RE: FINANCIAL SURVEILLANCE PROVISIONS
UNDER THE DATA PROTECTION AND DIGITAL INFORMATION BILL

LEGAL OPINION

A. INTRODUCTION AND SUMMARY OF ADVICE

1. We are asked to advise Big Brother Watch on provisions in the Data Protection and Digital Information Bill ('**DPDIB**') which would create new powers for the Secretary of State for Work and Pensions ('**SSWP**') to obtain information about the bank accounts and financial transactions of people in receipt of benefits. These powers would function by compelling financial institutions to monitor customers' accounts for the purposes of identifying fraud or mistakes in the payment of benefits.[1] This would involve the surveillance/monitoring of very large numbers of people without any requirement that they be suspected of wrongdoing. We have been asked to consider whether these powers are compatible with the right to a private and family life under Article 8 of the European Convention on Human Rights ('**the Convention**'), and the right not be subject to discrimination in the enjoyment of Convention rights under Article 14.

2. In summary, in our view:
   a) The exercise of the financial surveillance/monitoring powers contained in the DPDIB, as currently envisaged, is likely to breach the Article 8 rights of the holders of bank accounts subject to such monitoring. That is because interferences arising from the exercise of these powers are unlikely to be 'in accordance with the law' due to

[1] The Bill was introduced in the House of Commons in March 2023, and subsequently in the House of Lords as HL Bill 30) on 6 December 2023. The Bill is currently at the Report Stage in the Lords. The provisions with which we are concerned were introduced at the Report Stage in the Commons in late November 2023.

their conferring very broad discretions which are not properly circumscribed and do not contain key safeguards which must accompany surveillance of this kind.

b) There are real doubts about whether the exercise of the powers would be proportionate if they were used for detecting mistakes in claims made by people in receipt of benefits or the Department of Work and Pensions' ('**DWP**') own errors in the payment of benefits.

c) The exercise of the powers is likely to have a disproportionate impact on particular groups, including disabled people, people of colour, women and older people. It is not clear whether that disproportionate impact is justified.

B. PROVISIONS IN THE BILL AND THEIR EFFECT

3. The relevant provisions are set out in Sch 11 to the DPDIB (as brought from the Commons in December 2023), which contains proposed amendments to the Social Security Administration Act 1992 ('**the 1992 Act**') and its Northern Ireland equivalent, as well as more minor amendments to the Proceeds of Crime Act 2002. The key provisions concern the power of the SSWP to give so-called "Account Information Notices" ('**AINs**') to a "*person of a prescribed description*" (who are essentially '**financial institutions**')[2] requiring them to provide specified information about bank accounts that they administer or to which they have access.

4. The proposed amendments to existing legislation appear in Sch 11 to the DPDIB under the heading of "*Power to require information for social security purposes*." Para 6 of that schedule sets out what would be a new Sch 3B to the 1992 Act entitled "*Power of the Secretary of State to require account information*." The paragraph references below are to that proposed schedule to the 1992 Act.

[2] Such persons will be prescribed in secondary delegation; they will undoubtedly include banks and building societies. We have adopted the generic label 'financial institutions.'

5. Paragraph 2 describes AINs in the following terms:

> *(1) An account information notice is a notice requiring a person to give the Secretary of State—*
> (a) *the names of the holders of accounts that the person identifies as being matching accounts in relation to a specified relevant benefit,*
> (b) *other specified information relating to the holders of those accounts, and*
> (c) *such further information in connection with those accounts as may be specified.*
>
> *(2) An account information notice—*
> (a) *may require information relating to a person who holds a matching account even if the person does not claim a relevant benefit;*
> (b) *may not require information relating to any person who*
> (c) *does not hold a matching account.*

6. The Explanatory Notes state (at no 1140) that the information that persons who are the subject of AINs (i.e. financial institutions) may be required to provide under para 2(1) "*can include the names of the account holder, other information relating to that account holder such as whether capital breaches the permitted limits, and other specified information such as additional accounts related to the account holder*." An AIN can require information dating back a maximum of 12 months: para 2(8).

