## Chairman's statement on Data Protection and Privacy

1. This statement sets out the approach which the Inquiry will follow to reconcile its obligation to fulfil the terms of reference – in particular, to get at the truth about undercover police deployments – with its obligation to respect the data protection rights of those affected by the deployments. It is made following consideration of written submissions made on behalf of all necessary participants in the Inquiry and oral submissions made in two open hearings on 31 January and 25 March 2019. It addresses this issue only in respect of evidential documents and information provided to the Inquiry by state sources, including serving and former police officers, for the purpose of its substantive investigation.

2. The nature and scale of the task needs to be understood. In relation to the Special Demonstration Squad alone, the Inquiry has received or will receive tens of thousands of intelligence reports produced by undercover officers, which refer to thousands of people. They range from short reports about one or two individuals to lengthy reports concerning scores. They record a wide variety of information, such as, the membership of political groups and their organisation and management, the views expressed by leading figures and others in private and public meetings about their outlook and ideology, plans for future public events, such as, marches and demonstrations and the attitude of participants to public order and the commission of criminal offences. References to past participation in public disorder and convictions, now spent, of named individuals are not uncommon. In a smaller number of instances, there are references to more serious past or prospective criminal activity. A significant number of reports contain comment and information about personal relationships, in particular, between the members of infiltrated groups.

3. Once the reports have been obtained by the Inquiry, they are uploaded onto the Inquiry's secure computer system. As at 25 March 2019, 67,400 relevant documents have been uploaded, including the majority of Special Demonstration Squad intelligence reports created between August 1968 and February 1985. They are tagged by reference to the undercover officer, where identified, and named core participants. Tagging is necessarily imperfect, but will permit the Inquiry to provide sufficient documents to those from whom evidence is sought to produce a well-informed witness statement.

4. For the reasons given in paragraph 6 of my note dated 26 February 2019, I do not accede to the proposal made by the non-police, non-state core participants to

provide documents to them before former undercover officers. The first stage of the evidence gathering process after documents from state sources have been obtained and analysed will be that set out in paragraph 5(1) of the note dated 26 February 2019. This requires that the Inquiry provides a set of documents to the officer from whom a witness statement is sought. It includes the material which the officer needs to see to make a witness statement, principally, intelligence reports attributed to that officer. They will include the personal data, including special category data, as defined by article 9.1 of the General Data Protection Regulation (GDPR), of numerous individuals, including non-state core participants. The processing of data other than special category data is permitted by article 6.1(c) & (e) of the GDPR and section 8(c) of the Data Protection Act 2018: it is necessary for the exercise of a function conferred on me by sections 1, 2, 4 and 24 of the Inquiries Act 2005. The processing of special category data requires separate consideration.

5. One element of special category data is frequently referred to in intelligence reports: data revealing the political opinions of the data subject. Others, in particular, data revealing racial origin, trade union membership and data concerning a person's sex life, feature regularly, but less often. Processing of this data is only lawful for reasons of substantial public interest, on the basis of UK law: article 9.2(g) of the GDPR. It is undertaken for reasons of substantial public interest, because without it the Inquiry could not fulfil its terms of reference, but it requires a UK statutory basis for it to be lawful. That basis is to be found in section 10(3) of and Part 2 paragraphs 5 and 6 of Schedule 1 to the 2018 Data Protection Act. Some intelligence reports contain data relating to criminal convictions and offences. Processing of this data is only lawful when authorised by UK law: article 10 of the GDPR. The UK authorisation is to be found in section 10(5) of and Part 2 paragraphs 5 and 6 of Schedule 1 to the 2018 Data Protection Act.

6. Nothing in the GDPR or the 2018 Data Protection Act expressly requires that intelligence reports be shown to those named in them before they are shown to the undercover officer who produced them. However, unless there is a relevant UK statutory exemption, the Inquiry is required by article 14(1) – (4) of the GDPR, to provide certain information to the data subjects named in the intelligence reports within one month of obtaining them. That information includes the purposes of the processing for which the data are intended and its legal basis, the categories of personal data concerned and the recipient or categories of recipient of the data.

7. There is no difficulty in providing this information about how the Inquiry will process the data about those named in intelligence reports. The Inquiry has published a Privacy Information Notice and for some time now has been publishing cover names and associated details on a rolling basis. The note published by the Inquiry dated 26 February 2019 also provides that information, in respect of intelligence reports which the Inquiry already has and those which it expects to receive. It will provide more detailed information as set out in paragraph 5(iii) of my note dated 26 February 2019 in due course.

