



Department for
Science, Innovation
& Technology

Viscount Camrose
Parliamentary Under
Secretary of State
Department for Science,
Innovation & Technology
100 Parliament Street
London SW1A 2BQ

www.gov.uk/dsit

8th May 2024

House of Lords
London
SW1A 0PW

My Lords,

Thank you for your continued engagement with the Data Protection and Digital Information (DPDI) Bill during the sixth and seventh days of Committee stage. Now that Committee stage has come to an end, I am writing to follow up on questions raised by Noble Lords during the debate, to which I have provided a more detailed response below. I am also taking this opportunity to address some concerns raised by Baroness Kidron in letters to my Secretary of State and me.

I am copying this letter to all Noble Lords who were present during the sixth and seventh days of Committee stage and will deposit a copy in the House Library.

In addition, I will be scheduling meetings with Noble Lords present at the Committee Stage debates, to engage further ahead of Report stage.

Cookies

Lord Clement-Jones and Lord Bassam asked Lord Harlech to write with more detail on our engagement on these reforms. The Data Reform consultation, our engagement with Civil Society, and published research has shown that the public do want meaningful control over their personal data and privacy. The current consent requirements protect users who care about and wish to retain some control over their data. At the moment, customers will not automatically be opted-in to non-essential cookies on accessing a service but have to take a specific affirmative action (e.g. click a cookie banner) to agree to the use of cookies for specific purposes.

We have been clear through our engagement with industry groups such as IAB UK and the Advertisers Association, that we were including a small number of low privacy intrusive purposes on the face of the DPDI Bill and taking a power to enable the Government to keep the list of exemptions under review. In addition to continuing

official level engagement, industry groups have also met with Ministers and have been part of the Business Advisory Group.

As you will be aware the ICO's investigations into adtech and Real Time Bidding (RTB) have previously found compliance was lacking, with respect to transparency and that personal data was likely to be shared, matched and sold by many different advertisers and others in the ecosystem with the user often unaware of what is happening with their data and that it is happening on such a large scale. During our ongoing engagement with the sector, some respondents stated that some vendors re-use data for different purposes (e.g. targeting, profiling, re-sale to data brokers). This can make it challenging for advertisers to ensure that their own data is not being used for purposes they would not expect and, with so many different intermediaries collecting data it can be very difficult for individual consumers to understand what is happening with their data. We have also heard that types of platforms, data collection, data sharing and purposes are extensive and varied, and this makes it challenging to draft exceptions that are low privacy intrusive. We have also heard that it would be difficult to establish a singular set of safeguards that are universally applicable.

We have committed to continue to explore with the sector the use of cookies and similar technology for the placement of adverts and billing. This is a complex ecosystem and, as I have illustrated above, the inclusion of a new exemption on the placement and billing of adverts will require full consultation with industry, civil society and the regulator.

Telecommunications

Lord Leong sought clarification over the government's response to amendments 211 and 215, which focus on clause 116, the duty to notify the Information Commissioner of unlawful direct marketing.

As Lord Harlech mentioned in the debate, public communication network and service providers will not need to invest additional resources, implement new technology or systems in order to comply with the duty. It merely requires the communication providers to share with the Information Commissioner, any information that they already hold, which they have gathered through routine business activities. If this information indicates possible unlawful direct marketing transiting their network or service, they should notify the Information Commissioner. It will be the responsibility of the regulator to examine this information to determine if the law has been breached by an organisation. The communications providers are not required to undertake investigations of their own.

We have been clear through engagement with industry groups, such as Tech UK, that this duty does not require the providers to intercept and check communications to locate evidence of unlawful direct marketing activity. To reiterate this point, we amended the DPDI Bill's Explanatory Notes to explicitly say this in paragraph 809.

The Bill requires the Information Commissioner's Office (ICO) to publish guidance for complying with the duty. The guidance will be produced following full consultation with communication providers and the communications regulator Ofcom and will include details over what kind of information should be shared with the ICO.

The ICO has a very good relationship with industry and this duty will encourage more cooperation between the sector and the regulator, hence why we have set a very nominal fine of £1000 for non-compliance.

