IMAGES as EVIDENCE

By Glenn Porter

Technology involving image capture has significantly changed the way people engage, witness and experience the modern world. The inclusion of cameras in mobile phones and the proliferation of CCTV surveillance cameras installed in public and private spaces are key developments characterising the digital imaging revolution. The growing prominence of images as a form of communication can be seen in the exponential increase in the number of images taken each year. Determining how many photographs are taken worldwide annually has challenged researchers, and methods of calculating this figure have included estimates based on the number of Kodak™ employees during the days of film technology.[1]

According to Good,[2] in 1930 the total number of photographs taken worldwide reached the 1 billion per year mark for the first time. This milestone took a century to achieve from the time photography was conceived in 1826. By 1960, the total number of photographs taken each year had tripled to 3 billion and by 2000, around the end of the golden age of silver halide, this figure had increased to 87 billion. With the introduction of digital imaging technology, this figure had increased by 2011 to the yearly rate of 380 billion.[3] This is an extraordinary rate of increase and the incredible numbers do not end here. Digital images are now a more efficient and transient form of communication through cyberspace using email, messaging and social network sites. Facebook™ has the world's largest and most rapidly growing archive of images ever previously thought imaginable and recently reported that it holds over 140 billion photographs in its archive, with an increasing daily upload rate of more than 250 million images per day.[4]

It is not only the totality of images produced each year that is significant, but the way in which they are used. The consumption of visual media within our everyday lives has changed the way we act, think and understand the world. The legal system is not immune to this new phenomenon and images are increasingly being used as evidence in court. In most modern societies, almost everyone is now moving around carrying a camera integrated within smart phones that also allow immediate access to the internet, email and social media. Incidents can now be captured in situ and immediately published to a wider audience or sent to authorities and news bureaux. The number of CCTVs installed within the community also increases the notion of surveillance and the potential to record criminal activities.

The practice of image-making is now ubiquitous within society and is certainly having an impact on how evidence is presented and conceived within a court environment. Incriminating visual evidence is seen in several different forms and circumstances. Images have the potential to provide probative evidence; however, is this kind of 'evidence' given the same robust consideration as other types of forensic evidence and how can reliability be evaluated?

This article examines several conceptual and pragmatic concerns regarding this form of evidence, including:
- whether photographs, by definition, provide definitive and objective evidence;
- gaining identification evidence from images (CCTV);
- self-incriminating evidence from photographs;
- forensic capacity for photographic evidence; and
- methods of presenting photographs to a jury.

PHOTOGRAPHIC TRUTH: BUT WHERE IS THE EVIDENCE?

Understanding how to determine the meaning from photographs is a concept that has been argued among visual culture scholars and continues to raise concerns in the context of presenting images as evidence.[5] Within the discipline of visual culture, a concept referred to as 'photographic truth' exists around the belief that photographs inherently proffer a dependable level of certainty because the camera functions as a mechanical device that can only record what it sees in the real.[6] This idea is, however, flawed and the notion of photographic truth is a fallacy. It is a simplistic notion that does not take into consideration how visual stimuli are interpreted by the viewer and how a range of complex personal experiences and knowledge can influence or prejudice that view. In other words, the influence of the viewer may undermine the independence of the recording mechanism. However, this view and the persuasive influence of images when presented to a jury are not well understood within the justice system and the forensic sciences.

Considering the rate of increase of images taken by the community and the acute level of surveillance cameras, it is not surprising that images are now being used more frequently in court. But how they are being used is a complex question.[7] Four applications of images as evidence should be considered:
1. images used as a form of witness (for example, an item is found at a scene and a photograph is taken to show that it existed);
2. illicit images – it is an offence to take or possess this type of image (for example, child pornography);
3. images that provide evidence and are supported by a forensic examination; and
4. images presented to a jury without any forensic examination that rely on the jury to interpret and assess them for their evidential value.

>>

The transition from image to evidence is currently not well understood – certainly CCTV images are most useful when presented to suspects for the purpose of obtaining admissions.

Extensive research is needed to better inform the courts and forensic science about how images in all four categories are used within the justice system. However, the fourth application is one that is of greatest concern, illustrated widely by the inclusion of images sourced from CCTV.

