House of Commons Library

Research Briefing

By John Woodhouse

9 June 2023

Data Protection and Digital Information (No. 2) Bill: progress of the Bill

Contributing Authors
Lorraine Conway, Privacy and electronic marketing

Image Credits
Data protection. Licenced under Creative Commons CC0. No copyright required.

Feedback
Every effort is made to ensure that the information contained in these publicly available briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Please note that authors are not always able to engage in discussions with members of the public who express opinions about the content of our research, although we will carefully consider and correct any factual errors.

You can read our feedback and complaints policy and our editorial policy at commonslibrary.parliament.uk. If you have general questions about the work of the House of Commons email hcenquiries@parliament.uk.

Contents

Summary

The Data Protection and Digital Information Bill [Bill 001 2023-24] (PDF) was introduced in the House of Commons on 8 November 2023. It was first introduced during the 2022-23 session as the Data Protection and Digital Information (No. 2 Bill). The Bill has been carried over to the 2023-24 session. It had its remaining stages in the Commons on 29 November 2023. A House of Lords Library briefing summarises the amendments that were made (PDF).

The Bill [HL Bill 30 2023-24] (PDF) was introduced in the House of Lords on 6 December 2023. It is scheduled to have its second reading in the Lords on 19 December 2023.

This Library briefing was published in the last session and refers to the Bill under its 2022-23 title.

What would the Data Protection and Digital Information (No. 2) Bill do?

The Data Protection and Digital Information (No. 2) Bill [Bill 265 2022-23] was introduced in the House of Commons on 8 March 2023.

Much of the Bill is the same as the Data Protection and Digital Information Bill [Bill 143 2022-23] which was introduced in the Commons on 18 July 2022. The Bill was scheduled to have its second reading on 5 September 2022. A Library Briefing on the Bill (PDF) (31 August 2022) was published for the debate. However, in a Business Statement on 5 September 2022, the Government said that, following the election of Elizabeth Truss as Conservative Party leader, second reading would not take place. This was to allow Ministers to consider the Bill further. The Bill was withdrawn on 8 March 2023.

In a Written Ministerial Statement of 8 March 2023, Michelle Donelan, Secretary of State for Science, Innovation and Technology, said the new Bill followed a detailed codesign process with industry, business, privacy and consumer groups. The Bill would seize the post-Brexit opportunity to "create a new UK data rights regime tailor-made for our needs". It would reduce burdens on businesses and researchers and would boost the economy by £4.7 billion over the next decade. The Secretary of State explained that changes had been made to the original Bill that would:

- reduce compliance costs in the sector and reduce the amount of paperwork that organisations need to complete to demonstrate compliance.
- reduce burdens by enabling businesses to continue to use their existing cross-border transfer mechanisms if they are already compliant.

- give organisations greater confidence about the circumstances in which they can progress personal data without consent.
- increase public and business confidence in AI technologies.

The Bill would:

- establish a framework for the provision of digital verification services to enable digital identities to be used with the same confidence as paper documents.
- increase fines for nuisance calls and texts under the Privacy and Electronic Communications Regulations (PECR).
- update the PECR to cut down on 'user consent' pop-ups and banners.
- allow for the sharing of customer data, through smart data schemes, to provide services such as personalised market comparisons and account management.
- reform the way births and deaths are registered in England and Wales, enabling the move from a paper-based system to registration in an electronic register.
- facilitate the flow and use of personal data for law enforcement and national security purposes.
- create a clearer legal basis for political parties and elected representatives to process personal data for the purposes of democratic engagement.

The governance structure and powers of the Information Commissioner's Office (ICO, the data protection regulator) would also be reformed and transferred to a new body, the Information Commission.

Policy background to the Bill, as it was originally introduced, is set out in the Library briefing, Data Protection and Digital Information (No. 2) Bill (28 March 2023).

Progress of the Bill

The Bill had its second reading in the House of Commons on 17 April 2023. A carry-over motion, allowing it to be carried into the next parliamentary session, was approved on the same date.

The Bill was considered by a Public Bill Committee over eight sittings between 10 and 23 May 2023. Oral evidence was taken from expert witnesses during the first two sittings.

Line by line examination took place over six sittings between 16 and 23 May 2023. Nearly all divisions took place in relation to Labour amendments on the data protection provisions in Part 1 of the Bill. None of the amendments were

agreed. Two Labour amendments on the privacy and electronic communications provisions in Part 4 were not agreed. There were also divisions on three new clauses moved by Labour; these were again unsuccessful.

Government amendments, mainly minor or technical were agreed. Government new clauses 1 to 7 were added to the Bill.

This briefing mainly focuses on the Committee's debates on Part 1 of the Bill.

The Bill (Bill 314 2022-23)(PDF), as amended in Committee, has been published.

1 Second reading

The Bill had its second reading in the House of Commons on 17 April 2023.

Julia Lopez, Minister of State for Data and Digital Infrastructure, said that data was the "fuel driving the digital age" and that the challenge for democracies was to use data to "empower rather than control citizens".[1]

She claimed the UK could not simply rubber-stamp the latest iteration of the EU General Data Protection Regulation (GDPR) and that the UK had "a critical opportunity to take a new path" and lead the global conversation about how to best use data as a force for good. Julia Lopez said the Bill marked an evolution away from an "inflexible one-size-fits-all regime" towards one that was risk-based and focused on innovation, flexibility and the needs of citizens, scientists, public services, and companies.[2] The Minister also noted that the Government had been in contact with the European Commission (EC) about the Bill's proposals so there were "no surprises". She believed the UK would therefore maintain its EC adequacy decisions (these allow the free flow of data from the EU/EEA) following the enactment of the Bill.[3]

According to Lucy Powell, the Shadow Secretary of State for Digital, Culture, Media and Sport, the Bill did not rise to the challenges posed by technological developments (eg AI chatbots and AI image generators). Instead, it tweaked the edges of the GDPR and would make an "already dense set of privacy rules even more complex".[4] Lucy Powell agreed that data reform was "welcome and long overdue", did not disagree with the Bill's aims, but had "serious questions" about whether it would achieve them.[5] She raised the following issues:

- possible loss of data adequacy with the EU.
- business concerns about having to comply with the GDPR and the new requirements of the Bill.
- reducing protection for citizens – eg through the "diluting" of subject access requests and weakening protections against automated decision making.

1 HC Deb 17 April 2023 c67
2 HC Deb 17 April 2023 c67
3 HC Deb 17 April 2023 c70
4 HC Deb 17 April 2023 c73
5 HC Deb 17 April 2023 c74

- an increase in the Secretary of State's powers.[6]

Lucy Powell said the Bill failed to address how data was pooled together to analyse trends and predict behaviours. It also did not tackle how algorithms analysed data, often replicating and entrenching society's biases. Finally, after referring to exam algorithms and the mishandling of GP data, she said the Bill was a missed opportunity in relation to building public trust.[7]

Carol Monaghan, the Shadow SNP spokesperson for Science, Innovation and Technology, said the Bill should not put at risk the free flow of data with the EU.[8] She also raised concerns about:

- increased burdens on businesses.
- solely automated decision being permitted in a wider range of contexts.
- weakening the protections of UK citizens' data by allowing it to be transferred abroad in cases with lower safeguards.
- increased powers for the Secretary of State, the police, and the security services.[9]

Layla Moran, the Liberal Democrat spokesperson for Science, Innovation and Technology, said that where there was a conflict of interest between the citizen, business and the state, the citizen "always comes top". However, she was not convinced the citizen was always at the "heart of the Bill". Layla Moran said the Liberal Democrats were concerned that the Bill would:

- undermine people's data rights.
- concentrate power with the Secretary of State.
- jeopardise data adequacy with the EU.[10]

Stephanie Peacock, Shadow Minister for Digital, Culture, Media and Sport, said there were many areas where the Bill could be clarified and improved. She looked forward to working with Ministers to ensure the Bill put the UK at the "forefront of data use and data protection".[11]

6 HC Deb 17 April 2023 cc74-6
7 HC Deb 17 April 2023 c76
8 HC Deb 17 April 2023 c79
9 HC Deb 17 April 2023 cc79-81
10 HC Deb 17 April 2023 cc94-5
11 HC Deb 17 April 2023 c100

2 Public Bill Committee

The Bill was considered by a Public Bill Committee over eight sittings between 10 and 23 May 2023. Oral evidence was taken from expert witnesses during the first two sittings.

