IN THE MATTER OF THE UNDERCOVER POLICING INQUIRY

SUBMISSIONS ON BEHALF OF THE
NON-POLICE, NON-STATE CORE PARTICIPANTS
PRIVACY HEARING, 31 JANUARY 2019

A. INTRODUCTION

1. These submissions are made on behalf of the Non-Police, Non-State Core Participants (**"the NPNSCPs"**)[1] for the hearing of the privacy preliminary issue, listed for 31 January 2019.

2. In the *"Note to core participants and directions for hearing"* of 29 November 2018 (**"the Hearing Note"**), the Chairman invited submissions on the implications for the Inquiry of the coming into force of the General Data Protection Regulation (the **"GDPR"**) and the Data Protection Act 2018 (the **"DPA 2018"**).[2] In particular, the core participants were invited to consider whether these new data protection laws have any implications for the approach to privacy in the existing Restriction Protocol, and/or how effect is to be given to the privacy and data protection rights of those referred to in intelligence reports.

3. The Inquiry is a data controller, processing large amounts of personal data, some of it highly sensitive, about the NPNSCPs and other individuals. The Inquiry cannot fulfil its functions without processing that personal data. However, such processing constitutes an interference with the fundamental rights of the NPNSCPs and must be carried out consistently with data protection law. The GDPR and the DPA 2018 significantly strengthen the rights afforded to data subjects under EU and domestic law.

4. As with all data controllers, to ensure compliance with these new, stricter, data protection laws, the Inquiry's approach to the processing of personal data must be re-examined.

5. There are three areas where the Inquiry's current or proposed processing of personal data is not consistent with the GDPR:

---

[1] As with previous submissions on behalf of the NPNSCPs, these submissions are made on behalf of those NPNSCPs who have expressed a view and provided positive instructions.

[2] Hearing Note, §9. See also the email from the Inquiry of 21 November 2018, which confirmed that privacy issues raised by the NPNSCPs prior to the Chairman's decision to list this hearing would also be decided after it had taken place.

a. First, the Inquiry has not identified the correct provisions of the GDPR and DPA 2018 that apply to its activities, in particular for the purposes of determining whether its ongoing processing of 'special category' data is lawful. The Inquiry does not appear to have considered whether its current approach respects the essence of data subjects' rights, and includes suitable and specific measures safeguarding their rights and interests.

b. Second, the Inquiry has not taken, and does not currently propose to take, sufficient steps to comply with its notification obligations to third parties, i.e. to inform individuals who are not currently recognised as NPNSCPs that their personal data has been received by, and is being processed by, the Inquiry.

c. Third, the Inquiry's decision not to disclose any personal data to NPNSCPs until after it has obtained evidence from state witnesses, coupled with the indication that the Inquiry will not process subject access requests, is unlawful. The retention of NPNSCPs' personal data, and its provision to state witnesses and other individuals, constitutes significant data processing, subject to the requirements of the GDPR. In many cases that processing is causing distress, now compounded by the fact that NPNSCPs are apparently to be prevented from knowing what personal data is being processed about them, contrary to their rights under the GDPR and the EU Charter.

6. At the same time as emphasising the importance of compliance with fundamental privacy and data protection rights, the NPNSCPs recognise and support the need to ensure that the Inquiry is practically able to fulfil its public interest function of investigating unlawful undercover policing activities. The NPNSCPs and their lawyers have given careful consideration to a framework for the disclosure and publication of personal data, which the Inquiry could adopt, and which respects the fundamental rights of data subjects, while taking account of the need for the Inquiry to make meaningful progress. The details of the proposed framework are set out below, and the Inquiry is invited to consider how these pragmatic proposals can be incorporated into the timetable.

7. These submissions are structured as follows:

a. Section B sets out the relevant legal framework under the GDPR and DPA 2018;

b. Section C sets out the NPNSCPs' submissions on the law as it relates to the three issues identified above, and the NPNSCPs' proposals for the Inquiry's future data processing activities.

c. In addition, to assist the Inquiry and other core participants, the NPNSCPs have provided 'marked-up' versions of the Annexes to the Counsel to the Inquiry's Explanatory Note on Privacy ("**the Explanatory Note"**), to illustrate how their proposals could work in practice.

B. LEGAL FRAMEWORK

(1) Fundamental nature of data protection rights / purpose of the GDPR

8. The EU Charter recognises the right to privacy (Article 7) and a distinct right to protection of personal data (Article 8) as fundamental rights. Article 8 of the Charter provides, *inter alia*, that:

> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

9. The CJEU has made it clear that '*Article 8 of the Charter concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter* [right to privacy] *and which has no equivalent in the ECHR*'.[3] Consequently, the right to protection in relation to the processing of personal data is a discrete fundamental right guaranteed by EU law, as well as a means of giving effect to the separate fundamental right to respect for private life.

10. The importance of the right to protection of personal data is reiterated by Recital (2) and Article 1(2) of the GDPR. Recital (7) notes the need for a strong and more coherent data protection framework in the EU, ensuring that "*Natural persons should have control of their own personal data*". Recital (11) provides that:

> *Effective protection of personal data throughout the Union requires the strengthening and setting out in detail of the rights of data subjects and the obligations of those who process and determine the processing of personal data, as well as equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for infringements in the Member States.* [4]

[3] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen* EU:C:2016:970; [2017] QB 771; [2017] 2 WLR, at §129. See also GDPR, recital 1.
[4] Emphasis added.

(2) The EU & domestic data protection regimes

11. Since May 2018, there are, in effect, four data protection regimes that may apply to data processing in the UK:

    a. The GDPR, read together with Part 2, Chapter 2, of the DPA 2018 and related Schedules;
    b. The "applied GDPR", applicable pursuant to Chapter 3, Part 2 DPA 2018;
    c. The Law Enforcement Directive, read together with Part 3 DPA 2018, which applies only to law enforcement processing; and
    d. Part 4 DPA 2018, which applies to processing by the Intelligence Services.

12. The GDPR is the most well-known and widely applicable of the four regimes; it applies in most situations (see Articles 2 & 3 GDPR). As the Inquiry's Privacy Information Notice (**"the Privacy Notice"**)[5] confirms, *The Inquiry processes personal information in accordance with the General Data Protection Regulation"*.[6]

13. "*The applied GDPR"* applies to "*other general processing*" that is outside the scope of EU law, the Law Enforcement Directive or the Intelligence Services provisions, and which would otherwise be unregulated.

14. The Hearing Note refers to provisions of the "applied GDPR" (see §§58ff. below). Those provisions do not apply to the Inquiry's processing of personal data. This is relevant because the "applied GDPR" is a modified version of the GDPR, which in certain respects does not import the strict requirements of EU law that the GDPR applies to special category processing. This point is addressed further at §§58-64 below.

(3) Personal data and 'special category' data

15. The definition of personal data is broad. Article 4(1) GDPR provides as follows:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

[5] https://www.ucpi.org.uk/wp-content/uploads/2018/08/20180816-Privacy_Information_Notice_-Final.pdf
[6] See also the Inquiry's *"Policy on processing special categories of personal data and criminal convictions data"*, available at https://www.ucpi.org.uk/wp-content/uploads/2018/05/20180525-UCPI-Processing_Special_Category_and_Criminal_Convictions_Data.pdf. See, in particular, §§1-5.

16. Certain types of data are particularly sensitive. Article 9(1) identifies the following as 'special categories' of personal data: *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".* The processing of such data is *prima facie* prohibited, except in the defined circumstances set out in Article 9(2) GDPR.

(4) Lawful basis for processing special category data

17. A great deal of the personal data that the Inquiry is processing is special category data. In the Privacy Notice, the Inquiry identified the legal basis for its processing of special personal data as Article 9(2)(g) GDPR, which provides as follows:

> *(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.* [7]

18. The Privacy Notice also identifies the need for the Inquiry to comply with paragraphs 5&6 of Part 1 of Schedule 2 DPA 2018.

