The Fraud Lawyers Association Submission to the Independent Review of Disclosure and Fraud Offences

INTRODUCTION

1. This submission to the Independent Review of Disclosure and Fraud Offences ("the Review") has been prepared on behalf of the Fraud Lawyers Association ("FLA"). The FLA was established in 2012 and its members are practitioners from leading solicitors' firms and barristers' Chambers in the field of both criminal and civil fraud. Membership of the FLA is open to solicitors over 6 years PQE and barristers of over 8 years call. The FLA aims to provide a forum to represent experienced lawyers practising in the areas of civil and criminal fraud, including responding to Consultations; deliver education and training to its members and offer its members the opportunity to share knowledge and build professional relationships.

2. Given our area of expertise, this submission only addresses disclosure in the context of complex white collar crime cases.

3. In preparing this submission, the FLA Main Committee formed a sub-committee which consists of 8 members of the Main Committee. The sub-committee comprises senior solicitors and barristers, all of whom have a wealth of expertise in white collar crime. All the members of the sub-committee have significant experience defending in large scale white-collar crime prosecutions brought by agencies including the Serious Fraud Office (including notably LIbor, Tesco, G4S, Serco and London Mining) HMRC, CPS and the FCA. One member of the sub-committee also has considerable experience of prosecuting for the Serious Fraud Office across a number of its high-profile cases.

4. The FLA sub-committee recognise that in this digital age challenges are faced by both the prosecution and defence in relation to disclosure in large scale white-collar crime trials. Disclosure is a vital part of every criminal trial. A full and proper disclosure process is fundamental to ensuring a fair trial for all parties which is at the core of our criminal justice system. A defendant has a right to an open and honest prosecution and to be provided with any material which could assist them in defending themselves.

5. We also recognise that there are differing views within our membership as to what changes could or should be made to the existing disclosure regime. We have therefore focused our submission on identifying issues within the existing disclosure regime that in our collective experience are most frequently encountered in practice and suggesting workable solutions to the same.

6. One solution upon which we are all agreed is the introduction of a presumption in white collar crime cases that where a defendant is accused in a work capacity (as will usually be the case) they should be provided as of right for the indictment period with copies of their own electronic work calendar, work emails and other work documents to which they would have had authorised access. These items represent one of the central disclosure areas for any defendant in a serious fraud case and whilst they are usually disclosed, this tends to occur late in the process and only after much correspondence, legal argument and court time.

7. The operation of such a presumption in white collar crime cases would allow the early provision of these items, thereby ensuring a defendant has sufficient time to review key material, alleviating the disclosure burden on the prosecution, saving time and money for all parties and reducing the prospect that a trial will be derailed because of failures or delays in the disclosure process.[1]

[1] A different approach is required in white collar crime cases because such data is normally contained on devices belonging to their company or employer and hence there is no PACE 1984 entitlement to the same. In many non-fraud cases a defendant will have access to this type of relevant data because it is

8. Our response is structured as follows:

    a. Overview
    b. Common disclosure issues (summary)
    c. Solutions - keys to the warehouse: pros and cons
    d. Solutions – introduction of a presumption in respect of a defendant's work material
    e. Solutions - other
    f. Appendix 1 – Common disclosure issues (further detail)

A. OVERVIEW

9. Two members of our sub-committee attended the 12 March 2024 Legal Professionals Roundtable discussion as organised by Justice and the Review. At that discussion and indeed elsewhere there has been a focus on two issues said to be central to the effective operation of the current disclosure regime:

    a. Lack of defence engagement
    b. Managing the volume of digital material

10. In our collective experience giving primacy to these two issues runs the risk of missing other arguably more fundamental and pressing disclosure issues.

11. In our real world and very current experience, lack of defence engagement in serious fraud cases is extremely rare. One solution to this perceived problem raised at the Legal Professionals Roundtable discussion was the imposition of a strict disclosure timetable, including a provision that if the defence fail to make its section 8 Criminal Procedure and Investigations Act 1996 ["CPIA"] application according to that timetable, no such application would be permitted

stored on their own personal electronic devices (laptop, phone) which is returned to them (or copy provided) under PACE 1984.

other than in exceptional circumstances.

12. We would strongly urge the Review against any such approach. Firstly, it is seeking to address a problem which we very rarely encounter in serious fraud cases.[2] Secondly it would be wholly unworkable in practice. A fair trial cannot take place where disclosure issues are left unresolved.

