Updated to take account of the version of the Bill published March 2023

DATA PROTECTION AND DIGITAL INFORMATION BILL

Impact on data rights

Summary: The Data Protection and Digital Information Bill (the 'Bill') introduces significant changes to the data protection regime that threaten to undermine data rights.

In the new 'recognised legitimate interests' legal ground for processing and permissive rules on further processing, the Bill creates extensive new grey areas in which controllers will be free to interpret the GDPR loosely and in the way most convenient to their processing. The net result will be more hidden processing, fewer data subject rights, and the need for more complaints and challenges from data subjects.

At the same time, the new 'vexatious or excessive' test for the exercise of data subject rights places new barriers in front of data subjects. Our analysis suggests the new rules and time limits for complaints means data subjects face waiting 20 months or longer to resolve even basic breaches of their data rights.

Even where such challenges are successful, it is rarely possible to completely 'undo' processing that has already taken place. Processing under this new more flexible regime could have a lasting impact on data subjects, even where they successfully challenge it.

'Recognised Legitimate Interests'[1]

No consideration of data subjects' interests

1. s.5 of the Bill creates a new lawful basis for processing in a new Article 6(1)(ea) UK GDPR – recognised legitimate interests (REIs). This lawful basis shares little with the existing 'legitimate interests' lawful basis[2], as it creates an automatic

[1] Note that s.5 of the Bill gives examples of interests which may be legitimate interests – but *not* of 'recognised legitimate interests'. The addition of these non-exhaustive examples does not meaningfully alter the operation of the legitimate interests lawful basis.

[2] Although, like legitimate interests, it attracts the right to object to processing under Article 21 UK GDPR.

basis for processing that is 'necessary' for any one of a set list of interests (at Annex 1 of the Bill), which may be amended by the Secretary of State.

2. Of most concern is that there is no requirement for controllers to consider whether or how data subjects' interests against the processing might outweigh their own (which the wording of Article 6(1)(f) implicitly requires controllers to do when relying on legitimate interests under the current regime, and which is mandated by ICO guidance under the UK GDPR). Nor is there even a requirement for controllers to document why their processing is necessary for an RLI, making it difficult for data subjects to assess the lawfulness of the processing of their personal data.

3. The Government states in its consultation response that some controllers are *'concerned about the time and effort required to complete and record their legitimate interest assessments'.* The Bill addresses this need for an assessment by simply doing away with a vital safeguard for data subjects in a wide range of processing contexts.

4. This is especially concerning as the RLIs can be used by any non-public authority controller, and some of the RLIs proposed in the Bill are broad and vague, including:

   i. 'detecting, investigating or preventing crime'; and

   ii. 'democratic engagement'.

Interaction with vague processing purposes

5. It is foundational to the GDPR regime that each act of processing has a purpose; for example, assessing whether there is a lawful basis for processing under Article 6 requires a consideration of the purpose of the processing. Data rights are best protected where controllers identify with specificity for which purposes they process which data. In practice however, controllers often list *all* of their purposes (vaguely defined, and often relying at least in part on legitimate interests), and *all* of the data they process, with no indication of which data is

processed for which purposes (see e.g., Google's privacy policy and related legal challenges[3]).

6. The (over-)use of and / or overreliance on RLIs is likely to exacerbate the problem of using data for collateral purposes without an appropriate legal basis, as the existence of predetermined RLI incentivises data controllers to attempt to fit their processing (or at least part of it) into one of the RLIs. There is a real risk that controllers would stretch the definition of one or more RLIs to cover at least some of their processing, giving themselves flexibility over a wide range of processing and personal data, without an explicit requirement to consider how that processing affects data subjects. Even under the existing GDPR regime, we already see some controllers (e.g., private facial recognition companies[4]) using the 'prevention of crime' as a justification for extensive and intrusive processing at significant scale, primarily for private commercial purposes.

