Data (Use and Access) Bill [HL]

MARSHALLED

LIST OF AMENDMENTS

TO BE MOVED

ON REPORT

The amendments have been marshalled in accordance with the Instruction of 15th January 2025, as follows—

Clauses 1 to 56	Schedule 10
Schedule 1	Clauses 103 to 107
Clauses 57 and 58	Schedule 11
Schedule 2	Clauses 108 to 111
Clauses 59 to 65	Schedule 12
Schedule 3	Clauses 112 and 113
Clauses 66 to 70	Schedule 13
Schedule 4	Clauses 114 and 115
Clause 71	Schedule 14
Schedule 5	Clauses 116 to 119
Clauses 72 to 80	Schedule 15
Schedule 6	Clause 120
Clauses 81 to 84	Schedule 16
Schedules 7 to 9	Clauses 121 to 138
Clauses 85 to 102	Title

[*Amendments marked ★ are new or have been altered*]

Amendment No.

Clause 1

BARONESS KIDRON

1★ Clause 1, page 3, line 11, at end insert—

"(5A) In subsection (2), references to information includes inferred data."

Member's explanatory statement

This amendment ensures that when traders are required to provide information relating to goods, services and digital content supplied or provided to the customer that includes information that has been created using AI to build a profile about them.

Clause 2

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL

2 Clause 2, page 4, line 1, after "to" insert "the customer's data rights or"

Member's explanatory statement
This amendment adds enacting data rights to the list of actions that the Secretary of State or the Treasury can enable an "authorised person" to take on behalf of customers. This would make it possible for customers to assign their data rights to a third party to activate on their behalf.

Clause 3

BARONESS KIDRON
LORD CLEMENT-JONES

3 Clause 3, page 4, line 24, at end insert—

"(2A) The regulations must include data communities in the list of specified people."

Member's explanatory statement
This amendment would require the Secretary of State or Treasury to include data communities in the list of specific people who can activate on a customer's behalf.

BARONESS KIDRON
LORD CLEMENT-JONES

4 Clause 3, page 6, line 7, at end insert—

"(12) In this Act, a "data community" means an entity established to activate data subjects' data rights under Chapters III and VIII of the UK GDPR on their behalf."

Member's explanatory statement
This amendment provides a definition of "data community". It is part of a set of amendments that allow the assigning of personal data.

Clause 13

VISCOUNT CAMROSE
LORD MARKHAM

5★ Leave out Clause 13

Member's explanatory statement
The change would prevent the Secretary of State and the Treasury from becoming statutory financial backstops.

Clause 28

LORD LUCAS
LORD ARBUTHNOT OF EDROM

6 Clause 28, page 30, line 28, at end insert—

"(2A) In preparing the DVS trust framework the Secretary of State must assess whether the public authorities listed in subsection (2B) reliably ascertain the personal data attributes that they collect, record and share.

(2B) The public authorities are—

(a) HM Passport Office;
(b) Driver and Vehicle Licensing Agency;
(c) General Register Office;
(d) National Records Office;
(e) General Register Office for Northern Ireland;
(f) NHS Personal Demographics Service;
(g) NHS Scotland;
(h) NI Health Service Executive;
(i) Home Office Online immigration status (eVisa);
(j) Disclosure and Barring Service;
(k) Disclosure Scotland;
(l) Nidirect (AccessNI);
(m) HM Revenue and Customs;
(n) Welsh Revenue Authority;
(o) Revenue Scotland."

Member's explanatory statement
This amendment is to ensure that there is oversight that the public authorities that provide core identity information via the information gateway provide accurate and reliable information.

LORD CLEMENT-JONES

7 Clause 28, page 31, line 22, at end insert—

"(11) The Secretary of State must lay the DVS trust framework before Parliament."

Member's explanatory statement
This amendment will ensure Parliamentary oversight of the rules with which digital verification service providers must comply.

Clause 45

LORD LUCAS
LORD ARBUTHNOT OF EDROM

8 Clause 45, page 42, line 23, at end insert—

"(5A) A public authority must not disclose information about an individual under this section unless the information—

(a) is clearly defined and accompanied by metadata, and

(b) the public authority is able to attest that it—

(i) was accurate at the time it was recorded, and

(ii) has not been changed or tampered, or

(c) the public authority is able to attest that it—

(i) has been corrected through a lawfully made correction, and

(ii) was accurate at the time of the correction."

Member's explanatory statement
This amendment is to ensure that public authorities that disclose information via the information gateway provide accurate and reliable information and that if the information has been corrected it is the correct information that is provided.

After Clause 50

LORD CLEMENT-JONES

9 After Clause 50, insert the following new Clause—

"Digital identity documents and digital identity theft review

(1) The Secretary of State must review the need for—

(a) an offence regarding the false use of digital identity documents created or verified by digital verification services within the meaning of this Act, and

(b) a digital identity theft offence.

(2) Under subsection (1)(a) the review must consider whether an offence can be created within the Identity Documents Act 2010.

(3) Under subsection (1)(b) the review must consider as part of its determination into the need for a digital identity theft offence, the following definition—

"digital identity theft offence" means an offence where a person, without permission, obtains personal or sensitive information such as passwords, ID numbers, credit card numbers or national insurance numbers relating to an individual, or uses personal or sensitive information, to impersonate that individual and act in their name to carry out a digital transaction."

Member's explanatory statement
This amendment requires the Secretary of State to review whether an offence relating to the false use of digital identity documents is needed, and whether this offence could be created via the

Identity Documents Act 2010; further, it requires a review into the need for a digital identity theft offence.

Clause 56

LORD VALLANCE OF BALHAM

10 Clause 56, page 52, line 13, leave out "undertaker's" and insert "contractor's"

Member's explanatory statement
New section 106B(6) of the New Roads and Street Works Act 1991 (defence where certain people have taken reasonable care) refers to "the undertaker's employees" twice. This amendment corrects that by replacing one of those references with a reference to "the contractor's employees".

VISCOUNT CAMROSE
LORD MARKHAM

11★ Clause 56, page 53, line 17, at end insert—

"(2A) The Secretary of State must provide guidance to relevant stakeholders on cyber-security measures before they may receive information from NUAR."

Member's explanatory statement
This amendment will require the Secretary of State to provide guidance to relevant stakeholders on security measures before they receive information from NUAR.

Clause 58

LORD VALLANCE OF BALHAM

12 Clause 58, page 62, line 34, leave out "undertaker's" and insert "contractor's"

Member's explanatory statement
New Article 45B(6) of the Street Works (Northern Ireland) Order 1995 (defence where certain people have taken reasonable care) refers to "the undertaker's employees" twice. This amendment corrects that by replacing one of those references with a reference to "the contractor's employees".

Clause 61

VISCOUNT CAMROSE
LORD MARKHAM

13★ Clause 61, page 71, line 18, at end insert—

"(2A) The Registrar General must make provision to ensure the security of the registers of live-births, still-births, and deaths."

Member's explanatory statement
This amendment ensures that suitable cyber-security measures are put in place to secure the large and valuable data source made up of digital registers of live-births, still-births, and deaths.

Clause 67

VISCOUNT COLVILLE OF CULROSS
BARONESS KIDRON
VISCOUNT CAMROSE

14 Clause 67, page 75, line 10, after "scientific" insert "and that is conducted in the public interest"

Member's explanatory statement
This amendment ensures that to qualify for the scientific research exception for data reuse, that research must be in the public interest. This requirement already exists for medical research, but this amendment would apply it to all scientific research wishing to take advantage of the exception.

Clause 68

BARONESS KIDRON
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

15 Clause 68, page 76, line 16, at end insert—

"(e) the data subject is not a child."

Member's explanatory statement
This amendment ensures the bill maintains the high level of legal protection for children's data even when the protections offered to adults are lowered.

