Written Evidence from Dr Matthew White (CHIS0008)

1. I am a Doctor of Law who primarily focusses on State surveillance, particularly the Investigatory Powers Act 2016 (IPA). I have written on many aspects of the IPA for well-respected journals[1] and blogs.[2] Although, the Covert Human Intelligence Sources (Criminal Conduct) Bill (CHISB) does not only or primarily concern measures of secret surveillance, I am familiar with the regulatory framework and the impact upon fundamental rights. Thus, my understanding in this particular field leaves me well equipped to raise a few points in this call for evidence.
2. Your first question asks whether a statutory power to authorise criminal conduct by covert human intelligence sources (CHIS) can be justified. However, I am of the view that the Committee asks the wrong question. Asking this question implicitly accepts the power to authorise criminal activity by CHIS and only queries the avenue in which it can be utilised. It is not *what* is done, but *how* it is done. The question that should be asked is whether CHIS should be allowed to commit criminal offences in and of itself, not whether it should be granted statutory footing. The necessity of the CHISB will be considered later on in this submission. Considering it from a European Convention on Human Rights (ECHR/Convention Right(s)) perspective will answer most, if not all the questions raised. **Skip to paragraph 9 to go straight to the analysis.**

Summary of the CHISB

3. It is first necessary to look to the CHISB itself in that clause 1 amends Part II of the Regulation of Investigatory Powers Act 2000 (RIPA). Clause 1(2) amends section 26 by adding subsection 1(d) which states that this Part applies to "criminal

[1] e.g. M. White, "Protection by Judicial Oversight, or an Oversight in Protection?" (2017) 2(1) *Journal of Information Rights, Policy and Practice* 1; M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633.
[2] e.g. M. White, "Data Retention incompatible with EU law: Victory? Victory you say?' (24 May 2018) <https://eulawanalysis.blogspot.com/2018/05/data-retention-incompatible-with-eu-law.html

conduct in the course of, or otherwise in connection with, the conduct of covert human intelligence sources". Clause 1(3) inserts subsection 8A which essentially describes subsection 1(d) as *any* crime committed in connection with CHIS.

4. Clause 1(4) inserts subsection 6ZA into section 29 which separates CHIS criminal conduct and CHIS conduct in general. Clause 1(5) inserts subsection 29B which governs CHIS criminal conduct authorisations by designated persons. Section 29B(4) notes that said authorisations cannot be granted unless they are necessary on at least one ground of subsection (5)(5) is met, it is proportionate, and the arrangement satisfy the requirements that may be imposed by the Secretary of State. These grounds in subsection (5)(5) are national security, preventing or detecting crime or of disorder and the economic well-being of the UK. Subsection (5)(6) details that when considering the requirements of subsection (5)(4) (i.e. necessary, proportionate, satisfy the Secretary of State's requirements), account must be taken of whether the objective could be achieved without committing a crime. Subsection (5)(7) details that the Human Rights Act 1998 (HRA) must be taken into account so far as it is relevant.
5. Subsection (5)(8) further details authorised CHIS criminal conduct as conduct specified by an authorisation and is carried out for the purpose of, or in connection with the investigation or operation specified or described. Subsection (5)(9) details that CHIS criminal conduct ceases to have effect once an authorisation ceases to have effect so far as it relates to the CHIS, meaning an authorisation could still be valid for a different CHIS.
6. Subsection (5)(10) denotes that the Secretary of State may impose, by order, restrictions or requirements on authorisations.
7. Clause 2 inserts Part A1 into Schedule 1 into RIPA regarding the relevant public authorities for the purposes of CHIS criminal conduct. This includes any police force, the National Crime Agency, Serious Fraud Office, any intelligence service, any armed forces, Her Majesty's Revenues and Customs, the Department for Health and Social Care, the Home Office, the

Ministry of Justice, the Competition and Markets Authority, the Environment Agency, the Financial Conduct Authority, the Food Standards Agency and the Gambling Commission.

8. Clause 4 amends the IPA) by inserting subsection (4A) into section 229 to review the grant of authorisations. It also inserts paragraph (ba) into section 234(2) which includes information about the use of power in reports.

