IN THE MATTER OF THE UNDERCOVER POLICING INQUIRY

SUBMISSIONS ON BEHALF OF THE
NON-POLICE, NON-STATE CORE PARTICIPANTS
PRIVACY HEARING, 25 MARCH 2019

INTRODUCTION

1. These submissions are made on behalf of the Non-Police, Non-State Core Participants (**"the NPNSCPs"**)[1] for the further hearing on privacy / data protection issues listed for 25 March 2019. They should be read together with the submissions of the NPNSCPs for the last privacy hearing, dated 24 January 2019.

2. The Inquiry has issued two sets of directions / notes to assist parties in preparing for the second privacy hearing. The first note, dated 12 February 2019 (**"the Exemptions Note"**), explains at §1 that the purpose of the forthcoming hearing is to consider:

   a. the extent to which Articles 13, 14 and 15 of the GDPR apply to the work of the Inquiry; and

   b. the practical effect of any resulting obligations.

3. The Exemptions Note repeats the Inquiry's provisional view that it is within the scope of paragraph 7, Schedule 2, Part 2, to the Data Protection 2018 (**"DPA 2018"**).

4. §6 of the Exemptions Note sets out the three issues on which the Inquiry invites submissions, broadly: (1) the extent to which Articles 13, 14 and 15 GDPR apply to the work of the Inquiry; (2) insofar as they do and no exemptions apply, what obligations do they impose and with what practical implications for the evidence gathering exercise; and (3) if an exemption applies, what obligations do Articles 13, 14 and 15 GDPR impose, and with what practical implications for the evidence gathering exercise? Those questions are addressed below.

[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.

5. The second note issued by the Inquiry, dated 26 February 2019, provides an outline of the evidence gathering process that the Inquiry is conducting and intends to conduct unless persuaded otherwise at the hearing (**"the Process Note"**).

Summary & preliminary observations

6. These submissions are organised as follows:

   a. Part I addresses the provisional view of the Chair that paragraph 7, Schedule 2, Part 2, DPA 2018 is engaged in respect of the Inquiry's data processing, as well as the other exemptions raised by other parties. The NPNSCPs position, in summary is that there is no exemption which is engaged in respect of all of the Inquiry's data processing. Further, and in any event, irrespective of whether an exemption is so engaged, the Inquiry still has to comply with the requirements of strict necessity and proportionality. This means that the Chair should adopt the pragmatic proposals set out in Section C(iii) of the NPNSCPs' written submissions dated 24 January 2019.

   b. Part II addresses the implications of the legal arguments set out in Part I for the evidence gathering process set out in the Process Note.

   c. Annex A to these submissions provides an overview of the legislative history of paragraph 7, Schedule 2, Part 2, DPA 2018.

7. The NPNSCPs also make the following preliminary observations:

   a. In her written statement to the House of Commons on 12 March 2015 the then Home Secretary stated that the Inquiry would "*review practices in the use of undercover policing, establishing justice for the families and victims and making recommendations for future operations and police practice*". Those words were repeated by in the former Chair's Opening Remarks in July 2015.

   b. It is fair to say that, almost four years on from the announcement of the Inquiry, many of the victims, represented within the NPNSCP group, have limited faith in the ability of this Inquiry to deliver the truth about what was done to them, let alone the justice that they were promised. Many have feelings of anger, confusion and distress arising out of the fact that they still do not know the truth about the extent of the State-sanctioned invasion of their rights. The fact that highly personal information about them – information which they

have not seen and which there is no prospect of them seeing anytime soon – is being pored over by the former police officers who spied on them, by the Inquiry, and by other police employees, lawyers and others is understandably very distressing.

c. It is entirely at odds with the purpose of data protection laws, and the fundamental rights to which they give effect, that such processing and sharing of personal data should take place without the individuals concerned having any access to it, or any control over what is done with that data, or indeed any information at all about the nature and scale of what is recorded about them.

d. The Inquiry has spent the best part of three years, and millions of pounds, on work concerned with protecting, amongst other rights, the privacy rights of former undercover officers.[2] That process is set to continue, given the Inquiry's firm resolve that no disclosure of any material can be made to any non-state person (i.e. the families and victims to whom the Home Secretary referred) before undercover officers have had the opportunity to produce witness statements, including to inform a redaction process via those witness statements. There is no indication as to how much longer that part of the process will take, and the anticipated start date of hearings has been put back to 2020, in part in order to accommodate it.

e. In contrast to the attention and resources that have been devoted to the protection of state interests and the interests of former undercover officers, the Inquiry is contending that it would result in unacceptable delay and waste of resources for it to take steps to ensure that non-state individuals – even those who are readily contactable – have an opportunity to see the information that has been collected and recorded about them, and make any relevant representations about it, before that data is disclosed to others.

f. When it ultimately is disclosed to those individuals, the protection proposed by the Inquiry is that such data will be subject to a confidentiality ring, in general without more specific redactions. But confidentiality rings were expressly rejected by the Inquiry as insufficient to protect the rights and interests of the former officers: see Legal Principles Ruling §170. Given that most orders restricting disclosure of officers' cover names have been granted on the basis of the need to protect former officers' privacy rights, it is unfair for the Inquiry

[2] The restriction order process in respect of former UCOs has been underway since the May 2016 Legal Principles Ruling. Whilst it is not known exactly how much of the Inquiry's £13.2million expenditure to date is attributable to restriction order applications founded on protection of the private life rights of former UCOs it is reasonable to assess that it is several millions, given the amount of the Inquiry's time that has been addressed to such applications.

to take a less careful approach to its obligation to protect the privacy rights of those who were spied on.

g. For reasons set out further below, and in the submissions made at the first privacy hearing, the Inquiry's failure to give effect to data protection rights, including notification and subject access rights, is not only unfair but unlawful. The Inquiry and the NPNSCPs have a shared interest in adopting procedures that recognise, and give effect to, the fundamental data protection rights of those whose personal information the Inquiry is processing. Those rights must be respected, regardless of the Inquiry's preferred approach to disclosure of evidence.

h. It is in recognition of the difficulties that the Inquiry faces, and with the shared aim of minimising delay, that the NPNSCPs, in their submissions of 24 January 2019, proposed a pragmatic process for disclosure of personal data and documents. The proposals allow for personal data to be cross-disclosed within confidentiality rings, with lawful and proportionate protection in respect of particularly sensitive data. Compliance with the law, including the principle of proportionality, can be achieved through the proposed notification process– see §§80-93 of the 24 January 2019 submissions; disclosure of personal data to data subjects who are in contact with the Inquiry - §119; and the use of confidentiality rings, subject to the principles set out in §121 of the 24 January 2019 submissions.

i. Those proposals are not put forward to make the Inquiry's life difficult. They have been carefully considered and debated within the NPNSCP group. They are feasible and proportionate. They would allow the Inquiry to begin the process of providing families and victims with the information that is the subject-matter of the Inquiry, and which is their own personal data. The proposals would have benefits for the Inquiry's overall objectives. They would substantially deal with the Inquiry's data protection obligations, and they would, at the very least, begin to meet the concerns about the capacity of the Inquiry to get to the truth and provide justice for families and victims.

PART I – APPLICATION OF GDPR & EXEMPTIONS

A. THE INQUIRY'S PROVISIONAL VIEW ON PARAGRAPH 7

8. The Inquiry's provisional view is that the Chair is "carrying out a function designed to protect members of the public against, inter alia, malpractice or other seriously improper conduct":

> …I am of the view that I am discharging a function that is designated as described in column 1 of the Table set out in paragraph 7 of Schedule 2, Part 2 to the Data Protection Act 2018. That function is conferred on me by an enactment and is of a public nature and exercised in the public interest. My function, therefore, meets the relevant condition specified in column 2 of the Table. Accordingly, it is my view that "the listed GDPR provisions" specified in paragraph 6 of Schedule 2, Part 2 to the Data Protection Act 2018 do not apply to the Inquiry to the extent that the application of those provisions would be likely to prejudice the proper discharge of my function.

9. Paragraph 7, Schedule 2, DPA 2018, provides, in material part, as follows:

> *Functions designed to protect the public etc*
>
> 7 The listed GDPR provisions do not apply to personal data processed for the purposes of discharging a function that—
>
> (a) is designed as described in column 1 of the Table, and
>
> (b) meets the condition relating to the function specified in column 2 of the Table,
>
> to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function.

Table

Description of function design	*Condition*
…	…
2. The function is designed to protect members of the public against— (a) dishonesty, malpractice or other seriously improper conduct, or (b) unfitness or incompetence.	The function is— (a) conferred on a person by an enactment, (b) a function of the Crown, a Minister of the Crown or a government department, or (c) of a public nature, and is exercised in the public interest.

10. The NPSPCs understand that the Inquiry intends to proceed on the basis that the proposed evidence gathering process is lawful, i.e. compatible with the GDPR/DPA 2018, because, to the extent that it may conflict with or curtail the rights guaranteed by, in particular, Articles 13, 14 and 15 GDPR, the Inquiry can rely on the paragraph 7 exemption.