13. Effective management of a large volume of digital data is an important part of any workable disclosure regime in serious fraud cases. Ever increasing volumes of digital data present a substantial challenge for those responsible for the investigation and prosecution of serious fraud. However, many of the associated problems are likely to be addressed with the introduction of technology for example Technology Assisted Review which is currently being trialled by the SFO, and the use and disclosure of metadata to facilitate fair and effective block listing. Solutions in these areas are developed further in Section E below.

14. Provided there is proper funding, in our view the problems presented by the volume of digital material are eminently solvable by the use of emerging technologies and artificial intelligence.

15. However, it is not the volume of material (or volume alone) that has been at the core of disclosure failings in recent SFO cases. The prosecutions of individuals from Serco and Unaoil – considered in the Altman and Calvert-Smith reviews - share a common disclosure failing with the more recent prosecution of individuals from G4S. In each case key unused documents were identified as relevant and reviewed by the SFO but not disclosed to the defence when they could and should have been. When this material was later disclosed (either by chance, the due diligence of the defence or by order of the court) the previous failure to do so, or do so at the appropriate time, proved fatal to the case.

[2] Nor have we seen any empirical data suggesting our experience is atypical.

16. In Unaoil, the Court of Appeal concluded that communications between the Director (and others at the SFO) and a third party acting for co-suspects, should have been disclosed. This was material very familiar to the prosecution, but the wrong decision was taken that it not be disclosed.

17. In Serco, important material was identified by the SFO as relevant, but wrongly described on the schedule of unused material which when reviewed was not considered to be disclosable; it was material to which the defence was plainly entitled. The flawed decisions taken when reviewing the material were not subsequently identified in the disclosure review process.

18. In G4S, the existence of key documents supporting the defence was only disclosed weeks before the second trial date. Considered for disclosure by the SFO much earlier in the proceedings, a decision had been taken to classify these documents as sensitive and they were not disclosed. By the time their existence emerged it was too late for the SFO to conduct the extensive review of associated material that it then acknowledged was required. Instead of seeking a further adjournment of the trial and responding to an abuse of process application based on the failure to disclose, the SFO offered no evidence.

19. In each case, notwithstanding the volume of unused material, the documents in question were identified by the SFO as relevant and reviewed for disclosure. Difficulties resulting from unmanageable volumes of material were not the core contributor to these cases failing, it was the wrong decisions taken not to disclose material that was reviewed.

20. The decisions in these cases are not consistent with a disclosure test that is too generous to the defence or too onerous for the prosecution. They are consistent with a prosecutorial approach that fails to properly apply that test, either because the prosecutor does not understand or engage with the defence issues or is generally too defensive. In short, the issue in each case was that too little material was disclosed, not too much.

B. SUMMARY OF COMMON DISCLOSURE ISSUES ENCOUNTERED IN SERIOUS FRAUD CASES

21. In our experience, most disclosure problems in serious fraud cases are caused by a combination of the following:

    a. A defensive and dismissive culture toward defence disclosure requests, including a lack of early and meaningful engagement by the prosecution with issues and areas raised by the defence.
    b. Poor quality decision making about whether material is disclosable.
    c. Lack of consistency from case to case.
    d. Disclosure issues being resolved far too late in the trial process, exacerbated by the lack of any meaningful sanctions on the prosecution for failing to adhere to court orders.
    e. Unused schedules which fail to describe all material clearly and logically.
    f. Disclosed material being provided in a format which makes its review difficult.
    g. Over reliance on third parties within the disclosure process.

22. These factors are developed within either Section E or Appendix 1.

C. SOLUTIONS - KEYS TO THE WAREHOUSE: PROS and CONS

23. One solution sometimes posited as a remedy for disclosure failings is to compel the prosecution to either disclose or otherwise facilitate access to all unused material to all defendants, irrespective of whether it meets the CPIA test. This approach is often referred to as giving the defence the 'keys to the warehouse' (**KTW**).

24. On its face, KTW purports to solve the current disclosure challenges by placing the 'power' in the hands of defendants. By providing the defence with unfettered access to all unused material, KTW:

a. Bypasses ‘defensive culture’ on the part of investigators and prosecutors, by removing any discretion as to whether material is disclosed.
b. Prevents material that should have been disclosed being missed as a result of prosecution error.
c. Maximises the amount of time available for the defence to review unused material.
d. Ensures equality of access to unused material between co-defendants.