Legality under the ECHR

9. The CHISB undoubtedly has human rights implications. The Government's ECHR memorandum explains as such (para 12). However, the memorandum does not detail the severity of interference because it "would be impossible to seek to identify which if any of the Convention rights may or may not be engaged by any particular authorisation of criminal conduct" (para 12). Therefore, the question becomes *why* would it be impossible to determine which Convention Rights would be engaged?

10. Article 8 is a suitable starting point, for example, in the ongoing Spycops scandal, police have admitted to violating Article 8 due to the unlawful surveillance and the deceptive intimate and sexual relationship that occurred. Under the jurisprudence of Article 8, any interference with it must be "in accordance with the law". This not only requires the law to be accessible, but foreseeable.

11. Accessibility requires details of the arrangements made to be accessible to the public (*Liberty v UK*, [66]). Audits by the Investigatory Powers Commissioner (IPC) is not sufficient (*Liberty v UK*, [67]) for ECHR compliance.

12. Foreseeability requires the law to be formulated in a way that is sufficiently precise in that it enables (with appropriate advice) any individual to regulate their conduct (*S and Marper*, [95]). To meet this requirement, domestic law "*must* afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise" (*S and Marper*, [95]). The European Court went onto note that it is

essential measures such as "secret surveillance covert intelligence-gathering" have "clear, detailed rules governing the scope and application of measures" (*S and Marper*, [99]). The rules must also be binding (*Valenzuela Contreras v Spain*, [60]).

13. Given that secret surveillance and covert intelligence-gathering are treated in the same regard, the rules governing the former, should be applied to the latter. Therefore, in relation to the foreseeability of secret surveillance measures (and therefore, by extension CHIS criminal conduct) requires that the *nature of offences* must be delineated (*Sefilyan v Armenia*, [125-126]). This is especially so when the exercise of the power is conducted by the executive in secret as it would be contrary to the rule of law for said power to be utilised in an unfettered manner (*Sefilyan v Armenia*, [125-126]).

14. The CHISB constantly refers to "criminal conduct". And the grounds for authorising them, one at least is the prevention and detection of "crime" and/or "disorder". The CHISB makes no attempts to define these terms, and thus it applies to *any* crime/instance of disorder. The European Court of Human Rights have noted their concerns with laws that allow measures in respect of a very wide range of criminal offences because they do not provide adequate protection against abuse by the State.[3] Where the nature of offences is nowhere defined, such as "crime" and "disorder", (and therefore does not limit them) this will violate Article 8 for not being "in accordance with the law".[4] Even if the Government were to introduce a "serious crime" threshold, this currently, as envisioned in the IPA does not satisfy legality *either*.[5] Terminology such as "national security" and "economic well-being" suffer from the same problems in relation to its lack of definition, limitation and its nature, and too would ultimately violate Article 8.[6] Similarly, for example, the

---

[3] M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633, 639.
[4] M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633, 639.
[5] M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633.
[6] M. White, "Coronaveillance: Coronavirus, a threat to national security, economic well-being and serious crime? Exposing pre-existing and *ex post facto* deficiencies in the Investigatory Powers Act?" *European Human Rights Law Review* (forthcoming).

infiltration of trade unions would trigger the application of both Articles 10 and 11 (*Trade Union of the Police in the Slovak Republic and Others v. Slovakia*, [51-52]) and would too violate them for not being "in accordance with the law" (*Segerstedt-Wiberg and others v Sweden*, [107]).

15. Due to the lack of limitations on what criminal activity is permissible, this permits authorisations to authorise murder, sexual offences, torture and deprivation of liberty etc. All of which engage Articles 2, 3, 5 and 8 at the very least. The Home Office has argued that due to the HRA, the public authorities in question cannot authorise conduct which breaches Convention Rights (para 6). The Home Office also relies (para 4) upon the Investigatory Powers Tribunal (IPT) in the *Third Direction* case where they noted that "there is nothing inherent in the policy which creates a significant risk of a breach of Article 3 or indeed any other Convention right" (*Privacy International & Ors v Secretary of State For Foreign and Commonwealth Affairs & Ors*, [100]). However, not only was this judgment a 3:2 split (meaning that there is no certainty it will survive an appeal) it serves as to further undermine the rule of law.