Consider a 'gig economy' fast food delivery company that processes a wide range of data on its workers, including minute-by-minute location data. Location data processing may be primarily for performance management (e.g., setting and monitoring against target delivery times). In extremis, location data might be used by the controller to detect crime (e.g., fraud by workers via false statements about how long they have had to wait for an order to be ready for delivery).

There is a temptation for the controller to state in their privacy policy that location (and other) data is processed for both these purposes and on the basis of the controllers' legitimate interests, without particularising *which* processing is for the detection of crime. It is easier to provide fewer details, and the prevention of crime sounds like a compelling justification for processing, making it harder to challenge the processing of location data.

Under the current regime, there is at least the (limited) protection that the controller must consider (and document) the balance of their interests and those of the platform workers. Under the new regime, the temptation for the controller to conflate their performance management and crime prevention purposes will be even greater:

[3] https://policies.google.com/privacy?hl=en-GB and https://www.iccl.ie/digital-data/gdpr-complaint-against-googles-internal-data-free-for-all/

[4] https://www.awo.agency/latest/big-brother-watch-complaint-against-private-sector-facial-recognition/

the prevention of crime is explicitly recognised as a legitimate interest in the Bill, and no balancing of interests is required.

7. The Bill could be improved by:

   i. Preventing reliance on the lawful basis where data subjects' rights and interests override those of the controller (as is the case for the legitimate interests lawful basis – Article 6(1)(f) UK GDPR); and/or

   ii. Requiring controllers to document and publish (e.g., in a privacy notice) an assessment of their reliance on an RLI – i.e. why their processing is necessary for the specific purpose, and clearly delineating which of their processing activities they consider fall within the RLI; and/or

   iii. Removing the Secretary of State's discretion to change the list of RLIs.

Barriers to exercising data rights (substance)

Vexatious or excessive data subject requests

8. s.7 of the Bill inserts a new Article 12A into the UK GDPR which allows controllers to refuse the exercise of data subject rights in Articles 15 to 22 and 34 where the exercise is '*vexatious or excessive'*. These rights include the right of access, right to erasure, and right to object to processing.

9. 'Vexatious or excessive' replaces the current test in the GDPR under which requests can only be refused or charged for where they are *'manifestly unfounded'* or excessive. The intention of the change appears to be to afford controllers more discretion in refusing or charging for requests. For example:

   i. New Article 12A(4) UK GDPR lists a wide range of vague factors to be taken into account in determining whether it is vexatious or excessive, including 'the nature of the request', and 'the relationship between the data subject and the controller'. It is not at all clear whether or how such factors militate in favour of

or against a request. For example, in the data broking sector[5], there is little or no relationship between the data subject and the controller, such that the processing is hidden or 'invisible'[6]. Would this tend to indicate that a request under the GDPR is vexatious? Conversely, would an employment or work context, in which the controller and data subject have a close and complex relationship, militate in favour of or against a determination that a GDPR request was vexatious? The Bill itself is unclear, and the examples given in the Government's consultation response[7] both appear to describe situations which would be covered by the current, 'manifestly unfounded' test.

ii. New Article 12A(5) UK GDPR gives as examples of vexatious requests those that are 'an abuse of process' – wording mirroring concepts in civil litigation that sits uncomfortably in the context of the exercise of fundamental rights.

10. The new test reflects language used in the Freedom of Information Act 2000 (FOIA). "Vexatious" in FOIA requests has been interpreted by courts to have a particular meaning, with the starting point of the reasoning being that considering a FOIA request needs an "objective standard" looking for a "reasonable foundation" of "value to the requester" (or the public)[8]. This suggests controllers may be able to ask data subjects for their reasons for exercising their data rights – something not permitted under the current regime. Such a process would cause delay and increase avenues for controllers to refuse requests or tie data subjects up in lengthy correspondence, frustrating their rights. It would be particularly concerning if controllers used the fact of data subjects' awareness that a rights request might cause the controller discomfort to characterise it as 'vexatious'. Indeed, it is often in such cases that the facilitation of data subject rights and the rebalancing of power away from the data controller is of greatest importance. A request that is inconvenient to a controller is no less valid.