11. At the last privacy hearing, the Chair recognised that if the previous Act, the Data Protection Act 1998 (**"DPA 1998"**) was still in force, it would be difficult to rely on s. 31 DPA 1998, the predecessor of paragraph 7. The relevant passage of the transcript reads:

> MR FACENNA: … Just on the question of the applicability of the [paragraph 7 exemption], I have to reserve our position on it at the moment. Obviously it has been raised for the first time with us. I would say this about it. It is an exemption which is essentially carried forward from the 1998 Act. Under the 1998 Act, it was under a heading of "Regulatory functions".
>
> THE CHAIR: It was, but that side heading has now been removed –
>
> MR FACENNA: The heading has been removed, I see that.
>
> THE CHAIR: -- and it is applied to other functions further down the paragraph.
>
> MR FACENNA: It is applied to a more specific set of functions which we would say, I suspect, all still fall under the general heading of "Regulatory functions".
>
> THE CHAIR: Yes.
>
> MR FACENNA: They relate to the regulation of charities, health and safety at work, maladministration by public authorities, investigation by the Competition and Markets Authority, that kind of thing.
>
> There is a question and one of the things we have not had the opportunity to do is for example to go back to Hansard on the 1998 Act and just to understand the history. There is a clear read across, I think ... our provisional position is that we would not necessarily accept that that exemption does apply –
>
> THE CHAIR: That comes as no surprise. Had it been made under the 1998 Act I would have perhaps found the provisional view that I have advanced difficult to justify…[3]

B. THE CORRECT APPROACH TO EXEMPTIONS

12. In §§43-48 of their written submissions for the last hearing, the NPNSCPs summarised the correct approach to applying exemption(s) to data protection rights, which are fundamental rights guaranteed by the EU Charter. Given the present focus on the extent to which any exemptions

[3] Transcript, pp. 222(7)-223(11).

apply to the Inquiry's data processing, it is important to set out in greater detail the correct approach as a matter of law.

13. Perhaps the key authority is *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB), in which Warby J set out the four-staged approach that a controller or court must apply in determining whether an exemption is engaged and, if so, the extent to which it can be relied upon in a given case to justify a refusal to comply data protection rights. That case addressed the prejudice-based exemption in the former s. 29 DPA 1998 (now to be found in paras 2 and 3 Schedule 2 DPA 2018). For ease of reference, the key passages of Warby J's judgment in *Guriev* are set out here (with underlining added):

> 37 Section 29 was considered in detail by Munby J, as he then was, in *R (Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin)*. He held, among other things, that it is for those who assert the exemption to show that their case comes within it: [99]. Ms Addy does not argue the contrary. Nor does she dispute Munby J's further conclusions (ibid.) that the applicability of the exemption must be proved convincingly, by evidence. The ordinary civil standard applies: *Robertson v Nottinghamshire NHS Trust* [2009] EWHC 1934 (QB), [2009] PTSR 421 [12] (Cranston J).
>
> 38 The first issue is whether CSD [the controller] has proved in this way and to this standard that the claimants' personal data were being processed by it for one of the specified purposes…
>
> 40… [the limited evidence available] clearly suggests three different kinds of investigation: civil, regulatory and criminal. It also tends to suggest that the primary aim of CSD's client and hence the main purpose of the investigations is, as one might suppose, the pursuit of civil remedies for the alleged "theft". So far as criminal matters are concerned, I am not persuaded that there is any evidence that CSD's activities include any crime prevention purpose, or the apprehension of offenders. I accept that it is likely that some of the personal data held by CSD relating to these claimants is held and has been processed for the purposes of detecting crime, or prosecuting crime. However, it is clear that those are not the only purposes for which CSD has been retained, and I am not persuaded that all the personal data it holds in relation to these claimants is or has been processed for those purposes.
>
> 41 I am not persuaded, either, that CSD has satisfied the second condition. It has not shown in relation to any, let alone all, the personal data of the claimants that it holds that the application of s 7 would be likely to prejudice any of the matters specified in s 29(1). …
>
> 42… More generally, …, I consider that there is force in Mr Weekes' submission that in substance what CSD are claiming is a blanket exemption from s 7 for organisations such as themselves, or for criminal investigators, and that he is right to argue that such an approach is wrong in principle.
>
> 43 What s 29(1) requires is "a selective and targeted approach to non-disclosure, based on the circumstances of a particular case": *Lord* [124]. The court is required to make a finding of fact based on those circumstances (*Lord* [87]). The evaluation must be structured. The factual issue here is whether compliance by CSD with the duty of disclosure (or some particular facet of the s 7 duty) would be likely to cause prejudice to the investigation of

the alleged crimes, or to the prosecution of the alleged offenders. As the Information Commissioner's Office explains in "Using the crime and taxation exemptions" at [10–13], a blanket approach to such an issue [is] not legitimate; to apply the exemption it is necessary to identify the prejudice, show how disclosure would cause that prejudice, and show that failure to apply the exemption would be likely to cause that prejudice. "Likely" here means a very significant and weighty chance of prejudice to the particular public interest: *Lord* [100]. What needs consideration in the present instance, therefore, is what disclosure would reveal, how the revelation would affect the proceedings, and whether the effect would have a weighty and significant chance of prejudicing the public interest in the investigation or prosecution. It is necessary to focus on the specifics, not generalities.

44 Moreover, if the court concludes that some prejudice would be likely it will still need to consider "the extent to which" such prejudice would be likely. That is what s 29(1) requires. Part of this evaluation, as Mr Weekes points out, is whether the restriction of the right of subject access that would result from the application of the exemption in the particular case can be described as "necessary". This is because, as Munby J pointed out in *Lord* at [99], s 29(1) is based upon, and must be interpreted consistently with, Article 13(1) of the parent Directive; and Art 13(1) authorises Member States to adopt legislative measures to restrict the right of access "when such a restriction constitutes a *necessary measure* to safeguard … (d) the prevention, investigation, detection and prosecution of criminal offences,…" (emphasis added).

45 The test of necessity is a strict one, requiring any interference with the subject's rights to be proportionate to the gravity of the threat to the public interest. The exercise therefore involves a classic proportionality analysis: *Lin v Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB)* [78] (Green J). In making any proportionality assessment the court would naturally have to take into account the value of the access right. The right to verify the accuracy of personal data about oneself is an important one, which has been identified as an element of the fundamental right to a private life under Article 8 of the Convention: *Durant v. Financial Services Authority [2003] EWCA Civ 176, [2004] FSR 28* [4]. For all these purposes the court requires proper and convincing evidence.

14. Applying those principles, the following analysis must apply, on a case-by-case basis, before a prejudice-based exemption ion the DPA 2018 can be relied on by a controller to refuse to comply with fundamental data protection rights:

a. First, the controller must prove convincingly that the particular processing being undertaking is for the legitimate purposes specified by the particular exemption. That requires careful consideration of why the processing is being done, to determine whether it falls squarely within the exemption. EU law requires that an exemption or derogation from fundamental rights must be construed strictly or narrowly in order to comply with the principle of proportionality, and to ensure that it is only relied on where strictly necessary.[4]

[4] Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Englebert and others* [2014] 2 CMLR 9, at §39; *Zaw Lin, Wai Phyo v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), §80; *Dawson-Damer and ors v Taylor Wessing* [2017] 1 WLR 3255), §§35-56.

b. Second, the controller has to prove that compliance with the fundamental right in question would be likely to prejudice the specified purposes. A blanket approach is wrong, as a matter of principle. What is required is a case-by-case, selective and targeted approach to non-disclosure (or other non-compliance with fundamental rights), based on the circumstances of the particular case, not generalities. A structured evaluation has to be undertaken, which: (i) identifies the prejudice; (ii) shows how compliance with the right in issue would cause that prejudice; and (iii) demonstrates that the failure to apply the exemption would be likely to cause that prejudice. "Likely" means a very and significant and weighty chance of prejudicing the public interest covered by the exemption.

c. Third, even if the Court concludes that some prejudice is likely, it still needs to consider *the extent to which* such prejudice is likely: again, language inconsistent with a blanket approach.

d. Fourth, as part of the above assessment and more generally, the Court has to consider whether reliance on the exemption is *strictly necessary*. This requires the application of a classic proportionality analysis. In §80 of *Lin*, Green J (as he then was) rejected a claim that such a proportionality balancing exercise, weighing the interests of the individual against those of the controller, was not required where the Metropolitan Police could show that there was a legitimate reason for withholding personal data. He concluded that this argument was *"unsustainable"* because if:

> … it were correct then it would in effect reduce to nought the relevant individual's right to privacy or any other right including the even more fundamental right to life. The argument is inconsistent with (*inter alia*): (a) the Directive and the plain reference to the fundamental rights of the individual concerned; (b) the *raison d'etre* of the DPA 1998 as a protector of an individual's fundamental rights; (c) the view taken by the Court of Justice that derogations from the individual's fundamental rights had to be construed narrowly and in this regard see by way of illustration Case C-473/12 *IPI v Englebert et ors [2014] 2 CMLR 9* at paragraph [39] where the Court emphasised that derogations from the fundamental right to privacy *"…must apply only insofar as is strictly necessary" (* this being the traditional language of the Court of Justice when it is referring to a proportionality exercise); (d) the judgment of Mr Justice Munby in *Lord* at paragraph [99]: see below at paragraph [84] and with his explanation that because of the importance of the policy of protecting individual rights the burden of proof lay on the State to justify derogation to a high standard of proof; and I the judgment of Lord Sumption in *Catt* at paragraph [8].

15. As set out in the NPSPCs' previous submissions, the CJEU has confirmed on a number of occasions that derogations from, and limitations on, personal data rights should apply only in so

far as strictly necessary and proportionate. See, e.g.: *Tele2 Sverige AB v Post- och Telestyrelsen* (Joined Cases C-203/15 & C-698/15) [2017] 2 CMLR 30, at §96. This test requires that any interference with the subject's rights be proportionate to the gravity of the threat to the public interest, assessed on a case-by-case basis. The Government has confirmed that this is how the exemptions in Schedule 2 DPA 2018 must be interpreted and applied.[5]

16. In addition, *Guriev* makes it clear that at each stage the onus is on the controller, applying the ordinary civil standard, to prove the application of the exemption by way of convincing evidence.