7. The key notion of a "*matching account in relation to a specified relevant benefit is*" is defined in para 2(3) as an account:

> (a) *linked to the receipt of that benefit, and*
> (b) *in relation to which specified criteria relevant to that benefit, or specified criteria including such criteria, are met (for example, criteria about account balances or transactions outside the United Kingdom).*

8. The Explanatory Notes state that "*[t]hese are accounts which fit the risk criteria that will be outlined in the AIN sent to persons of prescribed description. For example, the criteria could specify rules relating to*

social security, such as capital holdings, or the legal limit for abroad stays." Paragraph 2(5) explains that:

> *[a]n account is to be regarded as linked to the receipt of a particular relevant benefit if it is—*
> (a) *an account into which the benefit is (or is to be) paid,*
> (b) *an account into which the benefit has been paid, or*
> (c) *an account linked to an account within paragraph (a) or (b).*

9. An AIN can require a financial institution to provide information to the SSWP at specified intervals for up to a year (which could be renewed): para 3(2).

10. To confer protection on financial institutions, Sch 3A would effectively disapply any protection to account information (and related liability) which would otherwise apply at common law (e.g. for misuse of private information) or in equity (e.g. breach of confidence) in respect of the provision of information in response to AINs: para 4(1).

11. The "relevant benefits" are broadly defined (with reference to the Social Security Administration Act 1992, s121DA). They include Universal Credit, Employment and Support Allowance, Personal Independence Payments, Disability Living Allowance, Child Tax Credit, Working Tax Credit and the State Pension: para 16. These include both means tested and non-means tested benefits.

12. Financial institutions will be required to comply with AINs, on pain of being issued with a penalty notice and fined, but they would have a right to appeal against the issuance of an AIN and/or penalty notice to the First-tier Tribunal: para 6(9), (13)-(14).

13. Information received by the SSWP from financial institutions in response to AINs can be used for any departmental functions: para 5(1).

14. The DWP has a power to issue a Code of Practice concerning AINs but is not required to do so: para 6(1).[3] This is significant given that the powers set out in the proposed primary legislation are broad and contain little detail. At the time of writing, there is no draft code of practice or any indication of what a code is likely to contain.

THE GOVERNMENT'S RATIONALE FOR THE PROPOSED POWERS

15. Because the proposed powers were added to the DPDIB late in its passage through the Commons, and has been subject to very limited debate, the government has provided little explanation of their rationale and the intended scope of AINs. In moving the amendment to include the AIN power in the DPDIB, the Minister said the following:[4]

> *In 2022-23, the Department for Work and Pensions overpaid £8.3 billion in fraud and error. A major area of loss is the under-declaration of financial assets, which we cannot currently tackle through existing powers. Given the need to address the scale of fraud and error in the welfare system, we need to modernise and strengthen the legal framework … The amendment will enable the DWP to access data held by third parties at scale where the information signals potential fraud or error. That will allow the DWP to detect fraud and error more proactively and protect taxpayers' money from falling into the hands of fraudsters.*
>
> *It will ensure that where benefit claimants may also have considerable financial assets, that is flagged with the DWP for further examination, but it does not allow people to go through the contents of people's bank accounts. It is an alarm system where financial institutions that hold accounts of benefit claimants can match those against financial assets, so where it appears fraud might be taking place, they can refer that to the Department.*

16. The further explanation of the government's rationale for introducing the powers is provided by a press release issued on 23 November:[5]

[3] This contrasts with the position in respect of other investigative and intrusive powers under, for example, the Investigatory Powers Act 2016 (see s243 and Sch 7) and the Terrorism Act 2000 (e.g. s47AA, Sch 14, para 6) which place the Secretary of State under a duty to issue one or more codes.
[4] Hansard, 29 November 2023, vol 741, col 879.
[5] https://www.gov.uk/government/news/changes-to-data-protection-laws-to-unlock-post-brexit-opportunity

> *The changes include new powers to require data from third parties, particularly banks and financial organisations, to help the UK government reduce benefit fraud and save the taxpayer up to £600 million over the next five years. Currently, Department for Work and Pensions (DWP) can only undertake fraud checks on a claimant on an individual basis, where there is already a suspicion of fraud.*
>
> *The new proposals would allow regular checks to be carried out on the bank accounts held by benefit claimants to spot increases in their savings which push them over the benefit eligibility threshold, or when people send more time overseas than the benefit rules allow for. This will help identify fraud take action more quickly.*

17. It is to be noted that the 1992 Act already contains powers for the Secretary of State to compel banks (and others) to provide information, inter alia, for the following purposes: (a) ascertaining whether a benefit is or was payable in accordance with social security legislation, (b) ascertaining whether provisions of social security legislation are being, have been or are likely to be contravened, and (c) preventing, detecting and securing evidence of the commission of benefit offences (s109B(1), read with s109A(2)). Those powers can be exercised with reference to a person who is identified either by name or description (s109B(2B)) provided that there are "*reasonable grounds"* for believing that they (or a family member) are "*a person who has committed, is committing or intends to commit a benefit offence*" (s109B(2C)). Under the same rubric, the Secretary of State has the power to require banks to enter into arrangements to allow his officials access to electronic records for the same reasons and subject to the same reasonable suspicion requirement (s109BA(1)). It is clear that the purpose of the *new* proposed powers is to carry out monitoring of bank accounts where there are no "*reasonable grounds"* for believing a particular individual has engaged in benefit fraud or has made any mistake in claiming benefits.[6]

LIKELY OPERATION/IMPLICATIONS OF ACCOUNT INFORMATION NOTICES

[6] Ibid.