19. Section 10(3) DPA 2018 provides that:

> *The processing meets the requirement in point (g) of Article 9(2) of the GDPR for a basis in the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 2 of Schedule 1.*

20. One of the substantial public interest conditions in Part 2 of Schedule 1 provides:

> ***Statutory etc and government purposes***
>
> *6 (1) This condition is met if the processing—*
>
> > *(a) is necessary for a purpose listed in sub-paragraph (2), and*
> > *(b) is necessary for reasons of substantial public interest.*
>
> *(2) Those purposes are—*
>
> > *(a) the exercise of a function conferred on a person by an enactment or rule of law;*

[7] Emphasis added.

(b) the exercise of a function of the Crown, a Minister of the Crown or a government department.

21. Thus, special category processing by the Inquiry must be necessary for the purposes of the exercise of its functions as a public inquiry; necessary for reasons of substantial public interest; proportionate; and respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

22. This imposes stricter requirements for lawful special category data processing than Article 9's predecessor, Article 8 of the former Data Protection Directive. It essentially imports the strict necessity and proportionality requirements that the CJEU has imposed in its case law on derogations from the data protection rights, and which are also reflected in Article 23 GDPR.

23. The processing of personal data relating to criminal convictions and offences is also subject to special protections under Article 10 GDPR:

> *Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.* [8]

24. Section 10(4) DPA 2018 provides that: *"The processing meets the requirement in Article 10 of the GDPR for authorisation by the law of the United Kingdom or a part of the United Kingdom only if it meets a condition in Part 1, 2 or 3 of Schedule 1."* The same condition would apply to processing of crime-related information as other special category data (see §20 above).

(5) Specific data protection rights

25. The GDPR, building upon Article 8 of the EU Charter, guarantees the following specific data protection rights.

(i) Rights to information - Articles 13 and 14 GDPR

26. The purpose of these rights is, essentially twofold: (a) to allow data subjects to obtain sufficient information about who is processing their data and why, and (b) to ensure that they are aware of

[8] Emphasis added.

their fundamental data protection rights, such as the right of access, and their right to complain if they are concerned about what is happening to their data.

27. Of particular relevance are the information rights in Article 14 GDPR, which apply where (as in this case) personal data have not been obtained from the data subject(s). It requires the controller (i.e. in this case the Inquiry) to provide certain information to relevant data subjects:

> *1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:*
>
> > *(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;*
> >
> > *(b) the contact details of the data protection officer, where applicable;*
> >
> > *(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
> >
> > *(d) the categories of personal data concerned;*
> >
> > *(e) the recipients or categories of recipients of the personal data, if any;*
> >
> > *(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.*
>
> *2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:*
>
> > *(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;*
> >
> > *(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
> >
> > *(c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;*
> >
> > *(d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;*
> >
> > *(e) the right to lodge a complaint with a supervisory authority;*
> >
> > *(f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;*
> >
> > *(g) …*
>
> *3. The controller shall provide the information referred to in paragraphs 1 and 2:*

> *(a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;*
>
> *(b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or*
>
> *(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.*
>
> *4. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.*

28. Again, Article 14 GDPR imposes wider and much stricter requirements on data controllers than its predecessor, Article 11 of the Data Protection Directive. In particular, Article 14 GDPR now imposes restrictions on the situation where a controller does not satisfy those notification and information obligations, and establishes the safeguards that must then be implemented.

29. The information rights do not need to be complied with if the data subject already has the information.[9] However, in respect of the NPNSCPs and third parties with whom the Inquiry has not had contact, that is not the case.

30. The only other potentially relevant exemption from these notification obligations is Article 14(5)(b), which applies where:

> *… the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.* [10]

31. As is clear from the text of Article 14(5)(b), and the case-law referred to in §§43-48 below, this does not provide a basis for a blanket refusal to take any steps to provide notification and information to individuals that processing of their personal data is taking place. In particular, before it could be said that no further steps need be taken to comply with the notification obligations, the Inquiry would need to consider what proportionate steps can be taken in order to

[9] Articles 13(4) And Article 14(5)(a) GDPR.
[10] Emphasis added.

notify such persons and protect their interests, including, if appropriate, making information publicly available about the data that is being processed.

(ii) The right of access – Article 15

32. Articles 15(1)-(3) set out the right of access to personal data. Broadly speaking, this has three elements: (i) the right to information about what data is being processed, how and why; (ii) the right to know whether the data has been transferred abroad; and (iii) the right to see the data itself.

33. Recital (69) GDPR, stresses that: *"A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing..."* The obligations imposed by Article 15 GDPR on data controllers are more onerous than those that Member States were required to implement under Article 12(a) of the former Data Protection Directive.

34. The GDPR envisages that the right of access should allow individuals to check how their data is being processed and, if necessary, to take steps to protect themselves from prejudice flowing from that processing. The right of access is recognised as a fundamental right in and of itself, and is also a gateway through which data subjects may obtain the data and information needed to protect or exercise other fundamental rights and freedoms, including their right to privacy. In Joined Cases C-141/12 & C-372/12 *YS v Minister voor Immigratie*[11] the CJEU emphasised, at [44] and by reference to recital (41) of the predecessor Data Protection Directive, that: "*the protection of the fundamental right to respect for private life means … that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner*."[12]

35. The right of access is subject to certain limited exemptions.[13] However, there is no provision that exempts a data controller from complying with the right of access in all cases.

(iii) The right to restriction of processing – Article 18

36. The term 'restriction of processing' is defined in Article 4 GDPR as the marking of stored personal data with the aim of limiting their processing in the future. Article 18(1) provides for a right to restriction of processing where, for example:

[11] [2015] 1 WLR 609; [2015] 1 CMLR 18.
[12] See also *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd and others* [2017] 3 W.L.R. 811, at §§82-83.
[13] See Article 15(4) and §§43-48 below.

a. The accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

b. The processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; and

c. The data subject has objected to processing pursuant to Article 21(1) pending the verification of whether the legitimate grounds of the controller override those of the data subject.

37. The Data Protection Directive did not contain any direct equivalent to Article 18 GDPR.

(iv) The right to object - Article 21

38. Article 21 GDPR guarantees the right to object to processing of personal data. It provides as follows:

> *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.* [14]

39. The Inquiry's Privacy Notice explains that it processes personal data relying on Article 6(1)(e) GDPR (task carried out in the public interest). Recital (69) GDPR explains that:

> *Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6(e)], or on grounds of the legitimate interests of a controller or a third party [Article 6(f)], a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.*[15]

40. This emphasis on the need for the *controller* to demonstrate that its processing serves a compelling legitimate interest capable of overriding the data subject's objections was not contained in Article

[14] Emphasis added.
[15] Emphasis added. Recital (72) GDPR also confirms that profiling is subject to the rules laid down by the GDPR.

14 of the Data Protection Directive. Under the old regime, it was the data subject that had to prove compelling legitimate grounds to object to processing.

(v) Rights to erasure / rectification:

41. Article 16 GDPR grants data subjects the right to rectification, on the following terms: *"The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."*

42. Article 17 GDPR enshrines the right to erasure of data, commonly referred to as the 'right to be forgotten'.

(6) Exemptions / derogations must be strictly necessary and proportionate

43. Given the fundamental status of data protection rights, EU law imposes strict requirements on any derogation.

44. Article 52(1) of the Charter provides that:

> *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.*

45. Article 23(1) GDPR provides that Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 GDPR, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard certain legitimate objectives. Those objectives include, *inter alia*, the prevention, investigation, detection or prosecution of criminal offences, and the protection of the data subject or the rights and freedoms of others.

46. Schedule 2, DPA 2018 contains the exemptions that the United Kingdom has enacted pursuant to Article 23 GDPR (see section 15 DPA 2018).