---

[5] See e.g. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/

[6] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

[7] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation

[8] https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/dealing-with-vexatious-requests-section-14/what-does-vexatious-mean/

11. Many data controllers – particularly those whose business models rely on processing large amounts of personal data – are reluctant to give effect to the exercise of data subject rights[9]. The new 'vexatious or excessive' test threatens to hollow out the rights under Articles 15 to 22 UK GDPR. This is particularly concerning for:

    i. The right of access, which is foundational to all other data rights. If data subjects cannot find out how their data is being processed, they cannot ensure that the processing is lawful, exercise their wider rights or have any meaningful control over their information.

    ii. The right to object. This includes an absolute right to object to processing for direct marketing processes which should not be unduly diluted by greater freedom for data controllers to refuse it on vague grounds.

12. Whilst Article 12A(3) in theory places the burden of demonstrating a request is vexatious on the controller, in practice data controllers are in control of actioning a request, meaning that it will often be for data subjects to argue that their request is *not* vexatious. The Bill does not oblige controllers to give data subjects a reason for a refusal based on Article 12A(2); data subjects who do not even know why a request has been refused will find it very difficult to demonstrate – whether to the controller, the Information Commissioner, or a court, that their request is not vexatious or excessive.

13. Even where controllers opt to charge a fee rather than refuse a vexatious request outright, this could be a barrier to the exercise of data subject rights to the point of frustrating them entirely. The Bill does not mandate how controllers can levy such a fee, leaving space for delay (e.g., where controllers insist on payment by cheque or to a third country using intermediaries).

[9] See for example a report from Worker Info Exchange on challenges for gig economy workers exercising the right of access: https://www.workerinfoexchange.org/wie-report-managed-by-bots

Reduced accountability requirements

14. The Bill makes a number of changes to the mechanisms provided for controller accountability in the GDPR which will make compliance with data subject rights more difficult. Most notably:

    i. s.13 of the Bill removes the requirement for controllers based outside the UK to nominate a representative in the UK. This is likely to create additional barriers to the exercise of data subject rights, requiring international correspondence and – in combination with Article 12A – the payment of fees internationally.

    ii. s.15 of the Bill restricts the requirement to keep any records of processing to controllers carrying out 'high risk' processing. Even in this case, controllers need only record the *categories* of recipients of personal data rather than the actual recipients[10]. It is not always possible to know in advance which processing is high risk. The Bill creates the situation that high risk processing becomes evident, only for there to be no records of how data subjects' personal data has been processed, creating a significant barrier to data subjects being able to exercise their rights or seek redress for unlawful processing.

15. We expect the impact of these changes to be:

    i. A significant increase in the number of refused requests under Articles 15 to 22, directly undermining data rights.

    ii. An increase in the number of 'satellite' complaints about the right of access, preliminary to substantive complaints about processing, before the Information Commission and the courts (with attendant costs).

    iii. An increase in data subjects relying on pre-action disclosure under the Pre-action Protocol for Media and Communications Claims, where they are unable

[10] In the recent case *Österreichische Poste Case C-154/21* the ECJ held that when a data subject exercises his or her right of access, this includes information on the *specific* recipients of his or her personal data. The changes envisaged by the Bill would make compliance on this basis impossible for many data controllers. This is a notable change, despite ECJ cases no longer having precedential value in the UK.

to establish how their data is being processed using Article 15 UK GDPR, in turn increasing costs for businesses.

16. The Bill could be improved by:

    i. Retaining the existing test for the exercise of data subject rights – 'manifestly unfounded or excessive' – and removing the list of factors and examples at Article 12A(4) and (5); and/or

    ii. Obliging controllers to give reasons to data subjects where requests are refused, or a fee is charged in reliance on Article 12A; and/or

    iii. Extending the right to restrict processing under Article 18 UK GDPR to cover any period during which a dispute as to whether an exercise of the rights under Articles 16, 17 or 21 are 'vexatious or excessive'; and/or

    iv. Requiring that any controller requiring a fee to be paid in reliance on new Article 12A GDPR nominates a sterling-denominated UK bank account for that purpose and provides for simple mechanisms for payments, such as debit card payment links.