18. The government has said very little about what AINs would contain and what, in practice, financial institutions would need to do to comply with them. In particular, the "*risk criteria*" (referred to in the Explanatory Notes), which will be included in AINs is entirely opaque. It seems likely, however, that AINs would contain criteria or indicators of transactions or account activity which may be indicative of whether or not an account holder (or someone whose benefits are paid into the account) satisfies eligibility criteria for one or more benefits. It is reasonable to assume that AINs would, for example, seek to compel financial institutions to identify whether accounts linked to the receipt of a benefits hold capital above thresholds which would reduce or extinguish entitlement to the benefit and/or have been involved in transactions which would indicate that the account holder is or has been outside the UK (which, again, would reduce or extinguish entitlement to the benefit). There may also be other factors that are regarded as indicators about a person's health or income or lifestyle that are considered relevant to their benefit entitlement.

19. Plainly, financial institutions would not be able manually to assess this information, or, if they could, it would be extremely resource intensive. It is almost inevitable, therefore, that financial institutions would need put in place some form of algorithmic surveillance or monitoring of accounts.[7] That monitoring seems likely to involve the scanning/automated examination and analysis of large numbers of accounts in order to identify accounts matching parameters laid down in an AIN. It is reasonable to assume that (a) AINs would be issued on a rolling basis to most financial institutions which provide banking

[7] The proposed powers suggest that the DWP could exercise some control over how this is done because AINs can require that information is "*compiled in a specified manner*" (para 3(5) of Sch 3B to the 1992 Act). It is unclear whether the DWP interprets this power as permitting them to mandate the use of particular technology or whether they would in fact do so.

services, and (b) in order to comply, financial institutions would need to subject most if not all of their accountholders to algorithmic surveillance.

20. Beyond the reference in para 2(2) of proposed Sch 3B of the 1992 Act to AINs requiring the disclosure of names of matching account holders, we know very little about what information financial institutions would be required to turn over to the DWP. Subparagraphs (b) and (c) of that provision refer only "*other specified information relating to the holders of those accounts*" and "*further information in connection with those accounts*." We assume that such information would include, at least, the details of relevant figures or transactions suggesting why a person / account satisfied criteria laid down in an AIN.

21. It is not clear whether financial institutions would carry out any human check or analysis prior to disclosing information under an AIN. This may depend on the number of accounts flagged by an automated system as corresponding to specified criteria. It may also depend on whether/how the DWP exercises the proposed power to require that information "*be compiled or collated in a specified manner*" or that it be "*provided [to DWP] in a specified way*" (para 3(5) of Sch 3B to the 1992 Act).

22. The DWP intends to use information provided pursuant to AINs as the basis for conducting further investigations as to whether persons in receipt of benefits have incorrectly/improperly claimed benefits. What is not clear is whether these people risk having their benefits suspended on the basis of this information alone while investigations are undertaken. That would raise obvious concerns about risks that criteria could be applied incorrectly and/or that persons / their account may be incorrectly flagged.

C. ASSESSMENT

23. The power to issue AINs to financial institutions is essentially a power to mandate private companies to conduct surveillance or monitoring on

behalf of the state and then to hand over the fruits of that surveillance. This monitoring is likely to take place on an ongoing and systematic basis, it will inevitably lead to the examination of obviously private and sometimes highly sensitive information about a very large number of people and will be used not just in relation to detection of fraud but also error.

