Attorney General's Guidelines on Disclosure:
Supplementary Guidelines on Digitally Stored Material (2011)

These Guidelines are issued by the Attorney General for prosecutors, investigators and defence practitioners on the conduct of disclosure in investigations and prosecutions involving digitally stored material. They supplement the Attorney General's Guidelines on Disclosure published in April 2005.

1. The Guidelines are intended to supplement the Attorney General's Guidelines on Disclosure (reissued in April 2005) and specifically paragraph 27. Paragraph 27 explains that the disclosure officer's obligation to inspect retained material may be fulfilled in relation to digitally stored material by using search terms or dip sampling methods, so long as the material is described on the schedules as clearly as possible and the manner and extent of the inspection is recorded along with the justification for adopting that approach.

2. As a result of the number of cases now involving digitally stored material and the scale of the digital material that may be involved, more detailed guidance is considered to be needed. The objective of these Guidelines is to set out how material satisfying the tests for disclosure can best be identified and disclosed to the defence without imposing unrealistic or disproportionate demands on the investigator and prosecutor.

3. The approach set out in these Guidelines is in line with existing best practice, in that:

   (i) Investigating and prosecuting agencies, especially in large and complex cases, will apply their respective case management and disclosure strategies and policies and be transparent with the defence and the courts about how the prosecution has approached complying with its disclosure obligations in the context of the individual case; and,

   (ii) The defence will be expected to play their part in defining the real issues in the case. In this context, the defence will be invited to participate in defining the scope of the reasonable searches that may be made of digitally stored material by the investigator to identify material that might reasonably be expected to undermine the prosecution case or assist the defence.

4. If this approach is followed the courts will be in a good position to use their case management powers effectively and to determine applications for disclosure fairly.

5. The Attorney General's Guidelines are not detailed operational guidelines. They are intended to set out a common approach to be adopted in the context of digitally stored material.

Types of digital material

6. Digital material falls into two categories: the first category is material which is created natively within an electronic environment (e.g. email, office files, system files, digital photographs, audio etc.); the second category is material which has been digitised from an analogue form (e.g. scanned copy of a document, scanned photograph, a faxed document). Irrespective of the way in which technology changes, the categorisation of digital material will remain the same.

7. Digital material is usually held on one of the three types of media. Optical media (e.g. CD, DVD, Blu-ray) and Solid-State media (e.g. removable memory cards, solid state music players or mobile devices etc.) cater for usually lower volume storage. Magnetic media (e.g. disk drives and back up tapes) usually cater for the high volume storage.

General principles for investigators

8. The general principles[1] to be followed by investigators in handling and examining digital material are:

   (i) No action taken by investigators or their agents should change data held on a computer or storage media which may subsequently be relied upon in court;

   (ii) In circumstances where a person finds it necessary to access original data held on computer or storage media, that person must be competent to do so and be able to give evidence explaining the relevance and implications of their actions;

   (iii) An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes (see further the section headed Record keeping and scheduling below); and,

   (iv) The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are followed.

9. Where an investigator has reasonable grounds for believing that digital material may contain material subject to legal professional privilege, very strong legal constraints apply. No digital material may be seized which an investigator has reasonable grounds for believing to be subject to legal privilege, other than where the provisions of the Criminal Justice and Police Act 2001 apply. Strict controls need to be applied where privileged material is seized. See the more detailed section on Legal Professional Privilege starting at paragraph 27 below.

[1] Based on: Association of Chief Police Officers: Good Practice Guide for Computer Based Electronic Evidence Version 0.1.4

Seizure, relevance and retention

10. The legal obligations are to be found in a combination of the Police and Criminal Evidence Act 1984 (PACE), the Criminal Justice and Police Act 2001 (CJPA 2001) and the Criminal Procedure and Investigations Act 1996 (the CPIA 1996).

11. These Guidelines also apply to digital material seized or imaged under other statutory provisions. For example, the Serious Fraud Office has distinct powers of seizure under warrant obtained under section 2(4) of the Criminal Justice Act 1987. And in cases concerning obscene material special provisions apply to the handling, storage and copying of such material. Practitioners should refer to specific guidance on the application of those provisions.

