INVESTIGATORY POWERS (AMENDMENT) BILL
EUROPEAN CONVENTION ON HUMAN RIGHTS MEMORANDUM

1. This memorandum addresses issues arising under the European Convention on Human Rights ("the Convention") in relation to the Investigatory Powers (Amendment) Bill ("the Bill"). The memorandum has been prepared by the Home Office.
2. Lord Sharpe of Epsom has made a statement under section 19(1)(a) of the Human Rights Act 1998 that, in Lord Sharpe's view, the provisions of the Bill are compatible with the Convention rights.

Summary of Bill

3. The Bill amends the Investigatory Powers Act 2016 ("IPA"). The IPA provides a framework governing access to communications and data by public authorities (including law enforcement and the intelligence services[1]) by setting out the extent to which certain investigatory powers may be used to interfere with privacy (s1(1) IPA). The IPA was developed to consolidate various investigatory powers used by public authorities and provide oversight, transparency and safeguards.
4. The amendments to the IPA made by the Bill are a necessary update to the IPA, required in part due to technological advancements since that Act's passing. The amendments to the IPA are broadly in line with recommendations considered in detail by Lord Anderson in his independent report of June 2023 (*Independent Review of the Investigatory Powers Act 2016).*
5. The main elements of the Bill are:

[1] The Security Service (Mi5), Secret Intelligence Service (Mi6) and GCHQ.

a. Changes to the Bulk Personal Dataset (BPD) regime, which will improve the intelligence services' ability to use less sensitive datasets (such as publicly and commercially available data).

b. Placing the intelligence services' examination of bulk personal datasets held by third parties (I.e. an external organisation outside of the intelligence services) on a statutory footing. If the examination was of datasets retained by intelligence services, existing provisions in the IPA 2016 would apply.

c. Changes to the Notices regimes, which will help the UK anticipate and develop mitigations against the risk to public safety posed by multinational companies rolling out technology that precludes lawful access to data – in order to reduce the risk of the most serious offences such as child sexual exploitation and abuse or terrorism.

d. Creating a new condition for the use of Internet Connection Records by the intelligence services and the National Crime Agency (NCA).

e. Improvements to the oversight regime to support the Investigatory Powers Commissioner (IPC) to effectively carry out their role, including powers to enable the IPC to delegate some of their functions to Judicial Commissioners (JCs), appoint deputies and putting certain functions on a statutory basis.

f. Measures to increase resilience of the warrantry authorisation processes for the intelligence services as well as for the NCA.

g. Changes to the Communications Data regime to provide greater

certainty on the circumstances for lawful data acquisition.

Introduction

6. The provisions in the Bill engage Articles 8 and 10, and Article 1 of the First Protocol of the Convention. These are all qualified rights, which means that interference with the rights may be permissible. Any interference must be set down and regulated by a clear and ascertainable legal regime ("in accordance with the law", "prescribed by law", or "subject to the conditions provided for by law"). Furthermore, Articles 8 and 10 require that any interference is necessary in a democratic society and is a proportionate means of achieving a legitimate aim, while Article 1 of the First Protocol requires that any deprivation of possessions must be "in the public interest".
7. In order for an interference with an ECHR right to be in accordance with the law, there must be a lawful domestic basis for it, this law must be adequately accessible to the public, and its operation must be sufficiently foreseeable, so that people who are subject to it can regulate their conduct.
8. There is an inevitable tension between the requirements of foreseeability and the covert use of investigatory powers. In *S and Marper v United Kingdom*, the ECtHR found that the level of precision required in respect of foreseeability depends heavily on the context and cannot, in any case, cover every eventuality. The law does not need to set out each and every way that the powers may be used.[2]

[2] *S and Marper* v. *United Kingdom,* 4 December 2008, (2009) 48 EHRR 50

9. The requirement that the law be foreseeable does not mean that a target of covert techniques should be able to foresee when powers are likely to be deployed against them, so that they may adapt their conduct accordingly.[3]

10. In *S and Marper*, the ECtHR set out that:

> "... *it is essential ... [in the context of] secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning,* inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction*…".

11. In order to address the 'foreseeability' and 'compatibility with the rule of law' requirements of Article 8, where possible those minimum safeguards should be set out expressly in legislation, codes of practice or published guidance.

12. The requirement of legality goes further than the law being adequately prescribed, accessible and foreseeable. The law must contain sufficient safeguards to avoid the risk that power will be arbitrarily exercised and thus that unjustified interference with a fundamental right will occur. This was endorsed by the Grand Chamber of the ECtHR in *Big Brother Watch v the United Kingdom*[4].