24. This power shares many features of the bulk or mass surveillance powers which exist in relation to communications and communications data, or other information held on electronic devices, as well as bulk personal datasets. In particular, it involves:

a) Searching a large volume of information concerning/relating to a significant number of people which is clearly private in nature. In this regard, and as we explain further below, there is an obvious analogy with surveillance of communication data. Communication data indicates when, where, how and with who a person communicates (but not the contents of communications). As with communication data, a search through large quantities of an individual's financial transactions enables a very detailed picture to be built about a person, including potentially details about their personal and family life, their sexual orientation, their political views, their medical histories etc.

b) Searching a large volume of information concerning/relating to a significant number of people using search criteria or search terms by way of automated or algorithmic analysis. This is, in essence, what is done under the various bulk surveillance powers contained in the Investigatory Powers Act 2016 ('**IPA 2016**'), such as the bulk interception of communications,[8] the exploitation of retained

[8] See the process described in *Big Brother Watch (BBW) & ors v UK* [GC], App Nos. 58170/13, 62322/14 and 24960/15, 25 May 2021 ('***BBW***'), §325-329.

communications data, and the obtaining and exploitation of bulk personal datasets.

c) The subsequent analysis (by human or by machine) of results or information thrown up by those searches and the further use of the information (including sharing it with third parties, here: the DWP). This too is an integrated part of the use of bulk investigatory powers.

d) As with the use of many bulk powers (including e.g. the bulk interception and the bulk exploitation of personal datasets), the overwhelming majority of persons whose private and personal information is searched/analysed will not be suspected of any wrongdoing or improper conduct.

e) The power would be exercised covertly/in secret. The fact of an AIN being issued to a particular financial institution would almost certainly be secret to avoid tipping off account holders. The same is true of the parameters of any AIN. Account holders would most likely not know (either before or after the event) that their accounts (i) had been the subject of algorithmic surveillance by their financial institutions and (ii) where relevant, found to correspond to "*risk criteria*" laid down in secret by the DWP. The holders of accounts found to correspond to particular criteria and whose information would be passed to the DWP would also be unaware of this. Again, these are features of bulk investigatory powers.

25. In the UK, bulk investigatory powers are conferred primarily upon the intelligence and security services for the purposes of protecting national security and combating serious criminal activity. Those powers are subject to detailed regulation under the IPA 2016 and statutory codes of practice, as well as external oversight by a range of bodies. By comparison the proposed financial surveillance power is striking: it

would involve outsourcing bulk monitoring to the private sector, and it would not be anchored in or constrained by anything like the same legal and regulatory framework. We return to the legal significance of that below.

INTERFERENCE WITH THE RIGHT TO A PRIVATE AND FAMILY LIFE

26. The primary right with which we are concerned is the right to a private and family life under Article 8 of the Convention. It is conceivable that in some cases, the exercise of the powers in question could also interfere with the right to freedom of association and assembly under Article 11 of the Convention and, possibly, the right to freedom of expression under Article 10 of the Convention. We have, however, confined our analysis to Article 8 because this is the right that is most clearly relevant and the assessment of whether the proposed powers are likely to be compatible would be substantially the same under these other qualified rights.

27. The exercise of the proposed powers may interfere with the right to a private and family life in three related but discrete ways:

a) The algorithmic analysis/examination/monitoring of individuals' bank accounts to assess whether they include transactions or information corresponding to the criteria set out in an AIN. This is the interference that would affect the largest number, likely millions, of people.

b) Any further examination by financial institutions of accounts identified on the basis of the first stage of monitoring to assess whether the accounts properly satisfy the criteria set out in an AIN.

c) The sharing/disclosure by financial institutions with the DWP of information about account holders and their transactions/accounts identified through the above steps.

Examination of accounts

28. In our view, there is little doubt that the examination/application of search criteria to bank accounts (and transactions therein) constitutes an interference with account holders' right to a private and family life (and possibly that of third parties).

29. Financial/banking data will in and of itself constitute private information within the meaning of Article 8.[9] That is particularly clear where, as set out above, data about financial transactions reveals other things about a person's private and family life. In some cases, information contained in a person's bank account will be highly sensitive. It may reveal, inter alia, (a) information about their movements (on the basis of geographical location where they made payments[10]), particularly if they make a regular card/electronic payments; (b) on the basis of the identity of retailers from which they have purchased goods or services, information concerning their (i) opinions and beliefs (e.g. payments for political party, union or other organisational memberships or donations), (ii) sexual preferences or interests, (iii) the fact of their receiving medical treatment and possibly the nature of that treatment (e.g. payments to an IVF clinic); (c) information revealing potential addictions (e.g. gambling), and (d) information revealing financial difficulties. If information about financial transactions were to be collated with or juxtaposed with information from other sources, this could reveal far more.