C. ISSUE 1 – ARE ANY EXEMPTIONS ENGAGED?

17. The first issue (**"Issue 1"**) on which the Inquiry invites submissions is:

> The extent to which Articles 13, 14 and 15 of the General Data Protection Regulation apply to the work of the Inquiry, having regard to the effect of any applicable exemptions.

18. The NPNSPCs' submissions on his question are in two parts: first, a response to the Inquiry's provisional view that paragraph 7, Schedule 2, Part 2 DPA 2018 applies; second, a response to other exemptions identified, in particular by the MPS, in submissions at the last hearing.

Response to the Inquiry's provisional view

19. The NPSPCs submit that the exemption in paragraph 7, Schedule 2, Part 2 DPA 2018 does not apply to the Inquiry.

(i) S. 31 DPA 1998

20. As the Inquiry recognised at the last hearing, the paragraph 7 exemption is one of the successors to the exemption previously found in s. 31 DPA 1998.

21. S. 31 DPA 1998 was headed *"Regulatory activity"*. It covered a range of regulatory activities. It broke down as follows:

    a. First, s. 31(1) DPA 1998 set out the prejudice test applicable to processing falling within the scope of the exemptions provided for in sub-paragraphs 2-3:

[5] Skeleton argument dated 10 January 2019 submitted by the Secretaries of State for the permission hearing in *R (Open Rights Group and the3million) v SSHD and SSDCMS*, §13.

Personal data processed for the purposes of discharging functions to which this subsection applies are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

b. Second, s. 31(2) set out the relevant functions to which the section applied. It applied to any relevant function which is designed:

(a) for protecting members of the public against—

i. financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,

ii. financial loss due to the conduct of discharged or undischarged bankrupts, or

iii. dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity,

(b) for protecting charities or community interest companies against misconduct or mismanagement (whether by trustees directors or other persons) in their administration,

(c) for protecting the property of charities or community interest companies from loss or misapplication,

(d) for the recovery of the property of charities or community interest companies

(e) for securing the health, safety and welfare of persons at work, or

(f) for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.[6]

c. Third, s. 31(3) defined the term "*relevant function"* for the purposes of subsection (2) as being:

(a) any function conferred on any person by or under any enactment,

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

(c) any other function which is of a public nature and is exercised in the public interest.

[6] Emphasis added.

d. Fourth, s. 31(4) made special provision for data processed for the purpose of discharging functions performed by specified bodies. It provided that where such processing:

(a) is conferred by or under any enactment on—

i. the Parliamentary Commissioner for Administration,
ii. (ii) the Commission for Local Administration in England,
iii. the Health Service Commissioner for England,
iv. (iv) the Public Services Ombudsman for Wales,
v. (v) the Assembly Ombudsman for Northern Ireland,
vi. (vi) the Northern Ireland Commissioner for Complaints, or
vii. (vii) the Scottish Public Services Ombudsman, and

(b) is designed for protecting members of the public against—

i. maladministration by public bodies,
ii. (ii) failures in services provided by public bodies, or
iii. a failure of a public body to provide a service which it was a function of the body to provide,

are exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

22. Following the enactment of the DPA 1998, numerous amendments were later made to s. 31 to add equivalent prejudice-based regulatory exemptions in respect of the activities of various specified regulators / functions performed under specified Acts (see ss. 31(4A) – (5I). These included, for example, exemptions for processing in relation to certain activities performed by the Legal Services Board and the Competition and Markets Authority.

23. These new exemptions mirrored those previously provided for under s. 31(6)-(8) in respect of: (a) processing for the purposes of discharging a function to consider complaints under s. 113(1) or (2) or 114(1) or (3) of the Health and Social Care (Community Health and Standards) Act 2003, or ss. 24D, 26 or 26ZB of the Children Act 1989; and (b) processing for the purpose of discharging any function which is conferred by or under Part 3 of the Local Government Act 2000 on specified authorities.

24. S. 31 DPA 1998 appears to have been based on Article 13(1)(f) of the Data Protection Directive, which permitted necessary exemptions to safeguard: *"a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in I, (d) and I".*

25. As discussed at the last hearing, there is little mention of s. 31 DPA 1998 in the authorities, and no authority that provides any real insight into its scope. The leading practitioner text, *Coppel*,

Information Rights, 4th edition 2014, provides only a relatively limited overview of s. 31 DPA at **[5-068]**. It essentially explains that s. 31 provided exemptions for data held for certain regulatory functions. It does, however, cross-refer to a separate discussion of how the various different information regimes protect regulatory functions, noting that while there are some differences in the language used between, *inter alia*, the Freedom of Information Act and the DPA 1998, they cover broadly the same kind of information (see **[20-027] – [20-032]**).

26. S. 31 FOIA provides exemptions for, *inter alia*, public authorities engaging in a range of regulatory functions. Public inquiries, however, are covered by a different exemption, s. 32 FOIA (which s. 18 of the Inquiries Act 2005 disapplies in certain circumstances).

(ii) Comparing Paragraphs 7-11 of Schedule 2, Part 2, DPA 2018 to S. 31 DPA 1998

27. Paragraphs 7-11 of Schedule 2 DPA 2018 replace the detailed provision in s. 31 DPA 1998 which, as described above, covered a wide range of regulatory activity. In many respects, the current provisions map directly onto provisions of s. 31.

28. Paragraph 7 is entitled *"Functions designed to protect the public etc"*, adopting the language used to describe the functions that were covered in s. 31(2)(a). The main body of paragraph 7 sets out the prejudice test that was found previously in s. 31(1). The Table then sets out the *"Description of function design"*, in column 1, and the *"Condition"*, in column 2:

a. Row 1 deals with functions to protect the public from financial loss due to dishonesty etc., mirroring subsections 31(2)(a)(i) and (ii).

b. Row 2, which is the subject of the Inquiry's provisional view, reflects subsection 31(2)(a)(iii) DPA 1998, which applied to a relevant function designed to protect members of the public against dishonesty, malpractice or other seriously improper conduct, or unfitness or incompetence of persons authorised to carry on a profession or other activity.

c. Rows 3 and 4 reflect subsection 31(2)(b)-(f) DPA 1998.

d. Row 5 replicates subsection 31(4) DPA 1998.

e. Row 6 replicates subsection 31(5) DPA 1998.

29. Paragraphs 8 and 9 add new exemptions for different types of regulators that were not covered previously by s. 31 DPA 1998, specifically: (a) the Comptroller and Auditor General; (b) the Auditor General for Scotland; (c) the Auditor General for Wales; (d) the Comptroller and Auditor General for Northern Ireland; and I the Bank of England. The reasons for these additions are discussed in Annex A to these submissions.

30. Paragraph 10, *"Regulatory functions relating to legal services, the health service and children's services"*, replaces and reflects s. 31(4B)-(4C) and (6) DPA 1998.

31. Paragraph 11 enshrines an exemption for *"Regulatory functions of certain other persons".* That list incorporates regulators that were covered previously by s. 31(5A)-(5B), and (7)-(8). However, it has been expanded to cover a range of other listed regulators when they are exercising powers conferred by specified legislation. These include, for example, a number of Ombudsmen, and the Information Commissioner.

32. None of the provisions address specifically the position of statutory inquiries or those acting in accordance with the Inquiries Act 2005.

(iii) Parliamentary intention / Legislative history of paragraph 7

33. The Chair acknowledged at the last hearing that textual differences between paragraph 7 Schedule 2 DPA 2018 and s. 31 DPA 1998 were important in informing his provisional view.

34. Annex A to these submissions sets out the legislative history of paragraphs 7-11 of Schedule 2 DPA 2018. From that history, the NPNSCPs draw the following three points:

    a. First, the new heading introduced for paragraph 7 was not intended to broaden the scope of the exemption provided for in respect of functions designed to protect the public from, *inter alia*, seriously improper conduct. Instead, the new heading reflects a decision to break down the various exemptions provided for regulatory activities under s. 31 DPA 1998, as amended, into different paragraphs of Schedule 2.

    b. Second, where gaps in coverage for other regulators / regulatory functions were identified, these were addressed by adding new provisions / adding regulators to the lists set out in paragraphs 7-11 DPA 2018. For example, a new exemption was introduced for the regulatory activities of the Bank of England. No provision was made for public inquiries constituted under the Inquiries Act 2005.

c. The limited technical amendments made to Paragraph 7 during the course of the Bill's passage through Parliament do not demonstrate any intention to apply the exemption now included in Row 2 of the Table to situations to which s. 31(2)(a)(iii) would not have applied.

35. The Inquiry is invited to consider the legislative history set out in Annex A.

(iv) The correct construction of paragraph 7, row 2, of Schedule 2, Part 2

36. The language and legislative history of row 2, paragraph 7, suggest that it was not intended to introduce a new exemption for processing activities which were not covered previously by s. 31(2)(a)(iii) DPA 1998.

37. As was acknowledged at the last hearing, it is difficult to suggest that this Inquiry, as constituted under the Inquiries Act 2005, is engaged in regulatory within the scope of s. 31 DPA 1998. That conclusion applies equally to paragraph 7, row 2, of Schedule 2, Part 2. That row forms part of a suite of exemptions targeted at regulatory activities. It does not extend to an inquiry which, in accordance with its terms of reference, is investigating an array of matters with a view to making recommendations for the future conduct of activities of the police or others. Any regulatory activity prompted by the Inquiry's report will involve processing by other bodies.

38. As set out above, exemptions to fundamental data protection rights must be construed narrowly if they are to be applied only where strictly necessary. Maintaining the Inquiry's provisional view would involve adopting an expansive and broad approach to paragraph 7 which is not supported by the change of heading between paragraph 7 and the former s. 31, or by any analysis of the legislative history.

39. Thus, applying the four-staged approach set out by Mr Justice Warby in *Guriev*, the Inquiry should conclude that the first stage is not satisfied in relation to paragraph 7, as the Inquiry is not processing data for regulatory purposes.