Line by line examination took place over six sittings between 16 and 23 May 2023. Nearly all divisions took place in relation to Labour amendments on the data protection provisions in Part 1 of the Bill. None of the amendments were agreed. Two Labour amendments on the privacy and electronic communications provisions in Part 4 were not agreed. There were also divisions on three new clauses moved by Labour; these were again unsuccessful.

Government amendments, mainly minor or technical were agreed. Government new clauses 1 to 7 were added to the Bill.

The remainder of this briefing mainly focuses on the Committee's debates on the Bill's data protection provisions in Part 1.

Further background and detail on the clauses discussed below can be found in the Library briefing, Data Protection and Digital Information (No. 2) Bill (28 March 2023).

Written evidence submitted to the Committee is available from the parliament website.

The Bill (Bill 314 2022-23)(PDF), as amended in Committee, has been published.

2.1 Part 1: Data protection

Meaning of research and statistical purposes

Clause 2 of the Bill would amend Article 4 of the UK GDPR. Under new Article 4(3), references to the processing of personal data for the purposes of scientific research (including references to processing for "scientific research purposes") would mean "references to processing for the purposes of any research that can reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity".

When **clause 2** was debated, Stephanie Peacock moved **amendment 66** to exempt children's data from being used for commercial purposes under the

definition of scientific purposes.[12] She said that extra safeguards needed to be in place for children's data to ensure that any processing was in their best interests. She also hoped it would create a precedent for automatically giving children's rights the best protection possible.[13]

John Whittingdale, Minister for Data and Digital Infrastructure, resisted the amendment, claiming it could "obstruct important research by commercial organisations, such as research into children's diseases".[14]

Amendment 66 was negatived on division by 9 votes to 6.[15]

Stephanie Peacock also moved **amendment 65**. This would require the Information Commissioner (ICO) to publish a statutory code of practice on how the clause's definition of scientific research should be interpreted.[16] The Shadow Minister said it was important that the definition was not open to exploitation, or so broad that any controller could reasonably identify their processing as falling under it.[17]

John Whittingdale said that examples of the types of activity that would be considered scientific research would be best placed in non-statutory guidance produced by the ICO. This would give flexibility to amend and change the examples when necessary. The Minister said that, when the Bill was in force, the Government would work with the ICO to update its guidance on the definition of scientific research as necessary.[18]

Amendment 65 was negatived on division by 9 votes to 6.[19]

Lawfulness of processing

Clause 5 of the Bill would create a new lawful ground for processing personal data by inserting new Article 6(1)(ea) into the UK GDPR. This would mean that processing would be lawful where it was necessary for a recognised legitimate interest.

Clause 5 would also insert new paragraphs into Article 6 of the UK GDPR. New Article 6(5) would define processing necessary for a recognised legitimate interest for the purposes of new Article 6(1)(ea) as processing that met a condition in new Annex 1 to the UK GDPR. Under new Articles 6(6) to (8), the Secretary of State could make regulations to amend the recognised legitimate interest activities in Annex 1. Before laying regulations, the Secretary of State would need to consider the effects of any changes on the

12 PBC 16 May 2023 c89
13 PBC 16 May 2023 cc91-2
14 PBC 16 May 2023 c89
15 PBC 16 May 2023 c94
16 PBC 16 May 2023 c89
17 PBC 16 May 2023 c90
18 PBC 16 May 2023 c93
19 PBC 16 May 2023 c94

interests and fundamental rights and freedoms of data subjects, particularly children. The regulations would be subject to the affirmative procedure.

When **clause 5** was debated, Stephanie Peacock moved **amendment 68**. This would make the Secretary of State's ability to amend the conditions in Annex 1 subject to a requirement for consultation with interested parties and with the Information Commissioner. The Commissioner and interested parties would be required to publish their views on any proposed change.[20] Stephanie Peacock said the amendment would move the responsibility for judging the impact of changes away from the Secretary of State. It would ensure that amendments would only proceed if they were deemed to be in the "collective societal interest". There would be independent assurance that any amendments were not "politically or maliciously motivated".[21]

John Whittingdale said the amendment was unnecessary because clause 5 would already require the Secretary of State to consider the impact of any changes to the list on the rights and freedoms of individuals and, where relevant, the need to provide children with special protection regarding their personal data. The regulation-making powers in the clause would also be subject to the new requirements in clause 44. These provide that any regulations made under the UK GDPR would be subject to consultation with the Information Commissioner and other persons that the Secretary of State considered appropriate. The affirmative procedure would also apply.[22]

Amendment 68 was negatived on division by 9 votes to 6.[23]

Stephanie Peacock also moved **amendment 67**. This would require data controllers to document and publish a statement on their reliance on a "recognised legitimate interest" for processing personal data.[24] This would explain exactly which processing the company was conducting under which purpose and why it was necessary.[25]

John Whittingdale said the amendment would "significantly weaken" the clause and would reintroduce something similar to the legitimate interests assessment. This could "unnecessarily delay some very important processing activities".[26]

Amendment 67 was negatived on division by 9 votes to 6.[27]

Government new clause 6 and amendments

Government new clause 6 (Special categories of personal data: elected representatives responding to requests) was debated. John Whittingdale

20 PBC 16 May 2023 c96
21 PBC 16 May 2023 c99
22 PBC 16 May 2023 c100
23 PBC 16 May 2023 c101
24 PBC 16 May 2023 c96
25 PBC 16 May 2023 c98
26 PBC 16 May 2023 c100
27 PBC 16 May 2023 c101

explained that data protection law prohibited the use of "special category" data unless certain conditions or exemptions applied. One exemption is where processing is necessary on grounds of substantial public interest:

> Schedule 1 to the Data Protection Act 2018 sets out a number of situations where processing would be permitted on grounds of substantial public interest, subject to certain conditions and safeguards. That includes processing by elected representatives who are acting with the authority of their constituents for the purposes of progressing their casework. The current exemption applies to former Members of the Westminster and devolved Parliaments for four days after a general election—for example, if the MP has been defeated or decides to stand down. That permits them to continue to rely on the exemption for a short time after the election to conclude their parliamentary casework or hand it over to the incoming MP. In practice, however, it can take much longer than that to conclude these matters.[28]

John Whittingdale said the new clause would extend the "four-day rule" to 30 days to give outgoing MPs and members of the devolved Parliaments more time to conclude casework. The new clause would avoid the "unwelcome situation" where an outgoing MP, who was doing their best to conclude constituency casework, could be acting unlawfully if they continued to process their constituents' sensitive data after the four-day time limit had elapsed.[29]

New clause 6 was added to the Bill.[30]

Government amendments 30 and 31 were also agreed. These would make identical changes to other parts of the Bill that relied on the same definition of "elected representative". John Whittingdale explained:

