomers to this country or courts will have to enforce some kind of constraint on the process and how we will stop the Home Office embarking on unending processes in a Jarndyce *v.* Jarndyce-like way, which we know is the way these cases are sometimes prosecuted. The Home Office is full of some of the most amazing civil servants on earth, but perhaps, a little like the Under-Secretary, they are sometimes good people trapped in bad systems and, dare I say it, bad arguments.

Question put, That the amendment be made.

The Committee divided: Ayes 9, Noes 10.

Division No. 4]

AYES

Byrne, rh Liam	Murray, Ian
Elmore, Chris	O'Hara, Brendan
Haigh, Louise	Snell, Gareth
Jones, Darren	Zeichner, Daniel
McDonald, Stuart C.	

NOES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

Question accordingly negatived.

Amendments made: 95, in schedule 2, page 138, line 15, at end insert—

"( ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);"

This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by provisions in Part 2 of Schedule 2 to the Bill.

Amendment 96, in schedule 2, page 139, leave out lines 17 to 27 and insert—

"2. The function is designed to protect members of the public against— (a) dishonesty, malpractice or other seriously improper conduct, or (b) unfitness or incompetence.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest."

This amendment extends the exemption provided for in paragraph 7 of Schedule 2. It amends the second entry in the table (functions designed to protect members of the public against dishonesty etc) by removing the requirement that the function relates to people who carry on activities which bring them into contact with members of the public. It also amends column 2 of the table to bring the second entry into line with the first and third entries.

Amendment 97, in schedule 2, page 140, line 42, at end insert—

"Audit functions

7A (1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function listed in sub-paragraph (2) to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) The functions are any function that is conferred by an enactment on—

(a) the Comptroller and Auditor General;

(b) the Auditor General for Scotland;

(c) the Auditor General for Wales;

(d) the Comptroller and Auditor General for Northern Ireland."

This amendment inserts a new paragraph into Schedule 2 to provide for an exemption from "the listed GDPR provisions" (defined in paragraph 6 of Schedule 2) where personal data is processed for the purposes of discharging statutory functions of certain auditors.

Amendment 98, in schedule 2, page 140, line 42, at end insert—

"Functions of the Bank of England

7B (1) The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a relevant function of the Bank of England to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

(2) 'Relevant function of the Bank of England' means—

(a) a function discharged by the Bank acting in its capacity as a monetary authority (as defined in section 244(2)(c) and (2A) of the Banking Act 2009);

(b) a public function of the Bank within the meaning of section 349 of the Financial Services and Markets Act 2000;

(c) a function conferred on the Prudential Regulation Authority by or under the Financial Services and Markets Act 2000 or by another enactment."

This amendment inserts a new paragraph into Schedule 2 to provide for an exemption from "the listed GDPR provisions" (defined in paragraph 6 of Schedule 2) where personal data is processed for the purposes of discharging specified functions of the Bank of England.

Amendment 99, in schedule 2, page 141, line 18, leave out "body" and insert "person".

This amendment and Amendment 100 amend paragraph 9 of Schedule 2 to replace the reference to a "body" with a "person" for consistency with the table at paragraph 9, which includes functions that are conferred on individuals.

Amendment 100, in schedule 2, page 141, line 19, leave out "body" and insert "person".

See the explanatory statement for Amendment 99.

Amendment 101, in schedule 2, page 142, line 7, column 2, at end insert—

"() section 244 of the Investigatory Powers Act 2016;"

This amendment amends column 2 of the table at paragraph 9 of Schedule 2 so that functions conferred on the Commissioner by section 244 of the Investigatory Powers Act 2016 will be included within the scope of the exemption provided for by paragraph 9.

Amendment 102, in schedule 2, page 142, line 37, at end insert—

"1A. The Scottish Information Commissioner.	By or under— (a) the Freedom of Information (Scotland) Act 2002 (asp 13); (b) the Environmental Information (Scotland) Regulations 2004 (S.S.I. 2004/520); (c) the INSPIRE (Scotland) Regulations 2009 (S.S.I. 2009/440)."

This amendment amends the table at paragraph 9 of Schedule 2 so that functions conferred on the Scottish Information Commissioner by the legislation listed in column 2 of the table will be included within the scope of the exemption provided for by paragraph 9.

Amendment 103, in schedule 2, page 143, line 7, leave out "or under any" and insert "an".

This amendment amends the reference to functions conferred by or under any enactment in entry 5 of the table at paragraph 9. The words "or under" are not necessary because the definition of "enactment" in Clause 198 includes subordinate legislation.

