

Evidence Management – A Policing Perspective



Bill Blackburn provides an understanding of the operational practices in policing where the establishment of reliable evidence is critical for prosecutions. Bill draws parallels with the evidential requirements to support a safety case for safety-critical systems and asks what we can learn from policing practices, such as how we can better position ourselves should a safety incident result in a more formal investigation, potentially leading to court.

The Safety-Critical Systems Club (SCSC) ran an event – What Makes Good Evidence for a Safety Case? – on 30th November 2023, held at the Wellcome Collection in London.

Speakers and discussions provided the participants with an opportunity to reflect on the best practices and pitfalls across a number of fascinating exemplars. With my background in high integrity systems and my experience gained through working within the police and justice sectors, I could see many parallels that are worth exploring.

This article emerged from that event and sets out in broad terms how evidence management operates in the UK and most other jurisdictions. It aims to provide an understanding of operational practice in policing and where there are opportunities to align safety engineering methods. This cross-fertilisation is hopefully useful in its own right but also to put ourselves in a better position should a safety incident result in a more formal investigation, potentially leading to court.

Context for handling evidence in policing

Police gather evidence as a result of an incident occurring and generally a victim making an allegation of a crime. A crime is something that is defined for a particular jurisdiction (e.g. England and Wales) to be an offence subject to investigation, prosecution and dealt within the context of one or more court hearings.

An offence is defined in legislation which is translated into offence wording and aspects such as mode of trial and sentencing provisions. Let's take criminal damage as an example. The Criminal Damage Act (CDA) 1971 has sections setting out a range of situations in which criminal damage might be done, along with various aggravating factors.

The legislation is subject to further codification to allow police, prosecution and courts to put this into practice. For the purpose of investigation and subsequent case building for decisions on whether the crime report can be progressed, the key element is an understanding of the "points to prove". Once that is clear, then the investigation focus is on gathering evidence in relation to these points.

Expanding on CDA 1971, the investigation and prosecution need to be able to prove that person A damaged a specific item of property (smashed a window of a garden shed at 38 Acacia Avenue) belonging to person B by some means (by throwing a brick from nearby) at a point in time (around 3:30 Wednesday afternoon) with an intent to cause damage or by being reckless. To make it easy from an information management viewpoint this can be considered as made up of Persons, Objects, Locations & Events (POLE). In our example:

- **Persons** (A & B)
- **Objects** (Garden Shed & Brick)
- **Locations** (38 Acacia Avenue)
- **Events** (Between 3pm and 4pm Wednesday afternoon)

All very straightforward then! But keep in mind UK legislation stretches back many years, with common law, bye-laws, subject to amendments and repeals, case precedence and other complicating factors. New legislation is enacted and the implications on prior legislation needs to be taken into account.

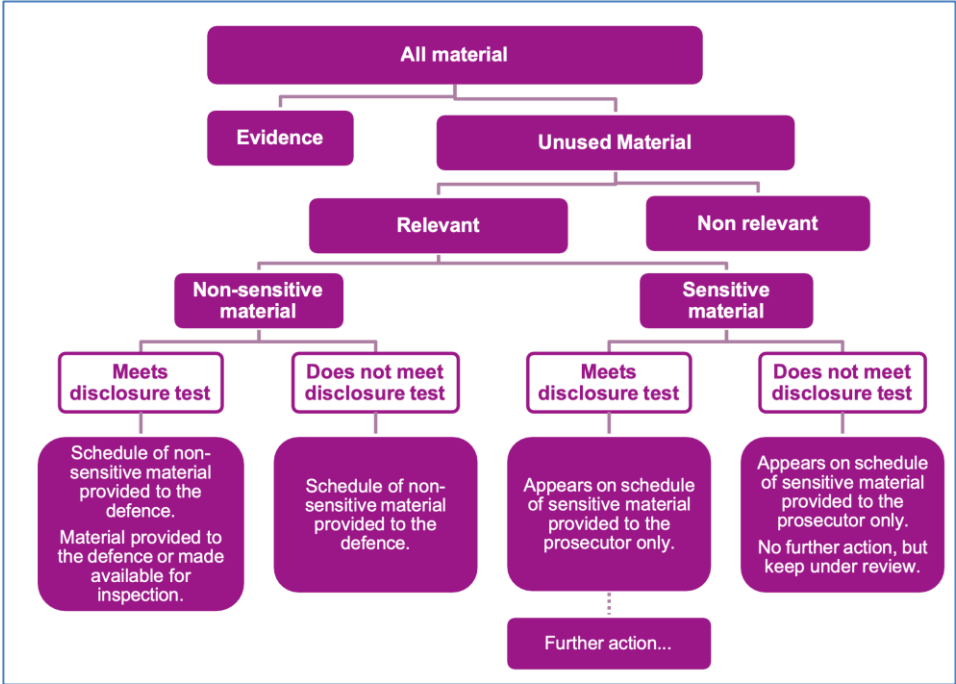
What is Evidence in Criminal Justice?