47. The CJEU has confirmed on a number of occasions that derogations from, and limitations on, the protection of personal data should apply only in so far as is strictly necessary and proportionate. See, e.g.: *Tele2 Sverige AB v Post- och Telestyrelsen* (Joined Cases C-203/15 & C-698/15) [2017] 2 C.M.L.R. 30, at §96, where the Grand Chamber confirmed:[16]

> *Due regard to the principle of proportionality also derives from the Court's settled case law to the effect that the protection of the fundamental right to respect for private life at EU level requires that derogations from and limitations on the protection of personal data should apply only insofar as is strictly necessary…*

48. A test of strict necessity has also been applied on a case-by-case basis by the domestic courts when interpreting and applying the specific exemptions included in the Data Protection Act 1998 (the **"DPA 1998"**) in accordance with the Data Protection Directive.[17] For a measure to be strictly necessary, no other measure or measures should exist that would be equally appropriate and less restrictive.[18] The Court has to *"rigorously verify that no other measure or combination of measures"* could be as effective.[19]

(7) Section 8(2) DPA 1998

49. The Inquiry has previously relied on section 8(2) DPA 1998 in response to requests made under section 7 DPA 1998. Section 8(2) DPA 1998 provided that:

> *The obligation imposed by section 7(1)(c)(i) [to provide a copy of the individual's personal data] must be complied with by supplying the data subject with a copy of the information in permanent form unless—*
>
> > *(a) the supply of such a copy is not possible or would involve disproportionate effort, or*
> >
> > *(b) the data subject agrees otherwise;*

[16] See also Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Englebert and others* [2014] 2 C.M.L.R. 9, at §39; *Opinion 1/15 of the Court* (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, at §140; *Digital Rights Ireland* [2014] 3 C.M.L.R. 44, at §52; and *Schrems* [2016] 2 C.M.L.R. 2, at §92.

[17] See, in particular: *Zaw Lin, Wai Phyo v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), §80; *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB), §45; and *Dawson-Damer and ors v Taylor Wessing* [2017] 1 WLR 3255), §§37 *et seq*.[17] See also *Stunt v Associated Newspapers Ltd* [2018] 1 W.L.R. 6060, §72 (where the Court of Appeal applied §56 of Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy* EU:C:2008:727; [2008] E.C.R. I-9831, in which the Grand Chamber applied a test of strict necessity).

[18] See *Lumsdon & Ors, R (on the application of) v Legal Services Board* [2015] UKSC 41; [2015] 3 WLR 121, at [50]ff. See also, by way of example, *Sky Österreich GmbH v Österreichischer Rundfunk* (Case C-283/11) [2013] All ER (EC) 633, §§54–57; *Reindl v Bezirkshauptmannschaft Innsbruck* (Case C-443/13) EU:C:2014:2370, §39 and *CHEZ Razpredelenie Bulgaria AD v Komisia za zashtita ot diskriminatsia (Nikolova, third parties)* (Case C-83/14) [2015] All ER (EC) 1083, §§120–122.

[19] Advocate General Saugmandsgaard's Opinion in *Tele2 Sverige*, §AG209.

> *and where any of the information referred to in section 7(1)(c)(i) is expressed in terms which are not intelligible without explanation the copy must be accompanied by an explanation of those terms.*

50. In *Dawson-Damer v. Taylor Wessing* [2017] EWCA Civ 74 the Court of Appeal confirmed that proportionality will, in appropriate cases, impose limits on the obligation to search for personal data (see §§74-79). However, the Court also stressed the weight that must be given to compliance with subject access rights:

> *Ezsias [v Welsh Ministers, unreported 23 November 2007] usefully shows that proportionality means that in appropriate circumstances there will be bounds to a search: the very words of section 8(2) assert that possibility. However, it is clear from the recitals to the Directive that there are substantial public policy reasons for giving people control over data maintained about them through the system of rights and remedies contained in the Directive, which must mean that where and so far as possible, SARs [subject access requests] should be enforced. Moreover, most data controllers can be expected to know of their obligations to comply with SARs and to have designed their systems accordingly to enable them to make most searches for SAR purposes.*

51. In *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd and others* [2017] 3 WLR 811, the Court of Appeal confirmed that s. 8(2) and the *"principle of proportionality cannot justify a blanket refusal to comply with a SAR…*"[20]

52. The DPA 2018 does not contain a provision equivalent to section 8(2) DPA 1998. There is no general exemption under the DPA 2018 from subject access or other fundamental data protection rights based on disproportionate burden or administrative inconvenience.

C. SUBMISSIONS

53. Given the nature of the Inquiry, it is unlikely (save perhaps in exceptional circumstances) that any NPNSCP would wish to exercise rights such as the right to object, or the right to erasure / rectification against the Inquiry at this stage, given that they will (in accordance with the established order of evidence-gathering) have an opportunity to serve their evidence in reply when they have seen the evidence provided by State Witnesses.

54. Nevertheless, NPNSCPs do have a specific right of access to their personal data. Some NPNSCPs may have submissions they would wish to make, e.g. about the safeguards necessary to secure adequate protection of their personal data when it is being processed by the Inquiry, including

[20] §100.

restrictions on disclosing it to third parties for the purposes of evidence gathering (see the NPNSCPs pragmatic proposals in this regard at §§119 *et seq.* below).

55. The essential point is that none of the rights granted under GDPR can meaningfully be exercised until a data subject: (a) is aware that their data are being processed; (b) knows what personal data are being processed about them; and (c) knows the nature of that processing. It is a matter of concern for many NPNSCPs that their personal data is continuing to be processed by the Inquiry, including by being provided to police witnesses, before data subjects have seen the data, been given any information about it, or been put in a position where they can exercise their rights in relation to it.

56. In regard to third parties, the concern is that they may never even know that their data is being processed, or may only find this out if their data is made public.

57. The NPNSCPs consider that the Inquiry's current and/or proposed approach to: (a) processing of special category data; (b) notification to third parties; and (c) evidence gathering / non-disclosure / compliance with subject access requests, is incompatible with the GDPR. The points are developed below, together with the NPNSCPs' suggestions for a GDPR-compliant approach.

(1) Legal test applicable to processing of special category data

58. The Inquiry has recognised in the Privacy Notice that the GDPR applies (see §12 above). However, the Hearing Note refers to paragraph 12(c) of Schedule 6 DPA, which amends Article 9(2)(g) GDPR. Yet that provision applies to *"other general processing"*, i.e. processing outside the scope of the GDPR and covered by the "applied GDPR" (see section 22(4) DPA 2018).

59. Paragraph 12(c) of Schedule 6 DPA 2018 substitutes Article 9(2)(g) with the following:

> *processing is necessary for reasons of substantial public interest and is authorised by domestic law (see section 10 of the 2018 Act);*

60. This omits important elements of Article 9(2)(g) of the GDPR, including the requirement that relevant national law should respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

61. Given the reference to the 'applied GDPR' provisions, the Hearing Note does not grapple with the issue of what suitable safeguards and measures to respect the fundamental rights of all data subjects, including the NPNSCPs, need to be put in place (see further §§65 *et seq* below).

62. As set out above, under Article 9(2)(g) GDPR, the processing of special category must be necessary for the purposes of the exercise of the Inquiry's functions as a public inquiry; necessary for reasons of substantial public interest; proportionate; respect the essence of the right to data protection; and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

63. Certain aspects of the Inquiry's current approach or proposed approach do not meet these requirements. In particular, the approach to notification, and proposals for dealing with third party disclosure, addressed below, do not satisfy the EU law requirements of strict necessity and proportionality, including the principle that no less restrictive and equally appropriate approach is possible.