> Government amendment 30 will change the definition of "elected representative" when the term appears in schedule 1…clause 5 and schedule 1 to the Bill create a new lawful ground for processing non-sensitive personal data, where the processing is necessary for a "recognised legitimate interest". The processing of personal data by elected representatives for the purposes of democratic engagement is listed as such an interest, along with other processing activities of high public importance, such as crime prevention, safeguarding children, protecting national security and responding to emergencies.
>
> Government amendment 31 will make a similar change to the definition of "elected representative" when the term is used in clause 84. Clauses 83 and 84 give the Secretary of State the power to make regulations to exempt elected representatives from some or all of the direct marketing rules in the Privacy and Electronic Communications (EC Directive) Regulations 2003…[31]

Labour supported the amendments.[32]

---

28 PBC 16 May 2023 c102

29 PBC 16 May 2023 c102

30 PBC 23 May 2023 c283

31 PBC 16 May 2023 c103

32 PBC 16 May 2023 cc103-4

Purpose limitation

Clause 6 sets out the conditions for determining whether the reuse of personal data ("further processing") is permitted in compliance with the purpose limitation principle outlined in Article 5 of the UK GDPR (this principle prohibits further processing that is not compatible with the original purpose for which the personal data was collected). Clause 6 would permit the reuse of personal data by a controller when:

- the new purpose was "compatible".
- fresh consent was obtained.
- there was a research purpose.
- the UK GDPR was being complied with (eg for anonymisation or pseudonymisation purposes).
- there was an objective in the public interest authorised by law.
- certain specified objectives in the public interest set out in a list in schedule 2 were met.

Clause 6 contains a power to add, amend, or remove conditions added by regulations from the list to ensure it could be kept up to date with any future developments in how personal data should be reused in the public interest. It also sets out restrictions on reusing personal data that the controller originally collected based on consent.

When clause 6 was debated, Stephanie Peacock moved **amendment 69**. This would mean the Secretary of State could not make changes, through secondary legislation, to the way purpose limitation would operate.[33] The Shadow Minister said the clause would give the Secretary of State new Henry VIII powers to add to the new list of compatible purposes whenever they wished, with no provisions made for consulting on, scrutinising or assessing the impact of such changes. Secondary legislation was "absolutely not a substitute for parliamentary scrutiny of primary legislation".[34]

John Whittingdale said the power would only be used "when necessary and in the public interest". It could only be used to safeguard an objective listed in article 23 of the UK GDPR. Clause 44 of the Bill would also require the Secretary of State to consult the Information Commissioner, and any other persons considered appropriate, before making any regulations.[35]

Amendment 69 was negatived on division by 9 votes to 6.[36]

33 PBC 16 May 2023 c104
34 PBC 16 May 2023 c105
35 PBC 16 May 2023 c107
36 PBC 16 May 2023 c107

Stephanie Peacock moved **amendment 70** to **schedule 2** (purpose limitation: processing to be treated as compatible with original purpose). This would clarify that personal data could be processed as a "legitimate interest" under this paragraph only when the processing was carried out for the purposes of the assessment or collection of a tax or duty or the imposition of a similar nature levied by a public authority.[37] When speaking to the amendment, Stephanie Peacock referred to concerns expressed by Which? - ie that the current wording was too vague, especially without a definition of "tax" or "duty" for the purposes of paragraph 10 of annex 2, leaving the data open to wider commercial use. Amendment 70 would close any potential loopholes by linking the condition to meeting a specific statutory obligation to co-operate with a public authority such as His Majesty's Revenue and Customs.[38]

Stephanie Peacock also moved **amendment 71** to **schedule 2** that she said would correct a similar oversight in paragraph 1 of annex 2, as identified by the AWO and Reset.tech:

> Paragraph 1 aims to ensure that processing is treated as compatible with the original purpose when it is necessary for making a disclosure of personal data to another controller that needs to process that data for a task in the public interest or in the exercise of official authority and that has requested that data. However, the Bill says that processing is to be treated as compatible with the original purpose where such a request simply "states" that the other person needs the personal data for the purposes of carrying out processing that is a matter of public task. At very least, those matters should surely be actually true, rather than just stated. Amendment 71 would close that loophole, so that the request must confirm a genuine need for data in completing a task in the public interest or exercising official authority, rather than simply being a statement of need.[39]

On amendment 70, John Whittingdale said that taxation was not included in the annex 1 list of legitimate interests. That meant that anyone seeking to use the legitimate interest lawful ground for that purpose would need to carry out a balancing-of-interests test, unless they were responding to a request for information from a public authority or other body with public tasks set out in law.[40] Stephanie Peacock said she was reassured and withdrew her amendment.[41]

When responding to amendment 71, John Whittingdale explained the purpose of the first paragraph in new annex 2 to the UK GDPR, as inserted by schedule 2:

> The purpose of that provision is to clarify that non-public bodies can disclose personal data to other bodies in certain situations to help those bodies to deliver public interest tasks in circumstances in which personal data might have been collected for a different purpose. For example, it might be necessary for a commercial organisation to disclose personal data to a

37 PBC 16 May 2023 c108
38 PBC 16 May 2023 c108
39 PBC 16 May 2023 c108
40 PBC 16 May 2023 c109
41 PBC 16 May 2023 c109

> regulator on an inquiry so that that body can carry out its public functions. The provision is tightly formulated and will permit disclosure from one body to another only if the requesting organisation states that it has a public interest task, that it has an appropriate legal basis for processing the data set out in law, and that the use of the data is necessary to safeguard important public policy or other objectives listed in article 23.[42]

The Minister said non-public bodies would not be expected to hand over personal data "on entirely spurious grounds" because of the safeguards he had described. Stephanie Peacock said he had not addressed all of her concerns and put amendment 71 to a division. It was negatived by 9 votes to 6.[43]

Vexatious or excessive requests by data subjects

Clause 7 of the Bill would insert new Article 12A into the UK GDPR. This would amend the threshold for charging a reasonable fee or refusing a subject access request from "manifestly unfounded or excessive" to "vexatious or excessive".

When clause 7 was debated, Stephanie Peacock moved three amendments. **Amendment 74** would oblige data controllers to issue a notice to a data subject explaining why they were not complying with a subject access request, charging for a request, their right to make a complaint to the ICO, and their ability to seek to enforce this right through a judicial remedy.[44]

Amendment 73 would clarify that, when considering "resources available to the controller" for deciding whether a subject access request was vexatious or excessive, this could not include where an organisation had neglected to appoint staff but had the resources to do so.[45]

Amendment 72 would require the ICO to produce a code of practice on how the terms "vexatious" and "excessive" should be applied, with examples of the kind of requests that might be troublesome to deal with but were neither vexatious nor excessive.[46]

When speaking to the amendments, Stephanie Peacock noted that the right of access was key to transparency and often underpinned people's ability to exercise their other rights as data subjects.[47] She said that stakeholders such as the TUC, the Public Law Project and Which? had expressed concerns that, as currently drafted, the terms making up the new threshold were too subjective and could be open to abuse by controllers who might define any request they didn't want to answer as vexatious or excessive.