Existing Safeguards in the IPA

13. The IPA established (or enhanced) a number of safeguards against the arbitrary or unlawful use of investigatory powers by the Executive. These safeguards include:

[3] *Weber and Saravia v. Germany,* Admissibility Decision, 29 June 2006

[4] Big Brother Watch v the United Kingdom 25 May 2021. (2022) 74 E.H.R.R. 17.

a. Judicial approval of warrants – a fundamental safeguard included in the IPA is an authorisation process (a ‘double-lock’) that provides that decisions by the Secretary of State (which have to be taken personally by the Secretary of State) to issue warrants are subject to approval by independent judges called Judicial Commissioners (“JCs”). The Secretary of State has to decide, amongst other things, that the warrant is necessary and proportionate, and that decision is reviewed by a JC according to the principles that would apply on a judicial review. There is an appropriate mechanism for urgent cases (e.g. where there is an imminent threat to a person’s life). In such cases, an urgent warrant, which may be issued without JC approval, must be reviewed by a JC within three working days and will cease to have effect if it is not approved. This means that a JC can effectively cancel an urgent warrant that he does not consider to be both necessary and proportionate. Where an urgent warrant is (in effect) cancelled, the JC has the power to determine that any information that has already been obtained should be destroyed.

b. Investigatory Powers Commissioner -- the Investigatory Powers Commissioner (“the Commissioner”) is obliged by the Act to keep under review, by way of audit, inspection and investigation the exercise by public authorities of the powers in the Act. The Commissioner is supported by the staff of the Investigatory Powers Commissioners Office ("IPCO"). The Commissioner, in addition to an annual report, may report at any time, on anything of which the Commissioner has oversight. Reports are made to the Prime Minister and, subject to the Prime

Minister's power to exclude matters from the report on narrowly defined grounds, published and laid before Parliament. This means that the Commissioner can highlight any arbitrary or potentially unlawful use of the powers under the Act, including those amended or inserted by the Bill. Where the Investigatory Powers Commissioner becomes aware of an error, either through inspections or through self-reporting by public authorities, the Commissioner may inform the member of the public concerned if the Commissioner regards the error as serious and that it is in the public interest for the person to be informed.

c. Investigatory Powers Tribunal ("IPT") – the IPT considers allegations of unlawful intrusion by the intelligence services. The Grand Chamber of the European Court of Human Rights described the IPT as providing "an effective remedy" for compliance with the rights enshrined in the ECHR[5]. The IPT rules and procedures were found to be lawful by the European Court of Human Rights in *Kennedy v United Kingdom*[6].

14. In relation to the Investigatory Powers Commissioner's ("the Commissioner") functions and roles, the Bill makes improvements to add resilience, remove unnecessary functions and improve oversight. For example, the Bill:

    a. amends s229 IPA to place on a statutory footing the Commissioner's existing non-statutory oversight of compliance by the Ministry of Defence ("MoD") with certain policies relating to overseas conduct;

    b. extends the power of the Prime Minister to issue Directions under s230 IPA to the Commissioner, which is currently limited to only the activities

[5] *Big Brother Watch v UK (58170/13)* (2022) 74 E.H.R.R. 17.

[6] [2011] 52 EHRR 4.

of the intelligence services and the Ministry of Defence, to oversee other public authorities that use the IPA, so far as engaging in intelligence activities;

c. amends the IPA to allow the Commissioner to appoint up to two Deputy Investigatory Powers Commissioners who are to be allowed to exercise functions personally conferred on the Commissioner in certain circumstances;

d. extends the Commissioner's power to delegate functions to a JC under s227(8) IPA to the Commissioner's powers relating to Communications Data under sections 60A and 65(3B) IPA;

e. removes the Commissioner oversight functions relating to telecommunications restrictions orders for prisoners under s229(3)(c) IPA as these are already adequately provided by the County Court;

f. provides a power to formally appoint temporary JC in exceptional circumstances that lead to a shortage of Judicial Commissioners;

g. clarifies the scope of error reporting notifications that are made to the Commissioner.

Provisions in the Bill

15. Consideration of the provisions within the Bill is provided below. As set out, the Bill also strengthens and enhances the Investigatory Powers Commissioner's role. These amendments do not interfere with rights under the ECHR, and so are not discussed further in this section. An explanation of the amendments is provided above.