64. It is also not currently apparent how the Inquiry proposes to:

    a. Identify whether personal data is special category data;

    b. Consider whether such data is of particular sensitivity and/or whether its sharing (e.g. with other core participants), or public disclosure, might have a particularly adverse impact on the individual, such that the processing may not be proportionate;

    c. Identify whether data has been made public by the data subject, or is otherwise in the public domain, which is a relevant consideration for the application of Article 9 GDPR[21] and any proportionality exercise; or

    d. Consider whether in certain cases it should adopt specific safeguards and measures to respect the fundamental rights of data subjects, including NPNSCPs and third parties.

(2) Third party personal data

(i) The Inquiry's approach to notification and redaction of third party data

[21] Article 9(2)(e) GDPR.

65. On its website[22] the Inquiry has published a table with details of SDS officers whose cover names have been confirmed by the Inquiry, with provisional information about some of the groups/areas of deployment. This information is provided *"…to enable members of the public to identify whether they may have known officers who were deployed undercover and to prevent cases of mistaken identity. They are not intended to be a comprehensive list of groups with which the officer may have interacted, and do not constitute a factual finding by the Chairman that any group was or was not targeted…"*

66. The webpage provides limited, high-level information, which is not searchable by reference to specific dates. It does not purport to provide information enabling all those whose data are being processed by the Inquiry to find out that this is the case.

67. The NPNSCPs have asked the Inquiry to compile a more complete database, identifying the names of all the groups affected by the undercover policing being investigated by the Inquiry (see, for example, the NPNSCPs' email of 8 June 2018). The Inquiry's position has been as follows (letter of 2 July 2018):

> *Though over 1,000 groups are referred to in Special Demonstration Squad documentation, this does not necessarily mean that each group was infiltrated by an undercover officer. The Inquiry releases the names of main groups infiltrated with the name of the relevant officer when cover names and dates are released. This is in order to assist members of the public, including Core Participants, to identify whether or not they met the undercover police officer in question and come forward to assist the Inquiry with evidence. Information about the specific activities will become public as the work of the Inquiry progresses, notably as we move towards the public hearings detailed in the Hearings Schedule at paragraph 82 of the Strategic Review…*
>
> *As more cover names are published further groups will be added to the Inquiry's cover names table.*[23]

68. The Inquiry has said that it will publish only the *"main targets"* of specific deployments (letter 16 November 2018).

69. §26 of the Restrictions Protocol summarises the procedure and approach being adopted by the Inquiry in respect of redacting material for publication alongside and/or after the completion of the third-stage of its evidence gathering process. It explains that:

> *(i) Irrelevant and/or unnecessary personal information will be redacted by the Inquiry legal team (paragraphs 27 and 28 below).*

[22] At https://www.ucpi.org.uk/cover-names/
[23] Emphasis added.

(ii) Core participants and witnesses will have the opportunity to consider references to themselves in documents which the Inquiry proposes to use at the point in time when they are provided to them for the purposes of making a witness statement. They will then be able to make any application for a restriction order over such information (paragraph 29).

(iii) Persons who are neither core participants nor witnesses will be contacted by the Inquiry, unless in all the circumstances it would be disproportionate to do so, and given the opportunity to make an application for a restriction order over any relevant and necessary personal information (paragraph 32).

(iv) References to relevant and necessary personal information relating to persons whom it would be disproportionate to contact will be considered for redaction by the Inquiry legal team. The Inquiry legal team will decide whether to provisionally redact references to such persons applying the relevant legal principles and mindful of the fact that the person affected will not have had an opportunity to apply for a restriction order (paragraph 33).

(v) If any issue arises which is not expressly covered by the protocol the Inquiry legal team will decide how to deal with it and will do so in a way which complies with the affected person's Article 8 rights, the Data Protection Act 1998 and the duty to act fairly (paragraph 34).

70. §§32-34 provide further detail on how the Inquiry will consider whether to contact third parties and/or redact their data:

32. Where a document contains relevant and necessary personal information about a person who is neither a core participant nor a witness then the Inquiry will consider whether it is conceivable that an arguable application for a restriction order might be made, and if so whether the person affected is readily contactable. In cases in which those two conditions are met, the person will be contacted and afforded the opportunity to make an application for a restriction order before further dissemination of the personal information about that person in the document.

33. In cases where the non-core participant, non-witness is not readily contactable then the Inquiry legal team will decide whether or not the information should be provisionally restricted having regard to the legal rights referred to in paragraphs 25 and 26 above and mindful when doing so of the fact that the individual concerned is not able to make his or her own application. In considering whether a person is readily contactable, the Inquiry will have regard to the risk of intrusion into private lives which may arise if documents are disclosed to the wrong person as a result of incomplete information, and to the intrusion inherent in contacting individuals.

34. In any eventuality relating to privacy which is not expressly covered above the Inquiry legal team will exercise its judgment as to how best to proceed having regard to the need to act in accordance with the legal obligations set out at paragraphs 25 and 26 above. The Inquiry legal team may refer any question arising from such an eventuality to the Chairman.

71. Thus, on its current approach the Inquiry will only seek to contact third parties where they are *"readily contactable"* and it is *"conceivable that an arguable application for a restriction order*

might be made". In other circumstances, the Inquiry intends to exercise its judgment on a case-by-case basis.

72. It is also clear that, having reviewed some of the material, the Inquiry is concerned about the implications of dealing with the large amount of personal data in the documents it is holding, reflecting the sheer scale of the invasion of privacy committed by undercover police officers.[24] The Hearing Note identifies the problem as follows:

> *5. This creates a problem for the Inquiry and, potentially, for those named in the reports. The problem for the Inquiry is how to deal with the data protection and privacy rights of those named. It will not be practicable for the Inquiry to attempt to contact all of them, or even many of them. If they cannot be contacted, they may be unaware of the possibility that their names may feature in the Inquiry's investigation and may be disclosed to others and/or published at or after a hearing…*
>
> *6. In most instances, the reports contain references to individuals, either as participants in private meetings or as the subject of observations by others speaking at them. The removal of names and other identifying features from the documents would result in documents so heavily redacted as to be incomprehensible. Public understanding of them would be much diminished if they were to be released in that form…*

73. In practice, this raises at least three issues:

a. What, if any, further steps should the Inquiry take to notify third parties that their data is being processed / they are affected by the deployments under investigation?

b. If direct notification is impossible, what other steps should be taken to enable third parties to identify whether they may be affected (and may therefore have relevant evidence to give to the Inquiry)?

c. How should the Inquiry strike the balance between privacy (and fundamental data protection rights) and the need for openness on the part of the Inquiry? In short, when and what type of data can it disclose publicly / to other core participants?

74. §9 of the Hearing Note sets out a number of proposed ways forward, as follows:

> *Given that it is impracticable to contact all, or even many, of those named in intelligence reports, to invite them to apply for a restriction order in respect of their name and, possibly, other identifying details, the following options, or some combination of them, appear to be open:*

[24] See Hearing Note, §§1-4.

> *(i) hearing all but general evidence about deployments in private, within a "confidentiality ring";*
>
> *(ii) redacting all lists of names from reports, but leaving in all references to individuals in the text of reports;*
> *(iii) publishing details of the dates of reporting by individual officers and of the subdivisions of the groups on which they reported, in advance of hearings, so as to permit those who believe that they were present to apply for a restriction order in respect of their name and/or other details reported on;*
>
> *(iv) publishing a limited selection of redacted reports, based on those which appear to the Inquiry to be most relevant; and*
>
> *(v) providing to all core participants and eventually publishing an unredacted set of relevant reports…*

(ii) Existing approach does not comply with Article 14 GDPR

75. The Inquiry is understandably concerned about the burden of having to contact every individual whose personal data appears in the documents under consideration, and the delay and difficulties that might arise.

76. However, the starting point must be to find an approach to notification that is consistent with the Inquiry's obligations under Article 14 GDPR. As set out above, the notification obligation may only be derogated from where the provision of the Article 14 information "*proves impossible or would involve a disproportionate effort*", in which case "*the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available*". A blanket approach is not permissible.