42 PBC 16 May 2023 c109
43 PBC 16 May 2023 c110
44 PBC 16 May 2023 c110
45 PBC 16 May 2023 c110
46 PBC 16 May 2023 c110
47 PBC 16 May 2023 c111

Stephanie Peacock said that without clarity on how the new threshold and considerations would apply, the ability of data subjects to raise a legal complaint about why their request was categorised as vexatious and excessive would be severely impeded.[48]

John Whittingdale resisted the amendments. In relation to amendment 73, he pointed out that controllers could already consider resourcing when refusing or charging a reasonable fee for a request. The Government did not wish to change that.[49] On amendment 72, the Minister claimed the new "vexatious or excessive" language in the Bill gave greater clarity than there had previously been. Regarding amendment 74, John Whittingdale said the current legislation set out that any request from a data subject, including subject access requests, had to be responded to. The Government was retaining that approach. ICO guidance set out the obligations of controllers and the Government did not plan to suggest a move away from that approach.[50]

All three amendments were negatived by 9 votes to 6.[51]

Clause 7 was added to the Bill after a division (9 votes to 6).[52]

Automated decision-making

Clause 11 of the Bill would substitute Article 22 of the UK GDPR with new Articles 22A-D so that automated decision-making would not be restricted to the three circumstances as at present - ie where the processing is:

- necessary for the purposes of a contract between the data subject and an organisation;
- authorised by law; or
- based on the data subject's explicit consent).

A decision would be based solely on automated processing if there was "no meaningful human involvement in the taking of the decision".[53] A decision would be a "significant decision" in relation to a data subject if it:

- produced a legal effect for the data subject; or
- had a similarly significant effect for the data subject.[54]

48 PBC 16 May 2023 c112
49 PBC 16 May 2023 c114
50 PBC 16 May 2023 c114
51 PBC 16 May 2023 c116
52 PBC 16 May 2023 c117
53 Article 22A(1)(a)
54 Article 22A(1)(b)(i) and (ii)

Article 22A(2) would require controllers to consider, among other things, the extent to which a decision had been taken based on profiling when establishing whether or not human involvement had been meaningful.

A significant decision involving special category personal data could not be taken based solely on automated processing unless one of two conditions was met:

1. the data subject had given explicit consent; or
2. the decision was required or authorised by law. The decision would also have to be in the substantial public interest.[55]

Safeguards for when a significant decision had been taken through solely automated processing would include:

- notifying the data subject after such a decision had been taken.
- enabling the data subject to make representations about the decision.
- enabling the data subject to obtain human intervention on the part of the controller in relation to such a decision.
- enabling the data subject to contest such a decision.[56]

The Secretary of State would have the power, through regulations, to amend what would constitute a significant decision that produced an effect on a data subject that was similarly significant to a legal one.[57]

When clause 11 was debated, Stephanie Peacock moved **amendment 78**. This, together with **amendments 79** to **101**, would apply the rights given to data subjects by clause 11 to "decision subjects".[58] **New clause 12** would define a "decision subject" as "an identifiable individual who is subject to data-based and automated decision-making".[59]

When speaking to the amendments and new clause 12, Stephanie Peacock said that most data protection legislation operated on the assumption that the only people affected by data-based and automated decision-making were data subjects. Most protections available are therefore tied to being a data subject: an identifiable living person whose data has been used or processed. However, it is increasingly common (eg in healthcare, employment, and education) for algorithms created and trained on one set of people to be used to reach conclusions about another set of people. This means an algorithm can make an automated decision affecting an individual to a legal or similarly significant degree without having specifically used their personal data. New

55 Article 22B(1), (2), and (3)
56 Article 22C(1) and (2)
57 Article D(1) and (2)
58 PBC 16 May 2023 c123
59 PBC 16 May 2023 c125

clause 12 would define the "decision subjects" who were impacted by AI without their data having been used, to give them protections throughout the Bill that are equal to those for data subjects.[60]

Stephanie Peacock claimed the group of amendments would help the legislative framework "address the impact of AI, rather than just its inputs":

> … The various amendments to clause 11 would extend to decision subjects rights that mirror those given to data subjects regarding automated decision making, such as the right to be informed, the right to safeguards such as contesting a decision and the right to seek human intervention. Likewise, the amendments to clauses 27 and 29 would ensure that the ICO is obliged to have regard to decision subjects both generally and when producing codes of conduct.
>
> Finally, to enact the safeguards to which decision subjects would hopefully be entitled via the amendments to clause 11, the amendment to clause 39 would allow decision subjects to make complaints to data controllers, mirroring the rights available to data subjects. Without defining decision subjects in law, that would not be possible…[61]

John Whittingdale said the Government recognised concerns about automated decision-making and wanted all those affected to be given protection. However, he didn't recognise the distinction between data subjects and decision subjects that formed the basis of Labour's amendments. The Minister argued that the legislation's existing reference to data subjects already covered decision subjects:

> …That is because even if an individual's personal data is not used to inform the decision taken about them, the fact that they are identifiable through the personal data that is held makes them data subjects. The term "data subject" is broad and already captures the decision subjects described in the hon. Lady's amendment, as the identification of a decision subject would make them a data subject.[62]

Amendment 78 was negatived by 10 votes to 7.[63]

Stephanie Peacock moved **amendment 77** to require data controllers to proactively provide data subjects with information about their rights in relation to automated decision-making.[64] She said this was needed as there was currently an "imbalance of power between those who conduct automated decisions and those who are subject to them".[65]

John Whittingdale agreed that individuals who were subject to automated decision-making should be made aware of it and have information about the available safeguards. However, he said these requirements were already built into the Bill via article 22C, which would ensure that individuals were provided

60 PBC 16 May 2023 cc125-6
61 PBC 16 May 2023 cc126-7
62 PBC 16 May 2023 c127
63 PBC 16 May 2023 c128
64 PBC 16 May 2023 c128
65 PBC 16 May 2023 c129

with information as soon as practicable after such decisions had been taken.[66]

Amendment 77 was negatived by 10 votes to 7.[67]

Stephanie Peacock moved **amendment 76**. This would make the Secretary of State's ability to amend the safeguards for automated decision-making set out in new Articles 22A to D subject to a requirement for consultation with interested parties and with the Information Commissioner, who would be required to publish their views on any proposed change.[68]

When speaking to the amendment, Stephanie Peacock argued that clause 11 not only amended the threshold on automated decision-making so that it would be permitted in a far wider range of circumstances, but it defined solely automated processing as a "significant decision" that involved "no meaningful human involvement" and attached all available safeguards to that definition. The clause would give the Secretary of State the power to amend what would count within the definition – meaning that safeguards would be "applicable only at the whim of however the Secretary of State decides to define key terms".[69] Amendment 76 would ensure that the "true impact" of any changes to definitions and safeguards was considered, and that the regulator was consulted before any adjustments were made.[70]

Amendment 75 was also considered. This would require the ICO to produce a code of practice on the interpretation of references to "meaningful human involvement" and "similarly significant" in connection with automated decision-making, with examples of the kinds of processing that would not count as falling within these definitions.[71] Stephanie Peacock claimed this "would build clarity into the Bill by guaranteeing statutory guidance" from the Information Commissioner on how the terms would be applied in practice and clarifying the kinds of processing that would not count as falling within the definitions.[72]

On amendment 76, John Whittingdale said that clause 44 already provided for an overarching requirement on the Secretary of State to consult the Information Commissioner and other persons that they considered appropriate before making regulations under the UK GDPR, including the measures in article 22. Moreover, when the new clause 44 powers were used in relation to article 22 provisions, they would be subject to the affirmative procedure.[73]

66 PBC 16 May 2023 c130
67 PBC 16 May 2023 c131
68 PBC 16 May 2023 c132
69 PBC 16 May 2023 c134
70 PBC 16 May 2023 c134
71 PBC 16 May 2023 c132
72 PBC 16 May 2023 c135
73 PBC 16 May 2023 c135

On amendment 75, John Whittingdale argued that examples of the kinds of processing that would fall within the definitions of "meaningful human involvement" and "similarly significant" would be best placed in non-statutory guidance produced by the ICO, as this would give flexibility to amend and change the examples where necessary.[74]