16. Additionally, Lord Kerr has noted that:

> The fact that it is exercised sparingly has no direct bearing on its legality. A power on which there are insufficient legal constraints does not become legal simply because those who may have resort to it, exercise self-restraint. *It is the potential reach of the power rather than its actual use by which its legality must be judged* (*Beghal v DPP*, [102]).

17. This was a view endorsed by the European Court of Human Rights on appeal (*Beghal v UK*, [33-36]). Thus, it is no answer to suggest that the HRA prohibits public authorities in engaging in criminal activity which would otherwise breach the ECHR when there are no constraints within the CHISB itself. Nor is reliance upon the IPT appropriate. As can be seen from the IPA, a breach of the ECHR in and of itself is not even sufficient to notify victims of a violation (see section 231) thus

this demonstrates that the Government is quite capable of turning the HRA into a fig leaf.

18. Consequently, because criminal activity is not defined, it does not prevent the most heinous crimes. Article 2(1) prohibits the intentional taking of life (*Centre for Legal Resources on behalf of Valentin Câmpeanu v Romania*, [130]) and Article 3 absolutely prohibits torture, inhumane or degrading treatment (*Chahal v UK*, [79]). This again puts the CHISB directly in contrast with the ECHR.

19. Foreseeability also requires there is an adequate indication of the conditions and circumstances when authorities are empowered to resort to measures.[7] The European Court of Human Rights were aware that the risks of arbitrariness are evident when the power vested in the executive is done so in secret, thus requiring *particularly precise laws.*[8] Because the CHISB does not indicate in *what* circumstances an authorisation may be utilised, as all that is required is a connection to an investigation or operation, this ultimately grants unfettered discretion. This becomes ever-more problematic when for example, the police are institutionally racist, and this seeps into their covert actions. The abuse of CHISB is clear, and therefore cannot be "in accordance with the law".

20. The European Court have noted that when definitions are lacking, judicial authorisation may be a sufficient safeguard (*Roman Zakharov v Russia*, [249]). However, as the CHISB demonstrates, authorisation/and restrictions thereof lays with the Secretary of State and a designated person, which neither are independent (*Roman Zakharov v Russia*, [258]).[9] Similarly, on some occasions, the European Court of Human Rights (though in relation to interception, the principles are still transferrable) have urged that that "the *body issuing authorisations for interception should be independent* and that there *must be either*

---

[7] M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633, 637.

[8] M. White, "Data retention: serious crime or a serious problem?" (2019) 4 *Public Law* 633, 637.

[9] M. White, "Protection by Judicial Oversight, or an Oversight in Protection?" (2017) 2(1) *Journal of Information Rights, Policy and Practice* 1, 10.

judicial control or control by an independent body over the issuing body's activity".[10]

21. A safeguard the European Court of Human Rights insists on is the prevention of arbitrariness ((*Roman Zakharov v Russia*, [259]). The Judicial Commissioners (JC) in their role under the CHISB does not require them to assess legality. However, even the power authorise was transferred to a JC, they are structurally unable make much difference due to the problematic phraseology. Additionally, even if they were given the same authorisation powers as they possess in the IPA, this *too* would still contravene the ECHR,[11] because it would just transfer the unfettered power to the JCs, which they should not possess in the first instance (*Sefilyan v Armenia*, [125-126]). Furthermore, the IPT is subject to extraordinary rules of secrecy, and is subject to *intense* criticisms by many.[12]

Necessity of the CHISB

22. For measures to be ECHR compliant they must also be necessary. This requires a pressing social need, which must be more than desirable or reasonable (*Handyside v UK*, [48]). As the previously Committee explained "[t]here must be a sufficient factual basis for believing that there was a real danger to the interest which the State claims there was a pressing social need to protect" (Joint Committee on Human Rights, First Report (2000–01), HL 42/HC 296). Given that the CHISB does not explicitly prevent murder, torture, sexual violence etc, Article 2:

> [I]ndicates that *a stricter and more compelling test of necessity* must be employed from that normally applicable when

---

[10] M. White, "The Threat to the UK's Independent and Impartial Surveillance Oversight Comes Not Just from the Outside, but from Within" (2019) 5 *European Human Rights Law Review* 512, 519.