Exemptions raised by other parties

40. As set out in §4 of the Exemptions Note, other parties have suggested that the following exemptions to the rights granted by the GDPR are applicable or likely to apply to the Inquiry's work:

a. Crime and taxation: see paragraph 2(3) of Schedule 2, Part 1;

b. Legal proceedings: see paragraphs 5(2) and 5(3) of Schedule 2, Part 1;

c. Judicial capacity and judicial independence: see paragraphs 14(2) and 14(3) of Schedule 2, Part 2;

d. Protection of the rights of others: see paragraph 16 of Schedule 2, Part 3;

41. As set out below, there is no dispute that paragraph 16 (rights of others) may be engaged in respect of some of the Inquiry's data processing. However, none of the other exemptions are engaged. They were raised by the MPS in their supplemental submissions of 29 January 2019. In response, at the previous hearing the Chair observed that:

> At first blush, I don't think the ones you have identified do apply. But I am open to persuasion that I am wrong.[7]

42. The Chair's 'first blush' reaction is correct.

(i) Paragraph 16 – Rights and freedoms of others

43. Paragraph 16 will apply to some of the data processed by the Inquiry. In particular, there will be many documents that contain 'mixed personal data' of a number of data subjects. Paragraph 16 (and 17) provide that a data controller is not obliged to disclose information under Article 15 of the GDPR if to do so would mean disclosing information relating to another individual who can be identified from the information, except where there the other individual has consented; or it is reasonable in all circumstances to comply with the request without that individual's consent. These provisions retain the effect of ss. 7(4), (5), (6) and 8(7) of the DPA 1998.[8]

44. Essentially, the exemption requires the Inquiry to engage in an appropriate balancing exercise when deciding whether to disclose personal data of a third party to another data subject. That balancing exercise is built-in to the proposals made by the NPNSCPs in their previous written submissions on the use of confidentiality rings, with particular provision to be made for special category data.

(ii) Paragraphs 5 and 14 – Judicial capacity and legal proceedings

45. Paragraphs 14(2) and (3) provide:

> *Judicial appointments, judicial independence and judicial proceedings*

[7] Transcript, p.232 (6)-(8).
[8] See Explanatory Notes, §682.

14(1) …

(2) The listed GDPR provisions do not apply to personal data processed by—

(a) an individual acting in a judicial capacity, or

(b) a court or tribunal acting in its judicial capacity.

(3) As regards personal data not falling within sub-paragraph (1) or (2), the listed GDPR provisions do not apply to the extent that the application of those provisions would be likely to prejudice judicial independence or judicial proceedings.[9]

46. This exemption appears to be enacted pursuant to Article 23(1)(f) GDPR, which allows for strictly necessary measures to safeguard *"the protection of judicial independence and judicial proceedings".*

47. The Chair is of course a former judge of the High Court. But he is not acting in a judicial capacity as Chair of this Inquiry. Rather, he is acting as a Chair of a statutory public inquiry pursuant to the Inquiries Act 2015 (which does not require Inquiries to be chaired by judges or former judges), and the Inquiry does not have the power to establish the liability of any person. Having regard, in particular, to the need to adopt a narrow construction of exemptions from fundamental rights, this provision should not be given an expansive interpretation which extends it well beyond its natural meaning. At the previous hearing, the Chair noted that:

> … the Inquiry is not a court, at least as I'm presently advised. I know it is being suggested that I am sitting in the judicial capacity. I doubt that, but I will hear submissions about that in due course. [10]

48. Essentially, the NPNSCPs submit that the Chair was right to be advised to this effect.

49. A similar conclusion applies in respect of the suggestion that paragraph 5 may be engaged. Paragraph 5 provides, *inter alia*, that:

> (2) The listed GDPR provisions do not apply to personal data where disclosure of the data is required by an enactment, a rule of law or an order of a court or tribunal, to the extent that the application of those provisions would prevent the controller from making the disclosure.
>
> (3) The listed GDPR provisions do not apply to personal data where disclosure of the data—

[9] Italicised emphasis in the original.
[10] Transcript, p.203 (14)-(20).

(a) is necessary for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings),

(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

to the extent that the application of those provisions would prevent the controller from making the disclosure.

50. These exemptions operate to allow controllers to make disclosures required by law and/or in the context of legal proceedings. It is not clear how it is said that this exemption would apply to processing carried out by the Inquiry.

51. In any event, the Inquiry is not a type of 'legal proceedings'. It is to be noted that the Secretary of State also expressed that view in §23 of his submissions for the previous hearing (dated 24 January 2019), observing that: *"… it is not clear that the work of the Inquiry would fall within the definition of 'legal proceedings' under paragraph 5 of schedule 2 to the 2018 Act (the successor to section 35 of the 1998 Act)…*"

(iii) Paragraphs 2 and 3 – crime and taxation

52. The Inquiry is not processing personal data for the purposes of (a) the prevention or detection of crime, (b) the apprehension or prosecution of offenders, or (c) the assessment or collection of a tax or duty or an imposition of a similar nature. Thus, paragraphs 2 and 3 Schedule 2, Part 1, do not apply.

D. ISSUE 2 – WHERE ARTICLES 13-15 GDPR APPLY IN FULL

53. The second issue upon which the Inquiry invites submissions is:

> Insofar as Articles 13, 14 and 15 of the General Data Protection Regulation do apply to the work of the Inquiry, and no exemptions are applicable, what obligations do Articles 13, 14 and 15 impose upon the Inquiry, having regard in particular to Article 14(5)(b)? In those circumstances, what would be the practical implications for the Inquiry in relation to the evidence gathering exercise?

54. As set out above, it is unlikely that no exemption at all applies to any of the processing being carried out by the Inquiry, as it will be processing 'mixed personal data'. However, there is no exemption which covers all of its processing activities.

55. Article 13 GDPR applies where personal data is collected from the data subject. As the Inquiry publishes a privacy notice about its processing activities, and individual data subjects who provide personal data are likely to understand the implications of doing so, the absence of an exemption from Article 13 has no practical impact on the Inquiry.

56. The impact of Article 14 GDPR applying to the Inquiry in full was addressed by the NPNSCPs in their submissions for the privacy hearing on 30 January 2019. At §§27 to 28 of those submissions, the NPNSCPs set out the information rights granted by Article 14 where personal data is obtained from a third party. §§29-30 described the built-in exemptions to Article 14, including Article 14(5)(b) GDPR, 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. [11]

57. As set out in the previous submissions, it is clear from the text of Article 14(5)(b), and the case-law referred to in those submissions and above, that this derogation from Article 14 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 to notify such persons and protect their interests, including, if appropriate, making information publicly available about the data that is being processed.

58. At §§80-83 of their previous submissions, the NPNSCPs suggested, as pragmatic proposals, the steps they consider that the Inquiry should take in order to satisfy Article 14 GDPR, taking into account the derogation in Article 14(5)(b) GDPR. The effect of an absence of exemption applying to the activities of the Inquiry is, in the NPNSCPs view, that it should amend its evidence gathering process (Step 3 (§5(iii) of the Process Note) to align with their proposals on notification.

[11] Emphasis added.

59. For the avoidance of doubt, and as emphasised at the previous hearing, the NPNSCPs' position has never been that the Inquiry must contact directly each and every individual whose data is contained within the documents it holds. Article 14 GDPR requires the Inquiry to take proportionate steps to notify all affected data subjects: (a) directly, if they are readily or easily contactable; and (b) if they are not contactable, through the provision of widely disseminated, publicly available information. In Part II below, the NPNSCPs respond in more detail to the proposals for notification in the Process Note.

60. If Article 15 GDPR applies in full to the Inquiry, the implication for the Inquiry is that at any point in time core participants or affected individuals may submit subject access requests, and the Inquiry will be obliged to take proportionate steps to comply with those requests (subject to paragraph 16 / any other item of information specific exemption which may apply on the facts). The right of access is addressed at §§32-35 of the NPNSCPs previous submissions. It is a fundamental right, guaranteed by Article 8 the EU Charter as well as Article 15 GDPR.

61. It is also critical to note that the right of access applies to all data which falls within the definition of "personal data" in Article 4 GDPR. It is not restricted by any necessity/relevance test applied from the point of view of the Inquiry.

62. At present, the NPNSCPs' understanding of the Exemptions Note and the Process Note read together is that, on the assumption paragraph 7 of Schedule 2 applies, the Inquiry's position is that:

    a. This exemption provides in effect a blanket basis upon which the Inquiry could refuse any subject access requests it receives;

    b. The evidence gathering process set out in the Process Note will only allow the NPNSCPs to obtain access to information deemed relevant and necessary by the Inquiry after the same package of material has been provided to relevant state witnesses (which includes dissemination beyond the officer that recorded the data to include, for example, more senior officers / other officers involved in undercover operations at the time).

63. The process set out by the Inquiry in its Process Note makes no allowance at all for the exercise of Article 15 GDPR rights. The NPNSCPs consider that their rights to access their own personal information, which is being processed by the Inquiry, must be complied with. The NPNSCPs have, on the whole, refrained to date from making formal subject access requests, but they are seeking compliance with their Article 15 GDPR rights through the evidence gathering process.

64. If there is no exemption for the Inquiry to rely on, the practical implication is that, if the Inquiry receives subject access requests, the Inquiry will have to comply with those requests, irrespective of its evidence gathering process. Moreover, if individuals are concerned about processing that is already taking place / could take place while the subject access process is undertaken, it would be open to them to rely on their rights to restrict or object to processing of their personal data and/or seek an order from the Court to prevent further processing of their data pending receipt of access to it (see §§36-40 of the NPNSCPs previous written submissions).