Bulk personal datasets

16. The amendments to the IPA relating to bulk personal datasets ("BPDs") insert a new Part 7A into the IPA. This new Part does not extend the ability of the intelligence services to obtain bulk personal datasets, rather it creates a new set of safeguards, alongside the existing provisions in Part 7 of the Act, for the retention or retention and examination of less sensitive bulk personal datasets (such as publicly and commercially available data).
17. The intelligence services have the existing statutory power to acquire collections of data which contain personal information about a large number of individuals, the majority of whom are unlikely to be of any interest to those services. Bulk personal data can be acquired from a range of sources including government departments and agencies, other intelligence agencies and private sector bodies. Some of this data is publicly available, some of it is purchased and some of it is acquired covertly.
18. In the light of ECtHR and domestic case-law[7], it is clear that the acquisition, use/access, disclosure and retention of personal information engages Article 8 ECHR.
19. The Bill makes various changes to the BPD process, most significantly the creation of a new scheme which amends the safeguards that apply to the retention, or retention and examination, of datasets in respect of which there is a low, or no, reasonable expectation of privacy. The current safeguards, as set out in Part 7, will continue to apply to datasets that do not meet this description.
20. Part 7 of the IPA has been challenged and held to be compatible with the ECHR[8].

[7] *R. (on the application of Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9.
[8] *R(National Council for Civil Liberties) v Secretary of State for the Home Department & Anor* [2023] EWCA Civ 926

In accordance with the law

21. The acquisition and use of bulk personal datasets is in accordance with the law. The current basis in domestic law is clear. In addition to Part 7 IPA, section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 enable the intelligence services to obtain and use information where this is necessary for the proper discharge of their statutory functions. This includes the acquisition of bulk personal data. In addition, section 19 of the Counter-Terrorism Act 2008 provides that a person may disclose information to the intelligence services for the exercise of their functions and that any information disclosed to an intelligence service for one of its functions may be used for any of its other functions.
22. Bulk personal datasets are currently retained, or retained and examined pursuant to a warrant issued by the Secretary of State under Part 7. The decision to issue such a warrant must be approved by a Judicial Commissioner. Part 7 sets out various safeguards concerning the retention and examination of bulk personal datasets, and is supplemented by a statutory code of practice.
23. The amendments made by the Bill form part of the statutory framework governing the use of BPDs.
24. In addition to amendments to Part 7, the Bill introduces a new set of safeguards that will apply to datasets, the nature of which is such that the individuals to whom the data relates can have a low or no reasonable expectation of privacy (such as may be the case in respect of publicly or commercially available datasets) (new Part 7A). These safeguards are also set out in primary legislation and will be supplemented by a Code of Practice.

Necessary

25. Bulk personal datasets play an integral role in allowing the intelligence services to carry out their functions. They are used, for example, to establish links between subjects of interest or to validate information obtained from other sources. Without bulk personal datasets, the intelligence services would be significantly less effective in protecting the UK against threats such as terrorism, cyber-attacks and espionage. The amendments to Part 7 IPA are designed to enhance the operation of those provisions.

26. With regard to the new Part 7A of the IPA inserted by the Bill, the intelligence services' retention and use of bulk personal datasets can be authorised only where it is necessary for the purpose of the exercise of a function of the intelligence service. The head of each intelligence service, or a Crown Servant acting on their behalf, may authorise the retention, or retention and examination, of such a bulk personal dataset. Authorisations must be approved by a Judicial Commissioner.

Proportionate means of achieving a legitimate aim

27. With regard to both Part 7 and Part 7A, the use of bulk personal datasets is proportionate in that it can limit the use of intrusive powers in two ways. Firstly, it allows the intelligence services to obtain information that might otherwise be sought using more intrusive methods. Secondly, it allows the intelligence services to focus their efforts on individuals who threaten our national security or who may be of intelligence interest, whilst ensuring that the need to interfere with the privacy of others is minimised.

28. New Part 7A of the IPA, which is inserted by the Bill, introduces a new set of safeguards for the retention, or retention and examination, of datasets in respect of which those to whom the data relates have a low, or no, reasonable

expectation of privacy. As with Part 7, it will remain the case that the retention, or retention and examination, of a bulk personal dataset must be both necessary and proportionate. These changes bring the safeguards necessary to prevent unjustified interference in line with the nature of the datasets to which they apply. Statutory codes of practice provide further safeguards regarding how the intelligence services access, store, destroy and disclose information contained in bulk personal datasets.