Stephanie Peacock said she fundamentally disagreed on the power to change the definitions being concentrated in the hands of the Secretary of State.[75]

Amendment 76 was negatived on division by 10 votes to 6.[76]

Amendment 75 was negatived on division by 10 votes to 6.[77]

Automated decision-making in the workplace

Stephanie Peacock moved **amendment 121**. This would insert into new Article 22D of the UK GDPR a requirement for the Secretary of State to have regard to a statement of digital information principles at work when making regulations about automated decision-making.[78] There would be ten principles:

> 1. People should have access to a fair, inclusive and trustworthy digital environment at work.
>
> 2. Algorithmic systems should be designed and used to achieve better outcomes: to make work better, not worse, and not for surveillance. Workers and their representatives should be involved in this process.
>
> 3. People should be protected from unsafe, unaccountable and ineffective algorithmic systems at work. Impacts on individuals and groups must be assessed in advance and monitored, with reasonable and proportionate steps taken.
>
> 4. Algorithmic systems should not harm workers' mental or physical health, or integrity.
>
> 5. Workers and their representatives should always know when an algorithmic system is being used, how and why it is being used, and what impacts it may have on them or their work.
>
> 6. Workers and their representatives should be involved in meaningful consultation before and during use of an algorithmic system that may significantly impact work or people.
>
> 7. Workers should have control over their own data and digital information collected about them at work.
>
> 8. Workers and their representatives should always have an opportunity for human contact, review and redress when an algorithmic system is used at

74 PBC 16 May 2023 c136
75 PBC 16 May 2023 c136
76 PBC 16 May 2023 c136
77 PBC 16 May 2023 c137
78 PBC 16 May 2023 c137

> work where it may significantly impact work or people. This includes a right to a written explanation when a decision is made.
>
> 9. Workers and their representatives should be able to use their data and digital technologies for contact and association to improve work quality and conditions.
>
> 10. Workers should be supported to build the information, literacy and skills needed to fulfil their capabilities through work transitions.

Amendment 122 was also considered. This would insert into new section 50D of the Data Protection Act 2018 a requirement for the Secretary of State to have regard to the statement of digital information principles at work when making regulations about automated decision-making.[79]

Stephanie Peacock said the amendments would ensure that close attention was paid to the specific and unique circumstances of workers and the workplace when regulations were made under clause 11.[80]

In response, John Whittingdale said the changes proposed in clause 11 would "reinforce and provide further clarification…in respect of the important safeguards for automated decision making" that could be used in some workplace technologies. These would ensure that people were made aware of, and could seek human intervention on, significant decisions that were taken about them through solely automated means. The Minister said the reforms to article 22 would clarify employer obligations and employee rights in such scenarios. More broadly, he recognised that some workplace technologies needed to be considered across a wide range of different regulatory frameworks, not just data protection law - ie human rights law, health and safety, and employment law.[81]

Amendments 121 and 122 were both negatived on division by 10 votes to 6.[82]

Clause 11 was added to the Bill after a division (10 votes to 6).[83]

Obligations of controllers and processors

Assessments of high risk processing

When **clause 17** (Assessment of high risk processing) was debated, Stephanie Peacock moved **amendment 102**. This would remove the provisions of clause 17 - which replace data protection impact assessment (DPIA) requirements with new requirements about "high risk processing" - leaving only the requirement for the ICO to produce a document containing examples of the types of processing likely to result in a high risk to the rights and freedoms of

79 PBC 16 May 2023 c138
80 PBC 16 May 2023 c138
81 PBC 16 May 2023 c141
82 PBC 16 May 2023 cc142-3
83 PBC 16 May 2023 c144

individuals.[84] When speaking to the amendment Stephanie Peacock said, among other things, that the new tests under clause 17 would not "carry the same weight or benefit" as DPIAs. It was not appropriate to remove the need to properly assess the risk of processing, while simultaneously removing restrictions that helped to mitigate those risks. For that reason, the clause had to be opposed.[85]

John Whittingdale said that seeking to maintain the current DPIA requirements would represent a missed "important opportunity for reform".[86]

Amendment 102 was negatived on division by 10 votes to 6.[87]

Amendment 103 was also moved by Stephanie Peacock. This would insert a new requirement into Article 35 of the UK GDPR for any public authority which used public data to publish an assessment of any high risk processing they conducted under Article 35.[88] When speaking to the amendment, the Shadow Minister commented: "given the inherent importance of conducting risk assessments for high-risk processing, and their potential for use by data subjects when things go wrong, it seems only right that transparency be built into the system where it comes to Government use of public data".[89]

In response, John Whittingdale noted that assessments could already be requested by the ICO as part of its investigations, or by members of the public via freedom of information requests. It was therefore unnecessary to impose a "significant new burden" on all public bodies.[90]

Stephanie Peacock did not put amendment 103 to a vote.

Clause 17 was added to the Bill after a division (10 votes to 6).[91]

Law enforcement processing and codes of conduct

Clause 19 of the Bill would introduce an ability for public bodies with the appropriate knowledge and expertise to produce codes of conduct applicable to the law enforcement regime.

When clause 19 was debated, **Government amendment 1** was agreed. This would replace a duty on expert public bodies to submit draft codes of conduct relating to compliance with Part 3 of the 2018 Act to the Information Commissioner with a duty on the Commissioner to encourage such bodies to do so.[92]

84 PBC 16 May 2023 c154
85 PBC 16 May 2023 c156
86 PBC 16 May 2023 c157
87 PBC 16 May 2023 c158
88 PBC 16 May 2023 c154
89 PBC 16 May 2023 c156
90 PBC 16 May 2023 cc157-8
91 PBC 16 May 2023 c158
92 PBC 16 May 2023 cc159-60

Government amendment 4 was also agreed. This would make clear that the Commissioner's duty under new section 68A of the 2018 Act to consider whether to approve amendments of codes of conduct would relate only to amendments of codes that were for the time being approved under that section.[93]

Obligations of controllers and processors: consequential amendments

When **clause 20** was debated, **Government amendment 40** was agreed. This would provide that the Commissioner would be able to refuse to deal with vexatious or excessive requests made by any person, not just those made by data protection officers or data subjects. Technical amendments were also agreed.[94]

Transfers of personal data to third countries and international organisations

Clause 21 would insert schedules 5, 6, and 7 into the Bill. These would amend Chapter 5 of the UK GDPR and Chapter 5 of Part 3 of the 2018 Act to reform the UK's regime for international transfers of personal data.[95]

Government amendment 24 was agreed. This would revise new article 45B(3)(c) of the UK GDPR, inserted by schedule 5, and which would make provision about the data protection test that would have to be satisfied for data bridge regulations to be made. John Whittingdale said an amendment to the Bill was needed for the Secretary of State to retain the flexibility to make data bridge regulations covering transfers from the UK or elsewhere. The amendment would preserve the status quo under the current regime, in which the Secretary of State's power was not limited to covering only transfers from the UK.[96]

Safeguards for processing for research etc purposes

Clause 22 would amend the UK GDPR by creating a new Chapter 8A. This would consist of four new articles which would combine the existing safeguards currently found in Article 89 of the UK GDPR and section 19 of the 2018 Act for data processing for archiving in the public interest, scientific, historic, and statistical research purposes.

