NAVIGATING THE DOCUMENTARY MINEFIELD
&
THE ADMISSION OF DOCUMENTARY EVIDENCE IN WHITE-COLLAR CRIMINAL TRIALS[1]

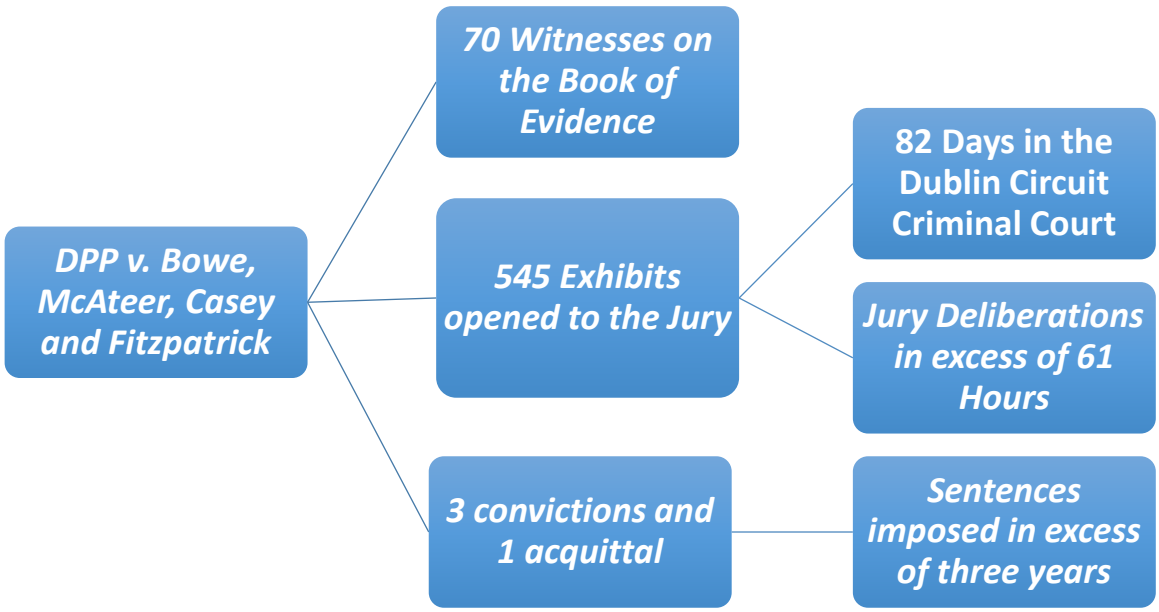
INTRODUCTION

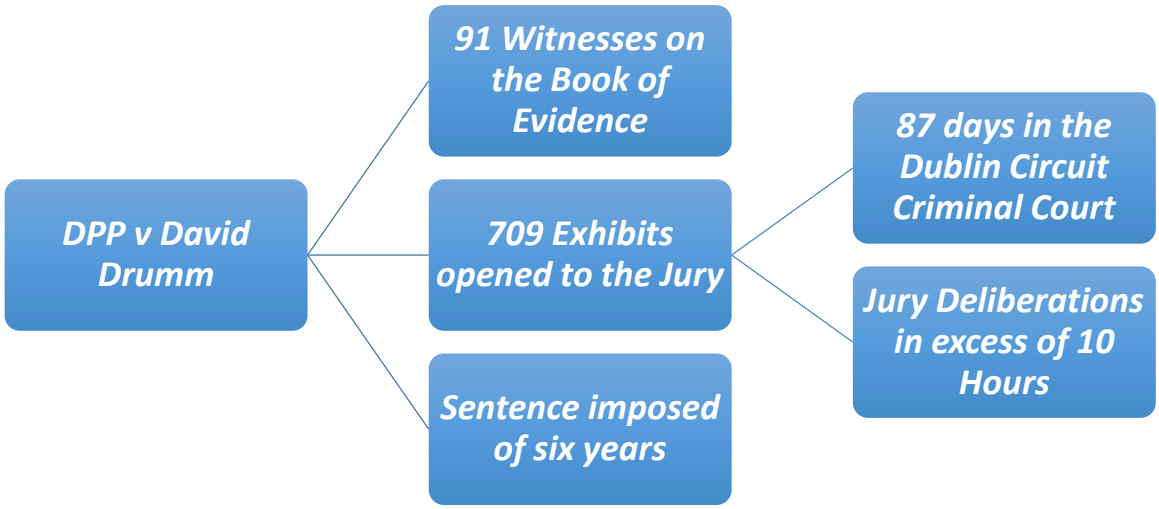
1. During the period of 2014 to 2018, a number of large-scale criminal prosecutions commenced at the Dublin Circuit Criminal Court in respect of activities at the former Anglo Irish Bank plc. These prosecutions involved senior banking executives charged with offences including conspiracy to defraud contrary to the common law and false accounting under section 10 of the Criminal Justice (Theft and Fraud) Offences Act 2001.

2. In the two 'back-to-back prosecutions', it was the prosecution case that Anglo Irish Bank plc. had completed a series of paired transactions with Irish Life & Permanent plc. in an amount of € 7.2 billion during September 2008 with a view to artificially increasing Anglo Irish Bank's corporate deposit figure on the year-end balance sheet and thereby bolstering public confidence in the institution at that time. These transactions were multi-jurisdictional, part-electronic, part-paper and, in the words of one of the accused, went through 'many hands'.

3. The back-to-back investigators uplifted thousands of documents and telephone calls and interviewed hundreds of witnesses. It is this volume of material that contributed to the extended nature of the trials. The following is an outline of the scale and duration of each back-to-back prosecution including the volume of evidence at trial:

[1] Paper by Sinéad McGrath B.L. 3rd November 2018.





4. The prosecutions involved extensive *voir dire* hearings on multiple legal issues ranging from the frontline collection of the evidence under s.52 of the Criminal Justice (Theft and Fraud) Offences Act, 2001 to the admissibility of the same under the Criminal Evidence Act 1992 and the Bankers' Books Evidence Acts 1879-1989.

PART 1: THE SECTION 52 ORDERS

5. During the period of 2010-2013, eighteen applications were made by the G.B.F.I. (now the G.N.E.C.B.) for orders pursuant to s.52 of the Criminal Justice (Theft and Fraud) Offences Act, 2001. S. 52 of the Act of 2001 provides for an order of the District Court to produce evidential material in respect of an offence under the Act, which is punishable by five years or more (s. 52 (1) of the Act of 2001). Over 800,000 documentary and electronic exhibits were uplifted together with in excess of 39,000 telephone recordings at Anglo Irish Bank alone. One of the most significant legal arguments arose, unsurprisingly, as regards the scope of the orders and whether the evidence was unlawfully and / or unconstitutionally seized by the G.N.E.C.B.