25. However, despite its immediate appeal, consideration of the likely practical experience of KTW suggests a number of likely flaws:

a. Whilst KTW may bypass ‘defensive culture’, it does nothing to address its root causes. It may even exacerbate the problem, as investigators decide not to seek out or review material that points away from the prosecution case, on the basis that the defence will be given the opportunity to do so in due course. The unintended consequence of KTW could be an increased number of reckless and ill-considered charging decisions, which might not have been taken had the prosecution conducted an objective and thorough disclosure review. Whilst the flaws in such prosecutions **might** be identified and remedied once the defendants are ‘given the keys to the warehouse’, it is by no means a guaranteed failsafe.

b. Irrespective of whether defendants are publicly or privately funded, there will inevitably be an ‘inequality of arms’ between prosecution and defence in ability to deal with disclosure in document- and data-heavy fraud cases. This is true with respect to both resources (with only the biggest defence firms being able to match agencies with respect to the number of suitably qualified lawyers at their disposal) and time (the prosecution having the life of the investigation to review disclosure, with the potential to extend that if needed, whereas the defence have the time prescribed by the court and Criminal Procedure Rules). It makes no sense for the burden of the disclosure exercise to fall on the defence

only after charge.

c. Legally Aided defendants will inevitably be disadvantaged by the limitations imposed by public funding. Whilst access to material with KTW might be unlimited, the amount of review work that their lawyers can conduct is far from it. As noted above, even if Legal Aid lawyers had unlimited funding, they would still be constrained by time and staff availability.

d. Peripheral to the above, any costs saved by investigative agencies in not conducting thorough disclosure exercises would almost certainly be lost by an increased burden on Legal Aid. It may even result in a multiplication of costs, as several defence firms seek to replicate the work that could have been done more efficiently by the prosecution in a consolidated exercise.

e. Beyond public funding, only a tiny minority of private-paying defendants have the means to conduct a full-scale 'warehouse' disclosure review, the cost of which will not be recovered even on acquittal. The current policy limits of Directors & Officers or other insurance funding is unlikely to sustain the amount of review work potentially required by the KTW approach. If such an approach were to become the norm, it may lead to D&O insurance routinely excluding criminal litigation, or particular elements of it. Alternatively, such cover might become so prohibitively expensive that companies opt not to take it, which in turn increases the pool of defendants either having to self-fund or reliant on Legal Aid.

f. KTW is also based on a presumption that a defendant will always be best placed to identify all items of unused material that may assist the defence or undermine the prosecution. Whilst this **may** be correct with respect to material which with the defendant is already familiar (and is therefore more likely to have access to by other means anyway), it is unlikely to be true of material generated by the prosecution or obtained from third parties. It is untenable to suggest that (even if funding were

available, which in the majority of cases it would not be) a defendant should be expected to spend finite resources speculatively trawling unfamiliar prosecution and third-party material in the hope of identifying exculpatory material, particularly in document- and data-heavy fraud cases. In this regard in particular, the KTW approach deprives defendants of the valuable advantage of having a disclosure exercise conducted on their behalf by a party with familiarity of the whole case, and not just the elements of which the defence is aware.

g. To the extent that there are any legitimate data protection issues arising from disclosure obligations, these are certain to arise in KTW, given that it necessarily involves all material being made available to all defendants.

h. KTW would not address a failure by the prosecution to pursue a reasonable line of enquiry. As such, it should not be presumed to be a panacea for avoiding pre-trial disclosure litigation.

D. SOLUTIONS – INTRODUCTION OF A PRESUMPTION IN RESPECT OF A DEFENDANT'S WORK MATERIAL

26. In serious and complex fraud cases, the same disclosure issues are repeatedly being litigated, with the parties and the court expending considerable time and resource on arguments about material that is eventually disclosed. A presumption in favour of disclosure of a small number of categories of this material has the potential to make a significant difference to the efficiency of the disclosure process.

27. The presumption would apply in cases where the allegations against a defendant occurred in the context of his work and would be limited to the indictment period. The categories of material to which the presumption would apply are as follows

a. A defendant's work emails

b. A defendant's work diary or calendar
c. Business documents to which the Defendant had authorised access

Such a presumption would allow the provision of this material to the defendant at a very early stage. This would minimise delay and afford the defence proper time to review the material.