Clause 70

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

16 Clause 70, page 77, line 36, after "interest" insert "and the data subject is not a child."

Member's explanatory statement
This amendment excludes children from "recognised legitimate interests" and ensures the Bill maintains the high level of legal protection for children's data even when the protections offered to adults are lowered.

LORD CLEMENT-JONES

17 Clause 70, page 78, leave out lines 9 to 30

Member's explanatory statement
This amendment removes powers for the Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

LORD VALLANCE OF BALHAM

18 Clause 70, page 78, line 23, after "children" insert "merit specific protection with regard to their personal data because they"

Member's explanatory statement
This amendment adds an express reference to children meriting specific protection with regard to their personal data in new paragraph 8(b) of Article 6 of the UK GDPR (lawful processing: recognised legitimate interests). See also the amendment in my name to Clause 90, page 113, line 20.

Schedule 4

LORD HOLMES OF RICHMOND

19 Schedule 4, page 183, line 21, at end insert—

"(c) the requester has notified the Commissioner of the nature and purpose of the request."

Member's explanatory statement
This amendment seeks to ensure that the person who has made the request has notified the Commissioner of the nature and purpose of the request.

Clause 71

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

20 Clause 71, page 81, line 14, at end insert—

"4A. Where the controller collected the personal data based on Article 6(1)(a) (data subject's consent), processing for a new purpose is not compatible with the original purpose if—

(a) the data subject is a child,

(b) the processing is based on consent given or authorised by the holder of parental responsibility over the child,

(c) the data subject is an adult to whom either (a) or (b) applied at the time of the consent collection, or

(d) the data subject is a deceased child."

Member's explanatory statement
This amendment seeks to exclude children from the new provisions on purpose limitation for further processing under Article 8A.

LORD CLEMENT-JONES

21 Clause 71, page 81, leave out lines 15 to 28

Member's explanatory statement
This amendment removes powers for the Secretary of State to override primary legislation and modify key aspects of UK data protection law via statutory instrument.

After Clause 72

BARONESS KIDRON
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

22 After Clause 72, insert the following new Clause—

"Protection of children: overarching duty on controllers and processors

(1) In complying with their UK data protection obligations, data controllers and processors must give due consideration to—
  (a) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data;
  (b) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;
  (c) the fact that children may require different protections at different ages and stages of development.

(2) Nothing in this Act is to be construed as reducing, minimising or undermining existing standards and protections of children's data under the 2018 Act or UK GDPR.

(3) In this section, a "child" is a person under the age of 18."

Member's explanatory statement
This amendment creates an obligation on data processors and controllers to consider the central principles of the Age-Appropriate Design Code when processing children's data. This ensures greater consistency in the level of protection children receive.

Clause 75

VISCOUNT CAMROSE
LORD MARKHAM

23★ Clause 75, page 87, line 18, at end insert—

"(za) in subsection (1), for "manifestly unfounded" substitute "vexatious","

Member's explanatory statement
This amendment changes the definition of request by data subjects to data controllers for which a fee can be charged from "manifestly unfounded or excessive" to "vexatious".

Clause 77

BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES
LORD BLACK OF BRENTWOOD
LORD STEVENSON OF BALMACARA

24 Clause 77, page 91, line 16, at end insert—

"(ia) after point (d), insert—

"(e) the personal data is from the Open Electoral Register. When personal data from the Open Electoral Register is combined with personal data from other sources to build a profile for direct marketing then transparency obligations must be fulfilled at the point the individual first provides the additional personal data to a data provider. Additional transparency must be provided by organisations using the data for direct marketing via their privacy policy and by including a data notification in a direct mail pack.""

After Clause 79

BARONESS KIDRON
LORD CLEMENT-JONES

25 After Clause 79, insert the following new Clause—

"Right to assign data rights to a data community

(1) Data subjects have the right to mandate a data community to exercise their data rights, as set out in Chapters 3 and 8 of the UK GDPR, on their behalf.

(2) The data subject has the right to specify which data and which rights over that data they assign to the data community, for what purpose, and for how long, and with respect to which data controllers.

(3) The data subject has the right to amend or withdraw the assignment partially or in full at any time.

(4) In this Act, a "data community" means an entity established to facilitate the collective activation of data subjects' data rights in Chapters 3 and 8 of the UK GDPR, and members of a data community assign specific data rights to a nominated entity to exercise those rights on their behalf."

Member's explanatory statement
This amendment creates a mechanism for data subjects to assign their data rights to be managed and asserted collectively. It seeks to address the asymmetry between the ability of data subjects and data controllers to understand and direct how data is used within data sets. It is one of a series of amendments that would establish the ability to assign data rights to a third party.

Clause 80

VISCOUNT CAMROSE
LORD MARKHAM

26★ Clause 80, page 94, line 24, at end insert—

"3. When an automated decision-making process involves artificial intelligence (AI), the AI programme must have due regard for the following principles—

(a) safety, security, and robustness;

(b) appropriate transparency and explainability;

(c) fairness;

(d) accountability and governance;

(e) contestability and redress."

Member's explanatory statement
This amendment inserts the five principles from the "A pro-innovation approach to AI regulation" White Paper, ensuring AI programmes used in automated decision making have due regards for safety, security, robustness, appropriate transparency and explainability, fairness, accountability and governance, and contestability and redress.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

27 Clause 80, page 95, line 6, at end insert "or,

(b) the data subject is a child or may be a child unless the provider is satisfied that the decision is in, and compatible with, the best interests of a child, taking into account their rights and development stage."

Member's explanatory statement
This amendment seeks to ensure that significant decisions that impact children cannot be made using automated processes unless they are in a child's best interest. This upholds data law introduced in 2018.

LORD CLEMENT-JONES
BARONESS KIDRON

28 Clause 80, page 95, line 12, leave out "solely" and insert "predominantly"

Member's explanatory statement
This amendment would mean safeguards for data subjects' rights, freedoms and legitimate interests would have to be in place in cases where a significant decision in relation to a data subject was taken based predominantly, rather than solely, on automated processing.

LORD CLEMENT-JONES

29★ Clause 80, page 95, leave out lines 26 to 32

Member's explanatory statement
This amendment removes the Secretary of State's powers to determine when meaningful involvement can be said to have taken place.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

30 Clause 80, page 96, line 33, at end insert—

"(4) Consent in accordance with subsection (2) cannot be given by persons under the age of 18."

Member's explanatory statement
This amendment prevents children giving consent for their special category data to be used in automated decision-making.

VISCOUNT CAMROSE
LORD MARKHAM

31★ Clause 80, page 96, line 33, at end insert—

"(4) The Secretary of State must publish guidance on how data controllers may obtain explicit consent, which must be published and reviewed at least annually, and any changes to which must be published as soon as practicable."

Member's explanatory statement
This amendment will ensure the Secretary of State provides guidance on how consent should be obtained for automated decision-making involving special category data. It also ensures that this guidance is readily available and is reviewed frequently.

VISCOUNT CAMROSE
LORD MARKHAM

32★ Clause 80, page 97, line 10, after "controller" insert ", by a human with sufficient competency and authority"

Member's explanatory statement
This amendment will ensure that recourse to human intervention is carried out by a person with sufficient competency and authority and is, therefore, effective.

LORD CLEMENT-JONES

33★ Leave out Clause 80

Member's explanatory statement
This is a probing amendment intended to elicit assurances from the Minister regarding the forthcoming ICO code of practice about automated decision-making.