When clause 22 was debated, minor, technical **Government amendments 34 to 39** were agreed. These would clarify that a controller was to use anonymous, rather than personal data, unless that meant that those purposes could not be fulfilled.[97]

93 PBC 16 May 2023 c160
94 PBC 16 May 2023 c1c160-1
95 For a summary of the changes, see PBC 16 May 2023 cc161-3
96 PBC 16 May 2023 c165
97 PBC 16 May 2023 cc166-7

Joint processing by intelligence services and competent authorities

Clause 25 would amend Part 4 of the 2018 Act to enable joint processing between a qualifying competent authority (or authorities) and an intelligence service (or intelligence services) under Part 4 of the DPA 2018. This would enable controllers to process data within a single, common regime. The controls and safeguards under Part 4 would apply to all such joint processing.

Stephanie Peacock moved **amendment 105** to clause 25.[98] This would seek to increase independent oversight of designation notices by replacing the requirement to consult the Information Commissioner with a requirement to seek the approval of the Commissioner. Stephanie Peacock said the amendment was needed to adjust the "concentration of power" when designation notices were approved so that power did not lie solely in the Secretary of State's hands:

> ..That would mean that should the Secretary of State act in bad faith, or lack the expertise needed to make such a decision—whether aware or unaware of this fact—the commissioner would be able to help to ensure that an informed and proportionate decision was made with regard to each notice applied for. This would not present any designation notices from being issued when they were genuinely necessary; it would simply safeguard their approval when they were.[99]

John Whittingdale said the ICO's expertise was in data protection, not in national security, and it would be inappropriate for it to decide on the latter. He also argued that clause 25 provided significant safeguards through proposed new sections 82B and 82E, which would provide for legal challenge and the annual review of a notice.[100]

Amendment 105 was negatived on division by 9 votes to 6.[101]

Information Commissioner's role

Duties of the Commissioner when carrying out functions

Amendment 106 to **clause 27**, in the name of Stephanie Peacock, would require the Commissioner to "have regard" to decision subjects as well as data subjects as part of its obligations.[102] The amendment was negatived on division by 9 votes to 6.[103]

98 PBC 16 May 2023 c168
99 PBC 16 May 2023 cc170-1
100 PBC 18 May 2023 c177
101 PBC 18 May 2023 c178
102 PBC 16 May 2023 c125
103 PBC 18 May 2023 c179

Strategic priorities

Clause 28 would require the Secretary of State, every three years, to publish a statement of strategic priorities for the Commissioner to consider, respond to, and have regard to. The statement would be subject to the negative resolution procedure. Stephanie Peacock warned that the introduction of a statement of strategic priorities could expose the Commissioner to "political direction". She said that, even though the clause might not be intended to threaten independence, it was important to be "extremely careful not to unintentionally embark on a slippery slope", particularly as there were other mechanisms for ensuring that the Commissioner had a transparent relationship with Government.[104]

Clause 28 was added to the Bill after a division (9 votes to 6).[105]

Codes of practice for the processing of personal data

Amendment 108 to clause 29, in the name of Stephanie Peacock, would require codes of conduct produced by the ICO to have regard to decision subjects as well as data subjects.[106] The amendmen was negatived on division by 9 votes to 6.[107]

Codes of practice: approval by the Secretary of State

Under **clause 31**, once the Commissioner had issued a final version of a code (under section 121, 122, 123, 124 or 124A of the 2018 Act), the Secretary of State would decide whether to approve it. If they approved the code, it would be laid before Parliament for final approval. If they did not, they would be required to publish their reasons.

Stephanie Peacock moved **amendment 111** so that the Secretary of State would be able to reject the final version of a code only once. She said this was needed to ensure there was no risk to the Commissioner's independence.[108]

John Whittingdale understood the concern but did not believe it was justified:

> ...We are absolutely committed to maintaining the commissioner's independence, but we think it also important that the Government have the opportunity to give a view before the code is laid before Parliament and for Parliament to give final approval. The amendment would unduly limit the Government's ability to provide as necessary that further degree of democratic accountability.[109]

The amendment was negatived on division by 9 votes to 6.[110]

---

104 PBC 18 May 2023 c182
105 PBC 18 May 2023 c183
106 PBC 18 May 2023 c183
107 PBC 18 May 2023 c183
108 PBC 18 May 2023 c187
109 PBC 18 May 2023 c187
110 PBC 18 May 2023 c188

Clause 31 was added to the Bill after a division (9 votes to 6).[111]

Vexatious or excessive requests made to the Commissioner

Clause 32 would amend the threshold for the Commissioner to charge a reasonable fee or refuse a request from a data subject or a data protection officer. The threshold would be changed from "manifestly unfounded or excessive" to "vexatious or excessive" and would align with the same change in threshold being made across the UK GDPR and the 2018 Act.

Government amendment 40 was agreed. This would add further amendments of section 135 of the 2018 Act to clause 32 to make clear that the Information Commissioner could refuse to deal with a vexatious or excessive request made by any person.[112]

2.2 Part 2: Digital verification services

Clause 54 would grant public authorities the power to share information with a registered digital verification service (DVS) provider when an individual made a request to the registered provider to verify their identity. HM Revenue and Customs (HMRC) would be one public authority able to share information under clause 54.

Clause 55 states that any information shared by HMRC with a registered DVS provider, for the purposes of DVS, should not be shared further (unless consent had been obtained from the Commissioners of HMRC).

Government new clause 3 (Information disclosed by the Welsh Revenue Authority), **Government new clause 4** (Information disclosed by Revenue Scotland), and **Government amendments 6** and **7** would establish safeguards for information reflecting those already in the Bill under clause 55 for HMRC. John Whittingdale explained:

> Information held by tax authorities in Scotland and Wales—Revenue Scotland and the Welsh Revenue Authority—is subject to similar statutory safeguards relating to confidentiality. These safeguards ensure that confidence and trust in the tax system is maintained. Under these provisions, registered DVS providers may not further disclose information provided by Revenue Scotland or the Welsh Revenue Authority unless they have the consent of that revenue authority to do so. The addition of these provisions will provide an equivalent level of protection for information shared by all three tax authorities in the context of part 2 of the Bill, avoiding any disparity in the treatment of information held by different tax authorities in this context. A similar provision is not required for Northern Irish tax data, as HMRC is responsible for the collection of devolved taxes in Northern Ireland.[113]

111 PBC 18 May 2023 c189
112 PBC 18 May 2023 cc189-90
113 PBC 18 May 2023 c212

Government amendments 6 and 7 were agreed.[114] Government new clauses 3 and 4 were added to the Bill.[115]

2.3 Part 4: Other provision about digital information

Privacy and electronic communications

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (S.I. 2003/2426), referred to in the Bill as the "the PEC Regulations", sit alongside the Data Protection Act 2018 (the 2018 Act) and the UK GDPR. The PEC Regulations place specific requirements on organisations in relation to use of personal data in electronic communications. They include, for example, rules on the use of emails, texts and phone calls for direct marketing purposes and the use of cookies and similar technologies.

Regulation 6(1) of the PEC Regulations prohibits an organisation from storing information or gaining access to information stored in the terminal equipment of an individual, unless the individual is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and the individual has given consent. This is commonly described as the "cookies rule". An exception to the consent requirements exists where the cookie is "strictly necessary" for the provision of a service explicitly requested by the individual.[116]

Clauses 79 to **86** of Part 4 of the Bill are concerned with privacy and direct marketing electronic communications. If enacted, these highly technical clauses would amend the PEC Regulations.

The privacy and electronic communications provisions of the Bill were considered in Committee on 23 May 2023 (seventh and eighth sittings). There were divisions on Opposition amendments 117 and 118 (both negatived by 8 votes to 4). New Government clauses 1 and 2 were added to the Bill. Further information is set out below.