Barriers to exercising data rights (time limits)

17. s.7 of the Bill introduces a new Article 12B UK GDPR, which gives data controllers greater flexibility in delaying responding to the exercise of data subject rights, including being able to ask for clarification merely by reason of processing a 'large amount of information concerning the data subject' (Article 12B(5)-(6)). Given many data controllers' business models, it is not at all clear why this alone should render a request unclear or in need of clarification. Indeed, this proposal creates a perverse incentive to gather more data.

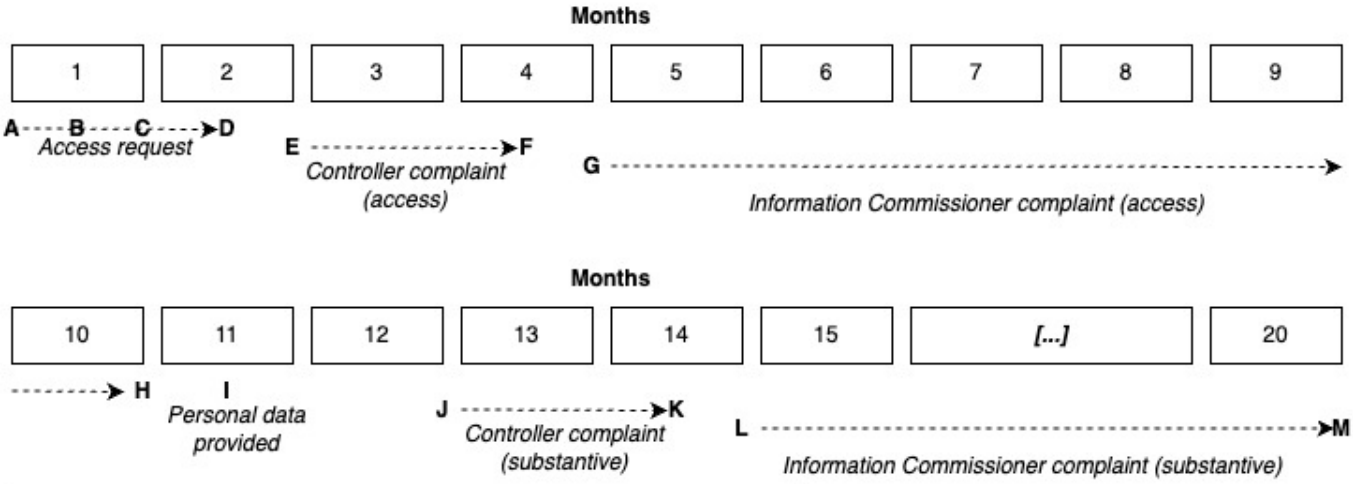
18. §.39 and 40 of the Bill insert new sections (164A and B, and 165A and B) into the Data Protection Act 2018 (DPA). The combined effect is that data subjects *must* first complain to the data controller before complaining to the Information Commission[11]. Whilst this reflects the Information Commissioner's Office

[11] Article 165A(3) has the effect of creating a waiting period of 45 days from complaining to a controller to being able to complain to the Information Commission.

approach under the current regime, the practical effect in combination with the likely increase in satellite complaints about the right of access, the impact could be that many complaints take *20 months* or longer to resolve. For the 10 months until the ICO determines that the user's access request is not vexatious or excessive, the user has no right to restrict or pause the processing complained of, heavily favouring the controller. The diagram below sets out how the Bill leads to this timeline.

19. The Bill could be improved by removing Article12B(6) (which gives processing a large amount of data as a specific reason for delaying a request) and by making the changes set out in para 16.