77. In particular, it is not permissible to adopt the approach that third parties will only be notified where they are readily contactable and it is conceivable that an arguable application for a restriction order might be made. In principle, every individual whose personal data is being processed by the Inquiry is entitled to be notified, in order that they can exercise their data protection rights. The scale of the undercover activities engaged in by the police cannot justify a failure to take proportionate steps to comply with the Inquiry's legal obligations now. In every case, a proportionate effort must be made to notify data subjects of the ongoing interference with their fundamental rights.

78. In cases where it "proves impossible" to make contact, or where further efforts to do so would be disproportionate, the Inquiry must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information (about the processing) publicly available. At present, the very limited information on the Inquiry's website is inadequate

and would not enable individuals to identify whether they were likely to be part of a group that was reported on, such that their data may be being processed by the Inquiry. As set out below, the information that should be published must be more comprehensive, including (at least) the names of all groups reported on (i.e. not just those actually 'infiltrated'), together with at least approximate dates and locations.

79. None of the proposals set out in §9 of the Hearing Note adequately address the issue of compliance with the data rights of third parties. Many of the proposals also raise separate concerns about the potential impact on the ability of the Inquiry effectively to fulfil its object and purpose in an open and transparent way. Certain of the proposed measures would lead, in effect, to a closed inquiry.

(iii) NPNSCPs Pragmatic Proposals – notification

(a) Publication of all groups reported on by sub-division / branch and dates

80. As an immediate practical step, the Inquiry should compile and publish on its website, subject to any applicable restriction orders, the names of all of the groups *reported on* within the documentation reviewed to date, including the sub-division / branch and the time period during which the reporting occurred.

81. This public database should then be updated on a routine basis as the Inquiry processes the documentation it has obtained. It is important that this database should include all groups about whom information was reported, not just those groups currently classed by the Inquiry and/or the state CPs as having been 'infiltrated': the personal data of those affected is being processed by the Inquiry, regardless of whether their group or organisation was the main target of a deployment, was 'infiltrated', or was reported on.

82. The Inquiry should take steps to ensure that this list of groups is widely publicised on a regular basis, so that it is brought to the attention of as many affected members of the public as possible. In particular, the Inquiry should publicise the database through news outlets to ensure that individuals are prompted to visit the website. Further, the database should be searchable, so that anyone who is concerned that their data may be held is able to ascertain quickly and easily whether the group(s) they were involved in were reported on during a relevant period. And the Inquiry should make clear how individuals who consider that they may have been affected can contact: (i) the Inquiry; (ii) support organisations such as the Undercover Research Group (**"URG"**); and/or (iii) relevant representatives of the existing NPNSCPs.

83. This would be a first, proportionate and appropriate step towards complying with the notification and publication obligations that arise in relation to the personal data of third parties that the Inquiry is processing.

(b) Pro-active contact by the Inquiry

84. The Inquiry is under a duty to notify individuals that their personal data is being processed unless it proves impossible to do so or involves disproportionate effort.

85. As set out below, the NPNSCPs, their representatives, and the groups supporting them, are ready to provide assistance, where appropriate, to the Inquiry. There are circumstances in which the Inquiry could appropriately call upon the expertise and knowledge of the NPNSCPs and organisations like URG to try to make contact with individual data subjects, where the Inquiry is otherwise unable to do so. However, the Inquiry cannot contract out its responsibilities under Article 14 GDPR. In principle, the Inquiry must conduct at least some initial assessment of whether individual data subjects are capable of being contacted, and assessing whether the information on the updated database suggested above is capable of indicating to the individuals in question that they are affected by the Inquiry's data processing.

86. The degree of effort that the Inquiry must make to contact individuals requires a case-by-case assessment. However, on the examples raised in Counsel to the Inquiry's Annex A, the NPNSCPs make the following observations:

a. Barbara Bennett, Gianpreet Grewal and Harald Hough are all easily contactable. Further, given that they are public figures, it is at least possible that publication of information about them by the Inquiry may receive media attention. They should definitely be contacted by the Inquiry and given the opportunity, should they wish it, to see their personal data prior to its further processing, including by disclosure to state witnesses (see the proposed framework for disclosure below).

b. Arthur Anderson and Chris Carter both appear to be individuals from whom the Inquiry may wish to receive evidence if they are willing to give it. Annex A states that the Inquiry believes it will be able to trace CC. It should do so and should not wait until tranche 3, given that his personal data is being processed and referred to in tranche 1. Annex A, question 7, asks whether the Inquiry should ask CC whether he has contact details for AA. The answer is yes; this question is addressed below in submissions on the assistance that the Inquiry may be able to obtain from the URG and NPNSCPs.

c. Derek Dentocole appears to be dead. In the example given in Annex A the information recorded about him concerns a minor conviction, which may have been spent. This appears to be unlikely to be of sufficient relevance to the Inquiry, or of sufficient severity to engage the Article 8 rights of DD's family, so as to require that the Inquiry take pro-active steps to contact DD's family. (The position is likely to be different if information were recorded about a deceased individual which was of greater relevance to the Inquiry and likely to cause significant distress to the deceased's family.)

d. Emma Evans is someone who is likely to have relevant evidence to give. If the Inquiry cannot make contact, it would be appropriate for the Inquiry to approach URG or relevant NPNSCPs, to see if it is possible to contact EE and ask her whether she wishes to make contact with the Inquiry.

e. As to Officer FF1234, no private information is being processed about the officer, only his public shoulder number. In theory, this may be personal data in the hands of the Inquiry, if the Inquiry has other information that identifies this officer, and this would therefore give rise to an obligation of notification. However, assuming that the Inquiry does not have other personal data, or does not propose to further process it, it may not be necessary for the Inquiry to make specific effort to contact the officer.

f. John Jackson – according to Annex A, JJ is entirely untraceable online. If this is the only mention of JJ/South West London University Students' Revolutionary League in the material held by the Inquiry, the provision of the more detailed and publicised database discussed above, providing the list of groups/sub-divisions and relevant dates is likely to be an appropriate and proportionate measure in place of direct notification. If, however, there is more significant reporting in relation to JJ / USRL, then the Inquiry should seek assistance from URG and/or other NPNSCPs who may be able to trace him (see below).

g. Kelvin King and Lynette Leigh are said to be untraceable and are only referred to as having attended the meeting. It is likely that KK is dead given that he was in his early 60s in 1979. In such circumstances, the provision of the improved public database described above would likely qualify as appropriate and sufficient notification.

87. In respect of Annex B:

a. For all of those who have CP status, the suggested approach to disclosure is set out in submissions below;

b. Carolyn Crump and Harley Hendricks are not CPs, but it is said that they may be witnesses in the Inquiry. The Inquiry should adopt the same approach to disclosure as set out in the "disclosure" section below in respect of NPNSCPs.

c. Brighton Reform Group, Campaign for Change, Justice Always Group, Women's Home, Women Today, Women Forever – all of these groups are mentioned in the report and are said not to have CP status. In respect of most of these groups, the provision of the improved database would likely constitute sufficient notification. However, additional efforts to trace those involved in What about Women Today and Women Forever should be taken, given that the report contains opinions about these groups that are likely to cause distress if publicised – i.e. the suggestion that those groups were *"using the family's grief for their own purposes"*.

d. New Age League – this group is also not a CP, but the distinction from the other groups is that NAL is recorded as having "*a well-known reputation for violence against property in order to achieve its aims".* This means that the Inquiry ought to give the group an opportunity to consider the information before it is published. It appears that a member of NAL, Gloria Gayle, is contactable. As long as the improved database is made available, it would probably be sufficient for the Inquiry to take specific steps only to contact her, given that she is the only member of NAL named in the report.

e. Elora Esposito is not a CP and nothing is known about her. The report simply records her as having been present at the meeting as the sole representative of the Justice Always Group. As with JJ (from Annex A above) it is unlikely to be necessary for the Inquiry to take further proactive steps to contact someone in those circumstances, if the improved database is available, unless perhaps there is further, more extensive reporting on EE / JAG in other reports.