Seizure

12. Before searching a suspect's premises where digital evidence is likely to be found, consideration must be given to what sort of evidence is likely to be found and in what volume, whether it is likely to be possible to view and copy, if relevant, the material at the location - it is not uncommon with the advent of cloud computing for digital material to be hosted by a third party - and to what should be seized. Business and commercial premises will often have very substantial amounts of digital material stored on computers and other media. Investigators will need to consider the practicalities of seizing computer hard drives and other media, the effect this may have on the business and, where it is not feasible to obtain an image of digital material, the likely timescale for returning seized items.

13. In deciding whether to seize and retain digital material it is important that the investigator either complies with the procedure under the relevant statutory authority, relying either on statutory powers or a search warrant, or obtains the owner's consent. In particular, investigators need to be aware of the strong constraints applying to legally privileged material.

14. A computer hard drive or single item of media, such as a back up tape, is a single storage entity. This means that if any digital material found on the hard drive or other media can lawfully be seized the computer hard drive or single item of media may, if appropriate, be seized or imaged. In some circumstances investigators may wish to image specific folders, files or categories of data where it is feasible to do so without seizing the hard drive or other media, or instead of taking an image of all data on the hard drive or other media. In practice, the configuration of most systems means that data may be contained across a number of hard drives and more than one hard drive or item of media may be required in order to access the information sought.

15. Digital material must not be seized if an investigator has reasonable grounds for believing it is subject to legal professional privilege, other than where sections 50 or 51 of the Criminal Justice and Police Act 2001 apply.

If such material is seized it must be isolated from other seized material and any other investigation material in the possession of the investigating authority.

The Police and Criminal Evidence Act 1984

16. PACE 1984 provides powers to seize and retain anything for which the search has been authorised or after arrest, other than items attracting legal professional privilege.[2] In addition, there is a general power to seize anything which is on the premises if there are reasonable grounds to believe that it has been obtained in the commission of an offence, or that it is evidence and that it is necessary to seize it to prevent it being concealed, lost, altered or destroyed.[3] There is another related power to require information which is stored in any electronic form and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible or from which it can readily be produced in a visible and legible form.[4]

17. An image (a forensically sound copy) of the digital material may be taken at the location of the search. Where the investigator makes an image of the digital material at the location, the original need not be seized. Alternatively, when originals are taken, investigators must be prepared to copy or image the material for the owners when reasonably practicable in accordance with PACE 1984 Code B 7.17.

18. Where it is not possible or reasonably practicable to image the computer or hard drive, it will need to be removed from the location or premises for examination elsewhere. This allows the investigator to seize and sift material for the purpose of identifying that which meets the tests for retention in accordance with the 1984 Act.[5]

The Criminal Justice and Police Act 2001

19. The additional powers of seizure in sections 50 and 51 of the CJPA 2001 Act only extend the scope of existing powers of search and seizure under the 1984 Act and other specified statutory authority[6] where the relevant conditions and circumstances apply.

20. Investigators must be careful only to exercise powers under the CJPA when it is necessary and not to remove any more material than is justified. The removal of large volumes of material, much of which may not ultimately be retainable, may have serious consequences for the owner of the material,

[2] By warrant under section 8 and Schedule 1 and section 18 of the 1984 Act
[3] Section 19 of the 1984 Act
[4] Section 20 of the 1984 Act
[5] Special provision exists for investigations conducted by Her Majesty's Revenue and Customs in the application of their powers under the 1984 Act – see section 114(2)(b) – and the 2001 Act
[6] Schedule 1 of the 2001 Act

particularly when they are involved in business or other commercial activities.

21. A written notice must be given to the occupier of the premises where items are seized under sections 50 and 51.[7]

22. Until material seized under the CJPA 2001 has been examined, it must be kept securely and separately from any material seized under other powers. Any such material must be examined as soon as reasonably practicable to determine which elements may be retained and which should be returned. Regard must be had to the desirability of allowing the person from whom the property was seized, or a person with an interest in the property, an opportunity of being present or represented at the examination.