After Clause 80

LORD CLEMENT-JONES

34 After Clause 80, insert the following new Clause—

"Requirements of public sector organisations on use of algorithmic or automated decision-making systems

(1) No later than the commencement of use of a relevant algorithmic or automated decision-making system, a public authority must—

(a) give notice on a public register that the decision rendered will be undertaken in whole, or in part, by an algorithmic or automated decision-making system,

(b) make arrangements for the provision of a meaningful and personalised explanation to affected individuals of how and why a decision affecting them was made, including meaningful information about the decision-making processes, and an assessment of the potential consequences of such processing for the data subject, as prescribed in regulations to be made by the Secretary of State,

(c) develop processes to—

(i) monitor the outcomes of the algorithmic or automated decision-making system to safeguard against unintentional

outcomes and to verify compliance with this Act and other relevant legislation, and

(ii) validate that the data collected for, and used by, the system is relevant, accurate, up-to-date, and in accordance with the Data Protection Act 2018, and

(d) make arrangements to conduct regular audits and evaluations of algorithmic and automated decision-making systems, including the potential risks of those systems and steps to mitigate such risks, as prescribed in regulations to be made by the Secretary of State.

(2) "Algorithmic decision system" or "automated decision system" mean any technology that either assists or replaces the judgement of human decision-makers.

(3) Regulations under this section are subject to the affirmative resolution procedure."

BARONESS FREEMAN OF STEVENTON
LORD CLEMENT-JONES

As an amendment to Amendment 34

35★ In subsection (1), after (d), insert—

"(e) evaluate the efficacy of the algorithmic and automated decision-making system in the situation in which it is being or is intended to be used, and make the results of that evaluation publicly available."

(1A) The evaluation required by (1)(e) must be repeated and made publicly available annually while the algorithmic and automated decision-making system remains in use."

LORD CLEMENT-JONES
BARONESS KIDRON
VISCOUNT COLVILLE OF CULROSS

36 After Clause 80, insert the following new Clause—

"Definition of meaningful human involvement in automated decision-making

The Secretary of State must, in conjunction with the Information Commissioner's Office and within six months of the day on which this Act is passed, produce a definition of what constitutes meaningful human involvement in automated decision-making or clearly set out their reasoning as to why a definition is not required."

Member's explanatory statement
This amendment requires the Secretary of State to produce a definition of meaningful human involvement in automated decision-making, in collaboration with the Information Commissioner's Office, or clearly set out its reasoning as to why this is not required, within six months of the Act's passing.

After Clause 84

LORD CLEMENT-JONES
LORD THOMAS OF CWMGIEDD

37 After Clause 84, insert the following new Clause—

"Impact of this Act and other developments at national and international level on EU data adequacy decision

Before the European Union's reassessment of data adequacy in June 2025, the Secretary of State must carry out an assessment of the likely impact on the European Union data adequacy decisions relating to the United Kingdom of the following—

(a) this Act;

(b) other changes to the United Kingdom's domestic frameworks which are relevant to the matters listed in Article 45(2) of the UK GDPR (transfers on the basis of an adequacy decision);

(c) relevant changes to the United Kingdom's international commitments or other obligations arising from legally binding conventions or instruments, as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

Member's explanatory statement
This amendment requires the Secretary of State to carry out an assessment of the impact of this Act and other changes to the UK's domestic and international frameworks relating to data adequacy.

Clause 90

LORD HOLMES OF RICHMOND

38 Clause 90, page 113, line 15, at end insert "in accordance only with the Commissioner's duties under section 108 of the Deregulation Act 2015 (exercise of regulatory functions: economic growth)."

Member's explanatory statement
This amendment ensures that the Commissioner's duty to have regard to the desirability of promoting innovation is referable only to the duty imposed under section 108 of the Deregulation Act 2015. This amendment seeks to ensure that the Commissioner's status as an independent supervisory authority for data protection is preserved given that such status is an essential component of any EU adequacy decision.

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA

39 Clause 90, page 113, leave out lines 20 to 22 and insert—

"(e) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data;

(f) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;

(g) the fact that children may require different protections at different ages and stages of development;"

"(2) In this section, a "child" is a person under the age of 18."

Member's explanatory statement
This amendment provides a list of the protections, rights and needs to children at different ages and stages of development that the Information Commissioner must take into account when exercising their regulatory functions.

LORD VALLANCE OF BALHAM

40 Clause 90, page 113, line 20, after "children" insert "merit specific protection with regard to their personal data because they"

Member's explanatory statement
This amendment adds an express reference to children meriting specific protection with regard to their personal data in new section 120B(e) of the Data Protection Act 2018 (Information Commissioner's duties in relation to functions under the data protection legislation). See also the amendment in my name to Clause 70, page 78, line 23.

After Clause 92

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD CLEMENT-JONES
BARONESS HARDING OF WINSCOMBE

41 After Clause 92, insert the following new Clause—

"Code of practice on children and AI

(1) The Commissioner must prepare a code of practice in accordance with sections 91 and 92 which contains such guidance as the Commissioner considers appropriate on standards of fairness and ethical practice in the use of children's data and personal information in the development of AI including general purpose AI and use of foundational models that impact children.

(2) In preparing a code or amendments under this section, the Commissioner must—

(a) have regard to—

(i) children's interests and fundamental rights and freedoms as set out in the United Nations Convention on the Rights of the Child and General Comment 25 on Children's Rights in relation to the Digital Environment,

(ii) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data as established in the 2018 Act,

(iii) the potential harm to future life chances, income, health and wellbeing, and

(iv) the need for products and services likely to impact on children to be safe and equitable by design and default.

(b) consult with—

(i) academics with expertise in the field, and

(ii) persons who appear to the Commissioner to represent the interests of children.

(3) In this section—

"fairness and ethical practice in the use of children's data and personal information in the development of AI" means having regard to—

(a) risk assessment;

(b) accountability;

(c) transparency;

(d) lawfulness;

(e) accuracy;

(f) fairness;

(g) ethical use;

"impacts children" means AI technology that is—

(a) based on data sets that include (or may include) children's data;

(b) used to automate services likely to be accessed by children and access their data;

(c) used to make decisions that impact children;

(d) used to surface or deprioritise content, information, people, accounts, services or products to children;

(e) used to predict or inform children's behaviour, opinions, opportunities and decision-making using personal data;

(f) used to imitate children's physical likeness, movements, voice, behaviour and thoughts using personal data;

"risk assessment" includes guidance on how controllers articulate and evaluate the following four stages—

(a) the intention and goals in creating an AI model and how these have evolved over time;

(b) the inputs used to build, train and evolve an AI model;

(c) the assumptions and instructions that inform the AI model's decision-making;
(d) intended and actual outputs and outcomes of the AI model;
(e) sufficient and consistent routes for complaint, redress and identification of emerging risk."

Member's explanatory statement
Given the rapid acceleration in the development of AI technology, this Code of Practice ensures that data processors prioritise the interests and fundamental rights and freedoms of children and sets out what this means in practice.

BARONESS KIDRON
LORD CLEMENT-JONES

42 After Clause 92, insert the following new Clause—

"Code of practice on data communities

(1) The Commissioner must prepare a code of practice which contains—
(a) practical guidance on establishing, operating and joining a data community,
(b) practical guidance for data controllers and data processors on responding to requests made by data communities, and
(c) such other guidance as the Commissioner considers appropriate to promote good practice in all aspects of data communities schemes.

(2) The data subject has the right to specify which data and which rights over that data they assign to the data community for what purpose and for how long, with respect to which data controllers.

(3) In this section—
"good practice in data community" means such practice as appears to the Commissioner to be desirable having regard to the interests of data subjects whose data forms part of a data community, including compliance with the requirements mentioned in subsection (1)."

Member's explanatory statement
This amendment requires the Commissioner to draw up a code of practice setting out the way in which data communities must operate and the requirements on data controllers and processors when engaging with data rights activation requests from data communities. In addition to the code of conduct, there would also be the full range of protections already in place with respect to any controller. It is one of a series of amendments that would establish the ability to assign data rights to a third party.

BARONESS KIDRON
LORD CLEMENT-JONES

43 After Clause 92, insert the following new Clause—

"Register and oversight of data communities

(1) The Information Commissioner must maintain a register of data communities and make the register publicly available.