6. There was, in the first instance, a simple *ultra vires* argument, namely, whether the audio and electronic material seized was outside the plain terms of the orders. This argument highlights the importance of the drafting of orders and warrants for large-scale electronic seizures. The language used, whether it is 'document', 'record', 'computer record' or 'storage media', is central when the matter comes to trial. It is also important to identify the period covered by the order or warrant given the risk that the material seized may fall outside that timeframe. This is a significant hurdle for any investigation team and illustrates the need for the involvement of prosecutors at the investigative stage of white-collar crimes, an issue addressed at the close of this paper.

7. This *ultra vires* argument was augmented in the second back-to-back prosecution in the light of the judgment of the Supreme Court in the *Competition and Consumer Protection Commission v CRH Plc, Irish Cement Limited and Lynch*[2]. This case concerned a complaint that the material seized was in breach of a third party's constitutional right to privacy under Article 40.3 of the Constitution and / or in breach of the right to respect for private life under Article 8 of the European Convention on Human Rights. This is one of the most significant recent

[2] [2017] IESC 34

judgments in the context of orders and warrants and it is both notable and extraordinary that in the aftermath of this case, one high profile solicitors firm has recently established a '*Dawn Raid Response Unit'* for their clients.

8. The *CRH* judgment is extremely lengthy and a detailed analysis of the same is outside the scope of this paper. However, it is important to highlight that there were significant differences between the judgments of the High Court (Barrett J.) and the Supreme Court. By way of example, Barrett, Laffoy and Charleton JJ. did not make any finding that the search itself was unlawful and / or resulted in a breach of rights. The foregoing concentrated in ensuring that the subsequent interrogation of the material was lawful. However, MacMenamin J. was severely critical of the search itself.

9. As a result of the various nuances in the judgment, it is difficult to disentangle the legal principles involved. However, what is certainly clear from the judgment, is that the legal and factual context of a large-scale electronic seizure is central to any allegations of unlawfulness or unconstitutionality in a criminal trial.

MacMenamin J. was heavily critical of the procedures followed by the Competition & Consumer Protection Commission (CCPC) on the morning of the search including the demand for access to the home drives of five named employees and all email data. MacMenamin J. was critical of the warrant, which he said was '*couched in broad and unspecific terms'.* He stated that:

> *"This warrant did not convey any information about the nature, timing, and location of the offences alleged or suspected. It did not identify any person as being involved in such activities, or disclose any basis for a reasonable suspicion that a criminal offence had been committed. The warrant simply stated, on its face, that there were reasonable grounds for believing that there was information necessary for the CCPC officials to exercise 'functions' and 'all or any of their powers' as conferred on them under the Act of 2014. These*

were not simply technical deficiencies, but went to the core of the jurisdiction involved…"[3]

MacMenamin J. referred to what he called '*bottom trawling'* and stated that:

"Here the degree of incursion impaired the right far more than is necessary. The dis-proportionality between means and ends in this search is very marked indeed. It cannot be rationalised by analogies which do not relate to this case. There is, beyond question, a most substantial disparity between the quantity of material seized, and the end sought to be achieved. No exceptional circumstances have been cited, or referred to, which might justify the nature, extent and scope of the CCPC's actions in this search, seizure and detention. It is necessary to analyse this in more detail."[4]

One of the central features of the Competition Act 2014 is that it does not outline pre and / or post-search supervision provisions or safeguards which might address the issues of privacy or confidentiality. This can be contrasted with s. 52 (7) of the Criminal Justice (Theft and Fraud) Offences Act, 2001 where a District Judge may '*vary or discharge*' the order on the application of any person to whom the order relates or a member of An Garda Síochana.

Mr. Justice MacMenamin did briefly reference a criminal context stating:

"*It would not be surprising, if in the very different circumstances of a search following on serious crime, substantial extraneous and irrelevant material might be seized. But there comes a point where the elements necessary for comparison with other situations in the criminal sphere break down. If the principle of proportionality is not applied in this case, even with a significant degree of latitude, the words of the statute could, under the guise of legality, almost become tantamount to a power of 'general search'. The CCPC was simply never entitled to have in its possession this vast quantity of irrelevant*

[3] *Ibid* at [7].
[4] *Ibid* at [70].

or extraneous material. It was not entitled to engage in this form of entry, search and seizure and retention, where it was highly probable that such amounts of material would be seized. In my view, the procedure adopted renders the search, and its fruits, null and void."[5]

Mr. Justice Charleton went somewhat further in his judgment addressing a criminal context as follows:

"While this was a business email address, not a private or family email address, the separate judgment of MacMenamin J. rightly emphasises the extraordinary scope of what was seized. It was every single email from a particular person. That may be justified within the general context of criminal searches under warrant, depending on the suspicion validly held; as with the necessity to research the activities of someone suspected of terrorist activity or of organised crime or money laundering.… This search was done without any relevant dates as target and without the consideration of using target search terms or some other means of limiting the material proportionately to what needed to be taken. That may be justified where the police or investigating authority needs to search out accomplices or co-conspirators to prevent or investigate an atrocity or where the identification or an organised crime or terrorist ring requires a complete analysis of all information available as to their communications."[6]

10. In *The People (Director of Public Prosecutions) v. David Drumm,* extensive evidence was adduced in respect of the scope of the s. 52 orders and the process of uplifting the material. Specifically, the court heard evidence as regards the use of the electronic data-mining tool called ClearWell, used by GNECB to 'tag' pertinent material and disregard irrelevant material. Judge O'Connor succinctly ruled in respect of the *CRH* argument that there was no breach of Mr. Drumm's rights and that the orders in the investigation were proportionate. This, she held, was distinguishable from *CRH* case having regard to the lack of specificity in the

[5] *Ibid* at [77].
[6] *Ibid* at [30]

warrants and the fact that no process had been put in place for the sifting or sorting of relevant from irrelevant material.[7]

Therefore, a *CRH* argument is inextricably linked to the underlying facts and the process followed by search agents with regard to any privileged and / or personal or private material. It again highlights the benefit of prosecution assistance during the investigative and seizure process.