Amendment 104, in schedule 2, page 143, line 7, at end insert—

"5A. The Financial Conduct Authority.	By or under the Financial Services and Markets Act 2000 or by another enactment."

This amendment amends the table at paragraph 9 of Schedule 2 so that functions conferred on the Financial Conduct Authority by the legislation listed in column 2 of the table will be included within the scope of the exemption provided for by paragraph 9.

Amendment 105, in schedule 2, page 143, line 22, at end insert—

"12. The Charity Commission.	By or under— (a) the Charities Act 1992; (b) the Charities Act 2006; (c) the Charities Act 2011."

This amendment amends the table at paragraph 9 of Schedule 2 so that functions conferred on the Charity Commission by the legislation listed in column 2 of the table will be included within the scope of the exemption provided for by paragraph 9.

Amendment 106, in schedule 2, page 146, line 22, leave out "16(4)(a) or (b)" and insert "16(4)(a), (b) or (c)".

This amendment is consequential on Amendment 112.

Amendment 107, in schedule 2, page 149, line 23, leave out

"with the date on which"

and insert "when".

This amendment is consequential on Amendment 71.

Amendment 108, in schedule 2, page 149, line 25, leave out "the date of".

This amendment is consequential on Amendment 71.

Amendment 109, in schedule 2, page 150, line 45, at end insert—

"( ) Article 19 (notification obligation regarding rectification or erasure of personal data or restriction of processing);"

This amendment adds Article 19 of the GDPR (notification obligation regarding rectification or erasure of personal data or restriction of processing) to the list of GDPR provisions that are disapplied by paragraph 24 of Schedule 2 to the Bill (journalistic, academic, artistic and literary purposes).

Amendment 110, in schedule 2, page 151, line 1, after "processor)" insert "—

(i) Article 34(1) and (4) (communication of personal data breach to the data subject);

(ii) "—*(Margot James.)*

This amendment adds Article 34 of the GDPR (communication of personal data breach to the data subject) to the list of GDPR provisions that are disapplied by paragraph 24 of Schedule 2 to the Bill (journalistic, academic, artistic and literary purposes).

Liam Byrne: I beg to move amendment 170, in schedule 2, page 151, line 8, at end insert—

"(f) in Chapter IX of the GDPR (provisions relating to specific processing situations), Article 89(1) (safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes)."

This amendment adds the restrictions imposed on archiving by the GDPR and the Bill to the list of matters in the Bill that benefit from the Journalism, Art and Literature exemption.

The purpose of this amendment is to protect some of our important national archives. We in this country are some of the greatest collectors on earth; the tradition established by Sir Hans Sloane all those centuries ago inspired many generations that followed him. Our ability and our tradition of collecting mean that this country is now home to some of the greatest collections on the planet.

It is fantastic to see many of these institutions now rapidly digitalising those archives. I was privileged to be able to visit the Natural History Museum recently, which I think is home to something like 83 million different specimens. It is now beginning to digitalise those archives in a way that opens them up not only to our schoolchildren, but to citizens of this country and those around the world who are keen on science.

The point of this amendment is that we cannot simply preserve those archives in aspic. They must be dynamic resources; they must be added to, and our success or failure in that task has a crucial bearing on the health of our democracy and our ability to, dare I say it, reflect on past mistakes and do better. I think it was the legendary Karl Popper who once said, "To err is human, to correct divine."

We make mistakes. It is important that we reflect on the mistakes we have made in the past, in order to do better next time around. Many of the more contemporary archives, particularly news archives, have had a crucial bearing on inquiries into historical child abuse, the injustices perpetrated at Hillsborough and at Orgreave, and HIV-contaminated blood. All those inquiries relied on records that were not necessarily historical; many were contemporary.

A range of crucial organisations entrusted with the delicate task of keeping our archives up to date are seriously worried about the provisions in the GDPR. In fact, they believe the inadequacy of the derogations and exemptions in the GDPR, as it is proposed that we draft it into law, means that they will be quickly put out of business. In particular, that will bite on thousands of smaller archives.

The point they have consistently made to us is that, although we have such great collections and archives in this country and a public interest culture around protecting some of those archives, we do not have any of the kind of legal protections that they enjoy in countries such as France. We do not have the defendable protections around archives that those abroad benefit from.