(2) The criteria for suitability for inclusion in the register will be set out in the Code of Practice on Data Communities.

(3) The Information Commissioner must create a complaints mechanism to receive, review and adjudicate complaints raised by data subjects about a data community controller.

(4) Complaints under subsection (3) can only be based on a failure to meet the standards set out in the Code of Practice on Data Communities.

(5) The Information Commissioner must create a complaints mechanism to receive, review and adjudicate complaints raised by a data community controller on behalf of its members about a data controller or processor.

(6) Complaints under subsection (5) must be based on a failure to meet the standards set out in the Code of Practice on Data Communities."

Member's explanatory statement
This amendment ensures that data communities operate transparently and are subject to regulatory oversight. It is one of a series of amendments that would establish the ability to assign data rights to a third party. A data community controller will have the responsibilities assigned to a controller as well as additional protections as set out the proposed code of conduct.

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
LORD CLEMENT-JONES
BARONESS HARDING OF WINSCOMBE

44 After Clause 92, insert the following new Clause—

"Code of practice on Children's Data and Education

(1) The Commissioner must prepare a code of practice which contains such guidance as the Commissioner considers appropriate on the processing of data in connection with the provision of education.

(2) Guidance under subsection (1) must include consideration of—
  (a) all aspects of the provision of education including learning, school management and safeguarding;
  (b) all types of schools and learning settings;
  (c) the need for transparency and evidence of efficacy on the use of AI systems in the provision of education;

(d) the impact of profiling and automated decision-making on children's access to education opportunities;

(e) the principle that children have a right to know what data about them is being generated, collected, processed, stored and shared;

(f) the principle that those with parental responsibility have a right to know how their children's data is being generated, collected, processed, stored and shared;

(g) the safety and security of children's data;

(h) the need to ensure children's access to and use of counselling services and the exchange of information for safeguarding purposes are not restricted.

(3) In preparing a code or amendments under this section, the Commissioner must have regard to—

(a) the fact that children are entitled to a higher standard of protection than adults with regard to their personal data as set out in the UK GDPR, and the ICO's Age Appropriate Design code;

(b) the need to prioritise children's best interests and to uphold their rights under UN Convention on the Rights of the Child and General Comment 25;

(c) the fact that children may require different protections at different ages and stages of development;

(d) the need to support innovation to enhance UK children's education and learning opportunities, including facilitating testing of novel products and supporting the certification and the development of standards;

(e) ensuring the benefits from product and service developed using UK children's data accrue to the UK.

(4) In preparing a code or amendments under this section, the Commissioner must consult with—

(a) children,

(b) educators,

(c) parents,

(d) persons who appear to the Commissioner to represent the interests of children,

(e) the AI Safety Institute, and

(f) the relevant Education department for each nation of the United Kingdom.

(5) The Code applies to data processors and controllers that—

(a) are providing education in school or other learning settings;

(b) provide services or products in connection with the provision of education;

(c) collect children's data whilst they are learning;

(d) use education data, education data sets or pupil data to develop services and products;

(e) build, train or operate AI systems and models that impact children's learning experience or outcomes;

(f) are public authorities that process education data, education data sets or pupil data.

(6) The Commissioner must prepare a report, in consultation with the EdTech industry and other stakeholders set out in subsection (4), on the steps required to develop a certification scheme under Article 42 of the UK GDPR, to enable the industry to demonstrate the compliance of EdTech services and products with the UK GDPR, and conformity with this Code.

(7) Where requested by an education service, evidence of compliance with this Code must be provided by relevant providers of commercial products and services in a manner that satisfies the education service's obligations under the Code.

(8) In this section—

"EdTech" means a service or product that digitise education functions including administration and management information systems, learning and assessment and safeguarding, including services or products used within school settings and at home on the recommendation, advice or instruction of a school;

"education data" means personal data that forms part of an educational record.

"education data sets" means anonymised or pseudonymised data sets that include Education Data or Pupil Data.

"efficacy" means that the promised learning outcomes can be evidenced.

"learning setting" means a place where children learn including schools, their home and extra-curricular learning services for example online and in-person tutors.

"pupil data" means personal data about a child collected whilst they are learning which does not form part of an educational record.

"safety and security" means that it has been adequately tested.

"school" means an entity that provides education to children in the UK including early years providers, nursery schools, primary schools, secondary schools, sixth form colleges, city technology colleges, academies, free schools, faith schools, special schools, state boarding schools, and private schools."

Member's explanatory statement

This amendment proposes a statutory Code of Practice on Children and Education to ensure that children benefit from heightened protections when their data is processed for purposes relating to education. Common standards across the sector will assist schools in procurement.

Clause 101

BARONESS KIDRON
LORD CLEMENT-JONES
LORD STEVENSON OF BALMACARA
BARONESS HARDING OF WINSCOMBE

45 Clause 101, page 129, line 38, at end insert—

"(5A) The report must—

(a) set out separately the information required under subsections (2) to (5) where regulatory action or policy relates to children;
(b) provide details of all activities carried out by the Information Commissioner to support, strengthen and uphold the Age-Appropriate Design Code;
(c) provide information about how it has met its child-related duties under section 120B (e)-(h)."

Member's explanatory statement
This amendment would ensure that the ICO's annual report records activities and action taken by the ICO in relation to children. This would enhance understanding, transparency and accountability.

After Clause 104

LORD CLEMENT-JONES

46★ After Clause 104, insert the following new Clause—

"Review of court jurisdiction

Within one year of the day on which this Act is passed the Secretary of State must review the impact that transferring the jurisdiction of courts that relate to all data protection provisions to tribunals would have on—
(a) the complexity of the appeals system, and
(b) legal barriers to representation and redress."

After Clause 107

LORD HOLMES OF RICHMOND

47 After Clause 107, insert the following new Clause—

"Data use: defences to charges under the Computer Misuse Act 1990

(1) The Computer Misuse Act 1990 is amended as follows.

(2) In section 1, after subsection (3) insert—

"(4) It is a defence to a charge under subsection (1) to prove that—
(a) the person's actions were necessary for the detection or prevention of crime, or
(b) the person's actions were justified as being in the public interest."

(3) In section 3, after subsection (6) insert—

"(7) It is a defence to a charge under subsection (1) in relation to an act carried out for the intention in subsection (2)(b) or (c) to prove that—
(a) the person's actions were necessary for the detection or prevention of crime, or
(b) the person's actions were justified as being in the public interest.""

Member's explanatory statement
This amendment updates the definition of "unauthorised access" in the Computer Misuse Act 1990 to provide clearer legal protections for legitimate cybersecurity activities.

LORD HOLMES OF RICHMOND

48 After Clause 107, insert the following new Clause—

"Data use: definition of unauthorised access to computer programs or data

In section 17 of the Computer Misuse Act 1990, at the end of subsection (5) insert—

"(c) they do not reasonably believe that the person entitled to control access of the kind in question to the program or data would have consented to that access if they had known about the access and the circumstances of it, including the reasons for seeking it, and

(d) they are not empowered by an enactment, by a rule of law, or by order of a court or tribunal to access of the kind in question to the program or data.""

After Clause 112

LORD VALLANCE OF BALHAM
LORD CLEMENT-JONES

49 After Clause 112, insert the following new Clause—

"Use of electronic mail for direct marketing by charities

(1) Regulation 22 of the PEC Regulations (use of electronic mail for direct marketing purposes) is amended as follows.

(2) In paragraph (2), after "paragraph (3)" insert "or (3A)".

(3) After paragraph (3) insert—

"(3A) A charity may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) the sole purpose of the direct marketing is to further one or more of the charity's charitable purposes;

(b) the charity obtained the contact details of the recipient of the electronic mail in the course of the recipient—

(i) expressing an interest in one or more of the purposes that were the charity's charitable purposes at that time; or

(ii) offering or providing support to further one or more of those purposes; and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of their contact details for the purposes of direct marketing by the charity, at the time that the details were initially collected, and,

where the recipient did not initially refuse the use of the details, at the time of each subsequent communication."