During the course of an investigation numerous lines of enquiry may be followed, statements taken and material gathered. However the concept of evidence relates to the offence that is being investigated. Further legislation defines clear rules for how investigations are done and how evidence is managed, such as the Police and Crime Evidence Act 1984 (PACE) and Criminal Procedure and Investigations Act 1996 (CPIA). These are operationalised through training, guidelines and codes of practice.

The Attorney General's Guidelines on Disclosure (AGO Guidelines) [1] were released in 2020 and updated regularly since to further clarify how evidence is managed to align with CPIA. The driver for this is that if challenged in court, material not appropriately managed and the right decisions not made for disclosure to the defence, can result in a case being dismissed, despite there being sufficient evidence. A suspect/defendant might simply be able to walk free and justice is not served.

"If challenged in court, material not appropriately managed ... can result in a case being dismissed."

The figure below is taken from the AGO Guidelines and provides a clear taxonomy for what is, and what is not, regarded as evidence but has been acquired during an investigation. It is worth bearing in mind that an initial view of evidence and unused material might change as new information comes to light. Also unused material (i.e. the prosecution is not relying on this) might become evidence that is used by defence to counter the prosecution. Dealing with evidence is in practice “Material Handling”, at which point, the complexities multiple and the volume of material expands.

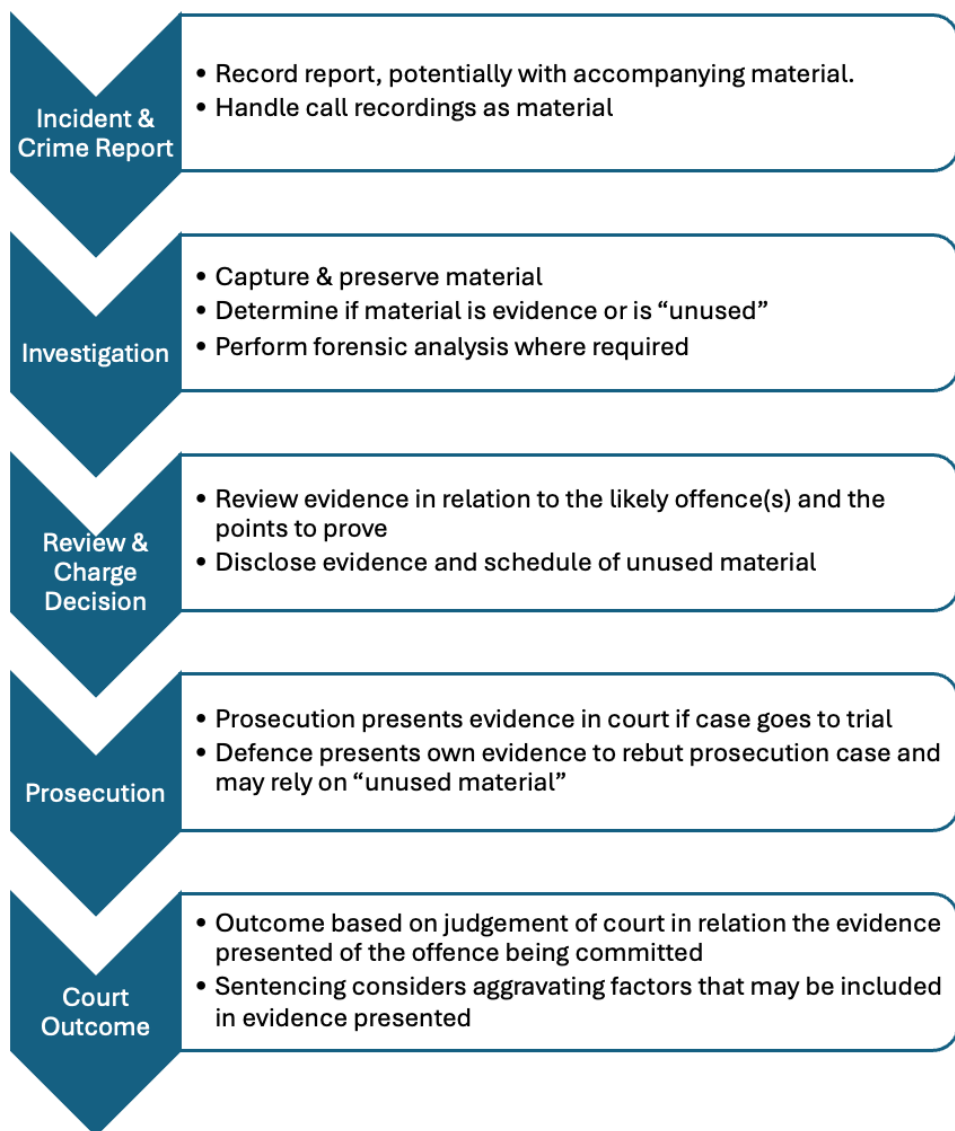