Updated to take account of the version of the Bill published March 2023



Day 1 A - Request Submitted
Day 15 B - Controller requests further information, pausing timeline for response (Article 12B(5)-(6))
Day 30 C - Data subject provides further information requested
Day 45 D - Deadline for controller's response (30 days, not counting time taken for data subject to provide further information - Articles 12 and 12B); controller refuses request. Note: this assumes that the controller does not extend the time period under Article 12(3) (which could be a further two months)

Day 60 E - Complaint to controller (required under s.164A DPA)
Day 105 F - Earliest date for complaint to Information Commissioner (165A(3)(c))
Day 120 G - Complaint to Information Commissioner about refusal of the right of access
Day 300 H - ICO resolves access complaint; orders controller to provide access to data (the ICO aims to resolve 90% of complaints within 6 months https://ico.org.uk/about-the-ico/our-information/our-service-standards/)
Day 315 I - Controller provides personal data originally requested

Day 360 J - After reviewing data provided, data subject makes substantive complaint to controller about its processing
Day 405 K - Earliest date for substantive complaint to Information Commissioner (assuming the controller does not deal with the complaint satisfactorily) (165A(3)(c))
Day 420 L - Substantive complaint to ICO
Day 600 M - Substantive complaint resolved by ICO (per service standards)

Lower standards for international transfers of personal data

20. s.21 and Schedule 5 of the Bill introduce a new UK-specific regime under which personal data may be transferred to third countries[12]. The main changes are:

    i. The Secretary of State is empowered under new Article 45A to issue regulations ('approval regulations' herein) that permit the transfer of personal data from the UK to third-countries[13]. These approval regulations function in a similar way to adequacy decisions under the EU GDPR. They can be issued where the 'data protection test' under new Article 45B is met. This data protection test is analogous to the requirement in Article 45(1) EU GDPR that a country awarded an adequacy decision 'ensures an adequate level of protection' – which has been interpreted as meaning that the standard of data protection must be 'essentially equivalent[14]. The data protection test in Article 45B UK GDPR, however, is that the standard of data protection in the relevant third country is 'not materially lower' than that in the UK. It is not clear from the wording alone what is intended by this change from "essentially equivalent" to "not materially lower". Whilst the Government's consultation response states that the new regime will 'retain the same broad standard that a country needs to meet in order to be found adequate', it is difficult to see why the wording of the test would be changed, unless with the intention is to allow transfers to countries with lower standards of protection than currently qualify for adequacy under the EU GDPR.

    ii. The data protection test in Article 45B differs from the adequacy test under the current GDPR regime in a number of respects, with the effect of giving the Secretary of State greater latitude in making approval regulations:

        a. It does not require consideration of whether there is an independent and effective supervisory authority in the third country;

[12] We explore the new international transfers regime and its potential impact on the UK's data adequacy decision from the European Commission in a separate briefing paper in this set.
[13] A new Article 4(27) of the UK GDPR defines third county as a country or territory outside the United Kingdom.
[14] Case C-362/14, *Schrems II*

b. It replaces the need for 'administrative and judicial redress' with 'judicial or non-judicial redress' (a key issue in the Privacy Shield dispute).

c. it permits consideration of the 'constitution and traditions' of the third country, though it is not clear from the Bill – or the Government's consultation response – how such factors affect consideration of the data protection test.

iii. The Secretary of State may consider 'the desirability of facilitating transfers of personal data to and from the United Kingdom' (Article 45A(3)) in making regulations under Article 45A, which again appears designed to increase the range of countries in respect of which approval regulations may be made.

iv. The 'data protection test' is used to assess the lawfulness of any standard data protection clauses promulgated by the Secretary of State under new Article 47A (effectively UK-issued standard contractual clauses).

21. The overall impact is that it is likely that controllers in the UK will have greater freedom to transfer personal data to a wider range of third countries than under the current regime (and by extension than controllers subject to the EU GDPR)[15]. Depending on how the UK's adequacy and standard clauses regime develops, this could significantly dilute the protection of UK data subjects' personal data.

22. Whilst the seemingly lower standard in the new data protection test is concerning, it reflects a high-priority policy objective for the Government.