f. Freya Fountain – apparently also not a CP (although not expressly stated). The report records her as having been a member of Women's Home and as having screamed at another person at the meeting and having accused them of being paid by police to sabotage the campaign. She is also said to have *"caused trouble"*. Given the negative comments about

FF, there is greater reason for the Inquiry to take steps to notify her than in relation to EE and JJ above. However, the extent to which it is necessary for the Inquiry to do so will again depend on the context, e.g. whether this is one-off mention, or if there is more extensive reporting about her. If it is a one-off mention, then publication and publicity on the improved database may be sufficient. If there is more extensive reporting of FF, proactive steps should be taken by the Inquiry to contact her.

g. Gloria Gayle – not a CP and unlikely to be a witness. She is said to be contactable. As set out above, a person in GG's circumstances should be contacted by the Inquiry and given disclosure as set out below, given what is recorded about her group having had a *"well-known reputation for violence against property"*, and other critical aspects of the reporting of her.

h. Inigo Irving – unknown person who is recorded in the report as having not been invited to the Argento Campaign's New Year's Eve event, because he (and FF) had *"caused trouble"*. It seems likely (subject to the content of other data held) that II falls into the same category as EE and JJ.

(c) Use of non-state groups (such as the URG) and non-state individuals to try to contact those who have been reported on

88. One of the issues raised in Annex A to the Note from Counsel to the Inquiry is to what extent the Inquiry can and should be asking the URG for assistance in trying to make contact with non-state individuals of potential interest to the Inquiry.

89. The NPNSCPs' view is that the Inquiry could benefit significantly from working with URG. URG has proven skills and experience in this regard. It has an extensive network of contacts and a trusted reputation within many of the groups who have been affected by the issues that the Inquiry is considering. It also has considerable experience of communicating sensitively and confidentially with non-state individuals who have been affected by undercover policing.

90. It is necessary for compliance with the Inquiry's notification obligations under GDPR, and also in the Inquiry's interests for the purposes of investigating its terms of reference, that it takes steps to ensure that as many people as possible who were reported on have the opportunity to ascertain that that was the case and to provide relevant evidence to the Inquiry should they wish to do so.

91. Subject to appropriate resources being made available to URG, and the Inquiry and URG agreeing an appropriate protocol, seeking help from URG would be an appropriate and proportionate step

for the Inquiry to take, and would materially improve the ability of the Inquiry to reach relevant data subjects / potential witnesses, and the scope and quality of the evidence overall.

92. Where appropriate, other NPNSCPs or their representatives could also provide assistance. Indeed, in some circumstances it may be preferable for non-official and non-state groups to make first contact with individuals of potential interest to the Inquiry whose data is being processed. Given the sensitivities involved, direct contact from the Inquiry may be unwelcome and distressing; some data subjects are more likely to engage if the initial contact is made through a non-state source.

93. The NPSCPs accordingly submit that:

a. For the purposes of taking proportionate steps to comply with its notification obligations, it is necessary and proportionate for the Inquiry to make limited disclosure of personal data about non-state individuals to the URG (and other groups / RLRs/ other non-state individuals, where appropriate) for the purposes of seeking to contact those individuals, or informing those reported on that their data is being processed, and enabling those with potentially relevant evidence to come forward, should they wish to do so.

b. The limited disclosure for these purposes could include: the individual's name; the group or groups with whom they were associated, and the dates of relevance to the Inquiry. The information would be provided to the URG (or other relevant groups / RLRs/ other non-state individuals) in confidence and for the sole purpose of attempting to contact the individual in question. This would be a limited (and, it is submitted,) proportionate interference with those third parties' rights;

c. The URG (or other group etc.) could use the information provided by the Inquiry to seek to make contact with the relevant individual, inform them that the Inquiry has relevant information about them, and tell them how to make contact with the Inquiry should they wish to do so. This would be done pursuant to a protocol or framework agreed between the Inquiry and the URG, which would also have to address the question of URG resources needed to enable it to carry out this work;

d. When contacted, it would be a matter for the individual whether they do in fact make contact with the Inquiry. Their contact with the URG or other organisation should be treated as confidential and the independence of URG / the other organisation should be maintained.

Any decision by the individual that they do not want their details or views communicated to the Inquiry would be respected by the URG / other organisation and the Inquiry.

(3) Disclosure / compliance with the right of access

(i) The Inquiry's approach to evidence gathering

94. The Explanatory Note, at §§5-10, summarises the steps that the Inquiry has taken and is taking to gather evidence since the issuing of the Restrictions Protocol on 30 May 2017. Broadly speaking, the evidence-gathering process involves three stages:

a. First, the initial process of obtaining, reviewing and processing of the police documents which appear to the Inquiry to be necessary and relevant to its terms of reference. During this process, the Inquiry will also determine any restriction order applications made by State core participants.

b. Second, the Inquiry makes requests pursuant to Rule 9 of the Inquiries Act 2005 (**"rule 9 requests"**) for witness statements from state witnesses. Alongside the rule 9 requests, the Inquiry has been providing, and intends to provide, un-redacted material which originated from the state witness or appears relevant to their evidence. The NPNSCPs have not had, and will not have, any opportunity to review the evidence, including their personal data, before that step is taken. The NPNSCPs understand that this process is ongoing in respect of SDS deployments, notwithstanding privacy concerns that have been raised by the NPNSCPs, and which are to be determined following this hearing[25]. At this stage, the Inquiry will also consider any restriction order applications made by state bodies in respect of the evidence.

c. Third, the Inquiry will approach members of the public and NPNSCP witnesses, requesting statements. This will only occur after the Inquiry has obtained witness statements from relevant state witnesses, and collected the *"associated relevant and necessary documents"*. The requests will be accompanied by a pack of documents, either in confidence or subject to a restriction order. That material will not contain all personal data processed by the Inquiry relating to the individual as it will have been subject to a necessity and relevance 'filter' (see below) by the Inquiry. It is only at stage 3 that the Inquiry will consider whether any redactions should be made to the material in accordance with pages 8-11, §§25-34 of the Restrictions Protocol (see §10 of the Explanatory Note).

[25] See email from the Inquiry dated 21 November 2018, as well as the Hearing Note.

95. Each of the three stages set out above will need to be completed for all of the deployments under consideration. As the Inquiry is taking an officer-by-officer, and chronological approach, it will need to complete each of these three stages of evidence-gathering on multiple occasions.

96. In its letter of 13 July 2017, the Inquiry also explained that: *"... We anticipate that the point at which we seek evidence from a non-police non-state core participant may well be a point at which we are provided with evidence which gives rise to the need to seek further evidence from the police and/or to review earlier decisions about relevance and necessity…*". Thus, the approach adopted by the Inquiry is not intended to be, and could not in practice be, strictly linear.

(ii) Inquiry's Approach to subject access requests and assessment of 'necessary' material for evidential purposes

97. §1 of the NPNSCPs' submissions re disclosure of personal files, dated 31 May 2017, made the following request:

> *These submissions are made on behalf of the [NPNSCPs] in support of their request for disclosure, subject to redactions permitted by the Data Protection Act 1998, of personal files, including, but not limited to, any Special Branch file, Registry file, "pink file", personal file prepared by Special Branch, and/or 'nominal' file concerning an identifiable [NPNSCP] which is in, or comes into, the possession of the Inquiry.*

98. §5 of the submissions made clear that: *"all personal data in the possession of the Inquiry is disclosable to the data subject, subject to lawful restrictions. In other words, it is not only personal files that are disclosable, but also, for example, information which mentions an identifiable individual even if it is held in a file that does not relate specifically to that individual…"*

99. However, <u>at that stage</u>, the submissions limited the requests in the following manner:

> *… the [NPNSCPs] are at this stage making a more limited request for disclosure of personal files including, but not limited to, any Special Branch file, Registry file, "pink file", personal file prepared by Special Branch, and/or 'nominal' file concerning an identifiable [NPNSCP]. This is to enable [NPNSCPs] to have at least some information as soon as possible so that they can begin to know what was recorded about them and so that they can assist the Inquiry in its determination of the significance of that information to its terms of reference. Nothing in the present request for disclosure of personal files is intended to limit the obligation on the Inquiry to make more complete disclosure to [NPNSCPs] in due course.*

100. As set out in its letter of 7 July 2017, the Inquiry treated the 31 March 2017 submissions as subject access requests made under the DPA 1998. The Inquiry decided only to consider data which fell

within the description provided in the submissions as it would have been, in its view, disproportionate to consider all of the data held.