8. The difficulties are twofold. The first lies in identifying, tracing and notifying the individuals concerned personally. The Inquiry only has contact details for a small fraction of those whose personal data it has in its possession or will acquire. The limited experience which the Inquiry so far has had (when tracing the surviving relatives of deceased children whose name has been adopted by an undercover officer) suggests that contacting individuals about whom the name, but little else, is known is problematic and time-consuming. Repetition of the exercise in many thousands of cases would impose a heavy burden of time and cost on the Inquiry. The second is that the Inquiry cannot establish the full extent of what could be safely communicated until it has put the relevant data through the restrictions order process.

9. In the absence of a statutory exemption, every one of the thousands of data subjects named in the intelligence reports would be entitled to make a request for access to personal data under article 15 of the GDPR, to which the Inquiry would be required to respond by providing a copy of the data undergoing processing, within one month of the receipt of the request, extendable by at most two further months: article 12.3 of the GDPR. It would not be possible for the Inquiry to discharge this obligation. If it were to use its legal team and IT and administrative resources to do so, the substantive work of the Inquiry would come to a halt. If it were to attempt to do so by obtaining additional capacity, it would require new office accommodation, a replacement IT system and additional staff and/or contractors. The individuals required to perform the task of extracting data and communicating it to data subjects would have to be security cleared, a process currently taking many weeks. The problems would not end there. The Inquiry has received documents from state sources on the footing that they will be entitled to apply under section 19 of the Inquiries Act 2005 for restriction orders in respect of their content, before they are disclosed to others. The Inquiry must determine that

application before it can know what can safely be disclosed. Thus far, it has taken several weeks to subject quite small batches of documents to this process.

10. Further, fulfilment of the data subjects' rights to access to personal data would have to be conducted in a manner which did not adversely affect the rights and freedoms of others: article 15.4 of the GDPR. This would require either the redaction of their personal data from documents containing information, securing their consent to disclosure or dispensing with it under Schedule 2 Part 3 paragraph 16 to the 2018 Data Protection Act. Redaction would, inevitably, result in documents so heavily redacted as to make them difficult for the data subject who had made the access demand to understand. Even if this process were practicable, which it is not, it could not be achieved within the timeframe required. The only certain outcome would be prolonged delay in the fulfilment of the terms of reference of the Inquiry.

11. Parliament cannot have intended that these consequences should flow from statutory provisions designed to qualify and give practical effect to the GDPR in the UK. A public inquiry set up under the Inquiries Act 2005 is the weapon of last resort available to the Government to get to the truth and inform remedial action about events which suggest that the existing regime for monitoring, inspection and regulation of activities, typically conducted by the state, has failed. Article 23.1(h) of the GDPR permits Member States to restrict by way of a legislative measure, the scope of the obligations and rights provided for in articles 12 to 22 to safeguard a monitoring, inspection or regulatory function connected to the exercise of official authority in the case of public security and the prevention investigation detection or prosecution of criminal offences. The restriction must respect the essence of fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society. By section 15(2) of and Schedule 2 Part 2 paragraphs 6 and 7 to the 2018 Data Protection Act, articles 14 and 15 of the GDPR are dis-applied to personal data processed for the purpose of discharging certain functions "to the extent that the application of those provisions would be likely to prejudice the proper discharge of the function". By paragraph 7.2 the function includes one "designed to protect members of the public against – (a) dishonesty, malpractice or other seriously improper conduct, or (b) unfitness or incompetence" provided that the function is "(a) conferred on a person by an enactment … (c) of a public nature, and is exercised in the public interest".

12. This Inquiry discharges that function and fulfils both of those conditions. One of its purposes is to protect members of the public against malpractice or other

seriously improper conduct or unfitness or incompetence on the part of undercover police officers by getting to the truth of what happened in past deployments and making recommendations for the future in the light of those findings. It is unnecessary to look outside the clear words of the statutory provisions. They speak for themselves. They fit within the enabling provision – article 23.1(d) and (h) of the GDPR. The circumstances in which it is permissible to look behind the words of the statute, identified in *Pepper v Hart* [1993] AC 593 do not obtain.