29. As the nature of the datasets that fall within new Part 7A have a much lower reasonable expectation of privacy (e.g. because they are generally or commercially available), they do not require all of the same safeguards that are in place for BPDs in respect of which there is a higher reasonable expectation of privacy. Additionally, the Bill provides a mechanism in the event that potentially sensitive data is subsequently discovered in a dataset that is retained under Part 7A.

Third Party Bulk Personal Data

30. The amendments to the IPA relating to third party bulk personal datasets ("BPDs") insert a new Part 7B into the IPA. This new Part does not extend the ability of the intelligence services to obtain bulk personal datasets, rather they create a statutory regime to govern the examination of datasets held by third parties.

31. While the use of third-party BPDs does not include the acquisition or retention of personal information access to and the examination of third-party BPDs engages Article 8 ECHR.

In accordance with the law

32. The examination of third-party held BPDs is in accordance with the law. The basis in domestic law is clear. In addition to the measures in the Bill, section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 enable the intelligence services to use information where this is necessary for the proper discharge of their statutory functions. This includes the examination of bulk personal data. In addition, section 19 of the Counter-Terrorism Act 2008 provides that a person may disclose information to the intelligence services for the exercise of their functions and that any information disclosed to an intelligence service for one of its functions may be used for any of its other functions.

Necessary

33. Just as set out in relation to Part 7 and Part 7A above, the examination of third-party held BPDs play an integral role in allowing the intelligence services to carry out their functions. They are used, for example, to establish links between subjects of interest or to validate information obtained from other sources. Without BPDs, including the examination of third-party held BPDs, the intelligence services would be significantly less effective in protecting the UK against threats such as terrorism, cyber-attacks and espionage.

34. The intelligence services' examination of BPDs held by third parties can be authorised only where it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are relevant to the interests of national security. Under new Part 7B of the IPA as inserted by the Bill, the Secretary of State's decision that the warrant is

necessary must be approved by a Judicial Commissioner before the warrant can be issued.

Proportionate means of achieving a legitimate aim

35. The intrusion into privacy and the potential interference may be less significant in respect of third-party BPDs than for BPDs that fall under Part 7 as the datasets are not obtained by the intelligence services, rather they are examined *in situ*, remaining under the control of the third party.

36. In any event, as set out above, the use of BPDs is proportionate in that it can limit the use of intrusive powers in two ways. Firstly, it allows the intelligence services to examine information that might otherwise be sought using more intrusive methods. Secondly, it allows the intelligence services to focus their efforts on individuals who threaten our national security or who may be of intelligence interest whilst limiting the need to interfere with the privacy of innocent people. Further, with respect to third party held BPDs, where it is appropriate for the intelligence services to examine rather than retain and examine a BPD, it allows the intelligence service to examine information held in BPDs without the potential additional intrusion associated with retaining those datasets. Statutory codes of practice provide further safeguards regarding how the intelligence services access, store, destroy and disclose information contained in bulk personal datasets.

37. The intelligence services' examination of third-party BPDs can be authorised only if the Secretary of State decides that the warrant is necessary and proportionate and a Judicial Commissioner approves that decision. This mirrors

the approach in Part 7, and it is relevant that part 7 of the IPA has been challenged and held to be compatible with the ECHR[9].

Notices

38. Parts 4 and 9 of the IPA make provision for different types of notices, which impose obligations on telecommunications operators[10] to assist with national security and law enforcement investigations by ensuing that there is lawful access to data.

39. The amendments are designed to enhance this existing notices regime, to improve its effectiveness. Any operation of the regime must be carried out compatibly with the ECHR. The amendments do not (actually or effectively) prevent the provisions from being operated compatibly with the ECHR.

40. That said, the amendments to the IPA relating to notices engage, or may engage, Articles 8, 10 and A1P1 ECHR.

In accordance with the law

41. The amendments to the notices regime is in accordance with the law (as the existing regime is) because it is clearly set out in primary legislation and is supported by statutory Codes of Practice. In combination these provide clarity as to the situations under which notices operate.

Necessary

42. The amendments are necessary to make the existing notices regime operate effectively. Notices may only be issued when the Secretary of State considers that the requirement is necessary and proportionate for specified purposes,

[9] *R(National Council for Civil Liberties) v Secretary of State for the Home Department & Anor* [2023] EWCA Civ 926

[10] As defined under s261(10) IPA.

including in the interests of national security. On that basis, the justification for interference with rights under the ECHR is already an inherent aspect of the existing notices regime.