Amendment 117 to clause 79

Clause 79 of the Bill would amend regulation 6 of the PEC Regulations, by extending the circumstances under which cookies or other technologies (e.g tracking pixels) could be used to store or access information on people's devices without their express consent. These new exceptions would be for certain purposes considered to present a "low risk" to people's privacy (e.g the installation of software updates necessary for the security of the device).

---

114 PBC 18 May 2023 c213

115 PBC 23 May 2023 cc281-2

116 See Guidance on direct marketing (pdf), Information Commissioner's Office, 2018 (accessed 6 June 2023)

Clause 79 of the Bill would insert new regulation 6A and 6B into the PEC Regulations. New **regulation 6A** would introduce a power for the Secretary of State to add new exceptions to the cookie consent requirements. The power would also allow the Secretary of State to omit or vary any existing exceptions to the consent requirements.

If enacted, **new regulation 6B** would enable subscribers or users to effectively express their consent preferences regarding cookies to an operator of a website (commonly a browser) so that this could be applied automatically on visiting the website. New regulation 6B would introduce a power for the Secretary of State to make regulations providing that relevant organisations (eg browser and device suppliers) may not supply "information technology" of a specified description unless it meets the requirements specified in the regulations.

Under new regulations 6A and 6B, before making any new regulations the Secretary of State would have to consult the Information Commissioner and such other persons as the Secretary of State considers appropriate.

Stephanie Peacock moved **amendment 117** to **clause 79** to remove new regulation 6B from the Bill.[117] Although she supported exploring ways to reduce consent fatigue and cookie banners, she believed new regulation 6B required further consultation before entering the statute book.[118] Stephanie Peacock gave three reasons for opposing the inclusion of regulation 6B in the Bill:

- First, competition concerns if browsers are given centralised control and access to data surrounding cookies across the entire internet.[119]
- Secondly, it was argued that media owners should be able to "develop first-party relationships with their audiences and customers to better understand what they need without having browsers as gatekeepers of the information". Any system of this kind would "inevitably require browsers to be able to interrupt a provider's relationship with their customers by automatically overriding the consent directly expressed to them by their users". This might result in confusion if data is processed in a way the data subject would like to dispute.[120]
- Finally, there were concerns about the technological readiness of browser-based solutions. Stephanie Peacock acknowledged that new regulation 6B would allow for browser-enabled models to be implemented in the future rather than immediately but said it was "reasonable to expect that proper parliamentary scrutiny will be

117 PBC 23 May 2023 c239
118 As above
119 As above
120 PBC 23 May 2023 c239-240

> required at the point where we actually know what the technology looks like".[121]

In response, Sir John Whittingdale said the Government saw new regulation 6B as "an important tool" for reducing frequent cookie consent banners and pop-ups that "interfere with people's use of the internet":

> [...] clause 79 removes the need for organisations to seek consent to place cookies for certain non-intrusive purposes. One way of further reducing the need for repeated cookie pop-up notices is by blocking them at source – in other words, allowing web users to select which cookies they are willing to accept and which they are not comfortable with using browser-level settings or similar technologies. These technologies should allow users to set their online preferences once and be confident that those choices will be respected throughout their use of the internet.[122]

The Minister said that the regulation-making powers contained in new regulation 6B would enable the Secretary of State to require relevant technologies to meet certain standards or specifications:

Without regulations, there could be an increased risk of companies developing technologies that did not give web users sufficient choice and control about the types of cookies they are willing to accept. We will consult widely before making any new regulations under 6B, and new regulations will be subject to the affirmative resolution procedure.[123]

Having listened to stakeholders, the Minister said the Government intended to amend regulation 6B to provide an explicit requirement for the Secretary of State to consult the Competition and Markets Authority (CMA) before making new regulations.[124]

Amendment 117 was negatived on division by 8 votes to 4.

Amendment 118 to clause 85

Stephanie Peacock MP also moved **amendment 118** to **clause 85**.[125] The stated aim of clause 85 is to help to ensure that there is better co-operation between the industry and the regulator in tackling the problem of nuisance communications.

Clause 85 would insert new direct marketing regulations 26A-C into the PEC Regulations which, in turn, would impose a duty on public electronic communications service and network providers ("telecoms providers") to report to the Information Commissioner any "suspicious activity" relating to unlawful direct marketing within 28 days of first becoming aware of such activity. Once notified, the ICO would be required to investigate whether a

---

121 PBC 23 May 2023 c240
122 As above
123 As above
124 As above
125 PBC 23 May 2023 c246

breach of the PEC Regulations has occurred and take appropriate action where necessary. Clause 85 would also require the ICO to publish guidance on what might constitute "reasonable" grounds for such suspicions.

Speaking to amendment 118, Stephanie Peacock agreed that there was a need to tackle unwanted nuisance calls.[126] She said the explanatory notes clearly state there would be no requirement on telecoms providers to "monitor" communications, but this was not stated in the Bill, resulting in some confusion in the communications sector.[127] She also raised concerns about the technological feasibility of identifying instances of unlawful and unsolicited direct marketing:

> [...] the new duty will require telecommunications providers to be able to identify whether a person receiving a direct marketing call has or has not given consent to receive the call from the company making it. However, providers have said they cannot reliably know that, and have warned that there is no existing technology to conduct that kind of monitoring accurately and at scale. In the absence of communication monitoring and examples of how unsolicited direct marketing is to be identified, it is therefore unclear how companies will fulfil their duties under the clause.[128]

Stephanie Peacock said amendment 118 would remove confusion by requiring government guidance to:

- make clear that a telecoms provider would not be obligated to monitor the content of individual electronic communications in order to determine if they contrive the direct marketing regulations; and

- include illustrative examples of the types of activity that may cause a telecoms provider to "reasonably" suspect that a person is contravening, or has contravened, any of the direct marketing regulations.[129]

Responding to amendment 118, Sir John Whittingdale said clause 85 would not require network and service providers to put new systems in place to monitor for suspicious activities. However, where they have that capability already and have reasonable grounds to believe that unlawful activity is going on, "we would like them to share that information with the ICO".[130] He gave the example of a high number of calls originating within a very short space of time from the same number or from a small batch of numbers.[131]

The amendment was negatived on division by 8 votes to 4.

126 PBC 23 May 2023 c247
127 As above
128 PBC 23 May 2023 c247-8
129 As above
130 PBC 23 May 2023 c248
131 PBC 23 May 2023 c246

New government clauses

New government **clause 2** was added to the Bill.[132] John Whittingdale explained its purpose:

The Privacy and Electronic Communications (EC Directive) Regulations 2003 place specific requirements on organisations in relation to use of personal data in electronic communications. They include, for example, rules on the use of emails, texts and phone calls for direct marketing purposes and the use of cookies and similar technologies.

Trade associations have told us that sometimes their members need guidance on complying with the legislation that is more bespoke than the general regulatory guidance from the Information Commissioner's Office. New clause 2 will allow representative bodies to design codes of conduct on complying with the PEC regulations that reflect their specific processing operations. There are already similar provisions in articles 40 and 41 of the UK General Data Protection Regulation to help organisations in particular sectors to comply.

Importantly, codes of conduct prepared under these provisions can be contained in the same document as codes of conduct under the UK GDPR. That will be particularly beneficial to representative bodies that are developing codes for processing activities that are subject to the requirements of both the UK GDPR and the PEC regulations. New clause 2 envisages that representative bodies will draw up voluntary codes of conduct and then seek formal approval of them from the Information Commissioner. The Information Commissioner will approve a code only if it contains a mechanism for the representative body to monitor their members' compliance with the code.[133]

Government new **clause 1** would make a related amendment to article 41 of the UK GDPR to clarify that bodies accredited to monitor compliance with codes of conduct under the GDPR would be required to notify the Information Commissioner only if they suspended or excluded a person from a code.[134] **New clause 1** was added to the Bill.