Form of Birth and Death registers

Baroness Jones asked whether one national scheme was intended, with the move to an electronic birth and death register, to standardise the process of recording births and deaths across the UK.

The strategic direction for the registration of births and deaths is to remove the requirement for paper registers and move to a single electronic register. All registration officers will be required to use the same electronic register provided and maintained by the Registrar General. Only local registration officers and officials from the General Register Office on behalf of the Registrar General will have access to the electronic register to maintain the integrity of the birth and death data.

It is intended that the provisions of the Bill will make it easier for individuals to register a death in one part of the country when living in a different part of the country. Moving to an electronic register will remove the requirement for an individual to sign the 'paper' register in the presence of the registrar. This will allow for telephone registration to be re-introduced, as was used successfully during the Covid-19 pandemic and welcomed by individuals, registrars and funeral services. This will provide a more flexible service for individuals registering a death, although it is also intended that the possibility to attend in person at the register office will remain giving individuals more choice in how they register.

Registrars will be able to register births and deaths in more locations as they would only need an electronic device to complete a registration. Local authorities will be able to develop new business models to provide a better service for the public. Moving to an electronic register supports the national data strategy by improving the use of data in Government by removing paper from the system.

Information on sign-ups to National Underground Asset Register

In response to a query from Lord-Clement Jones, I committed to providing information on the number of apparatus owners who have signed up to the National Underground Asset Register (NUAR).

As you Noble Lords will already be aware, NUAR is a new digital map of the underground apparatus (pipes and cables) across England, Wales, and Northern Ireland.

To date, we have actively engaged with 689 out of 728 organisations who we believe own buried apparatus. This equates to an estimated 95% of all these organisations in England, Wales, and Northern Ireland. Of these 689, 97 organisations confirmed that they do not own buried apparatus, meaning the current number of apparatus owners is 631. With regards to the number of asset owners who have signed up, as of 1 May 2024, 391 (62% of all apparatus owners) have formally signed up to work with us by signing a Data Exploration Agreement, which allows us to receive, explore and map their data. Of these:

- 272 (43% of all apparatus owners) have shared their data with NUAR, with 226 of these (36% of all apparatus owners) having an agreed mapping of their data to the NUAR data model (known as a Data Ingestion Specification),
- 241 (38% of all apparatus owners) have signed a Data Distribution Agreement which allows us to make their data available to users of NUAR; and
- 200 (32% of all apparatus owners) have completed all the required steps to be 'fully onboarded' (having shared their data, agreed a Data Ingestion Specification, and signed a Data Distribution Agreement), meaning their data is now available to users within the live NUAR service. This includes all of the major energy and water providers in England and Wales, such as Welsh Water, Cadent Gas and UK Power Networks, several major telecommunications companies, including CityFibre and Virgin Media O2, as well as smaller providers of these services, transport organisations and local authorities.

In addition to the figures provided above I'd like to re-iterate my offer of a demonstration of the NUAR platform to provide further illustration of the benefits of the service. This would enable you to see first-hand how it differs from existing data exchange services by giving workers immediate access to all the data then need, when then need it, in a standardised, interactive digital format, whilst also providing opportunities for the data to be used in additional use cases, such as civil contingency and heat network/electric vehicle chargepoint rollout. If such a demonstration is of interest, please contact my office and we will arrange a time that is convenient.

Deepfakes

I committed to write to the House to provide further information on the amendments on deepfakes.

Firstly, I wanted to provide further information regarding amendment 293. As set out during the debate, the government recognises that there is significant public concern about the creation of sexually explicit deepfake images, which is why it has announced its intention to table an amendment to the Criminal Justice Bill, which is currently in the other place. I understand that the amendment the government is bringing forward is likely to capture a broader range of explicit images than amendment 293, which focuses on intimate 'acts'.

While amendment 293 does not define what “intimate act” should mean, the explanatory statement and the heading to the amendment suggests it is focused only on deepfakes that depict sexual activity. Our amendment to the Criminal Justice Bill, however, will capture a wider range of sexual images, including those that purport to show certain forms of nudity. It will ensure that those who create these images without consent, and for the purposes of sexual gratification or to cause alarm, distress or humiliation, are criminalised.