30. In this respect, we consider that there is an obvious analogy to be drawn between data concerning financial transactions and communications data or metadata associated with communications. In broad terms, that is data relating to the location and time of a communication (e.g. an

[9] See by analogy: *MN & ors v San Marino*, App No 28005/12, 7 July 2015, §51, 55; *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [GC]*,* App No 931/13, 27 June 2017, §138; *LB v Hungary* [GC], App. No. 36345/16, 9 March 2023, §103-104.
[10] Although payments are, of course, often made online or remotely without a person being physically present.

email or message) and the device/account with which the communication was made. The Court of Justice of the European Union ('**CJEU**'), has described such data as being: "*liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*."[11]

31. It is well established that the state's accessing/examining information falling within the scope of Article 8 constitutes an interference with that right. That is the case regardless of whether or not (a) the accessing / examining of information takes place by automated means without a human viewing the information, (b) it leads to any further examination of a person's account and/or other use of information contained therein, and (c) the person in question is caused any inconvenience or distress.[12] If an individual's account is further examined by the financial institution that would constitute a further interference.

Sharing/disclosure of information pursuant to Account Information Notices

32. If an individual's account or information relating to them and their account is transmitted to the DWP, that would constitute a discrete, further, and more serious, interferences.[13] This would require its own justification, see further below.

Interferences with privacy rights by financial institutions

[11] C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen*, EU:C:2016:970, §99. See also the remarks of the Grand Chamber of the ECtHR in *BBW* §342, 363.
[12] *BBW* §325– 331; Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net & ors v Premier ministre* & *anor*, EU:C:2020:791 ('***La Quadrature***'), §115-116; C-140/20, *GD v Commissioner of An Garda Siochana and others*, EU:C:2021:942, §44.
[13] See by analogy: *BBW*, §330-331; *Centrum för Rättvisa v Sweden* [GC], App No. 35252/08, 25 May 2021, §244-245. See further by analogy: *MS v Sweden,* App No. 20837/92, 27 August 1997, §35; *Christian Institute v Lord Advocate* [2016] UKSC 51, §78.

33. The surveillance/monitoring of bank accounts, and any subsequent sharing of information with the DWP, pursuant to AINs would be undertaken by private bodies, rather than directly by the state itself. That does not, in our assessment, prevent the application of human rights law to account holders' information. The courts have frequently applied human rights law to, for example, legislative measures compelling the collection, retention and disclosure of communications data retention by communications service providers,[14] as well as such companies' collection and retention of personal data in connection with SIM cards.[15] The surveillance/monitoring that the SSWP would require financial institutions to undertake would be carried out at the behest of the state and attributable to the state.[16]

JUSTIFICATION

Legal principles

34. In order to comply with the right to a private and family life, interferences must be "*in accordance with the law*," in pursuit of a legitimate aim, and "*necessary in a democratic society*" (Article 8(2) of the ECHR). Necessity encompasses a requirement that the interference corresponds to a pressing social need and is proportionate to the aim pursued.

35. An interference will not be "*in accordance with the law*" unless it has some basis in domestic law. The requirement, however, goes further and is concerned with the *quality* of the law. It requires that the law must be "*accessible*," and must secure that the exercise of the power is sufficiently foreseeable and must contain sufficient safeguards against

[14] See for example: *R (Davis & Watson) v SSHD* [2015] EWHC 2092 (Admin); *La Quadrature*; *Ekimdzhiev v Bulgaria*, App No.70078/12, 11 January 2022.
[15] See for example: *Breyer v Germany*, App No. 50001/12, 30 January 2020.
[16] See by analogy: *Ekimdzhiev*, §375.

the power's arbitrary and disproportionate exercise.[17] It is the last two of these requirements which is of particular importance in respect of the proposed powers. First, "*it must be possible for a person to foresee [a measure's] consequences for them and it should not 'confer a discretion so broad that its scope is in practice dependent on the will of those who apply it, rather than on the law itself*.'"[18] The "*law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which [a power will be exercised].*"[19] Second, the legal framework governing the exercise of a power must contain "*safeguards … to guard against overbroad discretion resulting in arbitrary, and thus disproportionate, interference with Convention rights*."[20] Where powers are obscure or ambiguous this will be relevant as to whether their exercise can properly be regarded as foreseeable and thus in accordance with the law.[21]

36. In the context of surveillance or other measures designed to obtain private information about individuals, the courts have laid down a set of minimum safeguards (which must be "*adequate and effective*") that are necessary to ensure that the interference with Article 8 rights arising from the use of such powers is "*in accordance with the law*".[22] Several of the minimum safeguards in Convention case law are of particular relevance: (1) there must be "*detailed rules on when the authorities may resort to such measures*" including "*sufficient clarity [on] the grounds*" on which measures can be ordered, that may include the nature of the conduct / categories of person in respect of which/whom