PART 2: THE ADMISSIBILITY ISSUES

11. The hundreds of exhibits on the Book of Evidence were individually examined in the context of admissibility. The material seized comprised of a mixture of the following:

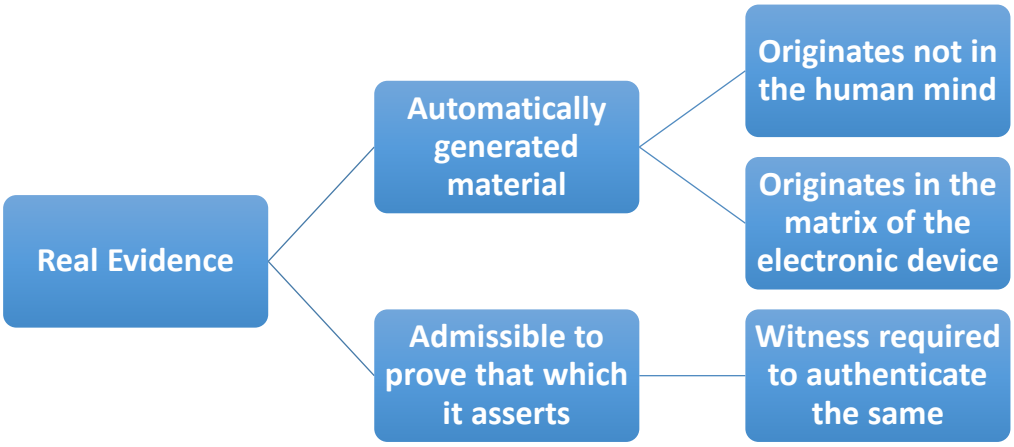
(i) Documents in hard copy format handed over by individual witnesses when making statements or handed over by a designated person at Anglo, including originals, copies and computer printouts;

(ii) Discs and hard drives handed over by a designated person at Anglo, containing thousands of documents, including email data, taken from the computer systems at Anglo by an IT team;

(iii) Audio data handed over by a designated person at Anglo, using encrypted hard drives and CDs, containing downloaded audio data taken from multiple telephone lines (both internal calls and calls between internal and external lines).

The first task was the separation of real evidence from inadmissible hearsay evidence in the foregoing categories.

[7] *The People (DPP) v David Drumm*, Trial Transcript 8th February 2018, p. 8



12. The position taken by the prosecution during the trials was that the extensive audio data was real evidence. This evidence was authenticated by the head of Technical Services at Anglo Irish Bank who was responsible for the maintenance and operation of the voice recording systems in the dealing rooms at Anglo and further gave evidence in relation to the extraction of each individual call from the audio data bank.

13. An examination of the electronic documentary data[8] indicated that some of this data was also automatically generated material falling within the category of real evidence. In the United States case of the *State of Louisiana v. Armstead*[9] the court referred to two categories of electronically generated records (a) those generated solely by the electronic operation and mechanical pulses of the computer and (b) computer-stored human inputted statements.

The back-to-back transactions themselves involved a combination of real and hearsay evidence. It was necessary to examine each 'step' of each trade involved in the transactions and determine what documentary material was automatically generated and what was a product of human intervention.

[8] The US Manual for Complex Litigation, § 21.446 (3rd ed, 1995) defines '*electronic documentary evidence*' as '*any information captured, generated or maintained in databases, operational systems, applications programmes, computer-generated models which extrapolate outcomes, electronic and voice mail messages and even instructions held inertly within a computer memory bank.*'
[9] 432 So.2d 837 at 839 (La. 1983)

14. There are a number of cases which assist in identifying real 'documentary' evidence and the following is a summary of examples:

Case Name	***Real Evidence***
The People (Director of Public Prosecutions) v. Murphy[10]	Telephone records established by reference to cell mast information.
The People (Director of Public Prosecutions) v. Meehan[11]	A printout of telephone traffic between mobile phones.
The Statue of Liberty[12]	A photograph of echoes recorded by radar at a shore station which was unmanned at the time. The court referred to tape recordings and photographs by way of examples of real evidence, including photographs taken by a '*trip or clock mechanism*'
R. v. Wood[13]	A printout from a a pre-designed computer programme (calculator) recording the chemical composition of metal samples. The court referred to '*…the results of a physical exercise which involves the use of some equipment, device or machine.'*
Castle v. Cross[14]	A printout from an 'Intoximeter 3000' breath testing machine. The court was prepared to apply a presumption in this case that the '*mechanical instrument'* was in order at the relevant time.
R. v. Spiby[15]	A printout from a Norex" machine which automatically recorded time, duration, cost etc. of telephone calls made from a hotel bedroom.
Reg. v. Governor of Brixton Prison, Ex parte Levin[16]	A screen printout from computerised banking records, which automatically captured a fund transfer request.

[10] [2005] 2 IR 125.
[11] [2006] 3 IR 468.
[12] [1968] 1 WLR 739.
[13] (1983) 76 Cr. App. R. 23.
[14] [1984] 1 W.L.R. 1372.
[15] (1990) 91 Cr. App. R. 186.
[16] [1997] A.C. 741.

Case Name	***Real Evidence***
R v Coventry Magistrates Court[17]	Printouts from a web server database which had recorded the click streams and access to websites and which had recorded the name, home address, email address and credit card details of those logging on were held to be admissible as real evidence.

15. In both *Murphy* and *Meehan,* the Court of Criminal Appeal was of the view that the English cases on real evidence had to be '*read through the lens'* of *R. v. Cochrane*[18] (a case involving the admissibility of computerised records) and that '*authoritative evidence'* was required to prove the function and operation of the relevant computer system ('foundation testimony'). The purpose of this 'foundation testimony' is (a) to clarify what side of the divide the proposed evidence is on (real or hearsay) and (b) to authenticate the same.

16. Mr. Justice McKechnie clarified in *The People (Director of Public Prosecutions) v A. Mc D*[19] that CCTV footage was '*so ubiquitous'* that no evidence as to the ordinary function of a CCTV camera was required. However, it is clear from his judgment that '*authoritative evidence'* remains central in relation to '*other devices*' as the finder of fact will require evidence to establish how the information was inputted. He referred to the '*possibility'* of hearsay evidence as follows:

> *"[42] The <u>possibility</u> of the evidentiary output of any of these devices or machines constituting hearsay existed because, without having heard evidence as to how the particular apparatus worked, the court/jury could not be sure whether that record/printout was merely displaying information fed to it by a person, or whether it had been produced without intervention by a human mind. Without evidence to explain the functioning of the machine, the court simply would not have known how the evidence was generated. This is not the*

[17] [2004] EWHC 905.
[18] [1993] Crim.L.R. 48.
[19] [2016] 3 IR 123.

case in respect of CCTV footage (see paras. 47 to 49 and para. 57, infra). " (emphasis added)

17. As noted by the Law Reform Commission it is unclear from *Murphy* whether this evidence must be provided by an IT specialist or by someone working in the company or bank.[20] In the back-to-back prosecutions, detailed statements were taken in relation to the function and operation of the relevant system automatically generating the material. Such 'foundation testimony' included statements dealing with automatic material generated by an international trading platform called SWIFT.