Retention

23. Where material is seized under the powers conferred by PACE 1984 the duty to retain it under the Code of Practice issued under the CPIA 1996 is subject to the provisions on retention under section 22 of the 1984 Act. Material seized under sections 50 and 51 of the CJPA 2001 may be retained or returned in accordance with sections 53-58 of that Act.

24. Retention is limited to evidence and relevant material (as defined in the Code of Practice issued under the CPIA 1996). Where either evidence or relevant material is inextricably linked to non-relevant material which is not reasonably practicable to separate, that material can also be retained. Inextricably linked material is material that is not reasonably practicable to separate from other linked material without prejudicing the use of that other material in any investigation or proceedings.

25. However, inextricably linked material must not be examined, imaged, copied or used for any purpose other than for providing the source of or the integrity of the linked material.

26. There are four categories of material that may be retained:

    (i) Material that is evidence or potential evidence in the case. Where material is retained for evidential purposes there will be a strong argument that the whole thing (or an authenticated image or copy) should be retained for the purpose of proving provenance and continuity;

    (ii) Where evidential material has been retained, inextricably linked non-relevant material which is not reasonably practicable to separate can also be retained (PACE Code B paragraph 7);

[7] Section 52 of the 2001 Act

(iii) An investigator should retain material that is relevant to the investigation and required to be scheduled as unused material. This is broader than but includes the duty to retain material which may satisfy the test for prosecution disclosure. The general duty to retain relevant material is set out in the CPIA Code at paragraph 5; or,

(iv) Material which is inextricably linked to relevant unused material which of itself may not be relevant material. Such material should be retained (PACE Code B paragraph 7).

27. The balance of any digital material should be returned in accordance with sections 53-55 of the 2001 Act and also note paragraph 28 of the Attorney General's Guidelines on Disclosure.

Legal professional privilege (LPP)

28. No digital material may be seized which an investigator has reasonable grounds for believing to be subject to legal privilege, other than under the additional powers of seizure in the CJPA 2001.

29. The CJPA 2001 enables an investigator to seize relevant items which contain LPP material where it is not reasonably practicable on the search premises to separate LPP material from non-LPP material.

30. Where LPP material or material suspected of containing LPP is seized it must be isolated from the other material which has been seized in the investigation. The mechanics of securing property vary according to the circumstances; "bagging up", i.e. placing materials in sealed bags or containers, and strict subsequent control of access, is the appropriate procedure in many cases.

31. Examination of material may be undertaken by a person independent of the investigation, who may be employed within an investigative body so long as he or she is not one of the investigators or anyone connected with the investigation, to determine whether material may attract LPP.

32. Where material has been identified as potentially containing LPP it must be reviewed by an independent lawyer. No member of the investigative or prosecution team involved in either the current investigation or, if the LPP material relates to other criminal proceedings, in those proceedings should have sight of or access to the LPP material.

33. If the material is voluminous, search terms or other filters may have to be used to identify the LPP material. If so this will also have to be done by someone independent and not connected with the investigation.

34. It is essential that anyone dealing with LPP material maintains proper records showing the way in which the material has been handled and those who have had access to it as well as decisions taken in relation to that material.

35. LPP material can only be retained in specific circumstances in accordance with section 54 of the CJPA 2001 i.e. where the property which comprises the LPP material has been lawfully seized and it is not reasonably practicable for the item to be separated from the rest of the property without prejudicing the use of the rest of the property. LPP material which cannot be retained must be returned as soon as practicable after the seizure without waiting for the whole examination of the seized material.

Excluded and special procedure material

36. Similar principles to those that apply to LPP material apply to excluded or special procedure material, as set out in section 55 of the CJPA 2001.[8]

Encryption

37. Part III of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigation of Protected Electronic Information Code of Practice govern encryption. See the CPS's Guidance RIPA Part III

38. RIPA enables specified law enforcement agencies to compel individuals or companies to provide passwords or encryption keys for the purpose of rendering protected material readable. Failure to comply with RIPA Part III orders is a criminal offence. The Code of Practice provides guidance when exercising powers under RIPA, to require disclosure of protected electronic data in an intelligible form or to acquire the means by which protected electronic data may be accessed or put in an intelligible form.