A thread running through is the concept of **relevance**. Evidence needs to be relevant to the offence and the points to prove and unused material needs to be determined to be relevant or not, largely in order to limit the scope of potential material. The relevancy test is therefore one of the key considerations. Similarly in the context of safety systems, evidence needs to be relevant to the system context and the safety case.

The concept of “Unused Material” in the AGO guidance, applies where there may be material that can potentially be relevant but potentially (subject to scrutiny) support the defence and/or undermines the prosecution case. Equally in safety cases, there may be a counter argument where existence of such material could be pertinent.

A Lifecycle Perspective

Across the lifecycle of investigation and prosecution, evidence is handled and shared with the relevant participants. This is illustrated below in a much-simplified way.



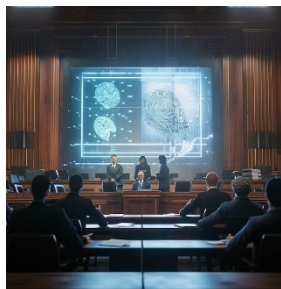
Handling material securely and providing transparency across the parties is a fundamental principle. Continuity and provenance need to be proven and documented as much as the case during the proceedings.

“Continuity and provenance need to be proven and documented as much as the case during the proceedings”

Accidental or even malicious tampering has been known to happen and current practices do the utmost to avoid these aspects from occurring. Information Confidentiality, Integrity and Availability (the security principles – CIA) are foundational principles.

Again the rules and regulations are embodied in the previously mentioned legislation (PACE, CPIA) and guidelines (AGO Disclosure) with relevant training especially for those roles with statutory responsibilities.

Forensic Capabilities



International standards are particularly relevant in forensic analysis, with ISO 17025 regarded as the benchmark for accreditation of forensic laboratories and associated capabilities. Forensics covers a range of scientifically established techniques such as fingerprint analysis, DNA profiling and ballistics.