(4) After paragraph (4) insert—

"(5) In this regulation, "charity" means—

(a) a charity as defined in section 1(1) of the Charities Act 2011,

(b) a charity as defined in section 1(1) of the Charities Act (Northern Ireland) 2008 (c. 12 (N.I.)), including an institution treated as such a charity for the purposes of that Act by virtue of the Charities Act 2008 (Transitional Provision) Order (Northern Ireland) 2013 (S.R. (N.I.) 2013 No. 211), and

(c) a body entered in the Scottish Charity Register, other than a body which no longer meets the charity test in section 7 of the Charities and Trustee Investment (Scotland) Act 2005 (asp 10),

and, in relation to such a charity, institution or body, "charitable purpose" has the meaning given in the relevant Act.""

Member's explanatory statement

Regulation 22 of the PEC Regulations prohibits the transmission, by means of electronic mail, of unsolicited communications to individual subscribers. This amendment creates an exception from the prohibition for direct marketing carried out by a charity for charitable purposes.

After Clause 114

LORD CLEMENT-JONES

50 After Clause 114, insert the following new Clause—

"Soft opt-in for email marketing for charities

(1) Regulation 22 of the PEC Regulations (use of electronic mail for direct marketing purposes) is amended as follows.

(2) In paragraph (2), after "paragraph (3)" insert "or (3A)".

(3) After paragraph (3) insert—

"(3A) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where—

(a) the direct marketing is solely for the purpose of furthering a charitable objective of that person,

(b) that person obtained the contact details of the recipient of the electronic mail in the course of the recipient expressing an interest in or offering or providing support for the furtherance of that objective or a similar objective, and

(c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of their contact details for the purposes of such direct marketing, at the time that the details were initially collected, and,

where the recipient did not initially refuse the use of the details, at the time of each subsequent communication.""

Member's explanatory statement
This amendment seeks to enable charities to communicate to donors in the same way that businesses have been able to communicate to customers since 2003. The clause intends to help facilitate greater fundraising and support the work charities do for society.

Clause 123

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES

51 Clause 123, page 153, line 14, leave out "may by regulations" and insert "must, as soon as reasonably practicable and no later than 12 months after the day on which this Act is passed, make and lay regulations to"

Member's explanatory statement
This amendment removes the Secretary of State's discretion on whether to lay regulations under Clause 123 and sets a time limit for laying them before Parliament.

LORD BETHELL

52★ Clause 123, page 153, leave out line 34

Member's explanatory statement
This amendment provides for any requirements under the researcher access regulations to be enforceable in the same way as other requirements in the OSA, obviating the need to design a bespoke enforcement system.

BARONESS KIDRON
LORD RUSSELL OF LIVERPOOL
BARONESS HARDING OF WINSCOMBE
LORD CLEMENT-JONES

53 Clause 123, page 153, line 35, at end insert—

"(l) requirements to facilitate independent research into online safety matters as they relate to people at different ages and stages of development, and people with different characteristics including gender, race, ethnicity, disability and sexuality."

Member's explanatory statement
This amendment seeks to ensure the regulations will enable independent researchers to research how online risks and harms impact different groups especially vulnerable users including children.

LORD BETHELL

54★ Clause 123, page 153, line 36, leave out from beginning to end of line 6 on page 154 and insert—

"(3) Any requirements or duties placed on providers of regulated services by regulations made under subsection (1) shall be made an enforceable requirement within the meaning of section 131."

Member's explanatory statement
This amendment provides for any requirements under the researcher access regulations to be enforceable in the same way as other requirements in the OSA, obviating the need to design a bespoke enforcement system.

LORD BETHELL

55★ Clause 123, page 154, line 6, at end insert—

"(3A) Regulations under this section may not prevent a person from seeking or accessing information in accordance with their terms solely because the person is located, or intends to carry out research, outside of the United Kingdom."

LORD BETHELL

56★ Clause 123, page 155, line 9, at end insert—

"154B Non-enforceability of contractual restraints on research provided for by this Act

(1) No contractual term shall be enforceable by a provider of a regulated service to the extent that—

(a) it is sought to be enforced against a person qualified to make applications for information pursuant to regulations made under section 154A, and

(b) its enforcement would prevent that person from carrying out research of the kind provided for by regulations made under section 154A.

(2) Subsection (1) applies regardless of whether the person against whom the contractual term is sought to be enforced has obtained any information under regulations made under section 154A.

(3) A contractual term shall not be unenforceable pursuant to subsection (1) by reason only of it requiring personal data to be processed in accordance with the data protection legislation."

Member's explanatory statement
This amendment further amends the Online Safety Act, making any contractual provision – such as a provision in a platform's terms of service – unenforceable if enforcing it would prevent

"research into online safety matters" as defined in and provided for by the regulations which the Secretary of State will make.

After Clause 132

LORD BASSAM OF BRIGHTON
LORD FREYBERG
THE EARL OF CLANCARTY

57 After Clause 132, insert the following new Clause—

"Private copy levy on digital access

(1) The Secretary of State may by regulations make provision for the establishment of an annual private copy levy, to be levied when online digital content is accessed or stored.

(2) Before making regulations under this section, the Secretary of State must consult such persons as the Secretary of State considers appropriate.

(3) The provisions made under subsection (1) must include but are not limited to—
  (a) establishing governance arrangements to calculate the rate and application of the levy,
  (b) permitting relevant copyright collecting societies to collect and distribute monies raised by the levy to rightsholder funds, and
  (c) distributing any surplus funds raised by the levy for the purposes of funding arts and cultural initiatives in the United Kingdom.

(4) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative resolution procedure.

(5) The Secretary of State must commission an annual transparency report on the operation of the levy.

(6) The Secretary of State must lay the report made under subsection (5) before Parliament."

Member's explanatory statement
This amendment seeks to allow the Secretary of State to establish a private copy levy for digital content, with revenue distributed to rightsholder funds and cultural initiatives.

BARONESS KIDRON
LORD TARASSENKO
LORD STEVENSON OF BALMACARA
LORD CLEMENT-JONES

58 After Clause 132, insert the following new Clause—

"Sovereign data assets

(1) The Secretary of State may by regulations define data sets held by public bodies and arm's length institutions and other data sets that are held in the public interest as sovereign data assets (defined in subsection (6)).

(2) In selecting data sets which may be designated as sovereign data assets, the Secretary of State must—

(a) have regard to—

(i) the security and privacy of United Kingdom data subjects;

(ii) the ongoing value of the data assets;

(iii) the rights of United Kingdom intellectual property holders;

(iv) ongoing adherence to the values, laws and international obligations of the United Kingdom;

(v) the requirement for public sector employees, researchers, companies and organisations headquartered in the United Kingdom to have preferential terms of access;

(vi) the need for data to be stored in the United Kingdom, preferably in data centres in the United Kingdom;

(vii) the need to design Application Programming Interfaces (APIs) as bridges between each sovereign data asset and the client software of the authorized licence holders;

(b) consult with—

(i) academics with expertise in the field;

(ii) the AI Safety Institute;

(iii) those with responsibility for large public data sets;

(iv) data subjects;

(v) the Information Commissioner.

(3) The Secretary of State must establish a transparent licensing system, fully reflecting the security and privacy of data held on United Kingdom subjects, for use in providing access to sovereign data assets.

(4) The Secretary of State must report annually to Parliament on the ongoing value of the sovereign data assets, in terms of—

(a) their value to future users of the data;

(b) the financial return expected when payment is made for the use of such data in such products and services as may be expected to be developed.

(5) The National Audit Office must review the licensing system established by the Secretary of State under subsection (3) and report annually to Parliament as to its effectiveness in securing the ongoing security of the sovereign data assets.