'Foundation testimony' was also given by the relevant personnel from the Central Bank in respect of end-of-day bank statements automatically generated by a European-wide financial trade settlement platform.

These statements addressed *inter alia*:

- identifying the particular data and information that was automatically created by the computer system (the real evidence);

- confirming the qualifications, experience, job description of the appropriate person in IT (the appropriate person);

- explaining, from an IT perspective, how the computer system was operating on a day-to-day basis (the function and operation of the system);

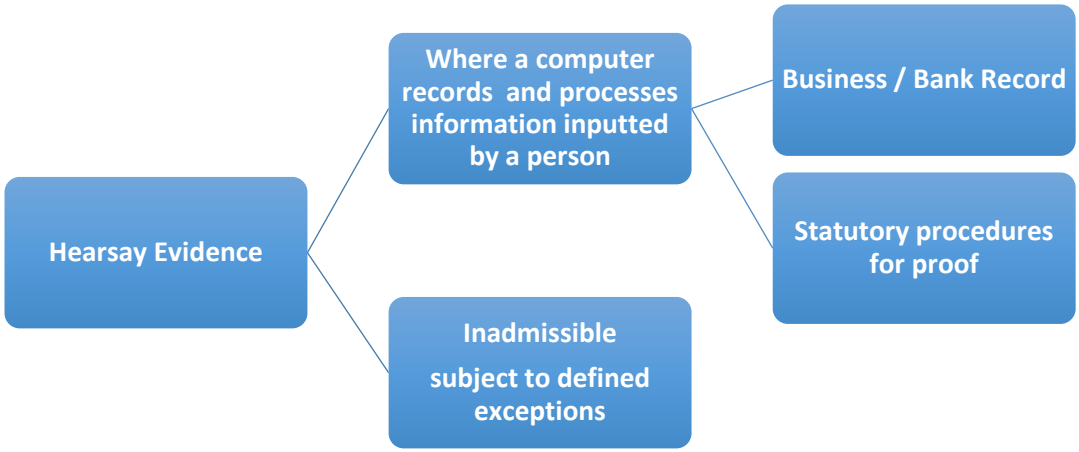
- outlining the period during which the data was generated (the relevant period);

- confirming that the system was functioning properly during the relevant period;

[20] Law Reform Commission *Report on the Consolidation and Reform of Aspects of the Law of Evidence* (LRC 117-2016), para. 2.52.

- explaining how the appropriate person would know that the system was not working properly and / or what data would be generated as a result;

- outlining sufficient information about the system to enable the court to be satisfied with the reliability of the real evidence produced by the computer system at that time.



18. The 800,000 documents uplifted during the investigation contained extensive hearsay evidence. In the judgment of the Court of Appeal in *The People (Director of Public Prosecutions) v. O' Mahony & Daly*[21] the Court outlined categories of such hearsay evidence as follows:

(1) Paper Bank Account Records –originals or copies – including statements of account, correspondence, intra-bank memos, signatory lists;
(2) Electronic Bank Records – printouts or screenshots- including statements of account on the core banking system, transaction records, customer names and addresses;

[21] [2016] IECA 111.

(3) Emails – printouts or copies – and email attachments – including 'routine internal emails re: customer transactions, communications to and from clients of the business;

(4) Paper documents or electronic documents created in the context of investigations;

(5) Court Orders.

Caution should be exercised with regard to this list as real evidence may be found in that material. A regular query from practitioners is whether electronic bank statements constitute real or hearsay evidence. When the content of bank statements is examined, it is clear that it can be a mixture of such evidence with fully automated transactions included (such as the application of an interest payment) or transactions with bank tellers manually processing a transfer, lodgement or withdrawal. In the back-to-back transactions there were end-of day bank statements from the Central Bank, which, as noted above, were generated automatically and therefore were real evidence.

PART 3: THE CRIMINAL EVIDENCE ACT 1992

19. Each individual witness prepared a certificate under section 6 of the Criminal Evidence Act 1992 (the CEA 1992) in respect of the electronic documentary exhibits that were handed over (as opposed to using a global certificate).

20. Each witness also prepared a certificate under s.52 (6) of the Criminal Justice (Theft and Fraud) offences Act 2001. S. 52 (6) (a) of the 2001 Act states that '*[i]nformation contained in a document which was produced to a member of the Garda Síochána, or to which such a member was given access, in accordance with an order under this section shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible'* unless it is excluded (e.g. is privileged from disclosure in criminal proceedings etc.). The section does not outline a certification process. However, it was determined, as a belt and braces approach, to prepare s. 52 certificates. These certificates were not ultimately required in the back-to-back prosecutions. The section, while open to challenge as overly broad, is currently on the statute book

and it remains to be seen whether the use of this provision for admissibility, standing alone, could withstand robust legal challenges.

21. The certificates in the back-to-back prosecutions were subject to extensive legal challenges which concerned *inter alia* the following issues:

- who was the 'compiler' of the 'information'?
- who was the 'supplier' of the 'information'?
- could the 'information' –now sought to be adduced as proof of a crime- be compiled '*in the ordinary course of business"*?
- was the 'information' in fact supplied by an accused who was not compellable?

22. A number of similar legal challenges arose in the case of *The People (Director of Public Prosecutions) v. O'Mahony & Daly*[22] (and later, the re-trial of *The People (Director of Public Prosecutions) v. O'Mahony*[23]) including whether computer printouts or data come within the CEA 1992 at all. A frequent criticism of the CEA 1992 in the Anglo prosecutions was whether the CEA 1992 was intended to encompass paperless business records. However, an examination of the Dáil and Seanad Éireann Debates in 1992 indicates that computerised records were in fact at the forefront of this legislative development. The Minister for Justice at the time, Mr. Padraig Flynn, referred to Part 11 of the Bill stating that it remedied a '*serious deficiency'* in our criminal procedure and that '*most commercial records are held nowadays on computer and there is no provision for the admissibility of computerised records…*'[24] Dr. Brian Hillery stated during the same debate that '*[t]o exclude much of the information stored in computers from use in a criminal prosecution because of the hearsay rule would be to ignore the practicalities of modern life.'*