28. The proposed presumption could be achieved by a change to the Attorney General's Guidelines on Disclosure [AGD] to create the presumption in the same way as is currently done at paragraphs 86-88 of the 2024 current AGD in respect of other categories of material.[3]

29. In our view, such material should also be cross-disclosed to other defendants in the same proceedings. Cross disclosure is normally the approach taken by the prosecution in serious fraud cases. That approach is sensible because it minimises the risk of unfairness caused by defendants having access to different sets of disclosed material.[4]

30. We develop below the reasoning behind the need for a presumption in favour of such categories of material.

(i) Work Emails and Calendar

31. Serious fraud cases often involve detailed scrutiny of events from years earlier and work emails will form the principal record of a defendant's working life during this period. As recollections inevitably fade, contemporaneous emails are often the only remaining record of what occurred during the working day many months or years before – both the relevant events which took place and of the understanding and approach of the individuals concerned. They are likely

[3] i.e. 'The following material ..is likely to include information which meets the test for disclosure: [list of categories]'

[4] It is appreciated that cross disclosure may raise data protection concerns but the tail should not wag the dog. If workable and effective solutions are needed to recurring disclosure problems there should be clear and consistent guidance provided about what redaction is actually required by law and proper funding provided to ensure technology assisted redaction where it is so required. See section E(iv) below.

to constitute admissible and largely independent evidence of these matters. They are the first source to which anyone would wish to turn if asked to recall and justify an aspect of their work many months or years after the event.

32. The prosecution's common approach in these cases is to refuse to disclose an individual's emails from this period as a block. Instead, defendants are asked to identify each email for relevance using imprecise tools such as date range or key word search, with the resulting material reviewed by the prosecution for disclosure. This is time consuming, far from pragmatic and risks disclosable material being missed or emails being disclosed in a way that paints an incomplete picture. It fails to acknowledge that an email box can be viewed as a block of material which taken together may satisfy the test for disclosure and might reasonably (and proportionately) be considered capable of assisting the defence, even where individual documents within the block when viewed in isolation would not do so.

33. It is an approach routinely challenged by the defence, first in correspondence and then by way of application(s) to the court. The result is often disclosure of most or all a defendant's emails from the indictment period.[5]

[5] The recent G4S case is an example. The SFO's approach was that only individual emails that met the test for disclosure would be disclosed and initially relied on key word searching to identify emails (and other material) that may be relevant.
One of the defendants had access to a copy of his work emails the other two did not and they sought disclosure of the emails as a block. The SFO refused. An application was made to the court which was opposed. The parties were directed to try to agree periods of time from which the prosecution would review all emails for disclosure, but agreement could not be reached.
After a further application, the court directed the SFO to disclose a schedule setting out the metadata for each email (information such as 'to' 'from' 'date' 'recipients' 'subject' and the names of attachments). This resulted in a schedule of over 500,000 entries, one for each email, which was disclosed to the defence. The defence were required to consider each entry in the schedule of metadata to identify those it thought may satisfy the test for relevance by reference to their defence statement. The SFO were then to consider each underlying email identified in this way on the schedule, to review for relevance and to determine whether it should be disclosed.
The SFO eventually accepted the impracticality of this process and asked the court to order that any emails sought by the defendants be provided under the Criminal Procedure Rules, circumventing the need to identify whether individual emails were relevant and to describe those emails. The outcome was that very late in the day, all the emails were disclosed but only after a huge amount of time and resource was spent litigating the issue in correspondence and before the court and in considering the 500,000 entry metadata schedule.

34. A presumption in favour of disclosure would have a huge impact by bringing significant savings of time and resource that is otherwise spent determining relevance, describing emails on the schedule of unused material, deciding whether to disclose and litigating the issue.

35. A work diary or calendar sits alongside an individual's work emails as an important part of the record of what they were doing during their working life; the reasons for a presumption in favour of block disclosure are common to both.

(ii) **Business Documents to which the Defendant Had Authorised Access**

36. During their working life, a defendant will have had access to and engaged with particular sets of business documents for example reports for meetings, agendas and minutes. This material is relevant to any defendant seeking to recall how they spent their time at work, the information which was shared with them and how it was viewed within the business. Taken together a set of reports or minutes spanning an indictment period will in most cases satisfy the test for disclosure as a block of material, even where individual documents within the block when viewed in isolation would not do so.

37. Where a defendant identifies a set of business documents relevant to their defence to which they had authorised access, for example meetings that they have attended or a set of reports that they regularly received, there should be a presumption in favour of disclosure of this set of documents.

38. A presumption in favour of disclosure in these limited categories of material would make a significant difference to the efficiency and fairness of the disclosure process. Where the prosecution considers the material in each category should not be disclosed, their reasons for not following the presumption could be explained in the DMD.

E. SOLUTIONS -OTHER

39. As has been illustrated above, many of the issues experienced under the current disclosure regime arise not from the legislative test under section 3 of the CPIA itself, but rather from the practicalities associated with the management, review and provision of unused material. The extent of these practical difficulties has been aggravated in recent years due to the increasing volume of digital material generated by investigations, particularly in complex cases of serious fraud.