The challenge in this Bill is a lack of precision. I do not want to pretend that this is a black-and-white case. Sometimes news archives in particular will be required to draw something of a grey line, and I am afraid the Minister has to earn her pay and be the one to decide where to draw that grey line. Sometimes there will be information stored in those archives that absolutely should be subject to the GDPR provisions. But if we are in effect granting a carte blanche for people to make requests of archives that require those archives to dip deep into the historical record, correct things and go through challenging processes to ensure they are right, I am afraid it will put a number of our archives out of business, and that will damage the health of our democracy.

We have drafted this amendment with a number of aims. We want to try to create a statutory definition for organisations that archive in the public interest. We have had a first attempt at drawing that in a narrow way, so it does not infringe on material that is stored that absolutely should be subject to general GDPR provisions. We have done our best to ensure that the archiving exemptions are proportionate to the public interest nature of the material being archived. We wanted to offer an amendment worded hopefully in such a way that, frankly, it excludes Google, Facebook and others from enjoying the exemptions sought here.

This is the first place in the Bill where the debate rears its head. I am grateful to the range of museums, archives and the BBC that have helped us to craft this amendment. It should not be particularly controversial. There should be agreement across the Committee on the need to protect our great collections, yet keep some companies, such as Google and Facebook, subject to the provisions in the Bill.

We offer the amendment as a starter for 10. Obviously, we would be delighted if the Government accepted it; we would be even more pleased if they could perfect it.

The Chair: I have just had a request to remove jackets, because of the warm temperature in the room. I give my permission to do so. I call the Minister.

Margot James: Thank you, Mr Hanson. I agree with the tribute paid by the right hon. Member for Birmingham, Hodge Hill to the custodians of some of the most wonderful archives in the world. I will comment on his proposals with regard to such archives shortly, but I hope that recent debates have left no doubt in

[Margot James]

hon. Members' minds that the Government are absolutely committed to preserving the freedom of the press, and maintaining the balance between privacy and freedom of expression in our existing law, which has served us well for so many years.

As set out in the Bill, media organisations can already process data for journalistic purposes, which includes media archiving. As such, we believe that amendment 170 is unnecessary and could be unhelpful. I agree with the right hon. Gentleman that it is crucial that the media can process data and maintain media archives. In the House of Lords, my noble Friend Lord Black of Brentwood explained very well the value of media archives. He said:

"Those records are not just the 'first draft of history'; they often now comprise the only record of significant events, which will be essential to historians and others in future, and they must be protected."—[*Official Report, House of Lords,* 10 October 2017; Vol. 785, c. 175.]

However, recital 153 indicates that processing for special purposes includes news archiving and press libraries. Paragraph 24 of schedule 2 sets out the range of derogations that apply to processing for journalistic purposes. That includes, for example, exemption from complying with requests for the right to be forgotten. That means that where the exemption applies, data subjects would not have grounds to request that data about them be deleted. It is irrelevant whether the data causes substantial damage or distress.

However, if media organisations are archiving data for other purposes—for example, in connection with subscriber data—it is only right that they are subjected to the safeguards set out in article 89(1), and the Bill provides for that accordingly. For that reason, I hope that the right hon. Gentleman agrees to reconsider his approach and withdraw his amendment.

Liam Byrne: I am happy to withdraw the amendment, although I would say to the Minister that the helpful words we have heard this afternoon will not go far enough to satisfy the objections that we heard from organisations. We reserve the right to come back to this matter on Report. We will obviously consult the organisations that helped us to draft the amendment, and I urge her to do the same. I beg to ask leave to withdraw the amendment.

Amendment, by leave, withdrawn.

Schedule 2, as amended, agreed to.

Schedule 3

Exemptions etc from the GDPR: health, social work, education and child abuse data

Amendments made: 111, in schedule 3, page 160, line 21, leave out

"with the day on which"

and insert "when".

This amendment is consequential on Amendment 71.

Amendment 112, in schedule 3, page 162, line 3, leave out paragraph 16 and insert—

"16 (1) This paragraph applies to a record of information which—

(a) is processed by or on behalf of the Board of Governors, proprietor or trustees of, or a teacher at, a school in Northern Ireland specified in sub-paragraph (3),

(b) relates to an individual who is or has been a pupil at the school, and

(c) originated from, or was supplied by or on behalf of, any of the persons specified in sub-paragraph (4).

(2) But this paragraph does not apply to information which is processed by a teacher solely for the teacher's own use.

(3) The schools referred to in sub-paragraph (1)(a) are—

(a) a grant-aided school;

(b) an independent school.