23. **Appendix A** of this paper is a breakdown of the terminology used in s.5 and s.6 of the CEA 1992 and a working interpretation of the same. It assists to clarify

[22] [2016] IECA 111.
[23] *The People (Director of Public Prosecutions) v O'Mahony* Bill No. DUDP-194/2014.
[24] Dáil Debates, 3rd March 1992.

who is the compiler, who is the supplier, what is the ordinary course of business, and who should prepare a certificate. **Appendix B** is a sample draft certificate that can be adapted for use in the context of computerised records. As noted at the outset, some of the witnesses handed over hard-copy documents, almost all of which had been printed from the Anglo computer system. It was important that the witnesses identified in the body of the certificate precisely where the document had been located (for example on a computer on the premises at Anglo Irish bank) and that the document had been printed in the normal course[25]. There were also a number of discs and hard drives containing electronic documents that were handed over by a central person, having been downloaded in an e-discovery process. This process was also addressed in the relevant certificate. It is important that each certifier has a full understanding of the statements in the certificate and, as the witness is attesting as to matters of law (such as privilege and compellability), should obtain independent legal advice where necessary.

24. A significant issue that may be highlighted is the effect of an objection to admissibility served under s. 7 (2) of the CEA 1992. Pursuant to s. 7 (2) of the CEA 1992, a party to the proceedings may *'object to the admissibility in evidence of the whole or any specified part of the information concerned'.* In simple terms, this is an objection to the admissibility of the information under s. 5 (1) conditions as opposed to an objection to the use of a certificate per se.

S. 6 (3) (a) of the CEA 1992 states that, where notice has been served under section 7 (2) *'objecting to the admissibility in evidence of the whole or any specified part of the information concerned'* the court shall require oral evidence to be given '*of any matter stated or specified in the certificate'.* In the case of *The People (Director of Public Prosecutions) v. O'Mahony & Daly*[26] the Court of Appeal was satisfied that this was a mandatory requirement and the trial court must hear oral evidence as to whether *'the statutory pre-conditions to any valid*

[25] Where information contained in a document is admissible in evidence, such evidence may be given by the production of a copy of the document as per s. 30 of the CEA 1992.
[26] [2016] IECA 111.

reliance on s. 5(1) existed'. [27] The Court of Appeal referred to a '*subsidiary issue'* following on from this ruling:

> *"75. There then followed lengthy submissions in respect of yet another subsidiary issue (whether or not the redundant s.6 certificate could itself be treated as a statement served for the purposes of s. 6(1)(d) the Criminal Procedure Act 1967 as amended by s. 10 of the Criminal Evidence Act 1992 in respect of any evidence that the prosecution might ultimately seek to lead from Mr Peake on the s. 5(1) issue, regardless of whether that would be in the course of the voir dire or before the jury), which resulted in a ruling that is not appealed against."* (emphasis added)

Simply put, the question arises as to whether the certificate is in fact redundant or simply a 'nullity' once an objection is made under s. 7 (2) of the CEA 1992 (as argued in the *The People (DPP) v O'Mahony*). Further, what is the witness speaking to when giving evidence during the *voir dire*?

25. S. 6 (1) of the CEA 1992 states that a certificate '*shall be evidence of any matter stated or specified therein'.* This must mean that it falls into a class of documentary evidence that is self-authenticating. However, where there is an objection to the admissibility of the whole or part of the information under the s. 5 (1) provision, the trial court shall hear oral evidence '*of any matter stated or specified in the certificate'* (as per s. 6 (3) of the CEA 1992).

Therefore, the certificate may be redundant in the sense that it is no longer self-authenticating, but it is the document to which the witness speaks when giving the relevant oral evidence. However, until this issue is clarified, a person signing a certificate should also make a statement addressing the relevant '*statutory pre-conditions'* for the purposes of s. 5 (1) of the CEA 1992.

26. It should also be noted that the use of a certificate is not a statutory prerequisite to the admissibility of information under s. 5 (1) of the CEA 1992. The matter can

[27] *Ibid* at [101].

simply proceed by oral evidence at the outset and the absence of a certificate does not preclude the application of s. 5 (1). Compliance is however required with s. 7 (1) (a) and s. 7 (3) of the CEA 1992, namely, that a copy of the relevant business document must be served on the accused under s. 6 (1) of the Criminal Procedure Act 1967 (as amended).[28]

27. The application of s. 8 of the CEA 1992 has also been litigated in the recent trials (the fairness provision). This section states that '*information or any part thereof*' that is admissible in evidence by virtue of s. 5 (therefore it's found to be admissible evidence at this point) '*shall not be admitted if the court is of the opinion that in the interests of justice'* the information or that part ought not to be admitted.

In making this decision, the court shall have regard to all of the circumstances of the evidence, including whether:-

(a) having regard to the content, source and compilation of the information, there is a reasonable inference that the information is reliable;
(b) having regard to the nature and source of the document containing the information, and any other relevant circumstance, there is a reasonable inference that the document is authentic;
(c) any risk, having regard in particular to the likelihood of it being possible to controvert the information, where the person who supplied it does not intend to give oral evidence in the proceedings, that its admission or exclusion will result in unfairness to the accused.

An objection may be raised as to whether it is '*fair*' to admit documents under s. 5 of the CEA 1992 where the supplier of the information is a witness on the book of evidence. This is not a strong objection *per se* unless there is some additional element, which would make admissibility under the statute unfair. In fact, it is specifically envisaged by s. 8 (2) (c) of the CEA 1992 that the court, in its assessment, may take account of the fact that the supplier of the information does

[28] See *The People (The Director of Public Prosecutions) v Byrne* [2001] 2 ILRM 134.

not intend to give evidence at the trial. The corollary of that is that, in many cases, the supplier may in fact be available and on the book of evidence but that admissibility comes through the statute and not through the witness.

However, there may be such additional elements as referenced above which would render admissibility under s. 5 (1) unfair to an accused person. This issue arose in the retrial of *The People (Director of Public Prosecutions) v. O' Mahony* where objection was taken to the admissibility of emails under s. 5 (1) of the CEA 1992.

Nolan J was satisfied that the remit of the CAE 1992 and the certificate evidence was '*very wide'*. However, he took the view that what was envisaged by the legislation '…*was technical data that would be very difficult to retrieve and give in the form of evidence by any other means other than a type of record type evidence produced by receipt."*[29] Nolan J ruled that all of the email evidence would not be admitted and that he would exercise his discretion under s.8 of the CEA 1992 to exclude three specified emails. While technically admissible, he took into account the nature of the content of the emails, whether the supplier was available to give evidence and whether the supplier was a former co-accused. In particular, he differentiated between an email where the content was '*just discussion'* as opposed to an email which was followed up by technical activities within the banking system and thereby admissible.