Sharing of information

Clause 92 of the Bill would amend section 35 of the 2017 Act to also enable the sharing of information to improve the delivery of public services to businesses.

When **clause 93** (Implementation of law enforcement information-sharing agreements) was debated, John Whittingdale explained the purpose of Government amendments **8** and **10** and **Government new clause 5**:

132 PBC 23 May 2023 c281
133 PBC 23 May 2023 c279
134 PBC 23 May 2023 c234

> Clause 93 creates a delegated power for the Secretary of State, and a concurrent power for Welsh and Scottish Ministers, to make regulations to implement international agreements relating to the sharing of information for law enforcement purposes. The concurrent power for Welsh and Scottish Ministers has been included in an amendment to the clause. While international relations are a reserved matter, the domestic implementation of the provisions likely to be contained in future international agreements may be devolved, given that law enforcement is a devolved matter to various extents in each devolved Administration.
>
> In the light of introducing a concurrent power for Welsh and Scottish Ministers, amendments to clauses 93 and 108 have been tabled, as has new clause 5. Together they specifically detail the appropriate national authority that will have the power to make regulations in respect of clause 93. The Government amendments make it clear that the appropriate national authority may make the regulations. New clause 5 then defines who is an appropriate national authority for those purposes. I therefore commend new clause 5 and the related Government amendments to the Committee...[135]

Government amendments 8 and 210 were agreed.[136] Government new clause 5 was added to the Bill.[137]

2.4 Part 5: Regulation and oversight

Processing biometric data

Section 24 of the Protections of Freedom Act 2012 inserted section 63AB into the Police and Criminal Evidence Act 1984 (PACE). This introduced the National DNA Database Strategy Board to oversee the operation of the National DNA Database. This requirement is being delivered through the Forensic Information Databases Strategy Board (FIND-SB).

Clause 106 (Oversight of biometrics databases) would amend section 63AB of PACE by increasing the scope of the statutory board to also provide oversight of the national fingerprint database (referred to as IDENT1). This would bring the legislation up to date with the latest governance rules for the FIND-SB, which added oversight of the national fingerprint database to the Board's terms of reference.[138]

When **clause 106** was debated, Stephanie Peacock moved **amendment 119**.[139] This would ensure that the definition of biometric data in the Bill includes cases where that data is used for the purposes of classification, and not just unique identification. Labour's **new clause 8** was also considered. This would extend the protections currently in place for the processing of biometric data for the purposes of identification to the processing of all biometric data,

135 PBC 23 May 2023 c256
136 PBC 23 May 2023 c256
137 PBC 23 May 2023 c282
138 As above, para 675
139 PBC 23 May 2023 c273

including processing for the purpose of classification (ie identification as part of a group, rather than identification as an individual).[140]

Stephanie Peacock said that changes to the Bill were needed because of concerns about biometric technologies classifying people "according to reductive, ableist and stereotypical characteristics, harming people's wellbeing and risking characterisation in a database or data-driven systems":

> ...these cases often use pseudoscientific assumptions to draw links between external features and other traits, meaning that the underlying bases of these technologies are often not valid, reliable or accurate. For example, significant evidence suggests that it is not possible accurately to infer emotion from facial expressions. Despite that, existing data protection law would not consider biometric data collected for those purposes to be special category data, and would therefore not give data subjects the highest levels of safeguards in these contexts.[141]

In response, John Whittingdale said, among other things, that using biometric data to draw "inferences about people" was not as invasive as using biometric data uniquely to identify someone. There was, therefore, a distinction between using biometric information for identification purposes and more general classification. In addition, using biometric data for classification or categorisation purposes was still subject to the general data protection principles in the UK GDPR.[142]

Stephanie Peacock withdrew amendment 119.[143] There was a division on adding new clause 8 to the Bill. It was negatived by 9 votes to 4.[144]

2.5 Other issues on which the Committee divided

Algorithmic transparency

The Algorithmic Transparency Recording Standard is part of the Government's National Data Strategy. The Strategy includes a commitment to explore an appropriate and effective way to deliver greater transparency on algorithm-assisted decision making in the public sector. The National AI Strategy reiterated the commitment. The Central Digital and Data Office (CDDO) and Centre for Data Ethics and Innovation (CDEI) developed the Standard by working with civil society groups and external experts. The Standard has been piloted with public sector organisations across the UK.[145]

140 PBC 23 May 2023 c273
141 PBC 23 May 2023 c274
142 PBC 23 May 2023 c275
143 PBC 23 May 2023 c275
144 PBC 23 May 2023 c283
145 GOV.UK, Algorithmic Transparency Recording Standard Hub (accessed 1 June 2023)

Labour's **new clause 9** would have placed a legal obligation on public bodies using personal data to use the Standard.[146] When speaking to the new clause, Stephanie Peacock said the Standard was "ready to go" and its benefits were "clear". Requiring its use would give people confidence in the public use of algorithms.[147]

John Whittingdale said the Algorithmic Transparency Recording Standard was still "maturing" and being progressively promoted and adopted. Enshrining it into law now could "hinder the ability to ensure that it remains relevant in a rapidly developing technology field".[148]

There was a division on adding new clause 9 to the Bill. It was negatived by 9 votes to 4.[149]

Data breach complaints

Labour's **new clause 10** would require the Secretary of State to exercise powers under section 190 of the 2018 Act to allow organisations to raise data breach complaints on behalf of data subjects, in the absence of a particular subject who wished to bring forward a claim about misuse of their own personal data.[150]

Stephanie Peacock explained that, at present, if one individual is prepared to launch a case, an organisation can help. However, where many individuals are affected, if no one has the evidence or resources to bring an individual case, that same organisation cannot lodge a complaint, even though the negative impact of the data infringement could be much larger, could have arisen by design and could have far-reaching consequences. Organisations such as Which?, Reset and 5Rights, have argued that an effective data protection redress framework requires a collective redress mechanism.[151]

John Whittingdale said the amendment would replace the current discretionary powers in section 190 of the 2018 Act with a duty for the Secretary of State to legislate to bring those provisions into force soon after the Bill had received Royal Assent. He said this would be "undesirable". The Government had already consulted and reported to Parliament on proposals of that nature. It concluded that there was not a strong enough case for introducing new legislation. Moreover, giving non-profit organisations the right to bring compensation claims against data controllers on behalf of individuals who had not authorised them to do so could prompt the growth of US-style lawsuits on behalf of thousands or even millions of customers. Some organisations could be forced out of business or prompted to increase prices

146 PBC 23 May 2023 cc284-5
147 PBC 23 May 2023 c285
148 PBC 23 May 2023 c286
149 PBC 23 May 2023 c286
150 PBC 23 May 2023 cc286-7
151 PBC 23 May 2023 c287

to recoup costs. The increase in litigation costs could also increase insurance premiums.[152]

There was a division on adding new clause 10 to the Bill. It was negatived by 9 votes to 4.[153]

[152] PBC 23 May 2023 c289

[153] PBC 23 May 2023 c289

The House of Commons Library is a research and information service based in the UK Parliament. Our impartial analysis, statistical research and resources help MPs and their staff scrutinise legislation, develop policy, and support constituents.

Our published material is available to everyone on commonslibrary.parliament.uk.

Get our latest research delivered straight to your inbox. Subscribe at commonslibrary.parliament.uk/subscribe or scan the code below:

commonslibrary.parliament.uk

@commonslibrary