13. For the reasons explained above, the application of articles 14(1) – (4) and 15 of the GDPR would certainly prejudice the fulfilment of the terms of reference of the Inquiry and so the discharge of its function. If it were to be contended that, notwithstanding that conclusion, the Inquiry was obliged to address the issue in relation to one or a limited number of identified data subjects, I would reject the contention. Article 14 cannot be applied in that way for the reasons explained at paragraphs 6 – 8 above. Nor is there any basis in the language of the statutory exemption for treating one request under article 15 in a manner different from any other request or number of requests. It is the application of article 15 which will cause prejudice to the proper discharge of the function of the Inquiry. If it applies, the Inquiry will have to establish arrangements for requests to be met within the timescale set by article 12.3.

14. For the reasons explained above, this cannot be done on an ad hoc basis. I accept the observation of Green J in *Zaw Lin and another v Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB) under the differently worded predecessor legislation that a "classic proportionality balancing exercise" is required between the rights of data subjects to access and the right of the Inquiry to refuse access; but it is the rights of the data subjects whose data the Inquiry holds, taken together, and the prejudice which will be caused to the discharge of its function, which must be balanced. What the data subjects will gain is the early disclosure to them of their personal data – a timing issue but also in less informative, more redacted form.

15. The cost of producing that benefit is that the substantive work of the Inquiry will be disrupted and delayed. This will, in turn, mean that the opportunity for others affected by undercover policing to learn about it and how it affected them, to provide information or evidence about it to the Inquiry and to have the information necessary to permit them to vindicate their rights will be delayed. The wider public will not be informed about what was undertaken by undercover police

officers on its behalf and about what went wrong. Recommendations for the future conduct of deployments will be delayed.

16. These considerations weigh heavily in the balance against providing early access to personal data to those making requests under article 15 of the GDPR. The result of the balancing exercise is that such early access cannot be given, save, perhaps, in exceptional circumstances.

17. In the light of that conclusion, it is not necessary to consider the further exemption contained in Schedule 2 Part 2 paragraph 14(2)(a) to the 2018 Data Protection Act.

18. Article 5.1(a) of the GDPR requires personal data processed by the Inquiry to be processed lawfully fairly and in a transparent manner in relation to the data subject. Step 1 of the evidence gathering process referred to in paragraph 4 above fulfils that requirement. More difficult problems arise in Step 4. To permit non-state core participants and witnesses to know what was reported about them so as to permit them to give information and evidence to the Inquiry and so to assist it to fulfil its terms of reference, they must be shown the relevant parts of the officer's witness statement and accompanying document. If lawful and practicable, it is the intention of the Inquiry that they will be shown copies of the intelligence reports which refer to them. Typically, these reports contain extensive references to the personal data, including special category data, of others. For the documents to make sense to the core participant to whom they are shown, substantially unredacted copies must be shown to them. Even if the practical problem of contacting large numbers of people to seek their permission to disclose documents in which they are named to the core participant could be overcome, there would still be an insoluble problem: to seek their permission, they would have to be told the name of the core participant and shown the documents in which both are named. The process of seeking permission would, in most cases, inevitably reveal to all concerned the personal data, including special category data, of all named in the documents.

19. The Inquiry has identified only two potential approaches to resolving this conundrum: making a severe selection of the documents which can be shown to core participants and redacting all references to others from them; or disclosing intelligence reports containing their personal data, to them, subject to a restriction order and/or an undertaking as to their use. This would, of course, result in the disclosure to them of the personal data, including special category data, of

others. It would also inevitably involve the disclosure of their personal data, including special category data, to other core participants and/or witnesses on the same terms.

20. In the light of written and oral submissions made by or on behalf of non-state core participants, a variant of the second option may be practicable. The Inquiry is willing to explore with non-state core participants the possibility of redacting references to intensely personal matters, such as sexuality, intimate personal relationships or relationships with children from intelligence reports before they are shown to other non-state core participants or witnesses. This will require trial consideration, with an individual non-state core participant of a set of intelligence reports referring to that individual produced by a single undercover officer. A proposal will be made to that effect by the Inquiry, and if agreed, the relevant reports will be disclosed, in the first instance to that individual, once they have gone through the public interest redaction process. This real life example will demonstrate the problems which will remain, even if a variant of this suggestion is approved, but may result in a process acceptable to most.

11 April 2019

Sir John Mitting
Chairman, Undercover Policing Inquiry