Locard's Exchange Principle holds that the perpetrator of a crime will bring something to the crime scene and will leave with something from it ("Every contact leaves a trace"). In our criminal damage example, we might therefore expect to have fingerprint and footprint analysis undertaken by an accredited laboratory and matched against relevant national, or potentially, international databases. Or else, against a print taken from the suspect once identified. Over the past few years, increasing use is made of mobile phone cell site analysis, images and video. These are time consuming and resource intensive, so typically the well-established techniques are used first.

Each of these techniques is typically developed in research environments and accuracy established using sophisticated analytical methods to build confidence and/or respond to challenges.

Impact of Novel Technologies

Keeping up with the bad guys is a continual process of response and counter-response. The nature of evidence and the techniques used across the lifecycle need to keep pace. Some of the forensic technologies are mentioned earlier and there are many developments in the area of digital forensics. The increase in data and need for data quality management in policing was the topic of a paper at the SSS'18 Symposium [3]. The key points of that paper related to the increasing importance of data quality as the police and partner agencies move to more digital ways of working. Neglecting this aspect can have major consequences for people who might be wrongly pursued or prosecuted.



As the amount and complexity of material acquired increases, the resource implications rise. Hence the use of Artificial Intelligence & Machine Learning (AI/ML) is finding its way into material handling and analysis. Even so, the basics of establishing continuity and applying CIA apply.

Use of AI in fingerprint analysis is already with us, to assist with detecting ridge details and identify minutiae, which form the basis for matching. Policing is proceeding with caution in order to build confidence and establish trustworthiness.

Concerns about facial recognition prompted an in-depth analysis of operational technologies. In the report “Facial Recognition Technology In Law Enforcement Equitability Study” [4] the National Physical Laboratory (NPL) team developed a study methodology and conducted a controlled data capture, followed by statistical analysis to establish accuracy in real-world situations. This was also based on existing standards for biometric testing and reporting (ISO 19795 parts 1 & 2). The outcome of this work provides guidance for operational users in terms of setting thresholds that are needed in the trade-off between sensitivity & selectivity.



The theme of trustworthiness is a thread through numerous areas of analysis particularly as we all contend with increasing complexity of technologies, interconnected systems and the sheer volume of data that is part of modern life.

“Trustworthiness is a product of the people, systems and processes within organisations...”

Trustworthiness has been promoted by the UK Statistics Authority as part of their Code of Practice [5]. In the context of national statistics the other principles of Quality and Value apply. Trustworthiness in this area is defined as “... a product of the people, systems and processes within organisations that enable and support the production of statistics and data.” Adopting and adapting this for data-centric technologies such as AI is already gaining traction. Standards and Codes of Practice for AI are introducing “Trustworthiness”.

As a principle for evidence management Trustworthiness could be useful in both the safety and policing communities. Sitting alongside other key considerations such as relevance and quality. Potential adaptation of the underlying practices set out in [5] would be a useful activity. For example, can the practices written for management of statistics be easily translated into management of evidence, are any redundant and are any additional practices needed?

Alignment of Evidence Management across Domains

Having set out in broad terms how material and evidence operates across policing we can turn our attention to where it is useful to align with safety engineering use of evidence. In safety, we look at evidence to support the development of a safety case and employ evidence to underpin the safety argument. If it all goes wrong, evidence is gathered during an investigation into an incident or accident.

That's a different starting point from evidence in policing, but broadly similar principles apply. Furthermore in those unfortunate circumstances where an incident might be dealt with through the criminal procedures, the evidential standards need to be fully aligned. Very briefly here are a few considerations to indicate the areas worth exploring further.

Parallels:

- a) In policing the key is gathering evidence to support the "point to prove" – just like we gather evidence to support a safety argument or the "claim"
- b) There is legislation, standards and guidance governing processes
- c) If processes are not followed then the prosecution can be challenged and might fail. Similarly, flawed evidence in a safety case may result in failure to be certified or ultimately manifest as a higher risk of accident
- d) There are process lifecycles where evidence can be pertinent and collected at each stage and each has an important part to play in the overall case. Accurate record keeping, provenance and demonstrating correct handling is important.

