David Spreadborough, CFVA, Forensic Analyst at Amped Software — Written evidence (NTL0015)

INTRODUCTION

As a Certified Forensic Video Analyst (LEVA) acting on a corporate basis on behalf of **Amped Software**, I believe my experience can support the "Justice and Home Affairs Committee" in the framework of this public call for evidence, particularly in the research and development of applications for the analysis and enhancement of video and images for legal use.

I was a UK Police Officer for 24 years, the last 12 being dedicated to CCTV Image evidence. I am now instructed by legal firms throughout the world, to advise and report on CCTV evidence and have given expert evidence in court. I sit on the Forensic Image Analysis Division of the Chartered Society of Forensic Sciences.

Amped Software is a software house that develops software for analysis and enhancement of images and videos. Applications include forensics, security, and investigations in over 100 countries worldwide. Founded in Trieste, Italy, in 2008, with a subsidiary in Brooklyn, NY, the company supports more than 800 organizations in the public safety and national security fields.

This submission details four main areas of concern and proposes some strategy to improve the reliability of the use of Digital Multimedia Evidence (DME) in the judiciary system:

a. The risk to the UK legal system caused by the uncontrolled use of technology within video surveillance systems to improve image quality or hide image errors using artificial intelligence
b. The risk to the UK legal system caused by the lack of forensic acquisition protocols for the recovery of Digital Multimedia Evidence. Current guidelines allow flexibility and differing interpretation.
c. The risk to the UK legal system caused by incorrect automated handling and processing of Digital Multimedia Evidence within policing data software.
d. The risk to the UK legal system caused by the manipulation of multimedia outside of a forensic framework.

1. Do you know of technologies being used in the application of the law? Where? By whom? For what purpose?

Digital Multimedia Evidence (DME), which includes CCTV imagery, is one of the most common forms of evidence used in law. Digital media technologies are now used to capture, transmit, store, search, export, convert, restore, enhance, and present this data. The technologies are used by video surveillance companies, the public, the police and the Criminal Justice System.

DME is used to gain intelligence and to identify the facts of an incident using a camera recording that has captured imagery of interest.

The technologies used shouldn't obstruct the integrity of the image or its authenticity. Therefore, we suggest that all handling, processing and necessary changes, follow a forensic process to maintain trust within a legal setting.

2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

New technologies should maintain trust in the image captured as well as in the image presented. Image technologies can now 'create' missing image data. They can quickly transcode the video to assist in transmission or viewing. They can enhance poor quality footage using image enhancement techniques based on artificial intelligence (AI) and datasets. However, these have no place within a legal system as they have changed and/or introduced data not originally present.

It is now technically possible for a CCTV system to have highly advanced error correction. Error handling is not something new and has been done for many years. If partial image data has not been written or transmitted correctly, then the image could not exist. To handle this, parts of the image may be copied. These errors are highly visible, but they allow the formation of the good parts of the image.

What shouldn't be accepted by the legal system, is the use of video or imagery with hidden or unknown error correction. Actually, parts of a vehicle, or a person, could be constructed artificially as there was an initial error in the capture.

Machine learning, or deep learning, could be used effectively to recognise known objects such as letters, logos or patterns, but they shouldn't be used to 'fix' the original image to create a different version more appeasing to the eye. On the other side, enhancement techniques which simply "show better" what's already there, applying deterministic algorithms on the existing image data, should be generally considered good for evidence if based on known and validated methodologies.

We make ourselves available to the UK Surveillance Camera commissioner to offer further advice and guidance on what parameters should CCTV systems respect to be more in line with the judicial use.

3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used?

While the national guidance for traditional forensics is very clear, the one concerning Digital Multimedia Evidence (DME) is very fragmented and allows for a too flexible interpretation. We suggest the committee to develop a more rigorous guideline which could ensure to always work with the original files as a starting point and that would clearly track all operations applied on them.

When a forensic process is used to capture, acquire, process and present DME evidence, then each stage can be referenced to the one before. Consequently, the process is reportable, repeatable, and reproducible. However, due to internal police procedures, and the requirements upon them to acquire, share and present DME quickly, not all processes are completed in a forensic manner.

Incorrect guidance within UK Policing, allows for imagery evidence to be acquired that is fundamentally different in its digital form to what was originally recorded. It is then possible for further versions of this file to be identically and incorrectly referenced, even when further changes have been made.

Members of the public and CCTV owners might not understand the importance of original material and, as such, the responsibility shouldn't lie with Policing. Video and image technology and the consequences of incorrect acquisition and handling are not understood, which explains why corners are cut. An example being the use of body worn cameras or mobile phones, recording a CCTV monitor to obtain the imagery being played on screen.

The main related issue is that judiciary and lawyers are often unaware of these challenges. A jury could be presented a copy of CCTV from a premise, and no one would be aware that it was not the original and that it had been converted with no forensic framework.