65. As the NPNSCPs have made clear, and wish to emphasise again, they are proposing a framework for the disclosure (and publication) of documents, which include their personal data, which properly respects their rights as data subjects, while taking account of the need for the Inquiry to make progress. Essentially, they are seeking to 'build-in' at least some level of compliance with Articles 14 and 15 to the evidence gathering process. Their proposed framework provides a proportionate way in which the Inquiry can strike a balance between fundamental rights and its public interest objectives, allowing the Inquiry to satisfy the requirements of Articles 6(1)(e) and 9(2)(g) GDPR, and paragraph 6, Part 2, Schedule 1 DPA 2018.

66. The NPNSCPs are conscious of the Inquiry's concerns about the workability of this approach due to the volume of documentation it has to consider and its need to make progress. However, in addition to the points on fairness and other preliminary observations set out at the beginning of these submissions, the NPNSCPs make the following observations:

    a. An indication was given at the last hearing about the volume of documentation. It is understood that the Inquiry has considered 26,000 pages of documentation for a ten-year period, with about 2000 individuals reported upon.[12] This poses a significant task. But it is comparable with the task faced by other Inquiries. For example, in its most recent update, the Grenfell Inquiry reported that it has disclosed over 20,000 documents to CPs to date, and the next phase of disclosure is underway, involving 14,000 documents.[13] IICSA has launched 13 investigations into a broad range of institutions alongside, *inter alia*, its truth project.[14] IICSA has received 163,814 documents as part of its Investigations and Public Hearings work. It has processed 1,857,135 pages of evidence (as set out in its most recent update).[15]

[12] 55-57
[13] https://www.grenfelltowerinquiry.org.uk/news/update-inquiry-11
[14] https://www.iicsa.org.uk/investigations https://www.truthproject.org.uk/experiences-shared
[15] https://www.iicsa.org.uk/privacy

b. Those Inquiries are not following a sequential disclosure procedure. Documents are subject to review, necessary redaction etc. and then disclosed to CPs subject to confidentiality requirements. There is no procedure where evidence is disclosed only to one party, or group of parties, before being provided to other CPs (and in so far as information amounts to personal data no such procedure would be lawful).

c. Other inquiries, in particular IICSA, have contracts in place with external data processors that allow it to conduct its work.[16] This Inquiry may be able to access database and processing services which assist it in its task; in so far as current IT arrangements are not considered to be effective, further consultancy and advice on more efficient IT solutions should be sought out.

d. Other Inquiries are not proceeding on the basis that they are protected by a blanket exemption from data protection rights. The Grenfell Inquiry, the IICSA Inquiry, and others, acknowledge that individuals have all of the rights set out in the GDPR, including the right of access, and have procedures in place (including contracts with external solicitors and processors) to enable them to meet those obligations.

67. Thus, the data management challenges identified by the Chair at the 31 January 2019 hearing and in the Process Note as arising from the process proposed by the NPNSCPs are neither unique to this Inquiry nor insurmountable. Part II below describes the particular steps that would need to be taken in the evidence gathering process set out in the Process Note to enable compliance with Articles 13, 14 and 15 GDPR.

E. ISSUE 3 – EXEMPTION(S) APPLY

68. Issue 3 invites the parties to provide submissions on the following:

> If I am performing a function to which any of the exemptions referred to above and/or set out in Schedule 2 to the Data Protection Act 2018 applies, what obligations do Articles 13, 14 and 15 of the General Data Protection Regulation impose upon the Inquiry? In those circumstances, what would be the practical implications for the Inquiry in relation to the evidence gathering exercise?

69. Even if an exemption is engaged in respect of a controller's processing activities of some or all personal data held, that is only stage one of the necessary analysis. As described above, *Guriev*, and the other case-law it refers to, make it clear that a four-stage analysis is necessary.

[16] https://www.iicsa.org.uk/privacy

70. On a case-by-case basis, a data controller has to:

a. prove that complying with the rights would prejudice the interests protected by the exemption (for example, it would have to cause real prejudice to protecting the public from malpractice if paragraph 7 applies);

b. determine the likelihood of that prejudice; and

c. assess whether reliance on the exemption is strictly necessary.

71. Thus, the implications for the Inquiry of an exemption or more than one exemption applying to its activities is that it would still need to consider whether a refusal to comply in whole or in part with the rights guaranteed under Articles 13-15 (and other fundamental rights guaranteed by the GDPR and the Charter) is strictly necessary and proportionate on the particular facts of an individual case. A blanket approach is wrong as a matter of principle.

72. In reality, this again points to adopting the pragmatic proposals put forward by the NPNSCPs, and amending the proposed evidence gathering process, as suggested below. The proposed approach would strike a proportionate balance between the fundamental rights of the individuals whose data are being processed, and the interests of the Inquiry achieving its public interest objectives. In particular, it would begin to address the the ongoing psychological harm and distress being caused to the NPNSCPs, especially those who had close or intimate relationships with undercover officers, by the unknown. It builds-in a rights-based approach to the design of the Inquiry's processes (in accordance with Article 25 GDPR, which requires controllers to engage in data protection by design and by default), which will heighten faith in its work, and allow NPNSCPs to get on with understanding how they have been affected by undercover policing. They will also be able to start the process of finding their own evidence and contacting other relevant witnesses.

73. A final, general concern, which applies irrespective of whether exemptions are or are not engaged in respect of Articles 13, 14 and 15 GDPR, is the implications of any evidence gathering process for the ability of the NPNSCPs to exercise other fundamental data protection rights guaranteed by the GDPR and the Charter. Neither the Exemptions nor Process Note refers to such other rights, including Article 18 (restriction of processing) and Article 21 (right to object). The NPNSCPs have made clear that if they were granted their rights of access, they would not anticipate that such rights will be exercised other than in exceptional circumstances. Everyone wants the Inquiry to be able to do its job properly.

74. However, the fact that the exercise of rights may be exceptional does not devalue their importance. Where such rights are in play, it will be because the personal data being processed is of such special sensitivity that the data subject has a genuine and real concern to ensure it is processed in as restrictive manner as possible, even if some officers may need to see it (for e.g. data about intimate relationships and mental health). The exercise of such rights should not be shut out in a blanket way. That is the implication, however, of applying a blanket exemption to Article 15 rights pending completion of the gathering of evidence from the state.

PART II – PRACTICAL IMPLICATIONS

SUBMISSIONS ON PROCESS NOTE

75. The Process Note sets out the evidence gathering process that the Inquiry is conducting and intends to conduct, to enable focused submissions on the practical effect of the data protection obligations to which the Inquiry is subject. The note includes a number of observations as to why proposed alterations to the process would, in the Inquiry's view, be impractical. This Part of the NPNSCP submissions addresses those practical concerns.

(1) Preliminary observations

76. First, the evidence gathering process set out in the Process Note is premised on the Inquiry being exempt from data subject rights, including the right of access. It approaches notification and disclosure solely from the perspective of relevance and necessity to the investigative task of the Inquiry. The NPNSCPs submit that, even from that perspective, there are errors in the approach, which are identified below. But, if, as the NPNSCPs contend, the Inquiry is obliged to comply with data rights, even if only to the extent of restricting the application of any exemption to a degree that is strictly necessary and proportionate, the Inquiry's proposed process will have to be reconsidered.

77. Secondly, it is noted that the Inquiry's proposed process is intended to achieve efficiency by ensuring that redactions to be applied to documents are cumulative, progressing from lesser to greater redaction as the documents move through each stage of disclosure. However, that process assumes that no new matters of significance, or lines of enquiry, emerge when documents are shown to NPNSCPs and civilian witnesses. That assumption is unlikely to be correct in a genuinely investigative process, particularly where non-State participants and witnesses will only be learning for the first time, when disclosure is made to them, the nature and extent of the surveillance to which they were subjected. It is reasonable to expect, indeed virtually inevitable, that new lines of enquiry and fresh evidence and allegations may emerge at the Inquiry's proposed stage 2, which will require the Inquiry to re-assess redactions imposed at stage 1, and indeed any prior assessment of what material may be relevant and necessary. The Inquiry has previously acknowledged this, observing 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…"[17].

78. That being so, the linear process suggested by the Inquiry is not truly reflective of what will happen in practice. The process will not be strictly linear, and redactions will not be merely cumulative. Indeed, it is likely that the more searching the investigation, the greater the prospect that decisions made on the basis of stage 1 information will need to be revisited as new evidence and lines of enquiry emerge. For this reason, the contended practical advantages of the Inquiry's proposed process are not as clear-cut nor overwhelming as the Process Note may suggest. In fact, the process proposed by the NPNSCPs will have overall benefits for the Inquiry's investigation – see further below - as well as being a proportionate means of giving effect to data rights and the need for those who have been subject to undercover policing activity to begin to understand the truth.

79. Thirdly, the NPNSCPs repeat the overarching observations at the beginning of these submissions. The Inquiry's approach and the proposed process is, from the point of view of NPNSCPs, fundamentally unfair and one-sided. It is simply not understood why, in a process set up to investigate activities of the police, including illegal activities which have outraged public opinion, and with the intention of establishing justice for families and victims, the Inquiry seems implacably opposed to making reasonable adjustments to its procedures to address the concerns of those who were the targets of that activity, and to ensure compliance with their fundamental privacy and data protection rights.

80. The remainder of this part of the submissions addresses specific points raised in the Process Note and seeks to explain why the proposals of the NPNSCPs in the 24 January 2019 submissions are both practicable and consistent with the Inquiry's aims and investigative interests.

(2) Notification

81. The NPNSCPs welcome the indication in §5(iii) that the Inquiry intends to publish additional information on its website about groups that were infiltrated and reported upon.