40. As such, significant improvements may be achieved within the existing legislative framework by enhancing prosecutors' technical capabilities and ensuring a consistent and workable approach to disclosure is employed across the various prosecuting authorities.

41. Several of the proposals outlined below echo suggestions presented in 2018 by the Attorney General's Office and House of Commons Justice Committee Reports on disclosure in the criminal justice system.[6] The issues arising from the present approach to disclosure have only become more pronounced in the years since these recommendations were made as the volume of material produced by investigations continues to increase – making the implementation of these proposals even more integral to the operation of the disclosure regime.

(i) Upgrade case management and document review systems, and increase the use of technology and AI to aid the disclosure process

42. As identified in the Attorney General's Office's 2018 Report, "*technology is part of the problem, but it can and should be a major part of the solution*."[7] At present, there is a significant range of information management systems employed by law enforcement which require upgrading and standardising at a national level.[8] The rollout of any new technology should be as wide as possible

[6] Attorney General's Office, "Review of the efficiency and effectiveness of disclosure in the criminal justice system", November 2018 (link); House of Commons Justice Committee, "Disclosure of evidence in criminal cases", 17 July 2018 (link).
[7] Attorney General's Office, "Review of the efficiency and effectiveness of disclosure in the criminal justice system", November 2018 (link).
[8] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).

so as to enable greater coordination across law enforcement, as well as to ensure equal treatment of defendants with regard to disclosure, regardless of which prosecuting authority is handling their case.[9] The adherence to common standards should be required of state and private prosecutors alike.

43. Technology may assist prosecutors, not only at the point of disclosure – but throughout the entire process – and it is therefore necessary to consider the full scope of improvements that technological advances may provide to the storage, acquisition and search components as well as the production and release components of the disclosure regime. [10]

44. As a starting point, improved case management systems should be introduced which are common across prosecuting authorities and allow for the effective indexing, cataloguing, and restructuring of the large volumes of digital material in their possession.[11] These systems are also integral in documenting disclosure decisions made in relation to individual documents and are especially important given the ongoing nature of the disclosure obligation.[12]

45. Increased analytical capabilities may also be applied, alongside the use of robust case management systems, through the introduction of enhanced search functions within the document review platform.[13] Although various data search functionalities are currently employed by prosecutors, these are often limited to basic text searches which raise issues of accuracy and consistency.[14] The increasingly broad sphere of digital data obtained during investigations also continues to raise new issues when it comes to review and upgraded technology is required to keep pace with these developments, such as by enhancing search capabilities through the use of video and image search technologies.[15] Given the scale of digital material which now characterises the

[9] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[10] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[11] CPS, "National Disclosure Improvement Plan – Progress Update", January 2020 (link); National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[12] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[13] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[14] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[15] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).

majority of fraud investigations, effective search capabilities are key to the identification of unused material for disclosure.[16]

46. The Altman Review has highlighted these points as a particular area for improvement by the SFO, recommending that it "*should invest (or continue to invest) in technology to ensure that document review and case management systems are obtained, designed and developed with a focus on the disclosure process.*"[17] Whilst the SFO has committed to implementing such systems,[18] it is clear that broader implementation of this technology across the various prosecuting authorities is needed to ensure that defendants are not penalised by varying disclosure management and document review capabilities amongst prosecutors.

47. Artificial Intelligence (AI) through the deployment of Technology Assisted Review, has the capability to analyse large volumes of data in an efficient, intelligent and iterative manner and may therefore vastly increase and improve prosecutors' disclosure capabilities. AI has already been employed by prosecutors on a case-by-case basis, for example by the SFO, which used OpenText "Axcelerate" to review documents for legal professional privilege in its Rolls-Royce investigation.[19] However, the full capabilities of AI in identifying unused material for disclosure are yet to be explored.[20]

48. Whilst the nuanced application of the section 3 CPIA test cannot wholly be outsourced to AI, under appropriate human supervision and with the correct checks and balances, the use of this technology is likely to vastly improve the speed and accuracy with which unused material can be reviewed.[21] The reality is that modern investigations now generate more data than can realistically be reviewed using present methods, and the adoption of new technologies is

[16] National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[17] SFO, "Implementation Update – May 2023: Altman Review", 24 May 2023 (link).
[18] SFO, "Implementation Update – May 2023: Altman Review", 24 May 2023 (link).
[19] SFO, "AI powered 'Robo-Lawyer' helps step up the SFO's fight against economic crime", 10 April 2018 (link); OpenText, "Serious Fraud Office uses artificial intelligence in the fight against crime" 2021 (link).
[20] Institute of Economic Affairs, "Fraud Focus – Is the Serious Fraud Office fit for purpose?" March 2023 (link).
[21] Information Commissioner's Office, "Mobile phone data extraction by police forces in England and Wales – Investigation Report", June 2020 (link).

