National Law Enforcement Data Programme:

LEDS: Evidence

Discussion Document

20 September 2018 [Updated 02 August 2019]

This Document has been written with the aim of stimulating discussion on the Code of Practice for LEDS. It is not intended to be viewed as current Home Office policy or intention. It is to be circulated to Law Enforcement Governance bodies and Civil Society Organisations for reflection.

1. This short paper has been written to describe the approach to ensuring that Law Enforcement Data Service (LEDS) has evidential quality data that can be used effectively within the Criminal Justice Sector. It is designed to stimulate a discussion prior to agreeing an LEDS Evidential Position. LEDS will replace the Police National Computer (PNC) which is primarily used by law enforcement to record records of fact such as arrest, detention and conviction information. LEDS will also replace the Police National Database (PND) which is the primary system used by the law enforcement community to share intelligence records.

2. Historically those intelligence records are not used in evidence but to guide investigations. It is the intention of LEDS to bring together at the point of query information from both sources. The first part of this paper presents some of the key issues in relation to LEDS and Evidence. Whereas the second is an interpretation of how LEDS information will be submitted into court as Evidence. This is largely presented for information to assist with the first part of this paper.

3. **The aim of this paper is to provoke questions on;**

    a. **providing greater understanding over the nature of the information within LEDS that will be used to support prosecutions**

    b. **what the conditions are for providing assurance for the court and for the public in general that material produced from LEDS has not been altered; and,**

    c. **providing reassurance around the audit process that will determine whether a LEDS user has accessed the LEDS system and what actions they have performed.**

4. To note this paper relates to evidence presented in England and Wales. Scotland, Northern Ireland and other jurisdictions will have similar concerns, but, different legislative and procedural approaches. Collaboration with those jurisdictions and relevant Scottish and Northern Ireland Civil Society Organisations is ongoing to ensure that suitable discussions occur and guidance is produced.

<u>Part 1 - LEDS and the Criminal Justice System.</u>

5. There are two broad challenges to overcome with the use of LEDS information as evidence. The first is that LEDS will contain significant amount of data that has previously been reserved for intelligence rather than evidential purposes, the second is ensuring consistency and transparency around the level of challenge that can be applied to the data.

6. The transition from PNC and PND to LEDS essentially means, at one level, the amalgamation of information which is a matter of public record (with some

exceptions) with information derived from intelligence sources which may comprise information which is within the experience of the reporting officer (i.e. seen, heard, touched), that which comes from covert human intelligence sources (CHIS) or from lawfully authorised technical deployments such as trackers or listening devices.

7. Some material will be inherently less reliable, which does not necessarily mean that it is less accurate, merely that it requires a higher degree of corroboration before operational action takes place. Some material will require more sensitive handling – where the nature of a particularly sensitive technique or the existence or identity of a CHIS may be exposed (the latter, with potentially devastating consequences).

8. PND deals with information gathered for intelligence purposes, rather than evidential use, its purpose being to garner and share information whilst protecting the human or technical source. A key tenet of LEDS is to preserve the utility of PNC whilst continuing the garnering and dissemination capabilities of PND – which has not to date been intended to be a source of evidential material.

9. The joining of this information at the point of use represents a distinct change, creating a single data service with a spectrum including broadly-accepted factual records, to data which less confidence might safely be attached. This does not mean that Intelligence data cannot either be evidence (requiring significant corroboration) or be a source of data which points to where evidence may be found.

10. It will therefore be necessary to record the data-source and potential confidence in the information provided. The existing National Intelligence Model might be instructive and could be managed by a system of 'data flags' on LEDS. Intelligence Management (modified in 2016 to a 3x5x2 model) is issued by the College of Policing for England and Wales[1]:

11. **The National Intelligence Model (NIM) addresses the use of such material as an intelligence product[2] and the proposition is to use the model to add "data flags" to intelligence material so that the material can be appropriately assessed at the point of use.**

[1] https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/

[2] Additional information about the National Intelligence Model is in part two of this paper

12. When considering the potential admissibility of this material, it is also necessary to consider specific rules on Hearsay Evidence[3], i.e. statements "not made in oral evidence in the proceedings that is evidence of any matter stated" (section 114 (1) Criminal Justice Act 2003). Part 2 of this paper outlines the principles to be followed prior to using Hearsay Evidence.

13. A computer printout is also 'real' evidence: the Common Law rule is that a presumption will exist that the computer producing the evidential record was working properly at the material time and that the record is therefore admissible as real evidence.