[17] *In re Gallagher* [2019] UKSC 3, §16–23.
[18] Ibid, §17.
[19] Ibid, §21 quoting *Malone v UK*, App No. 8691/79, 2 August 1984, §67.
[20] *Beghal v Director of Public Prosecutions* [2015] UKSC 49, § 31 and 32; *S v United Kingdom* [GC], App No. 30562/04, 4 December 2008, §95 and 99.
[21] *Catt v UK,* App No. 43514/15, 24 January 2019, §114.
[22] See the Grand Chamber's summary of the case law in *BBW* §335-337, 348-351, 361. See also the application of these safeguards to the acquisition, retention of and access to communications data in *Ekimdzhiev,* §291, 293, 395).

the measure may be used;[23] (2) independent *ex ante* authorisation of the measure, rather than its being implemented on the basis solely of the discretion of a member of the executive;[24] and (3) independent oversight/ review of the process of surveillance and the use made of information derived from it to ensure that it complies with relevant safeguards and remains necessary and proportionality.[25] We will return to these below.

37. These safeguards do not apply to every information gathering or retention measure and only apply to an interference with privacy of sufficient seriousness.[26] In our assessment the measures with which we are concerned would involve sufficiently serious interferences with account holders' Article 8 rights so as to trigger the requirements for the safeguards above. That is primarily because of the nature of information contained in bank accounts / transactions and the highly personal details about an individual's private life which it reveals (which we address above), but it also arises because of the secret nature of the exercise of the powers.

38. The power with which we are concerned is untargeted and does not require that there be any suspicion a person has engaged in benefits fraud or is even the beneficiary of a mistake before their account is subject to examination. Intrusive powers which do not require the person exercising them to form any grounds of suspicion or belief about a person's conduct prior to their exercise are not inherently incompatible with the Convention.[27] However, their exercise must be particularly carefully circumscribed and subject to even more rigorous safeguards than would be the case in respect of more targeted measures.[28]

[23] *BBW*, §335, 348.
[24] *BBW*, §350-351.
[25] *BBW*, §356, 361.
[26] See *Breyer v Germany*, §102-103.
[27] See for example: *BBW*; *Beghal v UK*, App No. 4755/16, 28 February 2019; *Roberts v Commissioner of the Metropolitan Police* [2015] UKSC 79.
[28] *BBW,* §349.

39. As noted above, in order to be lawful an interference with Article 8 rights must be "*necessary in a democratic society"* which means it must be proportionate. While the 'in accordance with the law' and 'necessity' requirements of Article 8(2) are discrete, when considering general legislative provisions concerning surveillance/information gathering measures, the ECtHR has tended to consider them in the round.[29] The link between these requirements is that the legal framework must be sufficient to ensure that such measures are applied only when it is necessary in a democratic society.[30] The Court has held that "*the level and supervision and review*" is an important element of the assessment of proportionality[31] and more specifically: "*when considering the necessity of interference, the Court must be satisfied that that there existed sufficient and adequate guarantees against arbitrariness … including the possibility of an effective control of the measure at issue*."[32] We consider that this is the approach to be taken to considering whether the proposed powers in this case would, in general terms, comply with the requirements of Article 8(2).

Application of legal principles to surveillance/monitoring pursuant to Account Information Notices

40. Having set out the legal requirements which we think apply, we turn now to consider whether the relevant powers in the DPDIB are compatible with these requirements.

41. In our view, there are four fundamental problems with the proposed financial surveillance powers which mean that they are unlikely to be compatible with the right to a private and family life under Article 8 of

[29] See for example: *Centrum för Rättvisa,* §248; *Breyer v Germany*, §85, 103, *Catt v UK*, §106
[30] *BBW*, §334. The approach taken by the EU court in applying EU law (under the influence of the ECtHR) is substantially the same, see *La Quadrature*, §132.
[31] *Breyer v Germany*, §103.
[32] *MN v San Marino*, §73

the Convention. That is principally on the basis that, as currently envisaged, the powers are not sufficiently circumscribed to be "*in accordance with the law*." They confer broad discretions which, in our opinion, are not sufficiently circumscribed or accompanied by sufficient safeguards so as to ensure that the inevitable interferences with privacy arising from their use are necessary in a democratic society and do not occur in an unforeseeable or arbitrary way.

42. First, there is a striking lack of clarity about the grounds on and circumstances in which the SSWP may exercise the powers in question. The starting point is that the purpose for which AINs may be made and, thus, surveillance undertaken in respect of bank accounts is "*assisting … in identifying cases which merit further consideration to establish whether relevant benefits are being paid or have been paid in accordance with the enactments and rules of law relating to those benefits*." That is vague and potentially extremely broad. It does not offer sufficient clarity on the types of conduct or categories of person who are likely to be targeted through the application of monitoring criteria.