101. In response to the subject access requests, a very limited amount of data was provided to four NPNSCPs. The disclosure provided was described as comprising all of the information which the Inquiry was required to disclose to those individuals under the DPA 1998. No statutory exemptions were relied upon specifically by the Inquiry.

102. In a subsequent letter of 13 July 2017 addressed to all of the non-state RLRs, the Inquiry responded to the submissions dated 31 May 2017 in respect of disclosure of personal files. In doing so it addressed two separate issues.

103. First, it responded to concerns about its evidence-gathering process. The Inquiry set out again its proposed three-stage, iterative approach to evidence gathering, and referred to the necessity 'filter' it is applying:

> *The Inquiry is not prepared at this stage to deem all of the contents of any personal Special Branch file relating to a non–police non-state core participant which might exist as relevant and necessary on a blanket basis. The Inquiry will only decide that the contents of such a file (or some of the contents as the case may be) are relevant and necessary having reviewed the file. By way of example, there were four files which the Inquiry considered under the subject access request. Collectively, these contained a substantial quantity of material which appeared unlikely to be relevant and necessary, and a substantial (and partially overlapping) quantity of material which appeared likely to require consideration for redaction in due course in order to protect the privacy of non-police, non-state third parties.*
>
> *We do not consider that it is either necessary, or efficient, immediately to obtain and disclose provisionally restricted versions of any personal Special Branch personal file which might exist in relation to a non-state non-police core participant as advocated in your submissions…*

104. In respect of the subject access requests the Inquiry explained that:

> *The Inquiry recognises the importance of the Data Protection Act 1998 ('the Act') and the underlying fundamental rights to which it gives expression. It has conscientiously assessed, based on the information currently in its possession and on a document by document and line by line basis, what material it held which constituted personal data of the category requested and which fell to be disclosed under the Act.*
>
> *Conducting this exercise has inevitably proved to be a time consuming task for the Inquiry, requiring both legal expertise and the best understanding which we can bring to bear of the documents in their proper context. As a result, it has necessarily distracted considerable resources at all levels within the Inquiry from the substantive work of the Inquiry, including work investigating deployments affecting non-police,*

> *non-state core participants. Preparation of the four responses occupied over 130 hours of the time of the Inquiry legal team (counsel and solicitors) and over 30 hours' paralegal time. It is likely that our experience in preparing these responses will inform the Inquiry's approach to any future requests, having regard to section 8(2) of the Act.*[26]

105. In its correspondence to date, no exemption, other than section 8(2) of the Data Protection Act 1998 (the **"DPA 1998"**) has been referred to in response to the subject access requests. However, it is notable that the disclosure made to, for example, Helen Steel was very limited in comparison to disclosure of personal data that has been provided to another NPNSCP, Kate Wilson, in the context of proceedings in the Investigatory Powers Tribunal (**"IPT"**). This apparent disparity gives rise to concerns that the Inquiry may have: (a) relied on exemptions to justify non-disclosure which were not expressly identified, and/or (b) adopted too restrictive an approach to documents containing information about other individuals. In any event, the greater amount of personal data that has been provided to Kate Wilson through the IPT proceedings has underscored the importance of disclosure for enabling victims of undercover policing to know and understand the nature and extent to which their lives were infiltrated and reported on. The disclosure made to Ms Wilson has provided considerable insight into the degree of manipulation of her personal and family life, and what was reported about her by an undercover officer to senior officers.

106. Further, it is clear that the Inquiry is not proposing to conduct an assessment of the data it holds in order to determine whether any of that material constitutes the personal data of identifiable individuals. Instead, the Inquiry intends to disclose only to NPNSCPs, at a later stage, material which is deemed necessary for them to give evidence to the Inquiry (see, for example, the Inquiry's letter of 27 June 2018).

(iii) Non-compliance with, and preventing of the exercise of, fundamental rights by NPNSCPs

107. As set out above, the rights of NPNSCPs under the GDPR and DPA 2018 are more extensive and more specific than under the 1995 Directive and the 1998 Act. The Inquiry's evidence-gathering process is not a substitute for compliance with those rights. In particular, a refusal to comply with a subject access request submitted under the GDPR must be dealt with in accordance with the legislation and the principles set out above. The Inquiry cannot rely on resource or generalised proportionality concerns to refuse individual subject access requests.

108. The combined impact of the Inquiry's approach to evidence-gathering, and its denial of subject access rights, is that NPNSCPs are to be kept in the dark about what personal data of theirs,

[26] Emphasis added.

including special category data, is being processed by the Inquiry. Only at some later stage, after state witnesses and others have already had access to the personal data, will some disclosure (based on a necessity analysis) be provided.

109. This approach is not consistent with fundamental data protection rights and is unlawful. The GDPR does not permit the Inquiry to refuse data subject access requests by reference to what material is deemed relevant and necessary to the Inquiry's investigation. There is also no exemption that allows the Inquiry to refuse to deal with such requests at all, simply because of the effect on the Inquiry's timetabling. It is not strictly necessary, in an EU law sense, for the NPNSCPs' right to access their personal data to be subordinated or overridden by the Inquiry's preferred evidence-gathering process. They are separate processes. If subject access requests are made now under Article 15 GDPR, the Inquiry must deal with them.

110. The NPNSCPs submit that, to give effect to their rights in a proportionate and appropriate way, it is necessary for NPNSCPs to be provided with access to their personal data, as identified in the relevant phase of material under consideration by the Inquiry (subject only to the documents being provided in the first instance to relevant personnel acting on behalf of state bodies for the purposes of determining whether a restriction order should be applied for).

111. The NPNSCPs have previously made submissions asking the Inquiry to adjust its approach in order to allow them to see their own personal data before it is further processed by being given to state witnesses. To date, the Inquiry has refused such requests. However, such a decision to refuse access to the relevant personal data now is unlawful in the absence of some identifiable exemption in the GDPR which is applicable.

112. The additional problem with the current approach is that it prevents data subjects from exercising their other data protection rights. For example, NPNSCPs may not know that there are grounds to apply for a restriction order in relation to what is said about them in the documents. Each individual NPNSCP has the right to seek the restriction of, or otherwise object to, processing of their data. If a particular piece of information is particularly sensitive or outrageous (including information that may be inaccurate and damaging), the data subject may wish to ask the Inquiry to impose additional protections on how that information is processed internally by the Inquiry and/or state witnesses (e.g. limits on access via databases; restrictions on access by state witnesses that no longer work for the police, etc.). NPNSCPs cannot do so without knowing what data is held about them.

113. There is, moreover, no compelling reason why the iterative approach that the Inquiry has adopted cannot be adjusted to allow NPNSCPs to access their data earlier in the process, without requiring a major departure from the three-staged evidence gathering approach. As set out below, providing access to personal data at an early stage is not only necessary to comply with the GDPR; it will enable NPNSCPs to begin the process of preparing their own evidence. The NPNSCPs do not advocate any change to the established order in which evidence is to be provided to the Inquiry. It is right that NPNSCPs should be asked to provide their evidence after they have been provided with relevant state evidence. However, affording access to their own personal data at an earlier stage will enable them to at least begin to prepare their evidence, gather documents etc., leading to greater efficiency later in the Inquiry.