This government amendment will build on the comprehensive legal framework to tackle intimate image abuse, established by the Online Safety Act 2023. It is already an offence to share, or threaten to share, a photograph or film that shows, or appears to show, another person in an intimate state without their consent. This includes any image which appears to be a photograph or film, so it is already an offence to share a ‘deepfake’ image of someone in an intimate state without their consent. As such I hope my Noble Lords will be reassured on this matter.

With regard to amendment 294, during the debate I highlighted that it is already an offence under section 7 of the Fraud Act 2006 (in England, Wales and Northern Ireland) to make, adapt or supply articles - which includes software and deepfakes - knowing that they are designed for fraud, or intending them to be used to commit fraud. That offence is punishable with up to 10 years imprisonment. I also set out that the Online Safety Act lists fraud as a priority offence, and also as a relevant offence for the duties on major services to remove paid-for fraudulent advertising.

I wanted to make a few additional clarifications. The offence in amendment 294 would lower the threshold to include suspicion – or reasonable grounds to suspect – that a deepfake “will or is likely to” be used for fraud. The threshold for the offence being set at suspicion or reasonable grounds to suspect that a deepfake is likely to be used for fraud would create a disproportionately low bar for this specific offence, compared with comparable offences under the Fraud Act which, like the section 7 offence, require actual knowledge or intent. I would also like to highlight that the Home Office has commissioned an independent review of the Fraud Act which will ensure it is fit to tackle the evolving nature of fraud, which we know has the potential to be impacted by AI.

Regarding amendment 295, I set out that there are already a number of criminal offences that can apply in the context of deepfakes, such as the new foreign interference offence under section 13 of the National Security Act 2023 and the false communications offence under section 179 of the Online Safety Act 2023, as well as existing election offences. These offences have appropriate tests to ensure we protect the integrity of democratic processes whilst also ensuring we do not impede the ability for robust political debate. I wanted to highlight that the offence in amendment 295 would set a significantly lower threshold for criminal conduct. It could potentially capture legitimate content and impact on people’s right to freedom of expression.

The foreign interference offence is a priority offence in the Online Safety Act, meaning regulated service providers, such as social media and search companies, will have to

take action against a wide range of state-sponsored disinformation and state-linked interference online targeted at the UK and our democratic processes. The false communications offence also falls within scope of the Online Safety Act's illegal content safety duties, which will require providers to swiftly take down such content when they are alerted to it.

I would also like to reassure you that, alongside the existing criminal offences and regulatory framework, we continue to work across government to ensure we are ready to respond to the risks to democracy from deepfakes. The Defending Democracy Taskforce is engaging regularly with key stakeholders, including Parliament and local authorities, on the range of threats facing our democratic institutions. The Security Minister has engaged with opposition parties to discuss the Taskforce's work, including election preparedness, and this dialogue will continue in advance of the next general election.

In addition, the Secretary of State and officials also continue to meet regularly with social media companies to ensure they continue to take action to protect users from election interference.

Given the time constraints during the debate, I wanted to explain my concerns around amendments 295 A, B, C, D, E and F in greater detail. These amendments would create duties for software developers and providers, providers of cloud computing platforms, and on providers of digital platforms. They would also establish Ofcom as the regulator for enforcing these duties and give the Secretary of State the power to produce guidance on how to meet these duties.

The government recognises the concerns raised around harmful deepfakes and has already taken action against illegal content online. Under the Online Safety Act, providers of user-to-user services and search services have duties to tackle illegal content and activity in a range of ways, including taking measures to proactively prevent users from encountering priority illegal content and swiftly remove any illegal content once the provider becomes aware of it. These duties apply to illegal deepfake content, some of which – as set out above – is priority illegal content under the Online Safety Act. Service providers also have additional duties to protect children from content that presents a material risk of significant harm – including harmful deepfake content, whether illegal or not. This should already have a significant impact on tackling these types of harm.