23. The potential impact of these changes on the UK's own adequacy decision from the EU is discussed in section **Error! Reference source not found.**.

Further processing for new purposes

24. s.6 clarifies when processing for purposes other than those for which personal data was collected ('new purposes') complies with the principle of purpose limitation. A new Article 8A creates notable new purposes that will be considered

[15] Indeed this is consistent with stated UK government policy - https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare - and with the way these changes are described in the Government's consultation response.

'compatible' with the purpose for which data was collected (i.e. not in breach of the principle of purpose limitation[16]):

i. Ensuring or *demonstrating* that processing complies with Article 5(1) (Article 8A(3)(c)). It is not clear why controllers should be given greater freedom to carry out further processing in an attempt to 'demonstrate' (perhaps spuriously or in vain) the lawfulness of their original processing.

ii. A specified list of purposes (Annex 2 of the Bill) including disclosures to *'any other person'* who makes a request which *'states that the other person needs the personal data for the purposes of carrying out processing'* for processing in the public interest (Article 8A3(d)). This appears to open up disclosures of a wide range of personal data to an unknown number and range of other controllers. The requirement that a request merely 'state' the relevant circumstances – rather than a requirement that those matters be true or demonstrable – also offers very weak protection for data subjects.

25. Article 8A(3)(e) also states that a new purpose will be compatible where it is 'necessary to safeguard an objective listed in Article 23' (public security, emergencies etc.). This contrasts with the current wording of Article 6(4) which makes new purposes compatible where they are:

> *"based on a Union or Member State law* ***which constitutes a necessary and proportionate measure in a democratic society*** *to safeguard the objectives referred to in Article 23(1)"* (emphases added)

26. The removal of the emphasised words appears to remove an important safeguard. Alongside the list of recognised compatible secondary purposes introduced by Article 8A(3)(d), the effect is to effectively do away with the principle of purpose limitation in a range of security, regulation, and crime prevention contexts.

[16] Where further processing is for a purpose deemed compatible with the original purpose, this does not *by itself* make the processing lawful: the further processing would still require a legal basis and must be fair and accurate (among other things). This is clarified by a new Article 5(3), inserted by s.6 of the Bill.

> Consider for example a data collected for a relatively 'everyday' purpose – such as in the context of the running of a small business (the 'first controller') – which is requested from the first controller by another person (the 'second controller', which need not be a public authority) for the purposes of investigating crime. Under the current regime, the first controller would need to consider the factors listed in Article 6(4) GDPR to assess whether further processing to make that disclosure was compatible with its original purpose. In many cases it will not be: there is no link between the original and secondary purposes, and there are potential negative consequences for the data subjects. This would make such further processing by the first controller unlawful, as it would breach the principle of purpose limitation.
>
> Under the new regime, it will be enough for the second controller *merely to state* that it requires the data for processing that is (i) in the public interest, (ii) within Article 6(3) UK GDPR and s.8 DPA, and (iii) necessary to safeguard an objective listed in Article 23 UK GDPR. The first controller's processing for the disclosure will be deemed compatible by Article 8A(3)(d) and Annex 2 para 1 GDPR, removing a significant protection for data subjects against this kind of unexpected and potentially very consequential disclosure of their personal data.

27. <u>The Bill could be improved by</u> – at a minimum – requiring that the matters listed in Annex 2 para 1(b) be *true* rather than merely *stated* in a request. Alternatively, the processing for disclosures described in Annex 2 para 1 could be limited to disclosures to public authorities.

28. The new Article 8A(2)(c) replicates unclear language about the relevance of data engaging Articles 9 or 10, which have caused confusion under the current regime. The section reads:

    "In making [a determination about whether a new purpose is compatible with an original purpose], a person must take into account, among

    other things— […]

(c) the nature of the personal data, including whether it is a special category of personal data (see Article 9) or personal data related to criminal convictions and offences (see Article 10).”