(4) The persons referred to in sub-paragraph (1)(c) are—

(a) a teacher at the school;

(b) an employee of the Education Authority, other than a teacher at the school;

(c) an employee of the Council for Catholic Maintained Schools, other than a teacher at the school;

(d) the pupil to whom the record relates;

(e) a parent, as defined by Article 2(2) of the Education and Libraries (Northern Ireland) Order 1986 (S.I. 1986/594 (N.I. 3)).

(5) In this paragraph, "grant-aided school", "independent school", "proprietor" and "trustees" have the same meaning as in the Education and Libraries (Northern Ireland) Order 1986 (S.I. 1986/594 (N.I. 3))."

This amendment expands the types of records that are "educational records" for the purposes of Part 4 of Schedule 3.

Amendment 113, in schedule 3, page 164, line 7, leave out

"with the day on which"

and insert "when".—*(Margot James.)*

This amendment is consequential on Amendment 71.

Schedule 3, as amended, agreed to.

Schedule 4 agreed to.

Clause 16

Power to make further exemptions etc by regulations

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

4.30 pm

Stuart C. McDonald: This morning we had a discussion about some of the Henry VIII clauses contained in the Bill. In essence, I said that when we are talking about personal information—particularly, in such circumstances, sensitive personal information—there should be a strong presumption against Henry VIII clauses, with the onus being on the Government to justify why delegated legislation is the appropriate way to make changes to our data protection rules.

Throughout the passage of the Bill we will continue to challenge the Government to justify delegated powers proposed under the Bill. This clause is the next example of that arising, so in our view it falls on the Minister to explain why she seeks delegated authority to exercise certain functions under the GDPR. I look forward to hearing what she has to say.

Liam Byrne: We agree that the clause offers Ministers a rather sweeping power to introduce new regulations. Over the course of what has been quite a short day in Committee we have heard many reasons to be alarmed about equipping Ministers with such sweeping powers. We proposed an amendment to remove the clause, which I think was not selected because we have this stand part debate. What we need to hear from the

Minister are some pretty good arguments as to why Ministers should be given unfettered power to introduce such regulations without the effective scrutiny and oversight of right hon. and hon. Members in this House.

Margot James: I am glad that the right hon. Gentleman feels we have had a short day in Committee. In answer to his questions and those of the hon. Gentleman, the order making powers in clauses 16 and 113 allow the Secretary of State to keep the list of exemptions in schedules 2 to 4 and 11 up to date. As I mentioned when we discussed order making powers in relation to clause 10 and schedule 1, we carefully reviewed the use of such powers in the Bill following recommendations from the Delegated Powers and Regulatory Reform Committee. We think an appropriate balance has now been struck. It might be helpful if I explain the reasons for our thinking.

Clause 16 includes order making powers to ensure that the Secretary of State can update from time to time the particular circumstances in which data subjects' rights can be disapplied. That might be necessary if, for example, the functions of a regulator are expanded and exemptions are required to ensure that those new functions cannot be prejudiced by a data subject exercising his or her right to object to the processing.

We believe it is very important that the power to update the schedules is retained. Several of the provisions in schedules 2 to 4 did not appear in the Data Protection Act 1998 and have been added to the Bill to address specific requirements that have arisen over the last 20 years.

For example, the regulatory landscape has changed dramatically since the 1998 Act. Organisations such as the Bank of England, the Financial Conduct Authority and the National Audit Office have taken on a far broader range of regulatory functions, and that is reflected in the various amendments we have tabled to paragraphs 7 to 9 of schedule 2, to provide for a broader range of exemptions. No doubt, there will be further changes to the regulatory landscape in the years to come. Of course, other exemptions in schedule 2 have been carried over from the 1998 Act, or indeed from secondary legislation made under that Act, with little change. That does not mean, however, that they will never need to be amended in the future. Provisions made under the 1998 Act could be amended via secondary legislation, so it would seem remiss not to afford ourselves that same degree of flexibility now. If we have to wait for primary legislation to make any changes, it could result in a delay of months or possibly years to narrow or widen an extension, even where a clear deficiency had been identified. We cannot predict the future, and it is important that we retain the power to update the schedules quickly when the need arises.

Importantly, any regulations made under either clause would be subject to the affirmative resolution procedure. There would be considerable parliamentary oversight before any changes could be made using these powers. Clause 179 requires the Secretary of State to consult with the Information Commissioner and other interested parties that he considers appropriate before any changes are made.

I hope that that reassures Members that we have considered the issue carefully. I commend clause 16 to the Committee.

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

The Committee proceeded to a Division.