Whilst these amendments are well intentioned, they pose significant risks. These amendments rely on the creation of new deepfake offences, such as the ones which were proposed in amendments 293, 294 and 295. As set out previously, we have a number of concerns about the deepfake offences that have been proposed and have argued against their inclusion. Amendments 295A-F are intended to build on the proposed offences but do not stand alone. Moreover, these amendments would pose significant risks to the freedom of expression of users. The duties on developers and providers in amendment 295A, for example, extend beyond taking action in relation to

illegal deepfakes and also risk capturing legal and legitimate content which might be defined as a deepfake. Furthermore, the breadth of the duties imposed by these amendments (for example, they require providers to revoke access to software or services on the basis of mere suspicion) and the lack of detail about the practical steps required to comply with them creates a significant risk of a chilling effect on freedom of speech. They could incentivise providers and developers to take action against non-harmful, legal content.

Compliance with these amendments could also be technically challenging, creating uncertainty for businesses and the regulator. Currently, AI identification and detection technology is still at an early stage. No specific technology has yet been proven to be both technically and organisationally feasible at scale, and industry is working to develop solutions to this. Even those AI labs who have promising solutions struggle to detect or label content generated by software made by other organisations and many AI labelling solutions currently available are relatively easy to remove or otherwise technically circumvent. It would not be right to legislate in this area until the potential benefits and risks are better understood.

The government confirmed in the AI White Paper Consultation Response that we think legislative action will be required in every country once the understanding of risk from the most capable AI systems has matured and legislating too soon could easily result in measures that are ineffective against the risks, are disproportionate, or quickly become out of date. Future binding measures targeted at the developers of highly capable, general-purpose models will be part of a coherent approach to AI regulation, and we are working with a range of experts to develop our thinking further.

Data risks from systemic competitors and hostile actors

I thank the Noble Lord Clement-Jones for his important proposed amendment 295G which seeks to provide greater scrutiny of national security and data privacy risks relating particularly to genomic data from systemic competitors and hostile actors. As I could not address his amendment fully due to time constraints, I want to respond in some detail in this letter.

This is an important issue that this Government takes extremely seriously.

Organisations which hold sensitive biological data are subject to the UK General Data Protection Regulation (GDPR). In addition, organisations such as Genomics England, UK Biobank and NIHR BioResource actively consider national security in decision making about partnerships with companies overseas. These organisations consult with security personnel on a regular basis to ensure partnerships are aligned with our national security interests.

As set out in the Integrated Review 2023, the Government committed to considering new levers to ensure that hostile actors cannot access and exploit bulk data to harm UK interests or secure strategic advantages, balanced against the need for access to data to support our S&T objectives.

In the 2023 UK Biological Security Strategy we highlighted the risk of the convergence of emerging technologies, including the risks associated with biological data. We committed to undertake a full assessment on the risks posed by biological data and update our policy accordingly. The Office for Life Sciences, in conjunction with other Departments and Agencies across Government, is conducting this at pace.

I agree with the Noble Lord that this should be a priority for HMG, hence why we started this work in earnest last year. Consequently, the Government thinks this risk should be managed holistically through the UK Biological Security Strategy rather than the amendment the Noble Lord has suggested.

The Deputy PM will be providing an update to the House in the Summer on progress on implementing the UK Biological Security Strategy.

Updates to the Age-Appropriate Design Code

Baroness Kidron wrote to the Secretary of State and I, suggesting updates to the AADC to include guidance on the use of children's data in AI and research. I am responding below on these points.

We wish for the AADC to remain an integral part of the UK's data protection framework and we are proud of the fact that the AADC is a global blueprint for the protection of children's data. We want the code to continue to evolve to take account of new technologies used by relevant Information Society Services likely to be accessed by children.

Under Section 126(D) of the Data Protection Act 2018, the Commissioner is required to keep under review each code that is issued under section 125(4) including the Age-Appropriate Design Code whilst it is in force. The Information Commissioner's Office may keep the AADC up to date in response to emerging technologies — including Artificial Intelligence — and to reflect any legislative changes.

We would be happy to continue to engage with you about potential gaps in the existing Code; and support the ICO to consider whether those gaps could either be addressed through updates to the existing code or via separate, bespoke guidance.