required to address the capacity issues created by the increasing volume of material.[22]

49. The CPS has piloted several proof of concept initiatives, employing new technology as part of its Disclosure Improvement Plan, which has reportedly proved "*successful* [in] *improving efficiency and enhancing evidence in cases*".[23] The success of these initiatives supports the proposal that AI should be standardised as a tool for review so that the benefits in time-saving and accuracy are felt by prosecutors, and in turn also defendants, in all cases as opposed to a select few.

(ii) Mandate the form in which all disclosure should be provided

50. Prosecution practice varies with regard to the way in which disclosure is made.[24] Section 10.7 of the CPIA (section 23(1)) Code of Practice 2020 permits disclosure either by giving the accused copies of material or allowing them to inspect disclosed materials. This can often lead to prosecutors supervising access to disclosed material, as opposed to providing copies.[25] Further inconsistency is created by the same provision permitting a disclosure officer not to supply documents which the accused has been permitted to inspect where it is not practicable to do so, for example *"because the volume of material is too great".*[26] It is clear that this exception could apply to the majority of fraud cases.

51. There is also no standard as to the format in which disclosure should be provided. As has already been seen, effective search capabilities are key to managing large volumes of material – both for the prosecution in determining the material for disclosure, and for the defence in analysing the unused material received. The unused material schedule, despite listing material in blocks, may

[22] Information Commissioner's Office, "Mobile phone data extraction by police forces in England and Wales – Investigation Report", June 2020 (link); National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[23] CPS, "National Disclosure Improvement Plan (NDIP) Report on Phase Two - March 2021", 23 March 2021 (link).
[24] Kingsley Napley & 6KBW College Hill, *Serious Fraud, Investigation & Trial,* Fifth Edition, March 2023.
[25] Kingsley Napley & 6KBW College Hill, *Serious Fraud, Investigation & Trial,* Fifth Edition, March 2023.
[26] Section 10.7 of the Criminal Procedure and Investigations Act 1996 (section 23(1)) Code of Practice 2020 (link).

itself comprise thousands of items.[27] All disclosed material, including the schedule itself, should therefore be disclosed in searchable format as standard to enable the defence to identify and categorise relevant material within the unused material provided.[28]

52. If the prosecution relies on block listing to describe material on the unused schedule, where it is available the metadata for the block should be disclosed to the defence as part of primary disclosure. In many instances, this is will considerably reduce the potential risks and unfairness that may arise with a block listing.

53. Consistency should also be adopted in the provision of metadata as standard within disclosure, which must only currently be *"considered"* by the disclosure officer.[29] Metadata, used in combination with an effective disclosure platform, is essential to the defence's disclosure review as it contains key information relating to the creation date, attachments and thread of emails related to a document which enable materials to be grouped and analysed more efficiently.[30]

(iii) Prosecution to provide the defence with a common platform for the review of disclosed material

54. Similarly, changes to the current approach whereby the prosecution is not obliged to share the advantages of its documentary control system with the defence would go a long way in encouraging a consistent approach to disclosure review among defendants.[31] As the volume of unused digital material disclosed to the defence continues to grow, this compounds the inequality between defendants who have the resources to instruct firms with more

[27] Kingsley Napley & 6KBW College Hill, *Serious Fraud, Investigation & Trial,* Fifth Edition, March 2023.
[28] Kingsley Napley & 6KBW College Hill, *Serious Fraud, Investigation & Trial,* Fifth Edition, March 2023.
[29] Attorney General's Guidelines on Disclosure 2022, Annex A, paragraph 52 (link).
[30] Law Gazette, "What is metadata and why should you care" 12 May 2006 (link); National Police Chiefs' Council, "e-Disclosure Landscape Review", May 2019 (link).
[31] Kingsley Napley & 6KBW College Hill, *Serious Fraud, Investigation & Trial,* Fifth Edition, March 2023.

advanced document review capabilities, compared to those who are receiving legal aid.[32]

55. Whilst legislative reforms which allow criminal barristers to be remunerated for reviewing unused materials in cases where legal aid has been granted are a welcome step,[33] the introduction of a standardised review platform available for use by the defence, is now necessary to ensure greater equality between defendants in this area.