The Chair: The ayes were 10, the noes were nine. No—*[Interruption.]* I have been here a long time.

The Committee having divided: Ayes 10, Noes 9.

Division No. 5]

AYES

Adams, Nigel	Jack, Mr Alister
Atkins, Victoria	James, Margot
Clark, Colin	Lopez, Julia
Heaton-Jones, Peter	Warman, Matt
Huddleston, Nigel	Wood, Mike

NOES

Byrne, rh Liam	Murray, Ian
Elmore, Chris	O'Hara, Brendan
Haigh, Louise	Snell, Gareth
Jones, Darren	Zeichner, Daniel
McDonald, Stuart C.	

Question accordingly agreed to.

Clause 16 ordered to stand part of the Bill.

Clause 17

ACCREDITATION OF CERTIFICATION PROVIDERS

Margot James: I beg to move amendment 15, in clause 17, page 10, line 16, leave out "authority" and insert "body".

This amendment corrects the reference in Clause 17(7) to the "national accreditation authority" by amending it to refer to the "national accreditation body", which is defined in Clause 17(8).

Clause 17 relates to the certification of data controllers. This is a relatively new concept and will take time to bed in, but it could also be a significant step forward in ensuring that data subjects can have confidence in controllers and processors and, perhaps even more important, that controllers and processors can have confidence in each other. It is likely to be particularly relevant in the context of cloud computing and other business-to-business platforms where individual audits are often not feasible in practice.

Before they can audit controllers, certification bodies must be accredited, either by the Information Commissioner or by the national accreditation body, UKAS. Clause 17 and schedule 5 set out how the process will be managed. Unfortunately, there is a typographical error in clause 17. It refers erroneously to the "national accreditation authority" in subsection (7), when it should refer to the "national accreditation body". Amendment 15 corrects that error.

Amendment 15 agreed to.

Clause 17, as amended, ordered to stand part of the Bill.

Schedule 5

ACCREDITATION OF CERTIFICATION PROVIDERS: REVIEWS AND APPEALS

Amendment made: 114, in schedule 5, page 170, line 21, leave out "In this paragraph" and insert—

"Meaning of "working day"

7 In this Schedule"

This amendment applies the definition of "working day" for the purposes of the whole of Schedule 5. There are references to "working days" in paragraphs 5(2) and 6(3) of that Schedule.—(Margot James.)

Schedule 5, as amended, agreed to.

Clause 18 ordered to stand part of the Bill.

Clause 19

PROCESSING FOR ARCHIVING, RESEARCH AND STATISTICAL PURPOSES: SAFEGUARDS

Amendment made: 16, in clause 19, page 12, line 2, leave out "(d)" and insert "(e)" *—(Margot James.)*

This amendment amends the definition of "relevant NHS body" in this Clause by adding special health and social care agencies established under Article 3 of the Health and Personal Social Services (Special Agencies) (Northern Ireland) Order 1990 (which fall within paragraph (e) of section 1(5) of the Health and Social Care (Reform) Act (Northern Ireland) 2009).

Clause 19, as amended, ordered to stand part of the Bill.

Clauses 20 to 22 ordered to stand part of the Bill.

Ordered, That further consideration be now adjourned.*—(Nigel Adams.)*

4.43 pm

Adjourned till Thursday 15 March at half-past Eleven o'clock.

Written evidence reported to the House

DPB 01 David Burns

DPB 02 Liberty

DPB 03 Michael Veale UCL, Dr Reuben Binns U Oxford), Prof Lilian Edwards U (Strathclyde)

DPB 04 Future Care Capital

DPB 05 Information Commissioner's Office

DPB 06 Big Brother Watch

DPB 07 Privacy International

DPB 08 Stephen Rickitt, Clerk to Glanton, Meldon, Milfield, Mitford and Whalton Parish Councils

DPB 09 British Dental Association

DPB 10 Optical Confederation

DPB 11 Press Association

DPB 12 WAN-IFRA, CPU Media Trust, and News Media Europe

DPB 13 Sport and Recreation Alliance

DPB 14 BMA (British Medical Association)

DPB 15 John Gordon

DPB 16 Immigration Law Practitioners' Association (ILPA)

DPB 17 British Paralympic Association

DPB 18 YoungMinds and The Children's Society

DPB 19 Pact

DPB 20 The Law Society

DPB 21 The Officers' Association

DPB 22 Amnesty International UK

DPB 23 Association for Financial Markets in Europe (AFME)

DPB 24 News Media Association