[11] M. White, "Coronaveillance: Coronavirus, a threat to national security, economic well-being and serious crime? Exposing pre-existing and *ex post facto* deficiencies in the Investigatory Powers Act?" *European Human Rights Law Review* (forthcoming).

[12] M. White, "The Threat to the UK's Independent and Impartial Surveillance Oversight Comes Not Just from the Outside, but from Within" (2019) 5 *European Human Rights Law Review* 512, 514.

determining whether State action is "necessary in a democratic society" under paragraph 2 of Articles 8 to 11 (art. 8-2, art. 9-2, art. 10-2, art. 11-2) of the Convention. In particular, the force used must be strictly proportionate to the achievement of the aims set out in sub-paragraphs 2 (a), (b) and (c) of Article 2 (art. 2-2-a-b-c). 150. In keeping with the importance of this provision (art. 2) in a democratic society, the Court must, in making its assessment, subject deprivations of life to the most careful scrutiny, particularly where deliberate lethal force is used, taking into consideration not only the actions of the agents of the State who actually administer the force but also all the surrounding circumstances including such matters as the planning and control of the actions under examination" (*McCann and others v UK*, [149-150])

23. Thus, this is stricter than the strict necessity that the European Court of Human Rights requires for secret surveillance (*Klass and others v Germany*, [42]). Furthermore, the applicability of Article 2 extends to situations where the State puts a person's life at risk even if they survive, even if the intention was not to kill (*Makaratzis v Greece*, [55]). Given that the *Third Direction* case was only 3:2 majority and the Government has not or has *ever* tried to justify CHIS criminal conduct in the interests of national security, it should not be seen as a given that this power is even necessary. How can one "critique and examine"[13] this point of view when the case has never been made? Where is the operational case as there was with the IPA? The *only* reason why this is even known about or discussed is because of the legal challenges brought upon by Privacy International and Reprieve. Rushing the CHISB through Parliament during the middle of a global pandemic is not an effective way to scrutinise the necessity, even if national security is a justification. National security should never be used as a trump card,[14] because even if there was a compelling

[13] T.Holman, "Why States Fail to Counter Foreign Fighter Mobilizations: The Role of Intelligence Services" (2016) 10(6) *Perspectives on Terrorism* 140, 152.
[14] M. Johnson and C. Gearty, "Civil liberties and the challenge of terrorism" in A.Park et all (eds.) *British Social Attitudes: Perspectives on a changing society* (London: Sage

justification, this should never permit murder, torture, sexual violence etc. Canada has ruled out crimes that include "murder, torture and sexual offences", what is this Government's excuse not to?

24. Crime, disorder and economic well-being should *never* be used as justification in this regard. The *Third Direction* case only concerned national security, so there is no reason why the Government felt the need to include these ill-defined grounds.

25. The range of public authorities' able to utilise these authorisations are *highly inappropriate*. Strong business cases for the inclusion of public authorities is required (Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, (2012-2013 HL 79 HC 479), 137). This has not been met, even with public authorities such as the police, let alone the Food Standards Agency.

26. Measures are not sufficient just because they fall within a class of exceptions i.e. national security (*Sunday Times v UK*, [65]). The Government has failed to demonstrate the need for the CHISB, in terms of the grounds for authorisations (including national security), for the lack of specificity regarding the range of crimes permissible under it, why authorisation is at the hands of the executive, and why there are a plethora of public authorities which can utilise this power. This would violate the ECHR (*Sunday Times v UK*, [63] and [67]).

27. A proportionality assessment is not necessary when the measures here regarded are unnecessary from the outset.

Conclusions

28. The Government seeks to introduce the CHISB amidst the revelations during the *Third Direction* case. Not only do they want to consolidate public authorities engaging in criminal activities into statute law, they want to extend the scope of the permissible grounds for criminal conduct and who can authorise this. The CHISB permits any crime to take place, with no restraints, and with no independent authorisation process. History and the present has shown how powers such as these

---

Publications, National Centre for Social Research 2006/7), p.169.

have been abused whether it is spying on the Lawrence family in indisputable institutional racist fashion, the murder of Pat Finucane or the Spycops scandal. The CHISB would maintain and extend these powers and provides ineffective and insufficient oversight. These powers are neither lawful or necessary in terms of the ECHR, and thus needs to be stopped.

16/10/2020