(6) In this section—

"sovereign data asset" means—

(a) data held by public bodies and arm's length institutions of government;

(b) data sets held by third parties that volunteer data to form, or contribute to, a public asset.

(7) Regulations under this section are to be made by statutory instrument.

(8) A statutory instrument containing regulations under this section may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament."

Member's explanatory statement

The UK has a number of unique publicly-held data assets, from NHS data to geospatial data and the BBC's multimedia data. This amendment would create a special status for data held in the public interest, and a licensing scheme for providing access to them, which upholds UK laws and values, and ensure a fair return of financial benefits to the UK.

LORD HOLMES OF RICHMOND

59 After Clause 132, insert the following new Clause—

"Data use: review of large language models

(1) On the day on which this Act is passed, the Secretary of State must launch a review to consider the introduction of standards for the input and output of data of large language models which operate and generate revenue in the United Kingdom.

(2) The review must consider—

(a) the applicability of similar standards, such as those that already exist in industries such as pharmaceuticals, food and drinks,

(b) whether there is a need for legislative clarity under section 27 of the Copyright, Designs and Patents Act 1988 about whether the input and output of large language models constitute an "article", and

(c) whether a minimum standard should be a condition for market access."

LORD HOLMES OF RICHMOND

60 After Clause 132, insert the following new Clause—

"Review: data centre availability

On the day on which this Act is passed, the Secretary of State must launch a review of the impact of the provisions in this Act on the availability of data centres which must consider whether there is a need to accelerate the buildout of data centres."

BARONESS KIDRON
LORD CLEMENT-JONES
LORD FREYBERG
LORD STEVENSON OF BALMACARA

61 After Clause 132, insert the following new Clause—

"Compliance with UK copyright law by operators of web crawlers and general-purpose AI models

(1) The Secretary of State must by regulations make provision (including any such provision as might be made by Act of Parliament), requiring the operators of web crawlers and general-purpose artificial intelligence (AI) models whose services have links with the United Kingdom within the meaning of section 4(5) of the Online Safety Act 2023 to comply with United Kingdom copyright law, including the Copyright, Designs and Patents Act 1988, regardless of the jurisdiction in which the copyright-relevant acts relating to the pre-training, development and operation of those web crawlers and general-purpose AI models take place.

(2) Provision made under subsection (1) must apply to the entire lifecycle of a general-purpose AI model, including but not limited to—
(a) pre-training and training,
(b) fine tuning,
(c) grounding and retrieval-augmented generation, and
(d) the collection of data for the said purposes.

(4) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure."

Member's explanatory statement
This amendment is part of a group of amendments that would clarify the requirement for web-crawlers and other "data gatherers" to observe UK copyright law. This is to counter the wide spread theft of IP by AI companies who use it as raw material for their products.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD FREYBERG
LORD STEVENSON OF BALMACARA

62 After Clause 132, insert the following new Clause—

"Transparency of crawler identity, purpose, and segmentation

(1) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose artificial intelligence (AI) models whose services have links with the United Kingdom within the meaning of section 4(5) of the Online Safety Act 2023 to disclose information regarding the identity of crawlers used by them or by third parties on their behalf, including but not limited to—
(a) the name of the crawler,

(b) the legal entity responsible for the crawler,
(c) the specific purposes for which each crawler is used,
(d) the legal entities to which operators provide data scraped by the crawlers they operate, and
(e) a single point of contact to enable copyright owners to communicate with them and to lodge complaints about the use of their copyrighted works.

(2) The information disclosed under subsection (1) must be available on an easily accessible platform and updated at the same time as any change.

(3) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose AI models to deploy distinct crawlers for different purposes, including but not limited to—
(a) web indexing for search engine results pages,
(b) general-purpose AI model pre-training, and
(c) retrieval-augmented generation.

(4) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose AI models to ensure that the exclusion of a crawler by a copyright owner does not negatively impact the findability of the copyright owner's content in a search engine.

(5) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under this section within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure."

Member's explanatory statement
This amendment is part of a group of amendments that would clarify the requirement for web-crawlers and other "data gatherers" to observe UK copyright law. This amendment requires the SoS to set out strict transparency requirements for web crawlers so that it is possible for IP holders to identify the owners of webcrawlers.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD FREYBERG
LORD STEVENSON OF BALMACARA

63 After Clause 132, insert the following new Clause—

"Transparency of copyrighted works scraped

(1) The Secretary of State must by regulations make provision requiring operators of web crawlers and general-purpose artificial intelligence (AI) models whose services have links with the United Kingdom within the meaning of section 4(5) of the Online Safety Act 2023 to disclose information regarding text and data used in the pre-training, training and fine-tuning of general-purpose AI models, including but not limited to—
(a) the URLs accessed by crawlers deployed by them or by third parties on their behalf or from whom they have obtained text or data,

(b) the text and data used for the pre-training, training and fine-tuning, including the type and provenance of the text and data and the means by which it was obtained,

(c) information that can be used to identify individual works, and

(d) the timeframe of data collection.

(2) The disclosure of information under subsection (1) must be updated on a monthly basis in such form as the regulations may prescribe and be published in such manner as the regulations may prescribe so as to ensure that it is accessible to copyright owners upon request.

(3) The Secretary of State must lay before Parliament a draft of the statutory instrument containing regulations under subsection (1) within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure."

Member's explanatory statement
This amendment is part of a group of amendments that would clarify the requirement for web-crawlers and other "data gatherers" to observe UK copyright law. This amendment requires the SoS to set out transparency requirements that would allow copyright holders to identify when and from where their work has been taken.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD FREYBERG
LORD STEVENSON OF BALMACARA

64 After Clause 132, insert the following new Clause—

"Enforcement

(1) The Secretary of State must by regulations make provision requiring the Information Commission (under section 114 of the Data Protection Act 2018) ("the Commissioner") to monitor and secure compliance with the duties under sections (*Transparency of crawler identity, purpose, and segmentation*) and (*Transparency of copyrighted works scraped*) ("the duties") by an operator of a web crawler or general-purpose artificial intelligence (AI) model whose service has links with the United Kingdom within the meaning of section 4(5) of the Online Safety Act 2023 ("a relevant operator"), including but not limited to the following—

(a) the regulations must provide for the Commissioner to have the power by written notice (an "information notice") to require a relevant operator to provide the Commissioner with information that the Commissioner reasonably requires for the purposes of investigating a suspected failure to comply with the duties;

(b) the regulations must provide for the Commissioner to have the power by written notice (an "assessment notice") to require and to permit the Commissioner to carry out an assessment of whether a relevant operator has complied or is complying with the duties and to require a relevant operator to do any of the acts set out in section 146(2) of the Data Protection Act 2018;

(c) the regulations must provide that where the Commissioner is satisfied that a relevant operator has failed, or is failing to comply with the duties, the Commissioner may give the relevant operator a written notice (an "enforcement notice") which requires it—

(i) to take steps specified in the notice, or

(ii) to refrain from taking steps specified in the notice;

(d) the regulations must provide that where the Commissioner is satisfied that a relevant operator has failed or is failing to comply with the duties or has failed to comply with an information notice, an assessment notice or an enforcement notice, the Commissioner may, by written notice (a "penalty notice"), require the person to pay to the Commissioner an amount in sterling specified in the notice, the maximum amount of the penalty that may be imposed by a penalty notice being the "higher maximum amount" as defined in section 157 of the Data Protection Act 2018;

(e) the regulations may provide for the procedure and rights of appeal in relation to the giving of an information notice, an assessment notice, an enforcement notice or a penalty notice.

(2) The regulations must provide that any failure to comply with the duties by a relevant operator shall be directly actionable by any copyright owner who is adversely affected by such failure, and that such copyright owner will be entitled to recover damages for any loss suffered and to injunctive relief.