82. However, §5(iii) of the Process Note envisages that the Inquiry will only take further steps to notify individuals that their data are being processed at Step 3. On that basis, the additional details will only be provided after the Inquiry has gathered evidence from the State, and it appears that

[17] Inquiry's letter date 13 July 2017.

additional details will only be provided on the Inquiry's website about deployments which have been assessed (based on the State's evidence) to be relevant and necessary to the work of the Inquiry. Further, no reference is made to the Inquiry taking steps to publicise more widely (e.g. in the press or on social media) the information released on the website. Direct contact will only be made with individuals that the Inquiry intends to call as witnesses.

83. This does not meet the requirements of Article 14 and/or, in any event, the requirements of strict necessity and proportionality. In particular:

a. It is not timely. The Inquiry has been and will continue to be processing individuals' personal data, including special category data, for a long time, without taking any steps to notify them that that processing is taking place. There is no good reason for this: steps can be taken now, at least as the documents are reviewed for the purposes of restrictions and identifying relevant and necessary material, to update the website on an ongoing basis (see §§80-93 of the NPNSCPs previous written submissions for the 31 January 2019 hearing). Steps should be taken to publicise this through mainstream and social media so that members of the public, and persons who may have an interest, know about it.

b. The delay in publishing additional details will in fact be prejudicial to the work of the Inquiry. It fails to take account of the real possibility that individuals will come forward as a result of notification to provide information that opens up new avenues of enquiry, which in turn requires further evidence to be gathered from the State witnesses or a re-assessment of what is relevant and necessary to the Inquiry's task. The process, and the assumption of a clean, linear approach, makes no allowance for that possibility.

c. The Inquiry intends to apply a test of relevance and necessity in deciding what additional details are to be provided on its website. This means that no steps will be taken to notify some individuals that their data is being processed. This is simply not compliant with Article 14. All data subjects have the right to be notified that processing of their personal data is taking place, even if that is only achieved through making sufficient information publicly available which allows them to discover for themselves that they are affected. Moreover, the proposed narrow approach is again likely to prejudice, rather than assist, the work of the Inquiry. A review of State-generated material, viewed only in the light of State submissions and evidence, may not allow the significance of, for example, one piece of apparently anodyne reporting to be recognised. However, a notified individual may come forward with material which sheds light on events that are critical to the Inquiry fulfilling its purpose.

d. It is not sufficient for the Inquiry only to contact individuals directly where, based on the evidence provided by the State, the Inquiry wishes to call them as witnesses. If individuals are readily contactable, they should be contacted. As noted at §93 above, the NPNSCPs have never submitted that the Inquiry must directly contact all affected data subjects. But there is no good reason why contact should be limited in the manner proposed in the Process Note (§§5(iii)-(iv)), and that would not comply with the requirements of Article 14. The pragmatic proposals set out in the NPNSCPs previous written submissions remain the proportionate and lawful way forward.

(3) Disclosure to NPNSCPs

84. The NPNSCPs are very concerned that the Inquiry only intends to disclose to NPNSCPs (and non-state witnesses) data which has been deemed relevant and necessary to the work of the Inquiry, not all of their personal data, and that this limited disclosure will only take place at some point after the Inquiry has finished collecting the State's evidence (Steps 1-2 and 4, §§5(i)-(ii) and (v)-(ix)).

85. The proposed approach is not compatible with data protection law, for at least the following reasons:

a. Even if an exemption is available to the Inquiry (beyond paragraph 16 for mixed personal data), no exemption provides the Inquiry with blanket immunity from compliance with data protection rights simply to the extent they conflict with, or may render less efficient, a preferred approach to evidence gathering. The onus is on the Inquiry to build-in compliance with rights, and to act in a proportionate manner consistent with those rights. The fact that there may be, in some cases, circumstances in which evidence from officers is needed to finalise the scope of any security redactions does not justify blanket refusal to comply with the fundamental rights of those whose personal data is being processed (§§5(ii) and 6(a) of the Process Note). At most, that should be an exception to the general rule that data subjects are given access to their data, via the proposed confidentiality rings, before it is processed further by being given to officers and former officers (who are now private citizens) for the purposes of evidence gathering.

b. The failure to provide any access to personal data until after it has been provided to State witnesses ignores the real psychological harm and distress caused by individuals being kept in the dark as to what information is held about them and their private life, and what is being done with it. The NPNSCPs rights have already been violated. Steps should be

taken now to start to address that by providing access before the data is shared (again or for the first time) with those who violated their rights, including individuals who are no longer police officers, and officers / former officers who have never seen the information before.

c. The proposed evidence-gathering process cuts across not only data subjects' rights under Articles 14 and 15 GDPR, but also other fundamental rights guaranteed by the GDPR (including, for example, the rights to restrict and object to processing). Even if the Inquiry is right to note in §6(b) of the Process Note that it will only be in rare or unusual cases that applications to rely on such rights would be upheld, that does not justify a blanket refusal to take steps that would enable them to be exercised at all. It is in those cases that do have merit that this blanket denial will result in the most harm to the individuals affected.

d. The Inquiry's points on delay (§6 of the Process Note) assume that a linear approach can be adopted to the evidence gathering process. As set out above, that appears to the NPNSCPs to be a simplistic and optimistic approach, based on the assumption there will be no need to go back to the State witnesses, pursue new lines of enquiry, or reassess questions of relevance and necessary, when material is disclosed to non-State individuals.

e. The Inquiry's concerns about duplication in effort for the NPNSCPs and non-state witnesses if the NPNSCPs proposals are accepted are noted (§6(d)), but they are not shared by the NPNSCPs. The NPNSCPs desire access to their personal data as soon as possible, both so that they can start to work out how they were affected by undercover policing, and start thinking about what evidence they may wish to bring at a later stage, or how they may be able to assist the Inquiry in its investigative task. The disclosure and gathering of evidence processes can be run separately and/or in parallel, as they are in almost all other types of litigation or inquiry. The point is that delay in finding out what data was collected and is held about them, and which is now being re-processed by the Inquiry and the police, is having a real psychological and distressing impact on NPNSCPs. Further delay is to their considerable detriment. NPNSCPs have already waited for many years while the Inquiry has dealt with other issues. They wish to have access to their personal data and to assert their rights over it, even if it means only receiving material on a piecemeal basis at first (§5(ix) of the Process Note).

(4) Confidentiality rings

86. §5(vii) of the Process Note sets out how the Inquiry intends to deal with special category data when disclosing material to NPNSCPs and non-state witnesses. The Inquiry does not intend to contact data subjects about the disclosure of their special category data into confidentiality rings even where they are readily contactable.

87. Where individuals are readily contactable, it cannot be necessary or proportionate for the Inquiry to make disclosure of their special category data to others without notifying them and giving them an opportunity to decide whether to consent to that disclosure, or wish to make other representations. The proposed approach of the Inquiry is not the approach adopted, for example by IICSA, which redacts all sensitive data which data subjects have not consented to be disclosed.[18] The approach set out in §5(vii) of the Process Note would not be compatible with Article 9(2)(g) GDPR read together with paragraph 6, Schedule 1, DPA 2018 (see §§17-24 of the NPNSCPs previous written submissions).

88. In their previous submissions, the NPNSCPs set out how the Inquiry could adopt an approach to confidentiality rings and special category data, which would be lawful (see Part II).

(5) Contacting third parties

89. The NPNSCPs welcome the indication at §5(viii) of the Process Note that the Inquiry intends to discuss with recognised legal representatives of the non-state core participants how others can be contacted, whilst protecting the data protection and privacy rights of those whom the Inquiry may wish to contact. The RLRs of the NPNSCPs will liaise with the Inquiry to arrange a time for that discussion to take place.

90. As set out at §84-87 of the 24 January 2019 submissions, the NPNSCPs submit that the Inquiry's duty under Article 14 GDPR to notify individuals that their personal data is being processed will, in some circumstances, require it to take positive steps to attempt to contact individuals– examples are discussed by reference to CTI's Annexes A and B at §86 and §87 of the 24 January 2019 submissions. RLRs and some non-state groups and individuals are willing to provide assistance to the Inquiry in this regard and would welcome the agreement of a protocol setting out the principles and procedures for such assistance. Such a protocol would help to avoid the

[18] https://www.iicsa.org.uk/inquiry-protocol-redaction-documents

type of misunderstanding / mischaracterisation that arose at the 31 January 2019 hearing in respect of the Undercover Research Group.

91. The NPNSCP submissions of 24 January 2019, at §91, stated that "*Subject to appropriate resources being made available to URG, and the Inquiry and URG agreeing to an appropriate protocol, seeking help from URG would be an appropriate and proportionate step for the Inquiry to take*". This appears to have been understood by the Chair as a suggestion that the URG would be seeking to be paid for any assistance it provided[19]. The Chair's comments also appear to suggest a mistaken impression that the URG is a lone individual: the Chair referred to the organisation as "he", presumably a reference to Mr O'Driscoll. For the avoidance of doubt, the URG does not solely comprise of Mr O'Driscoll, although he is one of the group's researchers. The URG comprises a small group of researchers, including political activists and academics, whose aim is to create an online resource on political policing and undercover surveillance[20]. It is an unincorporated association, funded by private donations from the public and some grant awards. The reference in the 24 January 2019 submissions to resources was not a suggestion that the URG should be remunerated for its work, in the sense of making a profit. It referred to the practical reality that if the Inquiry intends to seek assistance from a not-for-profit voluntary organisation, such as URG, then expenses incurred in providing that assistance – for example, the cost of telephone calls, or travel to visit individuals the Inquiry wishes to contact – should reasonably be met by the Inquiry. Any implication that Mr O'Driscoll was seeking some form of remunerative employment from the Inquiry is inaccurate and unfair.