Proportionate means of achieving a legitimate aim

43. As set out above, notices may only be issued when the Secretary of State considers that the requirement is necessary and proportionate for specified purposes including in the interests of national security. Before giving the notice, the Secretary of State must take reasonable steps to consult with the operator to whom the notice relates and take into account factors, such as, the likely benefits of the notice, the likely number of users of any postal or telecommunications service to which the notice relates and the technical feasibility and likely cost of complying with the notice.

44. The existing safeguards in the IPA will continue to apply in respect of notices. Specifically, notices issued by the Secretary of State are subject to the approval of Judicial Commissioners, applying the same principles as a court would apply on an application for judicial review. In carrying out this function, Judicial Commissioners will also consider the Secretary of State's necessity and proportionality justifications to ensure that the general duties in relation to privacy, set out in section 2 IPA, have been adhered to.

45. Following receipt of the notice, the operator may refer the notice (or part of it) back to the Secretary of State for review. Before deciding the review, the Secretary of State must consult the Technical Advisory Board and a Judicial Commissioner, who must respectively consider the technical requirements and financial consequences of the notice, as well as whether the notice is proportionate.

Communications Data

46. Part 3 of the Bill amends the IPA in respect of communications data and internet connection records (ICR). There are changes to sections 11, 12 and 261 and to the ICR provisions in section 62. The changes to section 11 are to focus the offence of acquiring communications data without lawful authority on the acquisition of communications data from private sector telecommunications operators as well as to define "lawful authority". The changes to section 12 reinstate various statutory powers to acquire communications data that are outside the IPA where the acquisition is for a regulatory or supervisory purpose and not in the course of a criminal investigation. Section 261 is amended to clarify the definition of communications data. Section 62 is amended to include a new condition under which ICRs may be obtained.

47. The ECtHR case of *Big Brother Watch v UK* held that the previous communications data regime in the Regulation of Investigatory Powers Act 2000 was contrary to both Articles 8 and 10 ECHR because it was both not in accordance with the EU law applicable at the time and did not contain sufficient protections for journalists. In 2018 and 2022 the IPA was amended to remedy that breach of EU law and has since been found to be compatible with the ECHR by the Court of Appeal in 2023[11] in relation to communications data acquisition and retention powers.

48. The acquisition of communications data may, exceptionally, lead to the identification of a source of journalistic information. Such acquisition may constitute an interference with Article 10.

[11] *R(National Council for Civil Liberties) v Secretary of State for the Home Department & Anor* [2023] EWCA Civ 926.

49. The amendments to the IPA made by the Bill allow for additional people to be identified from their activity on the internet, which engages Article 8.

In accordance with the law

50. Any interferences with Convention rights will be in accordance with the law because the Bill amends a clear provision in domestic legislation governing the requirement on operators to retain communications data and the circumstances in which the retained communications data may be obtained by relevant public authorities. The amendments in relation to internet connection records and sections 11, 12 and 261 also are clearly set out in primary legislation.

51. These provisions are formulated with sufficient precision to enable a person to know in what circumstances and to what extent the powers can be exercised. The test of foreseeability in the context of the retention of, and access to, communications data is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. The provisions of the Bill meet that test.

Necessary

52. The ability of law enforcement and intelligence services and other public authorities designated in Schedule 4 to the IPA to obtain communications data is vital in protecting national security, preventing and detecting crime and protecting the public.

Proportionate means of achieving a legitimate aim

53. Communications data is used not only as evidence in court, but also to eliminate people from law enforcement investigations. It can be used to prove a person’s innocence as well as his or her guilt. It is essential that

communications data of this sort continues to be available to be obtained by the law enforcement and intelligence services and other relevant public authorities and the amendments remove an unnecessary hurdle to the sharing of such data, lawfully acquired, between public authorities. The CJEU judgment in *Digital Rights Ireland* recognises that data relating to the use of electronic communications 'are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime' and concluded that their retention genuinely satisfies an objective of general interest. The CJEU case law since *Digital Rights Ireland* has focussed on the acquisition of CD for serious crime purposes and not on the acquisition of it for supervisory or regulatory purposes.

54. The provision related to internet connection records is in pursuit of a legitimate aim – the reason for the power is to help the intelligence services and NCA to identify people committing or connected to serious crimes, such as terrorism or child sexual abuse. In his report of June 2023, Lord Anderson concluded that "ICRs have the capacity to make a decisive contribution to the prioritisation and pursuit of both national security and serious crime investigations12".