(3) The regulations must provide that the powers of the Commissioner and the rights of a copyright owner will apply in relation to a relevant operator providing a service from outside the United Kingdom (as well as such one provided from within the United Kingdom).

(4) The Secretary of State must lay before Parliament a draft of the statutory instrument containing the regulations under this section within six months of the day on which this Act is passed and the regulations are subject to the affirmative procedure."

Member's explanatory statement

This amendment is part of a group of amendments that would clarify the requirement for web-crawlers and other "data gatherers" to observe UK copyright law. This amendment creates an enforcement procedure in line with the Data Protection Act 2018.

BARONESS KIDRON
LORD CLEMENT-JONES
LORD FREYBERG
LORD STEVENSON OF BALMACARA

65 After Clause 132, insert the following new Clause—

"Technical solutions

(1) The Secretary of State must conduct a review of the technical solutions that may be adopted by copyright owners and by the operators of web crawlers and general-purpose artificial intelligence (AI) models whose services have links with

the United Kingdom within the meaning of section 4(5) of the Online Safety Act 2023 to prevent and to identify the unauthorised scraping or other unauthorised use of copyright owners' text and data.

(2) Within 18 months of the day on which this Act is passed, the Secretary of State must report on such technical solutions and must issue guidance as to the technical solutions to be adopted and other recommendations for the protection of the interests of copyright owners."

LORD HOLMES OF RICHMOND

66 After Clause 132, insert the following new Clause—

"Consultation: data centre power usage

On the day on which this Act is passed, the Secretary of State must launch a consultation on the implications of the provisions in this Act for the power usage and energy efficiency of data centres."

LORD LUCAS
LORD ARBUTHNOT OF EDROM

67 After Clause 132, insert the following new Clause—

"Data dictionary

(1) The Secretary of State may make regulations establishing the definitions and associated metadata for core personal data attributes, and may require that these definitions are used in relation to—
  (a) Part 2 of this Act (digital verification services);
  (b) Part 4 of this Act (registers of births and deaths);
  (c) Part 7 of this Act (other provision about use of, or access to, data);
  (d) personal data recorded by public authorities in general.

(2) Regulations under this section are subject to the negative resolution procedure."

Member's explanatory statement
This amendment is to ensure consistency of definition of key personal attributes across government and over time, e.g. definition of "sex".

BARONESS KIDRON
LORD CLEMENT-JONES

68 After Clause 132, insert the following new Clause—

"Reliability of computer-based evidence

(1) Electronic evidence produced by or derived from a computer, device or computer system (separately or together "system") may be relied on as evidence in any proceedings —

(a) where that electronic evidence is not challenged;

(b) where the court is satisfied that the electronic evidence is derived from a reliable system or otherwise the court is satisfied that the evidence is reliable.

(2) Rules of Court must provide that electronic evidence sought to be relied upon by a party in any proceedings may be challenged by another party as to its correctness.

(3) For the purposes of subsection (1)(a), Rules of Court must provide for the circumstances in which the Court may be satisfied that the admissibility of electronic evidence cannot reasonably be challenged.

(4) For the purposes of subsection (1)(b), the matters that may be taken into account by the court in determining if a system is to be considered reliable include—

(a) whether the evidence is wholly obtained from a regulated system (such as a speed camera and DVLA database);

(b) the errors that have been reported in the system, the actions taken to correct them, and any errors that remain uncorrected (these may include the Known Error Log and Release Notices);

(c) the measures taken to ensure that the electronic evidence accurately records the facts that are being claimed (including measures to block, record and manage cyberattacks);

(d) the forensic measures taken to ensure that the electronic evidence has not been affected by accidental, privileged or unauthorised access;

(e) the route that the electronic evidence has taken from the originating system to the court and the measures taken to ensure its integrity;

(f) external independent audit of the system.

(5) If the materials under subsection (4) are not available or if the materials produced for the purposes of subsection (4) are considered by the court to be insufficient for the court to conclude that the system is reliable for the purposes of subsection (1)(b), the party seeking to rely upon the electronic evidence must otherwise satisfy the court that that evidence is reliable.

(6) For the purposes of this section—

"computer" means any device capable of performing mathematical or logical instructions;

"device" means any apparatus or tool operating alone or connected to other apparatus or tools, that processes information or data in electronic form;

"electronic evidence" means evidence derived from data contained in or produced by any device or computer the functioning of which depends on a software program or from data stored on a computer, device or computer system or communicated over a networked computer system."

BARONESS OWEN OF ALDERLEY EDGE
LORD CLEMENT-JONES
BARONESS KIDRON
LORD BROWNE OF LADYTON

69 After Clause 132, insert the following new Clause—

"Digitally created sexually explicit photographs or films

In the Sexual Offences Act 2003, after section 66D, insert—

"66E Creating or soliciting a non-consensual digitally produced sexually explicit photograph or film

(1) A person (A) commits an offence if—
  (a) A uses personal data or digital information, including a photograph or film, to create, or solicit the creation of, a digitally produced sexually explicit photograph or film of another person B,
  (b) B does not consent to the creation or solicitation of the photograph or film, and
  (c) A does not reasonably believe that B consents.

(2) For the purposes of subsection (1), it does not matter whether the data upon which the digitally produced sexually explicit photograph or film was based, was obtained consensually.

(3) Subsection (1) applies when the solicitation of the creation of digitally produced sexually explicit photograph or film has taken place in the United Kingdom, irrespective of the location of the person or persons who have been solicited for the creation of such a photograph or film.

(4) A person (A) may commit an offence under this section whether or not creation occurs.

(5) It is a defence for a person charged with an offence under subsection (1) to prove that the person had a reasonable excuse for creating, or soliciting the creation of, the photograph or film.

(6) A person who commits an offence under subsection (1) is liable on summary conviction to imprisonment for a term not exceeding the maximum term for summary offences or a fine (or both).

(7) In relation to section 127(1) of the Magistrates' Court Act 1980 (limitation of time) the date on which the "matter of complaint" arose will be taken as the date on which B becomes aware that an offence under this section may have been committed.

(8) In this section, "soliciting" means encouraging or facilitating the creation of a digitally produced sexually explicit photograph or film.

(9) In this section, "sexually explicit photograph or film" means a photograph or film, as defined in section 66A(3) to (5), which appears to be a

photograph or film of anyone in an "intimate state" as defined in section 66D(5), (6) or (7).""

BARONESS OWEN OF ALDERLEY EDGE
LORD CLEMENT-JONES
BARONESS KIDRON
LORD BROWNE OF LADYTON

70 After Clause 132, insert the following new Clause—

"Code of practice: Application of section 153 of the Sentencing Act 2020 to deletion of data in relation to sexual offences

(1) The Secretary of State must prepare and publish a code of practice for the court about the application of section 153 of the Sentencing Act 2020 (Deprivation order: availability) to the deletion of data following conviction for an offence under section 66A, 66B, 67 or 67A of the Sexual Offences Act 2003.

(2) The code of practice must include guidance for compelling the deletion of copies of an intimate photograph or film, including physical copies and those held on any device, cloud-based programme, or digital, messaging or social media platform they control.

(3) The Secretary of State may, by regulations, extend the application of the code of practice to offences under the Sexual Offences Act 2003 other than those set out in subsection (1).

(4) The Secretary of State may, by regulations, extend the application of the code of practice to copies of an intimate photograph or film stored in any form.

(5) A statutory instrument containing regulations under subsection (3) and (4) may not be made unless a draft of the instrument has been laid before and approved by a resolution of each House of Parliament.

(6) The Secretary of State must publish the code of practice within one year of the day on which this Act is passed and must revise and republish the code of practice annually thereafter.

(7) In preparing or revising the code of practice, the Secretary of State must consult such persons they consider appropriate or relevant.

(8) The requirement in subsection (7) may be satisfied by consultation undertaken before the coming into force of this section.