28. S.8 of the CEA 1992 refers to a '*reasonable inference'* that the information is reliable or authentic. This raises the issue as to whether, where evidence has been printed from a computer, it is also necessary to have 'foundation evidence' statements as to the reliability and authenticity of the actual computer system (the 'foundation testimony' discussed in respect of real evidence above). In the context of <u>business records</u>, this foundation evidence is found in s. 6 (1) of the CEA 1992, which sets out the legislative framework for the certification of those records hinging on the 'personal knowledge' of the supplier of the information. It is the pre-conditions (personal knowledge and routine compiling in the course of

[29] *The People (DPP) v O'Mahony*, Trial Transcript 9th October 2017 p. 51.

the business) which lend reliability or authenticity to the documents in question. The certifier vouches for the documents as a self-authenticating class of documents.

The Law Reform Commission argues against imposing a '*separate evidential regime'* with a '*higher foundation requirement'* for electronic documentary evidence as such a regime would create enormous costs and delays in legal proceedings.[30] In the United Kingdom, prior to the repeal of s. 69 of the PACE Act, 1984, it was necessary to prove the reliability of the computer before any statement in a document produced by a computer could be admitted in evidence. This applied whichever category the information fell within (real or hearsay evidence).[31] The repeal of s. 69 means that any evidence pertaining to the reliability of a computer will go to weight and that '*in the absence of any evidence to raise the issue of reliability, it would seem that the presumption of regularity will apply'*.[32]

Given the scale of the electronic material seized in the back-to-back prosecutions, detailed evidence was in fact adduced addressing *inter alia* the integrity of the Anglo computer systems, error checking mechanisms, record management procedures and storage, the integrity of the secondary media (discs, usb keys) upon which the information was downloaded and the security procedures for the storage of the records and data off-site.

PART 4: BANKERS' BOOKS EVIDENCE ACTS

29. In the light of the fact that the material in the back-to-back prosecutions was 'banking material', extensive affidavits were also prepared under the *Bankers' Books Evidence Acts 1879-1989.* The BBEA 1879 renders a copy of any entry in a bankers' book *prima facie* evidence in all legal proceedings[33] (defined to

[30] Law Reform Commission *Report on the Consolidation and Reform of Aspects of the Law of Evidence* (LRC 117-2016)
[31] *R. V. Shephard* [1993] A.C. 380, HL.
[32] Archbold *Criminal Evidence, Pleading and Practice 2019* [9.13].
[33] S.3 of the *Bankers' Books Evidence Act 1879.*

include civil and criminal proceedings[34]). However, admissibility is subject to formal proof, provided by an officer or partner of the bank, who can testify as to three pre-conditions:

- the book[35] must have been one of the ordinary books of the bank when the entry was made;
- the entry must have been made in the usual and ordinary course of business of the bank;
- the book must have been in the custody and control of the bank.[36]

The foregoing evidence of proof can be given orally or by affidavit and must be given by a partner or officer of the bank.[37] Furthermore, the evidence shall not be admitted unless '*some person'* (who does not have to be a partner or officer) gives evidence that the '*copy has been examined with the original copy'*.[38]

Again, the affidavit addresses issues of law and fact and the deponent should have independent legal advice where necessary.

In the case of *ACC Bank Plc. V Byrne*[39]*,* Mr. Justice Cregan addressed the use of computerised banking records under the BBEA regime as follows:

> *"51. In my view therefore what the Bankers' Books Evidence Acts now require, for modern applications to court in today's world, where details of loans and other accounts are kept on computer, (and where bank statements are then printed off from computer records) is as follows:*

[34] S. 10 of the *Bankers' Books Evidence Act 1879.*
[35] 'Book' includes correspondence (see *Volkering v Haughton* [2010] 1 IR 417 at 433). Also, s. 131 of the Central Bank Act 1989 updates s.5 of the 1879 Act to enable the reception of non-legible formats (i.e. computer records).
[36] S. 4 of the *Bankers' Books Evidence Act 1879.*
[37] S. 4 of the *Bankers' Books Evidence Act 1879.* '*Officer*' includes an employee as per O' Malley J in *Ulster Bank Ireland Ltd. V. Dermody* 2014] IEHC 140.
[38] S. 5 of the *Bankers' Books Evidence Act 1879.* See also *ACC Bank Plc. v Byrne* [2014] IEHC 530 as to the procedure to be followed when comparing copies and originals.
[39] [2014] IEHC 530.

1. A printed copy of a computer entry (e.g. a bank account statement) contained in the bank's computer records [see s.3 of the Act];

2. Formal proof, given by an officer of the Bank,
(1) that the computer records (from which the copy of the bank statement was taken) are one of the ordinary computer records of the bank [see s.4],
(2) That the entry of the account details into the computer records was made in the usual and ordinary course of the business of the bank[see s.4],
(3) That the computer records are in the custody or control of the bank [see s.4];

3. Formal proof that the bank account statements printed off from the computer and adduced in evidence have been reproduced directly from the bank's computer records [s.5 (1)(a)]. This must be proved by the person in charge of the reproduction [see s.5 (2) (a)];

4. Formal proof (if there is a copy of a copy) that the copy of the bank statement produced in court is a correct copy of the bank statement printed off from the computer (see 3 above) and that the two have been compared [see s.5 (1)(b)(i)]. This must be proved by the person who has compared the copy produced in court with the original copy [see s.5 (2) (b)];

5. Formal proof that the copy reproduced in court is also a copy which, in effect, <u>could</u> have been reproduced directly from the bank's computer records [see s.5 (1)(b)(ii)]. This must also be proved by the person in charge of the reproduction at 3 above [s.5 (2) (a)];

6. Formal proof that the copy of the bank statement produced in court has been examined with the original entry in the bank's computer records and that it is correct [s.5 (1)(c)]. This must be proved by a person who has examined the copy with the original entry in the computer [see s.5 (2)(c)].''

30. One recent objection to admissibility under the BBEA 1879 concerns the use of affidavits in a criminal trial. It has been argued that evidence in a criminal trial must be given in the witness box. However, the following observations can be made in respect of this argument:

- an affidavit, unlike a witness statement, is sworn evidence;
- it constitutes evidence of the formal proof of the compliance with the statutory conditions at the time of swearing;
- proof by way of affidavit of banking records is specifically provided for in the statute with s. 3 referring to '*all legal proceedings'* and '*legal proceedings'* is defined to include civil and criminal proceedings.