56. Well funded defence teams working on some large scale fraud cases will already share the same document review platform, with disclosed material only being ingested and stored once and the document being conducted by each team separately and confidentiality via the platform. If a prosecutor's document review platform was deployed in a similar way - with the defence given confidential access to disclosed material via the platform - this would achieve fairness between separate defendants and equality of arms between defence and prosecution. And it would do with very little additional cost.

(iv) Reduce the burden of GDPR issues

57. As disclosure activities amount to the "processing" of data under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), the need to redact "personal data" from large volumes of disclosure material places a significant burden on prosecutors' resources, creating a *"huge issue in terms of time"*[34] which has been described as one of *"the biggest problems affecting the police".*[35]

58. Increasing the technological capabilities of prosecutors would alleviate some of these pressures. The implementation of appropriate redaction software, such as the CPS' roll-out of Adobe Acrobat tools, is essential to improving the timeliness of the provision of disclosure material.[36] The use of improved

[32] House of Commons Justice Committee, "Disclosure of evidence in criminal cases", 17 July 2018 (link).
[33] The Criminal Legal Aid (Remuneration) Regulations 2020.
[34] House of Commons Justice Committee, "Disclosure of evidence in criminal cases", 17 July 2018 (link).
[35] Attorney General's Office, "Annual Review of Disclosure", May 2022 (link).
[36] CPS, "National Disclosure Improvement Plan (NDIP) Report on Phase Two - March 2021", 23 March 2021 (link).

document management software, as detailed in section *(i)* above, would also enable prosecutors to retain material in a manner which ensures compliance with their data protection obligations – enabling more straightforward and consistent retention, review, and deletion of material.[37]

59. Updated training and guidance is also key to addressing inconsistencies in this area, as both the application of redactions and the volume of personal data processed in the pursuit of reasonable lines of enquiry vary on a case-by-case basis.[38] Some police forces have reportedly produced internal guidance on redaction, which has been found to be over-extensive in requiring redaction which is not necessary to meet data protection standards.[39] These varying internal standards are likely contributing to the inconsistent approach to redaction, and therefore a single source of authoritative guidance would be preferable in this respect.[40].

60. The circumstances in which redaction of data prior to disclosure to the defence is required seems to be poorly understood by investigators and prosecutors. Unnecessary or poorly executed redaction can cause significant delay in the provision of material to the defence or delivery of material in an unintelligible format. Consistency and common understanding of when redaction is required will be enhanced by ensuring that all investigators and prosecutors are issued with a single source of comprehensive guidance about the circumstances in which redaction of material to be disclosed to the defence is and is not required. For example, redaction of personal information may not be required if there is no reasonable expectation of privacy, or disclosure is nonetheless necessary or the operation of redaction would be disproportionate.

61. Annex D of the recently published Attorney General's Guidelines on Disclosure 2024[41] provides some helpful guidance on redaction for investigators involved in redacting material prior to providing it to the CPS when seeking a charging

[37] Information Commissioner's Office, "The Information Commissioner's Response to consultation on the Attorney General's Guidelines on Disclosure and the CPIA Code of Practice", 22 July 2020 (link).
[38] Information Commissioner's Office, "The Information Commissioner's Response to consultation on the Attorney General's Guidelines on Disclosure and the CPIA Code of Practice", 22 July 2020 (link).
[39] Attorney General's Office, "Annual Review of Disclosure", May 2022 (link).
[40] Attorney General's Office, "Annual Review of Disclosure", May 2022 (link).
[41] Attorney_General_s_Guidelines_on_Disclosure_-_2024.pdf (publishing.service.gov.uk)

decision. The practical examples provided deal with footage and recordings rather than personal information in other types of material such as business records or electronic data. This guidance should be developed for all investigators and prosecutors involved in disclosure to the defence to include further information about what is and is not personal data[42], circumstances where there is no expectation of privacy and to provide more contextual guidance in respect of all types of material including of the type that the SFO or other fraud prosecutors would commonly encounter. If needed such guidance could be developed in further consultation with the ICO.

62. Any material that is disclosed to the defence can only be used for the purposes of the relevant criminal proceedings. Therefore, disclosure or use by the Defendant for any other purpose can be treated as a contempt of court. Where redaction would involve a disproportionate amount of time, consideration could be given to reinforcing safeguards by developing undertakings and NDA's to reinforce the point.

8 April 2024

[42] For example there are no data rights for legal entities, only natural persons

Appendix 1 - Common disclosure issues (further detail)

Culture and The Quality of Decision Making

1. The existence of a prosecutorial culture which is dismissive towards or suspicious of disclosure requests remains a significant problem. The quality of prosecution decisions about disclosure is also extremely variable and often inconsistent as between one case and the next.