14. That presumption can, however, be rebutted if information to the contrary is cited as evidence. In that event it will be for the party seeking to produce the computer record in evidence to satisfy to the court that the computer was working properly at the material time. This will require action on three fronts.

    a. Providing a convincing narrative around the end to end audit capability, (what it will do and how),

    b. Retaining information about the operation of LEDS, that it was working as expected at a material time, and,

    c. Retaining information about each external system interaction with LEDS

15. This rule generally applies where there is no additional human intervention and the information is generated or processed automatically – e.g. the creation of banking or telephony records. Some LEDS data will automatically fall into this category. It will be necessary (particularly in respect of this data-type) to consider additional authentication as to its provenance and integrity (for example by cryptographic hashing).

16. **In relation to Hearsay Evidence and proposed Printouts from LEDS, this paper proposes the Home Office with the CPS and Law Enforcement agree and document the approach to be taken in relation to LEDS information as a digital exhibit and discuss this with interested groups to identify further guidance or training materials that might be necessary.**

[3] Material on Hearsay Evidence in this document is substantially reliant on https://www.cps.gov.uk/legal-guidance/hearsay

17. The following list comprises some examples of the types of information which may be held on the LEDS system and likely evidential requirements. It is intended for discussion only and is therefore not designed to be exhaustive in nature. It will therefore be necessary, at a later stage, to examine in detail the various data-types, their source and therefore, their potential handling.

Type of information	**Evidential requirements**
Documents uploaded by police	May require: (a) Evidence from the originator, the officer responsible for uploading and/or the officer producing; and/or (b) Assurance of provenance: origin, continuity and integrity (either through oral evidence or by some other admissible means of assurance (e.g. crypto-hash)).
Information from individual officers	Will usually require a written statement from the originating officer, which may be 'admitted' under sec.10 CJA 1967; but should in any event be capable of being tested by the defence in any proceedings.
Evidence about the use of LEDS	A combination of technical and other evidence about system use. The technical information should be confined to transactional activity; additional evidence may be required (where activity by an individual rather than a machine is in dispute); broadly, this will relate to attribution of the activity, which may go beyond machine logs.

Part 2 - LEDS utility in the Criminal Justice System.

National Intelligence Model

18. The National Intelligence Model as referenced in part 1 of this paper is a UK wide universal approach for grading intelligence information.

19. The three categories in the model relate to **source evaluation, information/intelligence assessment** and **handling instructions**. However, the 'User Guidance' part of the model do not apply in this context, as the method of handling in the criminal justice system is determined by the rules of evidence.

20. There are three Source Evaluation gradings **Reliable**, **Untested** and **Not reliable**:

    a. Reliable – This grading is used when the source is believed to be both competent and information received is generally reliable. This may include information from human intelligence, technical, scientific and forensic sources. It is important that the two tests of competence and veracity of past intelligence are both met before a source is considered to be reliable. Where either test is not met, not reliable should be selected and the ground to doubt the reliability should be specified,

    b. Untested – This relates to a source that has not previously provided information to the person receiving it or has provided information that has not been substantiated. The source may not necessarily be unreliable, but the information provided should be treated with caution. Before acting on this information, corroboration should be considered. This would apply to information when the source cannot be determined, for example, Crimestoppers, and,

    c. Not reliable – This should be used where there are reasonable grounds to doubt the reliability of the source. These should be specified and may include concerns regarding the authenticity, trustworthiness, competence or motive of the source or confidence in the technical equipment. Corroboration should be sought before acting on this information.

21. There are five Information / Intelligence gradings: **Known directly**, **Known indirectly but corroborated, Known indirectly, Not known** and **Suspected to be false**:

    a. Known directly – Refers to information obtained first-hand, e.g. through witnessing it. Care must be taken to differentiate between what has been directly witnessed and what has been told or heard from a third party;

    b. Known indirectly to the source but corroborated – Refers to information that the source has not witnessed themselves, but the reliability of the information can be verified by separate information that carries the information/intelligence of assessment (a). This corroboration could come from technical sources, other intelligence, investigations or enquiries. Care should be taken when ascertaining corroboration to ensure that the information that is presented as corroboration is independent and not from the same original source;

c. Known indirectly to the source – Applies to information that the source has been told by someone else. The source does not have first-hand knowledge of the information as they did not witness it themselves;

d. Not known – Applies where there is no means of assessing the information. This may include information from an anonymous source, or partners such as Crimestoppers; and,

e. Suspected to be false – Regardless of how the source came upon this information, there is a reason to believe the information provided is false. If this is the case, the rationale for why it is believed to be false should be documented.

Hearsay evidence

22. Hearsay evidence is admissible in criminal proceedings only if:

    a. The 2003 Act or any other statutory provision makes it admissible - Section 114(1)(a);

    b. Any rule of law preserved by section 118 makes it admissible (see below) - Section 114(1)(b);

    c. All parties to the proceedings agree to it being admissible Section 114(1)(c); or

    d. The court is satisfied that it is in the interests of justice for it to be admissible - Section 114(1)(d).