43. It is notable that the government's intention is that this purpose captures not only deliberate wrongdoing by benefit recipients but also mistakes made by benefit claimants and, strikingly, mistakes made by the DWP in the payment of benefits. This is not something that features in the draft legal framework and it amounts to an additional, very different, purpose and ground for surveillance. This appears to be without precedent: we are not aware of any comparable power pursuant to which a person can have their private information monitored and harvested in order to assist the state in identifying its own mistakes.

44. Second, the scope of the surveillance/monitoring which financial institutions will be required to undertake will be dictated by the terms of AINs; in essence, these institutions have to work backwards from the

types of information they are required to disclose to the DWP. Other than specifying that the names of relevant account holders will have to be disclosed, proposed Sch 3B of the 1992 Act says nothing meaningful about what information will be provided. It specifies only that AINs may require financial institutions to provide "*other specified information relating to the holders of those accounts"* and/or "*further information in connection with those accounts as may be specified*." That confers an extremely broad discretion on the SSWP when setting the terms of AINs.

45. The consequence is that the potential scope of the surveillance/monitoring and the subsequent sharing of information with the DWP is wholly unclear (even in general terms) to persons who may be affected at both stages. This raises serious difficulties in terms of the foreseeability of the exercise of what is a very broad discretionary power. Without far more, we do not think there is sufficient clarity on the grounds on which surveillance can be undertaken, appropriately "*detailed rules on when the authorities may resort to such measures*" or sufficient clarity concerning what information about individuals would be transmitted to the DWP on the back of this surveillance for that intrusion to be lawful.

46. Third, the proposed surveillance power can be authorised by the SSWP (or a delegate) without any independent oversight or authorisation. The SSWP alone can mandate monitoring of bank accounts of millions of people and the compelled disclosure of information harvested from this process. As noted above, those processes will involve examination and in some cases disclosure of highly sensitive private information. The exercise of such a power without any external/independent involvement is inconsistent with the requirements of the case law concerning surveillance powers generally and bulk powers in particular. Not only is there no *ex ante* external involvement but there is no provision for independent review or oversight of the exercise of these powers after

they have been exercised. In the absence of these safeguards, it is difficult to see how the exercise of this power could ever be in accordance with the law for the purposes of Article 8.

47. Finally, it is striking that it appears the proposed power may be exercised for the purposes of identifying (a) whether people in receipt of benefits are mistakenly claiming benefits when they are not entitled to them, (b) whether people in receipt of benefits are improperly claiming benefits but in circumstances in which the sums are small; and (c) whether the DWP has mistakenly paid someone benefits to which they are not entitled. If the power is exercised, as we understand is intended, for the purposes set out at (a) and (c), and to a lesser extent (b), there are real doubts as to whether that would be proportionate.

48. That assessment is reinforced by a line of case law holding that surveillance and other information gathering measures are unlikely to be proportionate for the purposes of the rights to respect for private and family life[33] and data protection under the Charter of Fundamental rights (and primary EU legislation) unless their use is limited to preventing and detecting serious crime or safeguarding national security.[34] That is reflected in domestic legislation governing investigatory powers which cannot be exercised other than for the purposes of "*preventing or detecting serious crime*"[35] (or in "*the interests of national security*" or

[33] Which right has the same meaning and scope as the right to a private and family life under the European Convention on Human Rights: see Article 52(3) of the Charter.

[34] *La Quadrature*; C-207/16 *Proceedings Brought by Ministerio Fiscal*, EU:C:2018:788; C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs,* EU:C:2020:5/790.

[35] Under the IPA, s263 "*serious crime*" is defined narrowly as crime where:
(a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or
(b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose,

"*the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security*").[36] This case law and legislation reflect a recognition that surveillance and monitoring which affect the privacy rights of a large number of people requires weighty justification if it is to be regarded as being necessary in a democratic society. The financial surveillance powers in the DPDIB are not limited in this way and would permit monitoring for far less pressing reasons.