55. The interference is necessary and proportionate, and existing relevant safeguards already in place will apply to applications for authorisations under the new condition (including those amended by the Data Retention and Acquisition Regulations 2018 following the CJEU Judgment in *Tele2 and Watson* as interpreted in *R(Liberty) v SSHD* [2019] QB 481). The power to make ICR requests under the new Condition D1 or D2 will only be available to the intelligence services and the NCA (not to wider public authorities in

[12] Independent Review of the Investigatory Powers Act 2016 by Lord David Anderson KC, June 2023.

Schedule 4), and prior authorisation by the Investigatory Powers Commissioner (delegated to the OCDA) or a designated senior officer of the intelligence services (as appropriate) will be required.

56. The changes to section 12 will re-instate various statutory powers for public authorities to acquire CD from a telecommunications operator without the consent of that operator. Each request made by such an authority under those powers will need to be necessary and proportionate in accordance with the obligation on public authorities in section 6 of the Human Rights Act 1998 as well as in accordance with general public law principles.

Amendment to Schedule 3 to the IPA

57. The amendments to Schedule 3 to the IPA tidy up a discrepancy between references to legislation in different jurisdictions. This amendment does not amend the existing powers to intercept communications, rather they provide additional exceptions to the prohibition in s56. Section 56 criminalises doing anything in legal proceedings or Inquiries Act proceedings that would disclose the content of intercepted communication (or secondary data) where it could be inferred that it originated from intercept conduct, or would tend to suggest that intercept conduct has – or might have - occurred, or will occur in future.

58. The interception of communications and then the making available the content of private communications, even in a limited setting such as a parole board hearing, inevitably engages Article 8, and potentially Article 10.

59. In the context of interception of communications, the ECtHR has ruled that foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept their communications so that they can

adapt their conduct accordingly (*Leander v Sweden*[13]), but the domestic 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 public authorities are empowered to intercept communications. The law must indicate the scope of the competent authorities' discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

60. The ECtHR has developed a list of 'minimum safeguards' that need to exist within the legal framework governing the interception of communications. In order to ensure that the requirements of foreseeability are met, as many as possible of these minimum safeguards should be set out in statute. Those minimum safeguards, as set out in the *Weber and Saravia* case, are:

    a. the nature of the offences which may give rise to an interception order;

    b. a definition of the categories of people liable to have their telephones tapped;

    c. a limit on the duration of telephone tapping;

    d. the procedure to be followed for examining, using and storing the data obtained;

    e. the precautions to be taken when communicating the data to other parties; and

[13] *Leander -v- Sweden*; ECHR 26 Mar 1987. Slightly different safeguards exist under ECHR law in relation to bulk interception regimes. See *Big Brother Watch v United Kingdom* 25 May 2021.

f. the circumstances in which recordings may or must be erased or the tapes destroyed.

In accordance with the law

61. The IPA sets out a clear and accessible domestic basis for interception and the amendments are made to that basis. The regime is sufficiently foreseeable in that it builds on the safeguards in the existing interception regime which have been scrutinised by the ECtHR and found to be foreseeable. In *Kennedy v UK*, the ECtHR assessed the law governing the interception of communications between persons in the United Kingdom against the criteria set out in *Weber and Saravia v Germany.* The Court found that the regime was foreseeable and that Article 8 was therefore not violated. The Court explained that:

> "the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected."

62. The amendments to the Bill do not detract from the foreseeability of the use of intercept conduct, or of the resulting use of any intercepted communication. If anything, the Bill clarifies the regime by regularising discrepancies in the extent to which intercept related conduct may be used in relevant proceedings before the parole Board or a coroner's court.

Necessary

63. The amendments to Schedule 3 allow key intercept evidence to be provided to the Parole Board, to help the Parole Board to make more informed assessments as to the risk of harm to the public from terrorists and other dangerous prisoners by considering classified material in closed proceedings.

Proportionate means of achieving a legitimate aim

64. The use of material in reliance on the provisions in Schedule 3 would only arise in pursuit of a legitimate aim (national security and/or the prevention of disorder or crime). The use of the power to intercept communications, along with the performance of duties imposed by the IPA, are subject to scrutiny by the Investigatory Powers Commissioner.

65. The amendments are proportionate and do not disproportionately extend the potential recipients of intercept-related material.

Conclusion

66. The Department recognises that the Bill, and the relevant conduct that may be authorised under the IPA as amended by the Bill, engage Convention rights. It is the Department's view that, for the reasons set out in this Memorandum, the Bill is compatible with the Convention.

Home Office

November 2023