Differences:

- a) Novel evidential techniques are being developed all the time but this is perhaps less so in the safety domain that relies on tried and tested techniques. This is illustrated in the challenges of assuring AI – we don't have the techniques to do that reliably in safety at the moment. So we have novelty in systems but not novelty in techniques.
- b) Laboratory or testing facilities, at least in the UK, typically have quality management systems and meet the essential requirements around accreditation of capabilities and facilities plus equipment calibration standards apply across domains. In policing however, the specialist support and scrutiny of capabilities has been applied since 2007 through the Forensic Science Regulator with statutory powers provided through the Forensic Science Regulator Act 2021.
- c) Safety doesn't usually make much of evidence not selected as relevant although we are starting to see more dialectic arguments where the safety case deliberately seeks counterevidence for the claim. There is less formality about whether evidence is relevant (perhaps equivalent to a disclosure test) and there is scope for confirmation bias if data is ignored that doesn't fit the argument.
- d) Maybe the most significant differences are in the people aspects. In UK policing there are statutory responsibilities and defined roles such as investigators and disclosure officers, holding the authorities to account in a very testable manner. Whilst in safety engineering, there is a less prescribed set of roles and responsibilities with some aspects more open to interpretation.
- e) Prosecutions need to be understandable to the many (ultimately a jury of lay-people).

In safety, the safety case at times is understandable only by the few and requires specialist knowledge. Although, if an incident with safety implications results in a public enquiry or other proceedings, the understanding of evidential material will equally apply.

Potential improvements:

Some ideas based on practices within policing for potential improvements within the safety community are as follows:

- There may be opportunities to better define a taxonomy in safety engineering adopting whatever makes sense to do so from policing or indeed other domains. Establishing and maintaining a taxonomy of evidence and related matters can help ensure a common understanding, language and interpretation
- Consider something akin to a disclosure test and relevancy that determines if information can be safely set aside or explicitly regarded as evidence but also have a means of assessing if previously discarded evidence becomes relevant in the future.
- Ultimately it may be useful to adopt the mindset of an investigator or prosecutor. Considering if there was an accident and a resulting prosecution, how would the evidence/safety case stack up to form a defence? Are there special things we should be doing to help support such an eventuality? Perhaps even playing again to the ideas of storytelling and having a narrative in safety cases. Should safety cases be positioned so they are understandable to lay people like a jury?

Practitioners in both domains are encouraged to take time to understand the similarities and differences and hopefully this article will prompt some useful further discussion of mutual benefit.

References

- [1] Attorney General's Office "Attorney General's Guidelines on Disclosure " Gov.UK, 29 February 2024
- [2] Various legislation for illustration: CDA 1971, PACE 1984, CPIA, FSR Act <https://www.legislation.gov.uk/>
- [3] Data in Police & Criminal Justice Systems: How data errors could lead to harm to innocent citizens, Bill Blackburn, Paul Hampton, Mike Parsons SSS'18
- [4] Facial Recognition Technology in Law Enforcement Equitability Study Final Report, Dr Tony Mansfield, NPL Data Science Department, March 2023 https://science.police.uk/site/assets/files/3396/frt-eq-uitability-study_mar2023.pdf
- [5] Code of Practice for Statistics Ensuring official statistics serve the public, UK Statistics Authority Office for Statistics Regulation Edition 2.1 Code revised 05 May 2022

Image Attribution:

leading image: AI generated by MidJourney

fingerprints: AI generated by MidJourney

Facial recognition: ID 220039699 © Andrey Popov | Dreamstime.com

Bill Blackburn, Process Renewal Group Limited and SCSC Member

Bill has a background in mechanical engineering and has worked across aerospace, manufacturing, defence and other high integrity sectors for over 40 years. He is presently engaged in advisory roles with clients in UK policing and capability development in Europe. He has extensive experience in business and information architecture, with a focus on process and data management.