23. In exercising the discretion under Section 114(1)(d) the court must have regard to the following (and any others it considers relevant):

    a. How much probative value the statement has (assuming it to be true) in relation to a matter in issue in the proceedings, or how valuable it is for the understanding of other evidence in the case;

    b. What other evidence has been, or can be, given on the matter or evidence mentioned above;

    c. How important the matter or evidence mentioned is in the context of the case as a whole;

    d. The circumstances in which the statement was made;

    e. How reliable the maker of the statement appears to be;

    f. How reliable the evidence of the making of the statement appears to be;

    g. Whether oral evidence of the matter stated can be given and, if not, why it cannot;

    h. The amount of difficulty involved in challenging the statement;

i. The extent to which that difficulty would be likely to prejudice the party facing it.

24. Section 114(1)(d) will be considered only in cases where admissibility under the other statutory provisions and the retained common law rules is not allowed. The test for admissibility is "interests of justice".

25. Cases involving business and other documents: The Act deals differently with statements contained in general business documents and statements made in contemplation of criminal proceedings. Generally, a statement contained in a document is admissible of any matter stated if:

    a. Oral evidence would be admissible as evidence of the matter;

    b. The document or the part containing the statement was created or received by a person in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office;

    c. The person who supplied the information contained in the statement (the relevant person) had or may reasonably be supposed to have had personal knowledge of the matters dealt with; and

    d. Each person (if any) through whom the information was supplied from the relevant person to the person creating or receiving the information also received the information in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office (section 117(2)).

26. Although admissibility is generally automatic, there is limited discretion given to the court to exclude evidence if satisfied that the statement's reliability is doubtful in view of:

    a. Its contents;

    b. The source of the information contained in it; The way in which or the circumstances in which the information was supplied or received; or

    c. The way in which or the circumstances in which the document concerned was created or received (section 117(7)).

27. This provision is the only way of challenging the admissibility of business and other documents. The test is in favour of admissibility rather than in favour of exclusion.

28. To be capable of being adduced in evidence, material must be both relevant to the matter before the court and admissible according to the rules which govern admissibility. The Home Office has previously (in 2014) produced guidance on admissibility of evidence (Annex A).

Annex A

You can only present evidence in court:

a. if it has been produced by a witness in the form of a statement, and
b. under oath.

There are strict rules that govern whether a piece of evidence is admissible in court. To make sure it is a fair trial, the court can decide whether:

a. a piece of evidence is admissible, or
b. to exclude it.

The court has the power to exclude evidence, even though it may be admissible, if they feel it is too prejudicial (unfairly biased against the defendant). The court also has extra powers to do with evidence obtained by confession. The court's power to exclude evidence comes largely from:

a. section 78 of the Police and Criminal Evidence (PACE) Act 1984
b. common law, and
c. section 76(2) of PACE, in relation to confessions.

Depending on where you are working you must follow the provisions on admissibility in line with:

a. PACE (England and Wales), and
b. Police and Criminal Evidence (Northern Ireland) Order 1989.

The admissibility of bad character and hearsay evidence is outlined in the Criminal Justice Act 2003 … For evidence to be acceptable it must be:

Probative

It :

a. must have value to the case
b. must be credible, and
c. can be excluded if it has low probative value.

Not prejudicial

It:

a. must be factual and impartial, and
b. can be excluded if the court feels it is too prejudicial towards the defendant.

Relevant

It must:

a. make the matter that requires proof more or less probable, and
b. help to prove the guilt or innocence of the defendant.

Accurate

You must:

a. describe facts given in court as accurately as possible to assist the court in deciding what is true, and

b. remember, how you present your evidence can affect how the court views your evidence.

Coherent You must present your evidence in court in a way that:

a. makes sense to the court, and
b. is easy to understand, which is often chronological (in the order it happened), and
c. in full detail.

Provable

Your case must be capable of proof, unless the law provides otherwise, for example it may sometimes allow an assumption to be made.

The 'res gestae' rule

The 'res gestae' rule allows an event to be put into context. If an event is described on its own without the surrounding circumstances then it may not make sense, so it is for the judge to decide whether:

a. the court allows a witness to state facts with reasonable fullness and in context so that they make sense, and
b. to use this rule to allow evidence, even though it may:
c. not be probative, and
d. be hearsay

Note: 'Res gestae' refers to (if the statement was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion can be disregarded), the statement accompanied an act which can be properly evaluated as evidence only if considered in conjunction with the statement, or the statement relates to a physical or a mental state such as intention or emotion