Changes, and different versions, can be made, if those changes are required, they are documented and the process is transparent.

4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

Trust is at the forefront of forensic image and video analysis. A court should be able to trust what is visible. As explained in point 3, however, it is often not identified until the DME is examined correctly. Correct guidance and the improved use of legislation can mitigate any suggestion of altered evidence. This will avoid all the mistakes caused by incorrect handling, poor guidance and a lack of equipment, which often results in material that gets referenced as fake, manipulated or altered. The judicial system might set up a technical working group to ensure that all DME introduced has been correctly acquired, handled, processed, and interpreted before it is presented as fact.

5. With regards to the use of these technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that technologies cannot be used to serve purposes incompatible with a democratic society?

As the ease of consumer video and image processing increases, the requirement for safeguards to the judicial system should also be met.

I was involved in a video evidence acquisition proof of concept in 2007 to show how original multimedia could be acquired via protected, connected networks to save officers visiting and physically obtaining video footage. However, most Police services in the UK now reverse this and ask for multimedia to be sent to them. As stated previously, most CCTV owners or the public are not aware of

forensic acquisition and many CCTV systems now store two versions of a video. One is the original, and another is used for viewing on a mobile device. The footage can be trimmed and then sent to the Police. Consequently, the investigation never learns that there was once a much higher quality video, that has now been overwritten.

Image and Video capture, acquisition, processing, and presentation should be completed in a manner that maintains trust in the imagery. If the current misuse of DME is allowed to continue and trust in video evidence is questioned, the impact on the legal system could be very damaging.

6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place?

In recent years, Policing has looked to Digital Evidence Management Systems to store and collate the vast amounts of data linked to investigations. However, the use of technologies involved, has not been managed effectively and the processing of video and image data for compatibility reasons has overridden that of forensic resilience. The main challenge is that the users, in general, are not aware of these issues. Any technology introduced should have oversight by experts linked to the evidence being handled. Large technology companies may be adept at handling big data, but they are not aware of the issues in video evidence transcoding, interpretation or processing.

As an example, current courtroom presentation software used in the UK suffers with several limitations that any subject matter expert would have promptly recognised during development or testing.

I recommend that any technology introduced in the judiciary system should be validated and approved by people technically competent on the matter.

7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

"The Criminal Procedures and Investigations Act" along with guidance and policy documents, are the main legislation surrounding the handling of multimedia. Considering that both the guidance and policy documents might differ in the interpretation from the Act, we put ourselves at disposal to improve it, as we believe we could avoid mistakes in the application of the law and therefore dangerous flexibility to the legal system. As the technology to create, edit and manipulate video and image evidence has increased, it would be crucial that both the legislation and the guidance are more aligned and compatible to prevent the evidence from allegations of malicious manipulation.

The main issue is that there are very few checks on the integrity and authenticity of DME in the current system. Video and Images have been found to be incorrect within the press and education fields.

8. How can transparency be ensured when it comes to the use of these technologies, including regarding how they are purchased, how their results are interpreted, and in what ways they are used?

Forensic reporting on the handling and processing of DME is paramount in ensuring that it can be trusted throughout the legal system. The purchasing must be made through consultation with subject matter experts and the integrity of the evidence must be a priority.

9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered?

When traditional forensic evidence is obtained and entered as evidence, the reporting protocols dictate certain criteria to ensure any limitations are clearly documented. This must be mirrored with DME. The correct reporting will ensure that integrity, authenticity and, importantly, the evidence limitations are open and transparent.

As image and video evidence is the most common source of information for investigation, it is too often taken for granted, and we can see a similar situation even outside of the UK.

Actually, several initiatives to create guidelines have been put in place by organizations such as the ENFSI (European Network of Forensic Science Institutes), and the US OSAC (Organization of Scientific Area Committees) and SWGDE (Scientific Working Group on Digital Evidence). We suggest to seek a cooperation with them in order to avoid overlaps.

10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

We appreciate the effort the "Committee for Justice and Home Affairs" is making to improve the use of technologies in the application of the law and we propose what follows:

1. always use the original file as a starting point for any form of DME to be used for investigations and as evidence, and keep a safe copy of it throughout the process
2. any processing done on the images should be fully documented, based on validated scientific processes, be repeatable, and reproducible
3. any data to be used as evidence should be considered for evaluation of originality and authenticity
4. personnel should be trained on the proper acquisition and analysis of DME, and be aware of the risks of an incorrect interpretation

The processing and handling of Digital Multimedia Evidence should be completed within a forensic framework, ensuring that questions of integrity and authenticity can be answered easily to negate doubt within a legal setting.

The overarching principle of this proposal is that of trust. In the current day and age, digital image and video evidence is abundant, but it's very easy to cause alteration, voluntary or accidental, to the data. I think the "Committee for Justice and Home Affairs" should strive to guarantee trust on images and videos during any legal process.

3 September 2021