PART 5: REFORM

31. In the Dáil Debates surrounding the introduction of the CEA 1992, one deputy stated that it should be dealt with by way of Special Committee as it was a '*minefield'*[40]. I agree that these trials may certainly be documentary minefields. However, the current legislative framework, while requiring to be updated, has in fact withstood robust and sustained attacks in recent years. By 2009, the Law Reform Commission was satisfied that the system of checks and balances in the CEA 1992 provided a sufficient level of protection against any likely abuse or fraud concerning the admissibility of business records.[41]

32. It is noteworthy that the provisions of the CEA 1992 are largely replicated or unchanged in the Commission's draft *Evidence (Consolidation and Reform) Bill 2016.*[42] However, this proposed draft bill includes two important amendments. In the first instance, it includes a single technology neutral definition of 'document' with a view to addressing the meaning of a 'document' in the modern paperless world. It further proposes the application of a presumption applying to the admissibility of business records. The presumption, as noted by the

[40] Dáil Debates, 3rd March 1992
[41] Law Reform Commission *Consultation Paper on the Documentary and Electronic Evidence* (LRC CP 57-2009) at [5.59].
[42] Law Reform Commission *Report on the Consolidation and Reform of Aspects of the Law of Evidence* (LRC 117-2016)

Commission, would make the section 6 Certificate procedure redundant[43] and would work in the following way:

> "*In this case, establishing the basic fact under s. 5 (1) of the 1992 Act that the record is a properly constituted business record (i.e. was compiled in the ordinary course of business and supplied by a person with personal knowledge) will render it presumptively admissible.*
>
> *This presumption may be rebutted where the party challenging the admission of the business record can prove that it is inadmissible by virtue of any of the further provisions of s.5 of the 1992 Act, including that it was generated in anticipation of litigation. The evidential burden will shift to the party challenging the admission of business records to prove that they are inadmissible by virtue of any of the named conditions*." (emphasis added)

This presumption, in the Commission's view, would address the '*overly exacting demands'* on the adducing party in the current statutory regime.[44] This would clearly be welcomed by prosecutors.

33. One of the most pressing concerns is the duration of white-collar criminal prosecutions in this jurisdiction. In 2017, the Joint Head of Fraud at the Serious Fraud Office in the U.K. said that '*trials tend to be few in number and last 3-4 months. Years and years ago, I had an eight-month trial for two defendants at Blackfriars Crown Court-that wouldn't happen any more'.*[45] Unfortunately, Ireland is still firmly in the area of such eight-month trials. This highlights the necessity for a number of reforms including, in the first instance, the necessity for 'preliminary trial hearings' as outlined in the *Criminal Procedure Bill 2015* (submitted to Government for Approval in June 2015). The Bill provides (at s.2) that the trial court may, upon its own motion or that of the parties, conduct a preliminary hearing on *inter alia* whether certain material ought to be admitted in

[43] *Ibid* [2.185]
[44] *Ibid* [2.172]
[45] *The Serious Business of Fighting Fraud,* 19th January 2017.

evidence. This proposed legislation forms part of the current *Programme for Government* and is now well overdue.

34. Finally, such large-scale fraud trials also highlight the urgency of implementing the most recent recommendations of the Law Reform Commission in respect of the establishment of a multidisciplinary Corporate Crime Agency.[46] This would address the complexity of drafting warrants or orders and explaining to witnesses the meaning and legal effect of certificates or affidavits. This Agency would also play an important role in securing certificates and affidavits and 'foundation testimony' statements as the investigation progresses and when the material is handed over. This would ease the considerable complexity of putting the legal documentation together possibly years after the material was seized.

[46] Law Reform Commission *Report on Regulatory Powers and Corporate Offences* (LRC 119-2018)

APPENDIX: A

Is there a 'document'?	Document is defined to include: *a) a map, plan, graph, drawing, photograph or* *b) a reproduction in permanent legible form, by a computer or other means, (including enlarging) of information in non-legible form."*[47] Information in non-legible form is defined to include information on microfilm, microfiche, magnetic tape or disc.[48] The use of 'include' indicates broad definitions. The definition of '*document*' in s. 2 (1) the Criminal Justice (Theft and Fraud Offences) Act 2001 is almost identical save as to include a 'record'. The definition of '*document*' in s.2 of the Criminal Justice Act 2011 defines a '*document*' as including "*information recorded in any form and any thing on or in which information is recorded and from which information can be extracted".* S. 34 of the Competition and Consumer Protection Act 2014 defines *'records'* as including '(*a) discs, tapes, sound-tracks or other devices in which information, sounds or signals are embodied so as to be capable (with or without the aid of some other instrument) of being reproduced in legible or audible form.'* Criminal Justice (Surveillance) Act 2009 defines a document as including (a) *any book, record or other written or printed material in any form, and (b) any recording, including any data or information stored, maintained or preserved electronically or otherwise than in legible form*.' The UK Criminal Justice Act 2003 uses a non-prescriptive definition and describes a document '*anything in which information of any description is recorded'* (s. 134). The foregoing definitions are all useful when it comes to dealing with electronic or computer generated documents[49].
Is there 'information' in the document?	'Information' is defined as '*any representation of fact, whether in words or otherwise*'[50] and therefore can include graphs or pictures etc. Information in non-legible form that had been reproduced in

[47] S.2 CEA 1992.
[48] S.2 CEA 1992.
[49] See also definitions in sections 908C (1) and 908D (1) of the Taxes Consolidation Act 1997 (as amended)
[50] S.2 CEA 1992.

<table>
<tr><td></td><td colspan="2">legible form must have been reproduced in the course of the normal operation of the reproduction system concerned[51] (i.e. computer printouts)</td></tr>
<tr><td rowspan="2">Was the information 'compiled' in the 'ordinary course of business'?</td><td colspan="2">'Business' is defined very broadly to include 'any trade, profession or occupation carried on for reward or otherwise…'[52]

Includes a 'charity' as defined in the Charities Act 2009 (s.2).</td></tr>
<tr><td>Compiled' is not defined in the CEA 1992.

The word 'compile' means to collate, organize, systemise, anthologise. In simple terms, it should be read as meaning 'putting something on file'.

The date (or approximate date) of the compiling, if not on the document, should be outlined in oral evidence or section 6 certificate.[53]</td><td>Compiled in the ordinary course of business means compiling information routinely or systematically in the ordinary conduct of the business concerned and not for the purpose of investigating or prosecuting an accused person.

Therefore, the 'compiler' is in effect the business, the organisation, the medical practice, the sole trader business etc.