Sifting/examination

39. In complying with its duty of disclosure, the prosecution should follow the procedure as outlined below.

40. Where digital material is examined, the extent and manner of inspecting, viewing or listening will depend on the nature of the material and its form.

41. It is important for investigators and prosecutors to remember that the duty under the 1996 Act Code of Practice is to "pursue all reasonable lines of enquiry including those that point away from the suspect". Lines of enquiry, of whatever kind, should be pursued only if they are reasonable in the context of the individual case. It is not the duty of the prosecution to comb through all the material in its possession - e.g. every word or byte of computer material - on the look out for anything which might conceivably or speculatively assist the defence. The duty of the prosecution is to disclose material which might reasonably be considered capable of undermining its case or assisting the case for the accused which they become aware of, or to which their attention is drawn.

[8] Special provision exists for investigations conducted by Her Majesty's Revenue and Customs in the application of their powers under the 1984 Act – see section 114(2)(b) – and the 2001 Act

42. In some cases the sift may be conducted by an investigator/disclosure officer manually assessing the content of the computer or other digital material from its directory and determining which files are relevant and should be retained for evidence or unused material.

43. In other cases such an approach may not be feasible. Where there is an enormous volume of material it is perfectly proper for the investigator/disclosure officer to search it by sample, key words, or other appropriate search tools or analytical techniques to locate relevant passages, phrases and identifiers.

44. In cases involving very large quantities of data, the person in charge of the investigation will develop a strategy setting out how the material should be analysed or searched to identify categories of data. Where search tools are used to examine digital material it will usually be appropriate to provide the accused and his or her legal representative with a copy of reasonable search terms used, or to be used, and invite them to suggest any further reasonable search terms. If search terms are suggested which the investigator or prosecutor believes will not be productive - for example because of the use of common words that are likely to identify a mass of irrelevant material, the investigator or prosecutor is entitled to open a dialogue with the defence representative with a view to agreeing sensible refinements. The purpose of this dialogue is to ensure that reasonable and proportionate searches can be carried out.

45. It may be necessary to carry out sampling and searches on more than one occasion, especially as there is a duty on the prosecutor to keep duties of disclosure under review. To comply with this duty it may be appropriate (and should be considered) where further evidence or unused material is obtained in the course of the investigation; the defence statement is served on the prosecutor; the defendant makes an application under section 8 of the CPIA for disclosure; or the defendant requests that further sampling or searches be carried out (provided it is a reasonable line of enquiry).

Record keeping

46. A record or log must be made of all digital material seized or imaged and subsequently retained as relevant to the investigation.

47. In cases involving very large quantities of data where the person in charge of the investigation has developed a strategy setting out how the material should be analysed or searched to identify categories of data, a record should be made of the strategy and the analytical techniques used to search the data. The record should include details of the person who has carried out the process and the date and time it was carried out. In such cases the strategy should record the reasons why certain categories have been searched for (such as names, companies, dates etc).

48. In any case it is important that any searching or analytical processing of digital material, as well as the data identified by that process, is properly recorded. So far as practicable, what is required is a record of the terms of the searches or processing that has been carried out. This means that in principle the following details may be recorded:

    (i) A record of all searches carried out, including the date of each search and the person(s) who conducted it;

    (ii) A record of all search words or terms used on each search. However where it is impracticable to record each word or terms (such as where Boolean searches or search strings or conceptual searches are used) it will usually be sufficient to record each broad category of search;

    (iii) A log of the key judgements made while refining the search strategy in the light of what is found, or deciding not to carry out further searches; and,

    (iv) Where material relating to a "hit" is not examined, the decision not to examine should be explained in the record of examination or in a statement. For instance, a large number of "hits" may be obtained in relation to a particular search word or term, but material relating to the "hits" is not examined because they do not appear to be relevant to the investigation. Any subsequent refinement of the search terms and further hits should also be noted and explained as above.