(6) Hearing bundle and public disclosure of documents

92. The Process Note envisages that "*The Open Hearing Bundle (as opposed to bundles for Private or Closed hearings) will be the means by which officers and non-state core participants see documents, in confidence, relating to deployments with which they were not directly concerned*." – Process Note §5(x). The same bundles will also ultimately comprise the documents disclosed to the public, via publication on the Inquiry's website. There will presumably also be some means by which documents referred to during hearings will be made available to members of the public contemporaneously in order to enable them to follow the hearings – for example, by projecting the documents on screens in the hearing and over-flow rooms, as is done in IICSA and in the Grenfell Inquiry.

[19] See, for example, transcript of 31 January 2019 hearing at p.150 li.20-22.
[20] https://undercoverresearch net/about-us-2/

93. In respect of the contents of the Open Hearing Bundles, the Process Note states that "*after giving all witnesses the opportunity to make representations about which documents should be published, it is the intention of the Inquiry to publish and include in the Open Hearing Bundle only a selection, sufficient to demonstrate the nature of the deployment and the activities carried on during it and the principal issues raised by it."* – Process Note §5(x). The NPNSCPs make five submissions in respect of this.

94. First, in order for the Inquiry, and the public, to be confident that the Inquiry has indeed identified the relevant documents relating to a deployment, it is important, for all of the reasons set out at §50 of the NPNSCPs' submissions in support of disclosure of their personal files dated 31 May 2017, that the documents disclosed to those who were affected by undercover policing are not restricted to those pre-determined by the Inquiry to be "relevant and necessary". Those submissions are copied again here, for ease of reference:

> 50. Disclosure of personal files is not only a matter of significant importance and fundamental right for NPSCPs, it is also of importance to the efficacy of the Inquiry. It is respectfully submitted that in relation to much of the information the Inquiry will be required to consider, its true relevance will not properly be ascertainable without assistance from NPSCPs. The following is a non-exhaustive list of reasons for this:
>
> a. as noted above, publicly obtained information contained in personal files may be relevant to the Inquiry's investigations in ways that would not be apparent to the Inquiry team without assistance from the data subject. Without such assistance there is a real risk of the Inquiry discarding as irrelevant or unnecessary material that is in fact highly relevant to its terms of reference. For example, a file might contain information about a CP's attendance at public meetings and events that was obtained through open sources and therefore not apparently relevant to the Inquiry's investigation. Without input from the subject of the file, such material might be deemed by the Inquiry to be irrelevant and unnecessary and so be returned to the police without further investigation. However, had the material first been shown to the subject of the file, s/he would have been able to identify for the Inquiry that, for example, the information had been used by a UCO (or person now suspected of being a UCO) to obtain information about a potential target and manipulate a relationship or situation of significance to the Inquiry's investigation. See the witness statement of Harriet Wistrich at [84]-[88];
>
> b. the subjects of information will be aware of contextual information which makes apparently innocuous information significant to issues the Inquiry is tasked with investigating. For example, a particular UCO deployment recorded in a personal file may appear anodyne and therefore not necessary for the Inquiry to investigate. However, the subject spied upon may have information which shows that it was highly relevant. This is particularly important in cases of so-called "collateral intrusion" – sexual relationships, or relationships with children or young adults - because it is understood that these relationships were not referenced in the files and evidence of them can only be understood in the context of information supplied by those affected. So, for example, a file might contain an account of a social gathering at which X, the subject of the file, made comments about some innocuous subject. The Inquiry might conclude that this record does not contain

anything of relevance and so reject it as not necessary for the discharge of the Inquiry's functions. However, had X had access to her file, she would have realised that the social event reported on was significant because her child, Y, had been present and the person now suspected of having been a UCO was also present and had made particular efforts to befriend Y. There is no way that the Inquiry or the police could know of this contextual information, and therefore properly assess the relevance of the primary information to matters properly within the scope of the inquiry, without the input of X.;

c. at very least some of the information in the files will be false and cannot be assessed for relevance or necessity on its face value. A number of errors and falsehoods have been identified in the very limited documentation that has already been disclosed to some CPs [see the statement of Harriet Wistrich at [27], [73] and [75]-[80]]. This is important, not only for the Inquiry to get to the truth, but also in relation to a number of issues it is tasked with addressing. For example, where false intelligence is used to select new targets for UCO operations, or to justify continued deployment;

d. where UCOs were engaged in activity designed to undermine the cohesion of particular target groups, this is likely only to be fully apparent to those involved in the group, who would be able to identify where reports of group dynamics were being manipulated. It is difficult to see how the Inquiry could be alive to this type of issue without assistance from those targeted;

e. those who have been made core participants have been afforded that status for good reason. No one is able to understand the true impact of undercover activities on their lives without their input, but they in turn need to understand what has been recorded about them in order to contribute meaningfully;

f. as previously raised in the NPSCP submissions in advance of the 5 April 2017 hearing, a number of CPs are elderly and indeed some have already passed away. The more time that passes before disclosure is made, the greater the risk that further CPs will be lost without ever knowing that files were kept about them or the contents of those files. Of those who remain alive, memories will fade. There is a very real benefit in making disclosure of personal files as soon as possible, both in order that no further CPs are deprived of relevant knowledge about their lives, and in order that valuable evidence is not irretrievably lost. And there is, in any event, a legal obligation on the Inquiry pursuant to the Data Protection Act to make disclosure.

95. For these reasons, full disclosure, subject to lawful restrictions, of *all* personal data, is not only required for compliance with data subject rights, but is necessary for the proper conduct of the Inquiry's investigation. If, and only if, full disclosure, subject to lawful redactions, has been made to NPNSCPs and other relevant non-state individuals in accordance with the process identified in the 24 January 2019 submissions, then, subject to the submissions made below, the NPNSCPs agree that the contents of the hearing bundles could be more selective. The precise content of the hearing bundles should be determined following representations made on behalf of all CPs at the relevant stage – i.e. after disclosure has been made. There would seem to be little merit in seeking to delineate at this stage, where submissions would necessarily have to be abstract, what should and should not be included in the hearing bundles.

96. Secondly, in assessing what is "*sufficient to demonstrate the nature of the deployment and the activities carried on during it and the principal issues raised by it*" the Inquiry will need to have in mind that it is not only surveillance in relation to significant events, individuals or groups and obviously wrongful behaviour on the part of undercover officers that is relevant to the terms of reference. Also, of very significant public concern is the risk of more subtle and pernicious undermining and control of political activism and civil society through the widespread infiltration of, and collection and retention of data on, political groups, campaigns and individuals. That is plainly within the terms of reference. The Inquiry cannot properly assess the role and contribution made by undercover policing towards the prevention and detection of crime, nor the motivation for it, nor its scope and effect on individuals and the public, by focusing solely or primarily on the surveillance of significant events, groups or individuals. Such an approach is likely to give a materially skewed impression if, in reality, such surveillance represents only one aspect of the undercover activity of units such as the SDS and NPOIU and, in fact, another aspect of the undercover activity related to infiltration of and reporting on apparently mundane and insignificant activities of political groups and individuals. The Inquiry must be alive to the fact that, whilst, on its face, such reporting may not appear to be significant, taken cumulatively it may be one of the most pernicious consequences of political undercover policing. If the Inquiry is properly to address these aspects of its terms of reference, it must ensure that it investigates this aspect of undercover activity. This necessarily involves at least making some form of scope assessment in respect of documents and activities which may not immediately appear to be significant.

97. This is linked to the NPNSCP's third submission: it is important that all CPs should have an opportunity to make submissions in respect of the contents of hearing bundles – i.e. this should not be limited those directly affected by the deployments to be considered in the corresponding tranche. This is for two reasons. First, even if particular NPNSCPs were not directly affected by a particular deployment, they may often have a strong legitimate interest in its investigation. This could arise for a number of reasons: for example, identifying the development of discredited techniques; tracing the evolution of relationships between undercover policing and private sector bodies such as the Economic League and the Consulting Association; where undercover officers have gone on to be managers, their conduct whilst undercover may shed light on practices they encouraged or condoned as managers.

98. Moreover, there will be some, perhaps many, deployments where the Inquiry does not currently have any non-state witnesses. This is particularly the case with the early deployments. If the opportunity to make submissions on the content of the hearing bundles were limited to witnesses in those circumstances, there would be no opportunity for non-state input, even though the

deployments might be of very significant interest to NPNSCPs and the public, for the reasons given above.

99. It is not enough that the NPNSCPs would have disclosure of some of the documents when the hearing bundle is disclosed to them. By that stage, the scope of the investigation will already have been heavily determined by the Inquiry's selection of documents, based on the state submissions alone.

100. The NPNSCPs submit that, prior to determining the content of the hearing bundles, the Inquiry should disclose to all CPs a schedule of all of the documents relating to that tranche, with a brief description to enable the nature of the document, subject to any lawful restriction, to be ascertained. Given the requirement in Rule 18(1)(a) of the Inquiry Rules 2006 to have regard to the need to ensure that the record of the Inquiry is comprehensive and well-ordered, it is anticipated that the Inquiry is creating a comprehensive log of the documents it has received in any event. Disclosure of that log would enable CPs who are not witnesses in respect of a particular deployment to make submissions about the contents of the hearing bundle. This would help to ensure that thematic issues of particular concern to NPNSCPs are not missed, particularly in relation to deployments where there are no non-state witnesses or CPs available to the Inquiry.

101. The NPNSCPs' fourth submission is that hearing bundles should be published in sufficient time in advance of hearings to enable any further non-state evidence to emerge. On the Inquiry's proposed process, disclosure of the hearing bundles to CPs in advance of the hearings will be the first opportunity for NPNSCPs who are not directly affected by the deployments to see the documents. It must be envisaged that there will be circumstances where that disclosure enables NPNSCPs to realise that they have relevant evidence to give that has not been apparent to the Inquiry on the face of the papers. It is important that there should be *sufficient time* between disclosure of the hearing bundles and the hearings themselves to allow such evidence to be captured.