2. Poor culture and poor decision making often lead to protracted correspondence and unnecessary court time being taken up with section 8 CPIA applications which are either conceded by counsel on the morning of the hearing or only faintly resisted. They may also result in a miscarriage of justice or the collapse of a trial.

3. In our collective experience, there still exists an unhelpful culture amongst some but not all prosecutors in respect of disclosure. This manifests itself in a variety of ways but includes:

    a. A default stance of being defensive towards legitimate disclosure requests. Such requests often appear to be viewed as 'tactical' rather than substantive and hence the prosecution start with a mindset which excludes proper engagement with issues being highlighted by the defence.
    b. Taking the view that disclosure by the prosecution is synonymous with some failure on their part.
    c. A pre-occupation with the dangers of 'setting a precedent' in other cases rather than judging the individual request on its merits.
    d. The withholding of the existence of disclosable material which reflects badly on the conduct of prosecutors, investigators or witnesses

4. We continue to experience prosecutors who simply do not apply the test properly. One of the reasons for this appears to be the lack of contested criminal litigation experience by those making the decisions. There is also a difficulty

with the use of multiple document reviewers (often at a first sift stage) where they do not have a sufficient, in depth understanding of the issues in the case.

5. There are also frequent instances of the test being applied in a myopic or overly restrictive way, particularly on the basis that a precise point is not explicitly pleaded in a defence case statement.

6. Poor disclosure decisions also often arise from the failure of the prosecution to understand its case overall. This problem is often caused or exacerbated by numerous changes of prosecution personnel over the life of a long investigation.

7. Disclosure failures also occur in CPS cases where there are poor lines of communication between the police and the CPS. The police sometimes think that certain material has been served (and is relied on) when in fact it has not been.

Timing, Sanctions and Progress

8. Disclosure is considered far too late in the process, usually only being given serious consideration by the prosecution towards the end of an investigation when a prosecution case narrative has already been settled upon.

9. The progress of disclosure often proceeds at a pace dictated by the prosecution. Disclosure of significant amounts of key material often occurs far too close to a trial date when there is a lot of other time critical trial preparation to be done. Very often this late disclosure concerns material such as a defendant's own work emails or work documentation. The prevailing attitude is that the onus is on the defence to get on with it in the time now available.

10. Where, as often happens, disclosure is made late in breach of court orders there are no sanctions imposed upon the prosecution. The prosecution knows this and therefore may work on the basis that a court will allow late disclosure

without it impacting on the viability of the trial. The lack of sanctions encourages further such breaches.

11. It is probably the case that failures to meet deadlines are most often caused by the prosecution being under-resourced. If there is a real will to try and address the problems of disclosure this must be accompanied by a commitment to adequately fund prosecutors.[43]

12. Failures in disclosure, other than in the most egregious cases, also go effectively unsanctioned.

13. The process of redaction is often given as the reason for disclosure taking a long time. However, in our experience much of the redaction is overzealous, goes beyond what is required under the relevant statutes and is ill thought through. The redaction issue is addressed in more detail in Section E(iv) above.

Reliance on Third Party Within the Disclosure Process

14. In our experience there is an increasing tendency for prosecutors to effectively delegate important, initial parts of the disclosure process to third parties (e.g. a financial organisation which is an alleged victim of a fraud or who holds significant amounts of relevant material). This is presumably motivated by cost saving considerations.

15. Some of the key problems in SFO cases have arisen due to third parties being allowed to control significant parts of the disclosure process (including but not limited to LPP). The duty upon the prosecution where there is unused material in the hands of a known third party is to take all reasonable steps to obtain it, and that includes persistence and not taking 'no' for an answer (*R v Flook* [2010] 1 Cr App R 434 §37 and *R (AL) v SFO* [2018] 1 WLR 4557 §93).

[43] As well as a commitment to provide adequate funding to those on legal aid, such as to allow a proper review of disclosed material

16. The greater the involvement of third parties in the early stages of disclosure, the greater the potential for unfairness and injustice. For the system to work properly, the prosecutor must have visibility of and control over all relevant material.

Other Miscellaneous Issues

17. There is currently no consistent and transparent system of how a prosecutor conducts quality assurance checks in respect of disclosure.

18. The issue of cross disclosure as between co-defendants is often not confronted until a very late stage of the case and defendants are often left in the dark about what approach is being taken. The reality of a contested trial where some defendants have material disclosed to them and others do not must be considered. There should also be a consistent approach adopted in all cases.