(9) The Secretary of State may not publish the first version of the code of practice unless a draft of the code has been laid before, and approved by a resolution of, each House of Parliament.

(10) The Secretary of State may not republish the code of practice following its revision unless—

(a) a draft of the code as revised has been laid before each House of Parliament, and

(b) the 40-day period has expired without either House of Parliament resolving not to approve the draft.

(11) "The 40-day period" means—

(a) the period of 40 days beginning with the day on which the draft is laid before Parliament, or

(b) if the draft is not laid before each House on the same day, the period of 40 days beginning with the later of the days on which it is laid before Parliament.

(12) In calculating the 40-day period, no account is to be taken of any whole days that fall within a period during which Parliament is dissolved or prorogued or during which both Houses are adjourned for more than 4 days."

BARONESS KIDRON
LORD CLEMENT-JONES

71 After Clause 132, insert the following new Clause—

"Oversight of a National Data Library

(1) Before establishing a National Data Library, or similar entity, that has the power to give access to United Kingdom public data sets, the Secretary of State must consult on the legislative and regulatory basis on which the entity will exercise its functions and powers in relation to data use and access.

(2) A consultation carried out under subsection (1) must seek information on the considerations listed in subsection (5).

(3) If establishing a National Data Library, or similar entity, that has the power to give access to United Kingdom public data sets, the Secretary of State must by regulations set out the regulatory basis on which the entity will exercise its functions and powers in relation to data use and access.

(4) When making regulations under subsection (3), the Secretary of State must have regard to the findings of the consultation completed under subsection (1) and the considerations listed in subsection (5).

(5) Considerations for the purposes of subsections (2) and (4) are—

(a) anonymity of personal data,

(b) consent for access to personal data,

(c) data collection,

(d) data curation,

(e) data de-identification, pseudonymisation or anonymisation,

(f) data hygiene,

(g) data linkage between National Data Library datasets,

(h) data security,

(i) data sovereignty,

(j) data valuation,

(k) data wrangling,

(l) income from licensing access to public data sets,
(m) tariffs for data access,
(n) the location of data storage for National Data Library,
(o) the preferability of data storage for the National Data Library being located in the United Kingdom,
(p) the effect of the National Data Library on the national interests of the United Kingdom,
(q) the governance, transparency, accountability and independence of the National Data Library, and
(r) appointments to the National Data Library.

(6) Regulations under this section are subject to the affirmative resolution procedure."

BARONESS OWEN OF ALDERLEY EDGE
BARONESS GOHIR

72 After Clause 132, insert the following new Clause—

"Digitally created sexually explicit audio

In the Sexual Offences Act 2003, after section 66D, insert—

"66E Creating or soliciting a non-consensual digitally produced sexually explicit audio

(1) A person (A) commits an offence if—
(a) A uses digital audio to create, or solicit the creation of digitally produced sexually explicit audio of another person B,
(b) B does not consent to the creation or solicitation of the audio, and
(c) A does not reasonably believe that B consents.

(2) For the purposes of subsection (1), it does not matter whether the data upon which audio was based was obtained consensually.

(3) Overlaying audio onto sexually explicit photographs or films constitutes an offence for the purposes of subsection (1).

(4) Subsection (1) applies when the solicitation of the creation of digitally produced sexually explicit audio has taken place in the United Kingdom, irrespective of the location of the person or persons who have been solicited for the creation of such audio.

(5) A person A may commit an offence under this section whether or not creation occurs.

(6) It is a defence for a person charged with an offence under subsection (1) to prove that the person had a reasonable excuse for creating, or soliciting the creation of, the audio.

(7) In relation to section 127(1) of the Magistrates' Court Act 1980 (limitation of time) the date on which the "matter of complaint" arose will be taken

as the date on which B becomes aware that an offence under section 66E may have been committed.

(8) A person who commits an offence under subsection (1) is liable on summary conviction to imprisonment for a term not exceeding the maximum term for summary offences or a fine (or both).

(9) In this section, "soliciting" means encouraging or facilitating the creation of audio.

(10) In this section, "sexually explicit audio" means audio which appears to be audio of anyone in an "intimate state" as defined in section 66D(5)(a) or (b).""

VISCOUNT CAMROSE
LORD MARKHAM

73★ After Clause 132, insert the following new Clause—

"Data risks from systemic competitors and hostile actors

(1) The Secretary of State, in consultation with the Information Commissioner, must conduct a risk assessment on the data privacy risks associated with genomics and DNA companies that are headquartered in countries the Government determines to be systemic competitors and hostile actors.

(2) Within 12 months of the day on which this Act is passed, the Secretary of State must present a report on the risk assessment in subsection (1) to Parliament and consult the intelligence and security agencies on the findings, taking into account the need not to make public information critical to national defence or ongoing operations.

(3) This risk assessment must evaluate—
  (a) the degree of access granted to foreign entities, particularly those linked to systemic competitors and hostile actors, to genomic and DNA data collected within the United Kingdom;
  (b) the potential for genomic and DNA data to be exfiltrated outside of the United Kingdom;
  (c) the potential misuse of United Kingdom genomic and DNA data for dual-use or nefarious purposes;
  (d) the potential for such data to be used in a manner that could compromise the privacy or security of United Kingdom citizens or undermine national security and strategic advantage.

(4) The risk assessment must consider and include, but is not limited to—
  (a) an analysis of the data handling and storage practices of genomics companies that are based in countries designated as systemic competitors and hostile actors,
  (b) an independent audit, including digital and physical forensic examination, at any company site that could have access to United Kingdom genomics data, and

(c) evidence of clear disclosure statements to consumers of products and services from genomics companies subject to data sharing requirements in the countries where they are headquartered.

(5) This risk assessment must be conducted as frequently as deemed necessary by the Secretary of State or the Information Commissioner to address evolving threats and ensure continued protection of the genomics sector from entities controlled, directly or indirectly, by countries designated as systemic competitors and hostile actors.

(6) The Secretary of State may issue directives or guidelines based on the findings of the risk assessment to ensure compliance by companies or personnel operating within the genomics sector in the United Kingdom, safeguarding against identified risks and vulnerabilities to data privacy."

Member's explanatory statement
This amendment seeks to ensure sufficient scrutiny of national security and data privacy risks related to advanced technology and areas of strategic interest for systemic competitors and hostile actors, inform the development of regulations or guidelines to mitigate those risks, and ensure security experts can scrutinise malign entities and guide researchers, consumers, businesses, and public bodies.

LORD CLEMENT-JONES

74★ After Clause 132, insert the following new Clause—

"Retrospective application

Within one month of the day on which this Act is passed, the Secretary of State must publish a statement clarifying whether the changes enacted by its commencement will apply to controllers and processors retrospectively, or only to data first processed following its commencement."

After Clause 135

VISCOUNT CAMROSE
LORD MARKHAM

75★ Clause 135, page 169, line 18, at end insert ", subject to subsection (1A).

(1A) Except for this section, no provisions in this Act may come into force before the Secretary of State has published a technological standard for a machine-readable digital watermark for the purposes of identifying licensed content and relevant information associated with the licence."

Member's explanatory statement
This amendment will require the Secretary of State to publish a technical standard for a machine-readable digital watermark, helping people protect licensed content from data scraping.

Clause 136

LORD VALLANCE OF BALHAM

76 Clause 136, page 169, line 20, at end insert—

"(za) section 66 (meaning of "the 2018 Act" and "the UK GDPR");"

Member's explanatory statement
This amendment provides that the clause defining "the 2018 Act" and "the UK GDPR" for the purposes of Chapter 1 of Part 5 of the Bill comes into force on Royal Assent.

Data (Use and Access) Bill [HL]

MARSHALLED
LIST OF AMENDMENTS
TO BE MOVED
ON REPORT

17 January 2025

PUBLISHED BY AUTHORITY OF THE HOUSE OF LORDS