49. Just as it is not necessary for the investigator or prosecutor to produce records of every search made of hard copy material, it is not necessary to produce records of what may be many hundreds of searches or analyses that have been carried out on digitally stored material, simply to demonstrate that these have been done. It should be sufficient for the prosecution to explain how the disclosure exercise has been approached and to give the accused or suspect's legal representative an opportunity to participate in defining the reasonable searches to be made, as described in the section on sifting/examination.

Scheduling

50. The disclosure officer should ensure that scheduling of relevant material is carried out in accordance with the 1996 Act Code of Practice. This requires each item of unused material to be listed separately on the unused material schedule and numbered consecutively. The description of each item should make clear the nature of the item and should contain sufficient detail to enable the prosecutor to decide whether he needs to inspect the material before deciding whether or not it should be disclosed (see paragraph 24).

51. In some enquiries it may not be practicable to list each item of material separately. If so, these may be listed in a block and described by quantity and generic title. Even if the material is listed in a block, the search terms used and any items of material which might satisfy the disclosure test are

listed and described separately. In practical terms this will mean, where appropriate, cross referencing the schedules to your disclosure management document.

52. The remainder of any computer hard drive/media containing material which is not responsive to search terms or other analytical technique or not identified by any "hits", and material identified by "hits" but not examined, is unused material and should be recorded (if appropriate by a generic description) and retained.

53. Where continuation sheets of the unused material schedule are used, or additional schedules are sent subsequently, the item numbering must be sequential to all other items on earlier schedules.

Third party material

54. Third party material is material held by a person, organisation, or government department other than the investigator and prosecutor within the UK or outside the UK.

Within the UK

55. The CPIA Code and the AG's Guidelines makes clear the obligation on the prosecution to pursue all reasonable lines of enquiry in relation to material held by third parties within the UK.

56. If as a result of the duty to pursue all reasonable lines of enquiry, the investigator or prosecutor obtains or receives the material from the third party, then it must be dealt with in accordance with the CPIA 1996 i.e. the prosecutor must disclose material if it meets the disclosure tests, subject to any public interest immunity claim. The person who has an interest in the material (the third party) may make representations to the court concerning public interest immunity (see section 16 of the CPIA 1996).

57. Material not in the possession of an investigator or prosecutor falls outside the CPIA 1996. In such cases the Attorney General Guidelines on Disclosure prescribe the approach to be taken to disclosure of material held by third parties (paragraphs 51-54) as does the judicial disclosure protocol (paragraphs 52-62).

Outside the UK

58. The obligation on the investigator and prosecutor under the CPIA Code and the AG's Guidelines to pursue all reasonable lines of enquiry also applies to material held overseas.

59. Where it appears that there is relevant material, the prosecution must take reasonable steps to obtain it, either informally or making use of the powers contained in the Crime (International Co-operation) Act 2003 and any EU

and international conventions. See CPS Guidance Obtaining Evidence and Information from Abroad

60. There may be cases where a foreign state or a foreign court refuses to make the material available to the investigator or prosecutor. There may be other cases where the foreign state, though willing to show the material to investigators will not allow the material to be copied or otherwise made available and the courts of the foreign state will not order its provision.

61. It is for these reasons that there is no absolute duty on the prosecutor to disclose relevant material held overseas by entities not subject to the jurisdiction of the courts in England and Wales.

62. The obligation on the investigator and prosecutor under the CPIA 1996 is to take reasonable steps. Where investigators are allowed to examine files of a foreign state but are not allowed to take copies or notes or list the documents held, there is no breach by the prosecution in its duty of disclosure by reason of its failure to obtain such material, provided reasonable steps have been taken to try and obtain the material. Whether the prosecution has complied with its duty is for the court to judge in each case.

63. In these circumstances it is important that the position is clearly set out in writing so that the court and the defence know what the position is. Investigators and prosecutors must record and explain the situation and set out, insofar as they are permitted by the foreign state, such information as they can and the steps they have taken.

Issued on 14 July 2011
Reformatted on 29 November 2012