114. In short, and as explained below, there are less restrictive alternative measures available to the Inquiry, which can and should be explored.

(iv) NPNSCP's Pragmatic Proposals on disclosure and subject access

(a) Amended evidence-gathering process

115. The Inquiry should draw a clear distinction between disclosure of personal data, including mixed personal data, to data subjects, and publication of that data to the wider world.

116. As set out above, subject to any restriction order, documents which name a non-state individual (A) who is either a CP, or who is otherwise in contact with the Inquiry following the notification process discussed above, should be disclosed to that individual before the personal data is further processed by being provided to state CPs and/or witnesses for the purposes of evidence gathering. The only purpose for which such documents should be provided to state parties prior to disclosure to those whose personal data they contain (and who are in contact with the Inquiry following reasonable notification) is for the purposes of the state party seeking any lawful restriction order.

117. Disclosure of A's personal data to him/her before it is disclosed to state CPs and/or witnesses is necessary to give effect to the essence of the data protection rights:

a. It enables the data subject to exercise a measure of control over his/her personal data in so far as s/he would be in a position: (a) to challenge any overbroad disclosure of the data for the purposes of evidence gathering and (b) make submissions about appropriate measures attached to the further processing or disclosure of the data – e.g. not permitting those to whom it is disclosed to retain copies; and

b. Those who have had their personal data systematically collected and stored by the state are the victims of gross invasion of privacy. In some cases, the ongoing uncertainty and lack of information as to what has been reported and recorded, and is still being processed, is causing recognised psychiatric harm and distress. Prioritising the disclosure of personal data to the data subjects would be a significant step in beginning to address that harm, as well as a proportionate measure to comply with the fundamental right to privacy.

118. It is acknowledged that this will require some adjustment to the Inquiry's current approach and milestones. It may have an impact on the start date of public hearings. However, given that disclosure will have to be made to non-state CPs and witnesses at some point, and the process will inevitably be iterative, bringing forward the process of disclosure to NPNSCPs should not lengthen the process overall, or seriously undermine the effectiveness of the Inquiry.

119. The NPNSCPs propose the following framework:

a. Consideration of documents by state bodies for the purposes of applying for redactions only. This happens anyway under the redaction protocol;

b. Disclosure of documents containing personal data to the data subject where the data subject is either a CP, or is in contact with the Inquiry following the notification process described above. The suggested process for dealing with mixed personal data – i.e. where a document refers to more than one identifiable individual – is set out below. Recipients of this disclosure should then be given a short window (for example, 2 weeks (although the length of time required will depend on the volume and complexity of the material provided)) in which to make any submissions or applications, e.g. relating to onward disclosure of their personal data for the purposes of obtaining witness statements from state witnesses, or conditions of security under which disclosure should be made. Other than perhaps in exceptional circumstances, it seems unlikely that any NPNSCP would at this stage consider exercising a right to rectification, erasure etc. A longer timetable should be given for submissions as to redactions for the purposes of public publication at the time of relevant hearings, which will raise different issues – see below;

c. Disclosure of documents to state witnesses for the purposes of evidence gathering after the completion of the disclosure process to the affected data subjects; and

d. Once state witness statements have been obtained, these would then be disclosed, subject to any applicable restriction order, to non-state CPs and potential non-state witnesses to

whom they are relevant, together with any further relevant documents, for the purposes of obtaining non-state evidence.

(b) 'Confidentiality rings'

120. The Hearing Note and the Explanatory Note make clear that one of the practical issues troubling the Inquiry is how to deal with documents that refer to more than one identifiable non-state individual. Resolution of this issue is critical to ensuring protection for the privacy of non-state individuals, whilst at the same time ensuring that the whole Inquiry is not driven behind closed doors.

121. The NPNSCPs' proposal, designed to be a proportionate attempt to balance competing interests, is that a document containing mixed personal data should be disclosed to the NPNSCPs and readily contactable individuals who are identified in it in unredacted form (subject to any restriction order) and under conditions of confidentiality, subject to the following principles:

a. The overriding principle should be that where personal data referred to in the document would clearly have been known to the other individuals identified in the document – e.g. because it was something said openly at a meeting at which they were all present – it should not be redacted for the purposes of disclosure to those individuals;

b. Where it is unclear whether information would have been known to others who are also identified in the document – e.g. because it is the author's interpretation of the situation, or something that was conveyed in a side conversation to which others identified in the document were not privy - then that information should be redacted for the purposes of disclosure to the other identified individuals, if it is information about:

   i. health (interpreted broadly);
   ii. family circumstances;
   iii. sexuality and/or sexual relationships;
   iv. criminality (other than convictions which are readily identifiable as not spent);
   v. political or other views expressed or manifested by an identified individual which are contrary to those expressed or manifested by that individual's participation in the event(s) recorded in the document.

122. The NPNSCPs have annotated Annex A to the Explanatory Note to show how the above principles could be applied in practice for the purposes of disclosure to those identified within

that documents. Applying the above principles to Annex B would not require any redactions to be made for the purposes of disclosure to individuals mentioned by name within it.

123. As noted above, the mixed personal data disclosed under this process should be disclosed under conditions of confidentiality. However, if a data subject to whom the disclosure is made wishes to disclose any part of the confidential information for good reason – e.g. for the purposes of informing someone else who is named in the document, but with whom the Inquiry does not currently have contact – then s/he should be permitted to apply to the Inquiry for permission to do so.

124. The NPNSCPs approach to "confidentiality rings" in fact accords broadly with the approach outlined by the Inquiry in §31 of the Restriction Protocol, save in respect of the timing of disclosure.

(c) Publication of third parties' data

125. If the above processes are adopted, then by the stage at which the Inquiry is considering redactions for the purposes of publication to the wider world, NPNSCPs, non-state witnesses and other non-state individuals who have made contact with the Inquiry following the notification process will have had disclosure of the documents containing their personal data and will have been in a position to make informed and effective submissions about what should and should not be put in the public domain.

126. The more difficult issue then arises in relation to individuals whose personal data is contained in documents that the Inquiry wishes to publish, but who have not had any contact with the Inquiry, because attempts to make contact have proved unsuccessful and the Inquiry has deemed it to be disproportionate to take further proactive steps to contact them.

127. There is no single approach that can be adopted to third party data falling within this category. Instead, the NPNSCPs propose the following framework:

a. In practice there are different levels of identifying information. If a person's surname is redacted, in most cases that may be sufficient to ensure that they are not readily identifiable to members of the general public.

b. The starting position should be that the Inquiry will redact surnames and other personal information that would enable identification of individuals by members of the general

public by means of internet search, unless the information is already in the public domain in any event – for example, political views that the individual has put in the public domain.

c. Exceptions would need to be made where a person has an unusual first name, or is otherwise easily identifiable from other references to them in the text – e.g. reference to a position they held – in Annex A, the example is that Barbara Bennett was group treasurer of the South West London Revolutionary Campaign Movement in 1979, which might make her identifiable via a Google search, even if her name was redacted. Thus, the Inquiry would need to exercise its discretion in determining where information going beyond an individual's surname would enable them to be readily identifiable to the public.

d. In respect of information which would enable a non-state individual to be identified by those with pre-existing knowledge, a further exception to the above approach would need to be made where the data falls within one of the sensitive categories identified in §121.b above and is not information that the individual has already put into the public domain. Where personal information is redacted because it falls within one of these categories, it should be gisted so as to make clear where sensitive and/or inappropriate information has been collected and retained – e.g. "comment on X's family circumstances"; "reference to X's sexuality".

128. The NPNSCPs have produced separate versions of the Inquiry's annexes A and B to illustrate how this approach would apply to those documents.

GERRY FACENNA QC
Monckton Chambers

RUTH BRANDER
Doughty Street Chambers

JULIANNE KERR MORRISON
Monckton Chambers

24 January 2019