29. This clause attempts to address when data may be used for further purposes without breaching the principle of purpose limitation, replicating the language of the existing GDPR in Article 6(4). That existing language is however unclear. It would be reasonable to assume that the greater the sensitivity of the data, the less likely further processing would be considered compatible with the initial purpose. However, it would not be unreasonable to read this clause as suggesting that processing engaging Articles 9 or 10 *may* be compatible with an original purpose. This tension has led to differing readings by academics and others, particularly in the context of using data for research. It is therefore unclear how 8A(2)(c) is to operate, as the clause does not clarify how to determine whether the greater the sensitivity the less / more likely the processing is to be compatible, nor whether, if the new purpose is compatible, the original exemption under Article 9 or 10 can be relied upon for the new purpose. It would be preferrable for the clause to reflect the intended outcome. If it is designed to guard against using sensitive data for secondary purposes, the clause should use clearer language.

Expanded use of cookies

30. s.79 of the Bill amends the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). A new Regulation 6 PECR permits the deployment of cookies where this is *‘with a view to making improvements to the service’*, subject to a right to object to those cookies. This is a loose test, which would appear to cover a very wide range of use of cookies. It also appears to be subjective: if a controller or operator considers that the deployment will improve a service from their perspective (e.g. by increasing monetisation through increased surveillance and changes to choice architecture), then such a deployment would presumably be *‘with a view to making improvements to the*

service'[17]. It therefore places the burden of objecting to very extensive tracking-by-default online onto internet users, rather than placing the burden of collecting (free, informed, and unambiguous) consent onto controllers.

31. The use of cookies enables those placing cookies to share the data collected with third parties for the same purposes (Regulation 6(2A)(c); those third parties may be able to rely on the expanded freedoms for controllers provided for in the Bill (e.g. the broad definition of research, and/or RLIs).

32. This would have the effect of legitimising the means by which internet users can very quickly find their personal data has been transmitted through a vast network of third parties via the use of cookies (as is the case in the online gambling sector, for example[18]).

33. It may be true that current practices by which website operators purport to gather consent for the placement of cookies on users' browsers are unpopular with internet users. However, many operators are engaged in 'compliance theatre' rather than genuinely trying to comply with the law or protect users' interests. Indeed, the consent notices such operators use are being challenged for their attempts to work as compliance tools[19]. Those challenges are proving successful, because the intention behind the consent mechanisms is not to meet legal requirements but to frustrate users; the real problem with consent pop-ups is lack of compliance with the law rather than the law itself. The answer to operators creating deliberately frustrating and confusing means to gather invalid consent to cookies is not to legalise complex and pervasive architectures of surveillance online, but to fully enforce the laws designed to protect users data rights when they use the internet. The net effect of amending the law to facilitate the deployment of such cookies will be increased surveillance and reduced choices for consumers.

34. <u>The bill could be improved by:</u>

[17] It is notable however that some major advertising bodies do not believe that the changes would permit the use of advertising cookies without consent. See e.g. https://www.iabuk.com/news-article/what-do-data-protection-changes-mean-digital-advertising
[18] https://cdn.sanity.io/files/btrsclf0/production/2018e1d767bd4146d49cc9d854d24b9cd5c984a7.pdf
[19] https://www.awo.agency/latest/the-tcf-decision-and-the-future-of-digital-advertising/

i. Retaining – and strengthening – the requirement that website operators obtain freely given, informed, and unambiguous consent to the placement of cookies for the purpose of service improvements; and/or

ii. Reducing or more narrowly defining the list of purposes in new Regulation 6(2A) PECR (e.g. requiring 'improvements' to be considered exclusively from the user's perspective).

35. s.81 of the Bill creates a definition of 'direct marketing' – previously undefined. This is a positive change and likely has a broader impact given the term is used elsewhere (e.g. in Article 21 UK GDPR). A further positive change is the extension of GDPR-level penalties to breaches of PECR (s.86 and Schedule 10 of the Bill).

36. Note that the Bill envisages regulations making provision for the recognition of technology for users to communicate automatic opt-out signals for cookies, which would, when developed (per the Government's consultation response), underpin an opt-out model for *all* cookies.