Risk assessments for children's data

Baroness Kidron also wrote to me setting out some concerns about the provisions in the Bill on risk assessments. While I accept that the Bill removes some of the prescriptive requirements of the current UK GDPR in relation to Data Protection Impact Assessments (DPIAs) to reduce unnecessary burdens on organisations, risk assessments will still be required whenever a data controller intends to process personal data in a way that poses high risks to the rights of individuals.

As I explained in the debate, the ICO will be required to publish a list of examples of what it considers to be high risk processing to help data controllers understand when these obligations apply. Based on the ICO current guidance on DPIAs, this is highly

likely to include large scale or invasive uses of children's data. Any new processing activity would also have to comply with the data protection principles on lawfulness, fairness, and transparency and people will continue to be able to exercise their rights in respect of the processing. I would be happy to discuss this further with you when we meet.

Letter from Baroness Kidron to SoS

I will now separately respond to the other points raised by the noble lady Baroness Kidron during Committee stage, as well as in her letter to SoS:

a. AI-generated Child Sexual Abuse Material (CSAM)

I recognise this is an important area, and I want to first reassure you that the Home Office is continuing to assess whether new offences are needed to further bolster the legislation relating to AI enabled child sexual abuse, as part of our wider ongoing review of how laws need to adapt to AI risks and opportunity.

The government invests in capabilities across law enforcement to identify and disrupt child sexual abuse, including abuse that involves the use of AI. In particular, we created and fund the Online CSA Covert Intelligence Team (OCCIT), who produce invaluable reporting on emerging threats as well as carrying out operational activity. This is part of our wider commitment to fund the UCOL (Undercover Online Officers) network, who have delivered a year-on-year increase in arrests of the highest harm child sexual abuse offenders.

The Home Office chairs a working group on legislation with key stakeholders including law enforcement and the CPS to discuss the laws relating to child sexual abuse. This group meets quarterly and is considering the impact of AI on existing laws, including considering any legislative gaps. The HO is working closely with OCCIT specifically on the issue of models trained on or to produce child sexual abuse material. The Home Office is also in conversation with tech companies to drive forward the commitment of child safety in online spaces.

I am grateful for your continued advocacy in this area, and I look forward to continued engagement with you to determine how we can continue to uphold our commitment to child safety in online spaces.

b. Computer evidence admissibility

Computer evidence now proliferates in almost all prosecutions, with serious offences such as fraud and sexual offences involving significant volumes of material which has arisen from a digital device. The Lord Chancellor has committed to fully considering solutions to the issues raised in your letter, however this is a highly complex matter which requires careful thought and consideration to guard against unintended consequences. The government is carefully considering how to best address these

concerns, and the Lord Chancellor will continue to engage further with you on this matter.

c. Data processing by generative AI

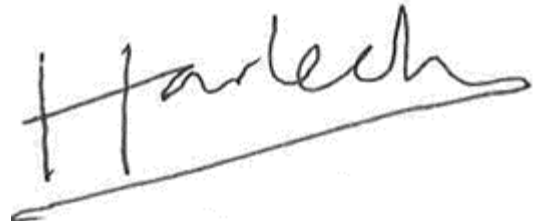
I understand that Baroness Kidron's amendments in this area were motivated by a concern around invisible types of processing such as web-scraping, when it may not be clear to people how their data is being used or how they can exercise their rights in respect of the data.

I would like to reiterate that the Bill does not remove fundamental data protection principles on lawfulness, fairness or transparency, or alter existing rights people have in respect of access to their data, objection to its processing, or requests for it to be rectified or deleted. These rights will continue to apply to processing activities undertaken by developers of innovative technologies. It is up to the developers of those technologies to make sure they can comply with existing requirements under data protection law. The current ICO consultation on its draft guidance on how aspects of data protection law apply to the development and use of generative AI models will also help make sure it is developed and deployed responsibly and with the trust of the people whose data it is built on.

Yours sincerely,



Viscount Camrose
**Parliamentary Under Secretary of State
at the Department for Science, Innovation
& Technology**



Lord Harlech
**Government Whip,
DCMS FCDO, MOD & WO**