102. The NPNSCPs' fifth submission is that, whilst plainly an onerous task, the processing and disclosure of sensitive documents is not unique to this Inquiry, either in volume or extent. The volume of documents reported to have been disclosed to date in the Grenfell Inquiry and in IICSA is cited at §65 above. These are comparable to the estimation of 26,000 pages over a ten-year period given by the Chair at the 31 January 2019 hearing. Further, in terms of sensitivity, it is plain that data relevant to the sexual abuse of children, some of which is simultaneously the subject of criminal investigations, will require extremely careful consideration prior to disclosure and publication; yet IICSA is successfully conducting public hearings, including with live-

streaming. It is understood that protection of private data is achieved in that Inquiry through use of ciphers – see Inquiry protocol on redaction of documents (version 3) https://www.iicsa.org.uk/key-documents/322/view/2018-07-25-inquiry-protocol-redaction-documents-version-3.pdf. And opportunities are also afforded to individuals to make representations in support of further redaction following disclosure to them and prior to wider publication.

103. It does not appear that redaction in order to protect the privacy of individuals in that Inquiry has rendered documents impossible to follow, or public hearings impossible to conduct.

104. The NPNSCPs submit that the same is achievable in this Inquiry. This is illustrated by the annotated versions of Annexes A and B prepared in advance of the 31 January 2019 hearing. The versions produced on behalf of the NPNSCPs to illustrate how those documents would look when redacted for the purposes of publication show that the level of redaction required in order to protect the privacy of those named is not particularly extensive and certainly does not render the documents unintelligible.[21] In the majority of cases, it will be sufficient simply to redact the surname of the individual referred to. If there has been adequate and proportionate notification and engagement with individuals who are contactable, the NPNSCPs proposed approach to redaction at the public hearing stage would be proportionate.

105. In respect of Annex B, the Chair queried the fact that Bella, the sister of Amanda Argento would be readily identified on the NPNSCPs' proposed version for publication – see transcript of hearing p.172 li. 18 et seq. As explained by Mr Facenna in response, on the understanding that the Argento family justice campaign was a matter of public record and the identity of the deceased and the relevant members of the family are all in the public domain, then there are no privacy or data protection concerns which would require redaction of family members in a document such as Annex B.

106. The Chair queried whether the position would be different if there were other documents in which individuals referred to in Annex B would be identifiable. Undoubtedly the Inquiry will need to be alive to jigsaw identification of individuals, particularly where this enables them to be linked to special category data that is not otherwise in the public domain. However, the process and principles proposed by the NPNSCPs provide a proportionate safeguard:

[21] CTI raised a query about the proposed gist in Annex A in relation to Andrew Anderson's sexuality, which the NPNSCPs accept, but it is a matter that can be easily rectified by minor adjustment to the proposed redaction.

a. through the redactions of surnames and other personal information that would enable identification of individuals by members of the general public, e.g. by internet search; and

b. through the process of proportionate notification, so that individuals about whom significant and/or sensitive personal data may be published by the Inquiry have a reasonable opportunity to know in advance that this is the case and to make representations accordingly.

107. The NPNSCPs do not deny that this process will require some additional work, and adjustment to the Inquiry's currently preferred approach. But it is a process that is: (i) required for the Inquiry to comply with its legal obligations; (ii) demanded by fairness to non-state individuals, given the resources that have been afforded to securing the privacy rights of former undercover officers; (iii) followed by other Inquiries, such as IICSA, demonstrating that it is possible to conduct a public inquiry into highly sensitive issues whilst affording protection to the privacy rights of those involved.

(7) Conduct of hearings

108. Paragraph 5(x) of the Process Note states that "*it is intended that, pursuant to Rule 10 of the Inquiry Rules 2006, the questioning of witnesses in public hearings will normally be conducted by counsel to the Inquiry who will ensure that any questions asked comply with any restrictions imposed on the written evidence*."

109. The NPNSCPs note that the Inquiry has previously said, in its Strategic Review, that it will "*issue a questioning protocol before the evidential hearings begin covering its approach to rule 10 of the Inquiry Rules 2006, which permits the Chairman to control questioning. There is likely to be room in appropriate cases, such as where there is a profound conflict of fact, for the use of cross examination, by recognised legal representatives of relevant witnesses, including core participants, provided that it is done in a cost efficient, timely and proper manner*."

110. The NPNSCPs welcome the indication from the Strategic Review that there will be room in appropriate cases for cross examination by RLRs and had understood that, prior to issuing the questioning protocol referred to, the Inquiry would consult with CPs, as it has in respect of its other protocols. The NPNSCPs would certainly wish to have the opportunity to make submissions in respect of how questioning is to be conducted. They strongly support the indication from the Strategic Review that in appropriate cases direct questioning of witnesses should be permitted by RLRs.

111. There is no basis for suggesting that RLRs will fail to comply with restrictions imposed on evidence. Further, RLRs have built up relationships of trust with the CPs they represent and will inevitably have more detailed and in-depth knowledge of the information known to their CPs, and will be better able to represent their concerns, through relevant questioning. In many circumstances, direct cross examination by RLRs is likely to be the most effective means of testing a witness' evidence and of getting to the truth. The NPNSCPs respectfully request that there be proper consultation in respect of this issue prior to any questioning protocol being issued.

(8) Live-streaming

112. The issue of live-streaming is not addressed in the Process Note, and the Chair stated at the 31 January 2019 hearing that the position indicated in his published statement of 19 December 2018 is not final. The NPNSCPs take this opportunity to make brief further submissions in support of their contention that live-streaming is a critical component of securing public access to the Inquiry's proceedings and should be supported to the greatest extent possible.

113. Public access to the Inquiry's proceedings is the starting point in accordance with s.18(1) of the Inquiries Act 2005. The MPS DLO are wrong to suggest that s.18(2) in any way overrides or qualifies the Chair's obligation arising from s.18(1) "*to take such steps as he considers reasonable to secure that members of the public are able to attend the inquiry or to see and hear a simultaneous transmission of proceedings at the inquiry*". The effect of s.18(2) is to make clear that any recording or broadcast of proceedings must be at the request of the chairman or with his permission and must not breach any restriction order. Those requirements do not alter or detract from the primary obligation in s.18(1) to take reasonable steps to secure public access. In other words, if it is reasonable to enable members of the public to see and hear a simultaneous transmission of the Inquiry's proceedings, then the fact that such transmission requires the permission of the chairman under s.18(2) does not alter that fact, it simply means that his permission should be given, subject to compliance with restriction orders. The relevant question remains the same: is it reasonable for there to be a simultaneous transmission, and, if so, in what form?

114. On the basis of the 19 December 2018 statement, the Chair appears to be of the view that because it will not be possible to live-stream some parts of the evidential hearings, it is undesirable for there to be any live-streaming. The NPNSCPs respectfully invite the Chair to revisit that conclusion. The importance of live-streaming for public accessibility to the Inquiry's proceedings is such that the question should properly be addressed on a case by case basis. For example, there are certain witnesses whose identity is so well-known that there cannot be any sensible suggestion

that further broadcasting of his or her identity will enable him or her to be identifiable to any greater extent that s/he is already. Former officers such as Mark Kennedy and Peter Francis would fall into this category. These are also witnesses in whom there is likely to be very significant public interest and in respect of whom it is unlikely to be possible to accommodate, in a regular hearing room and over-flow room, everyone who would wish to hear their evidence. In those circumstances, live-streaming is particularly important. The fact that it may not be possible in some other cases is not a good reason for ruling it out in all cases.

115. It is right that, even where a witness is not themselves subject to anonymity, some aspects of their evidence may be restricted and so would need to be approached carefully. However, that is the case whether their evidence is to be live-streamed or not. Inevitably there will need to be careful case by case decisions as to how a witness's evidence can be heard. This will involve a range of options, from closed hearings in respect of the most sensitive evidence, to fully public hearings wherever possible. Where hearings are conducted in public, steps will have to be taken to ensure that information that is subject to restriction is not disclosed. That is the case whether the hearing is live-streamed or not and is something that many courts and tribunals face. The IICSA hearings, many of which are available publicly online, provide one such example. Concerns about inadvertent disclosure are addressed by imposing a time delay on reporting and also on transmission of the proceedings. There is no reason why a similar approach could not be adopted in this Inquiry.

116. In short, the fact that live-streaming will not be possible in respect of some evidence is not a reason for rejecting it for all evidence. In many cases it will be the only means of securing reasonable public access to the Inquiry's proceedings. There are already over 200 NPNSCPs from all around the UK. The number of individuals directly affected by undercover political policing is inevitably very significantly higher than that. Further, the issues raised by the Inquiry are of significant wider public interest. The Inquiry has previously rejected the NPNSCPs' submissions that it should sit in different parts of the country, and regularly refuses applications for reimbursement of expenses to attend hearings. Live-streaming is, in reality, a necessary and cost-effective means of ensuring that those who would wish to see and hear the Inquiry's proceedings are able to do so.

117. Evidential hearings are not now due to take place until 2020. There is no imperative to reach a final view in relation live-streaming at this stage, let alone a blanket position. It is also an issue that requires a separate hearing at which wider interests, such as that of the press, before the Inquiry reaches a position on the correct approach in principle. Further, given the fundamental importance of live-streaming to public access to the Inquiry's proceedings, this is an issue which

falls to be determined on a case by case basis when the Chair is assessing how much of a witnesses' evidence can be given in public and whether any special measures are required.

GERRY FACENNA QC
RUTH BRANDER
JULIANNE KERR MORRISON
8 March 2019