DISCRIMINATION CONTRARY TO ARTICLE 14 OF THE CONVENTION

49. Article 14 of the Convention confers a right not to be subject to discrimination in the enjoyment of Convention rights, including on the grounds of race, sex and 'other status' (which includes disability and age[37]). One of the proscribed forms of discrimination is indirect discrimination, which arises where "*a neutrally formulated measure affects a disproportionate number of members of a group of persons sharing a characteristic which is alleged to be the ground of discrimination*" and that measure (which must be assessed with reference to its impact[38]) does not have an objective and reasonable justification.[39]

50. For the reasons we have addressed above, the surveillance/monitoring pursuant to an AIN and the subsequent sharing of information harvested from that process would engage the subject's right to a private and family life – that is more than sufficient to bring the treatment/measure within the "*ambit*" or "*general subject area*" of Article 8 for the purposes of Article 14.[40]

---

[36] See e.g. s60A and s61, 138, 158, 204, 205 of the IA 2016.
[37] *R (SC) v Secretary of State for Work and Pensions* [2021] UKSC 26, §112, 114.
[38] *R (The Motherhood Plan) v HM Treasury* [2021] EWCA Civ 1703, §101.
[39] *SC*, §53.
[40] *R (SC) v Secretary of State for Work and Pensions* [2019] EWCA Civ 615, §44.

51. The initial process of algorithmic analysis of accounts pursuant to an AIN seems likely to affect account holders to a similar extent (unless particular categories of account are isolated for analysis) regardless of, for example, whether they have a disability, their age, sex or race. However, it seems inevitable that any subsequent processes of (a) further analysing accounts identified by an algorithm as corresponding to particular "*risk criteria*," and/or (b) sharing information about accounts and account holders will disproportionately adversely affect particular groups sharing protected characteristics. This includes disabled people, people of colour, women and older people as they will disproportionately receive benefits and thus disproportionately be subject to financial surveillance. Those impacts would be amplified if the DWP subjected such people to intrusive investigations on the basis of information provided by financial institutions pursuant to AINs, and amplified still further if the payment of benefits was suspended during pending investigations. .

52. Whether, having regard to this disproportionate impact on particular groups, the application of the financial surveillance powers would amount to unlawful discrimination would depend on the strength of justification for their use. The points made above with reference to disproportionality under Article 8 apply equally here. In our view, it is at least arguable that disparate impacts on groups with the abovementioned characteristics, many of whom are disadvantaged and/or vulnerable, would be difficult to justify for the purpose of identifying mistakes made by benefits recipients and, even more so, the DWP's own errors in the payment of benefits or mistakes.

53. Further, it is striking that there does not appear to be any equivalent suspicionless bulk financial surveillance power available to HMRC (or at least none that is publicly avowed) to engage in bulk financial surveillance looking for indicators of transactions that might raise

suspicions that that, for example, income tax, capital gains tax or inheritance tax have not been properly paid. That is despite the government estimating that in 2021-2022 the tax gap (i.e. the difference between the amount of tax that should, in theory, be paid to HMRC and what is actually paid) for income tax, national insurance and capital gains tax was £12.7bn,[41] and for inheritance tax[42] it was £300m.[43] Such a power, in contrast to that which it is proposed to confer by the DPDIB, would impact wealthier and more powerful members of society. That wider context is relevant to an assessment of whether the proposed financial power for the DWP, which will inevitably lead to significant interference with the privacy of some of the most vulnerable members of society, could be justified.

D. CONCLUSION

54. Our assessment is necessarily confined to the scope of the powers as currently envisaged and understood. We cannot at this stage address the human rights compliance of any given AIN or surveillance which may be carried out by financial institutions pursuant to it. As noted above, while the DWP has the power to issue of Code of Practice there is no requirement for it to do so, nor is there any indication as to what such a Code, if one were issued, would contain. On that basis we can only analyse the safeguards contained in the proposed legislation itself. For the reasons set out above, we do not consider that the proposed legislation currently contains close to the safeguards required to ensure the powers set out in the Bill can be exercised compatibly with Article 8. As we have noted, that is in marked contrast to legislation permitting

[41] https://www.gov.uk/government/statistics/measuring-tax-gaps/4-tax-gaps-income-tax-national-insurance-contributions-and-capital-gains-tax
[42] https://www.gov.uk/government/statistics/measuring-tax-gaps/6-tax-gaps-other-taxes
[43] According to the DWP's Impact Assessment on Third Party Data Gathering (September 2023), the estimated annual loss (in 2022-2023) to error and fraud in the benefits system was £8bn; but the DWP's November 2023 press release states that it expects that the powers in the DPDIB would only save £600m over 5 years.

similar bulk surveillance where the legislation itself contains clear safeguards to prevent the disproportionate and arbitrary exercise of surveillance powers.

DAN SQUIRES KC
AIDAN WILLS
Matrix

11 April 2024