S. 6 (1) of the CEA 1992 which refers to the person signing the certificate being in the management 'of a business in the course of which the information was compiled'.</td></tr>
<tr><td>Was the information in the document 'supplied' by a person who had or may reasonably be supposed to have had, 'personal knowledge' of the matters dealt with?</td><td colspan="2">A person must have supplied the information in the document (e.g. wrote the email) and had (or may reasonably be supposed to have had), personal knowledge of the matters dealt with (Person A)[54].

It is not necessary that person A be identified so that their personal knowledge can be assessed (R v Ewing[55]) because their personal knowledge may be inferred (R v Foxley[56]).

Person A may be available and able to testify but may not be able to remember the matters dealt with in the information some time ago.</td></tr>
</table>

[51] S.5 (1) (c) CEA 1992.
[52] S.4 CEA 1992.
[53] S.6 (1) (g) CEA 1992.
[54] S.5 (1) (b) CEA 1992.
[55] [1983] 2 All ER 645.
[56] [1995] 2 Cr. App R 523 at 536.

	Person A may no longer be available or unable to testify for whatever reason e.g. dead, retired, ill. The CEA 1992 does not require that Person A has to supply the information in the ordinary course of business. This is significant where the supplier is supplying information, which may later be the foundation of a crime.[57]
Was the information supplied indirectly through an intermediary or intermediaries (who, or each of whom received it in the ordinary course of business)?	The information may be supplied by Person A and travel via Person C / D /E. However, Person C/ D / E must have '*received that information in the ordinary course of a specified business'*.[58] This section allows for several persons in the chain of supply. Sometimes the supplier of the information will be perfectly obvious e.g. the person who wrote the email or the letter. This may be complex in the case of a contract document for example and may lead to issues around whether that supplier was compellable and gives rise, in many instances, to the question of whether the information was supplied by the accused person who is not compellable such as the accused.
Is the information subject to the exclusionary provisions?	Is the information privileged from disclosure in criminal proceedings? Is the information supplied by a person who would not be compellable to give evidence? Was the information compiled for the purposes of a criminal investigation, inquiry, civil or criminal proceedings, proceedings of a disciplinary nature?[59] Does it come within any of the statutory exceptions to these exclusions?[60]
Who is the person signing the certificate?	The certificate should be signed by a person occupying a position in relation to the management of the business in the course of which the information was compiled <u>OR</u> who is otherwise in a position to give the certificate i.e. attest to the veracity of the information.[61]

[57] See Nolan J in *The People (DPP) v O'Mahony*, Trial Transcript, 6th October 2017 where he stated that "*Well you see, I think in a banking context …to commit wrongdoing or fraud or whatever you want to call it, you have to go through the banking systems normally…. Now, if you're saying because the purpose is illicit the fingerprints cannot be used, then it would nullify it, so the intention of the legislation is to collect evidence of wrongdoing*." (p. 35)
[58] S.6 (1) (d) CEA 1992.
[59] S.5 (3) CEA 1992
[60] S.5 (4) CEA 1992
[61] S. 6 (1) CEA 1992

	It is sufficient for a person to make the certificate in the best of his or her knowledge or belief. A certificate is signed NOT sworn. It comes in via the statutory provisions. If there is an objection, sworn evidence MUST be called.

APPENDIX: B

THE PEOPLE AT THE SUIT OF THE DIRECTOR OF PUBLIC PROSECUTIONS

V.

XXXXX

BILL NUMBER XXXXX

DRAFT / CERTIFICATE PURSUANT TO SECTION 6 OF THE CRIMINAL EVIDENCE ACT, 1992

I, **XXXX,** at XXXXXX aged 18 years and upwards, hereby certify:

1. I am a **{Insert}** at **{Insert}.**

2. I make this Certificate pursuant to Section 6 of the Criminal Evidence Act 1992. The matters set out in this Certificate are true to the best of my knowledge and belief.

3. **{Outline of job description, role in management position of the business, organisation, detail as to why this person can attest to the veracity of the document (s)/ OR if not in management, detail as to why this person can attest to the veracity of the information in the document (s)}**

4. **{Outline of the process for handing over the documents e.g. in compliance with an order made pursuant to the terms of s.52 of the Criminal Justice (Theft and Fraud Offences) 2001 / warrant etc.}**

5. I have described in my statement dated the **{Insert}** the provision of documents to An Garda Síochana in accordance with {orders or warrants} and I hereby adopt the

contents of that statement as correct for the purposes of this Certificate insofar as it is necessary to do so. I have set out in the Schedule 1 attached to this Certificate a list of specific material which was supplied by me to An Garda Síochána and I understand that this material is now contained on the List of Exhibits in the Book of Evidence in the above-named proceedings. Schedule 2 sets out my statement for ease of reference.

6. The information contained in the material set out in Schedule 1 is information that was compiled in the ordinary course of business of {**Insert}**.

7. The information contained in the material set out in Schedule 1 is information that was supplied by persons who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with. Given the detail of the information and the lapse of time since the information was supplied, the persons who supplied the information cannot reasonably be expected to have any, or any adequate, recollection of the matters dealt with in the information.

8. Insofar as information contained in the material was supplied indirectly, each person through whom it was supplied received it in the ordinary course of business of **{Insert}**.

9. Some of the documents set out in Schedule 1 were stored electronically in the computer systems of **{Insert}** and some were held in paper form by **{Insert}**. As regards the documents held on the computer system, they were and are legible on a computer screen. Copies of the documents have been and can be printed off in the normal way from the documents stored on the computer system.

   OR

   As regards the documents held on the computer system, the process of retrieving those documents and putting them onto a number of external hard drives and discs was facilitated by **{Insert}.** All the discs and hard drives that I gave to An Garda Síochána, as described in my statements, were discs and hard drives which I had

received from **{Insert}**. The information on the external hard drives and discs was legible when I received it.

10. I am advised and believe that the information contained in the documents set out in Schedule 1 is not privileged from disclosure from criminal proceedings.

11. I am advised and believe that the information contained in the documents set out in Schedule 1 is not information supplied by a person who would not be compellable to give evidence at the instance of the prosecution.

12. The information contained in the documents set out in Schedule 1 was not compiled for the purpose of, or in contemplation of any of the following: (a) a criminal investigation; (b) an investigation or inquiry carried out pursuant to or under any enactment; (c) civil or criminal proceedings; or (iv) proceedings of a disciplinary nature.

Signed:

Date:

Witnessed:

SCHEDULE 1

Number or other identifying mark on exhibit	**Description of Exhibit**