There are obvious advantages for the prosecution to link an accused to a criminal event which has been captured on CCTV. Linking a suspect to the scene has always been a valuable source of evidence, and traditionally fingerprints, DNA and eyewitness accounts were used. Identification of persons of interest from images has been a challenging concept for forensic science and, despite some claims, this forensic process remains problematic.[8] CCTV footage offers a different advantage in that the criminal event may be witnessed by people viewing the footage rather than the event itself. However, unlike fingerprints and DNA evidence, identifying a person of interest from images remains inconclusive. An inappropriate solution to this lack of forensic capacity is to present the evidence in such a way that the jury may determine identity. The jury, who are usually comfortable in examining images based on their wide exposure to images and the media, may believe they have the prerequisite skills to form a view regarding a person's identity from images. However, studies have shown that people's abilities to recognise unknown people from images are prone to error.[9]

An example of this problem was witnessed recently in a poster prepared for court presentation. The visual construction comprised a large central still image of the incident captured by CCTV, with cropped enlargements of two people depicted in the CCTV footage on one side of the poster. On the other side were the arrest photographs of the accused taken by police. There was no apparent forensic evidence supporting the linking of the identity of the accused to that of the persons of interest in the CCTV image and close-ups. The use of this as a court exhibit – aiming to get the jury to associate the accused with the persons of interest depicted in the CCTV footage – is highly questionable. Requesting juries to identify suspects from photographs, when there is no supporting forensic evidence to substantiate that claim, is fraught with reliability issues. Even instructing the jury not to make identifications from

such material but only to look for similarity is problematic, and especially when the quality of the CCTV is poor.

Other forms of evidence involving imagery are also presented to jurors without any forensic verification. The recent Gittany murder trial in Sydney (2013) provided footage from a pinhole camera of a struggle moments before the death of a women from a fall.[10] Evidence relying on images should be subjected to greater scrutiny: the lack of forensic capacity should not exempt this form of evidence from proper explanation. Images presented as evidence have the power to shift the onus of proof and can carry weight and influence, even where their claims of evidence are not supported by a rigorous forensic examination. Challenging the reliability of this form of evidence becomes difficult because often there is little or no substance behind the claims, only an image/s. Visual culture scholars would argue that there is no such thing as photographic truth, and that the accuracy of images will depend on their interpretation. The questions that need to be asked are; what is the interpretation, and what is the actual evidence?

CCTV IDENTIFICATION EVIDENCE

Obtaining CCTV footage from crime scenes has become a priority during the investigation of crime, yet the development of forensic processes around this form of evidence remains limited. Imagery obtained from CCTV sources has two distinctive functions: (i) to provide intelligence to assist an investigation; and (ii) to provide evidence. These two functions provide very different outcomes and should be considered separately. CCTV footage has significant benefits for forensic intelligence practices, and can provide investigators with important information, including:
- time, date and place;
- details regarding clothing and appearance;
- the number of offenders/witnesses;
- in cases of attacks, the footage may assist forensic pathologists by determining whether the victim was punched, kicked, stomped or hit with an object. It can also provide how many blows were inflicted and by how many perpetrators;
- details of how the offence took place (that is, points of entry and exit);
- where to focus the scene examination;
- registration details from vehicles used in the commission of an offence;
- facial recognition using facial data bases; and
- data for reconstruction.

These types of intelligence are useful for investigators and may also eventually lead to evidence, but not without proper forensic examination. This transition from image to evidence is currently not well understood for evidence obtained from images. Certainly the most useful application of CCTV is when investigators present images to a suspect for the purpose of obtaining admissions. Recognising themselves depicted in the footage can be a very persuasive influence when suspects are facing allegations, especially if they knowingly committed the offence. Admissions gained from CCTV footage can

save the public a significant amount of money in terms of investigation costs and lengthy court hearings.

The most practical application of CCTV evidence links the accused to the recorded incident by means of identification from the images. However, this type of evidence remains problematic for several reasons:

- **Suitability of the CCTV source.** Factors like camera placement, lighting, frame rate, screen height, and camera angle can all affect the suitability of CCTV images for obtaining the identity of persons of interest. Most CCTV placement is considered from the perspective of security personnel monitoring crowd behaviour rather than for forensic identification. Placing cameras in a high position with a sharp angle can also produce problematic changes in shape and distortion. Some operations, however, place certain CCTV cameras in choke points with close-up views of faces using highly resolved cameras. Choke points are spaces where people move through a controlled area like escalators, lifts and ticket gates. Choke point positioning combined with high-resolution cameras generally provides the most suitable form of CCTV images for identity purposes.
- **Resolution and lens distortion.** Most CCTV cameras are designed for crowd monitoring and offer poor resolution. Poor resolution combined with low screen height produces very little facial detail for identification. The collection of the CCTV data is also affected by whether the material has been compressed using codecs. Ideally, CCTV data should be retrieved using a native (uncompressed) file and later processed by forensic experts. Many CCTV camera lenses produce lens distortion which also affects the integrity of the shape of the subject.
- **Photographic conditions.** Recording a three-dimensional subject on to a two-dimensional medium, like a photograph, can change the relationship of detail represented in the image including spacial aspects, shape, size and form. Making observations from photographs is often not the same as viewing the subject in real life. This point is often misunderstood by anatomists when they are describing facial morphology (see *Morgan v R*[11]).
- **Provenance.** CCTV evidence should ideally be collected by crime scene technicians and be subject to the same principles of evidence continuity and integrity as any other forensic evidence collected from a crime scene.
- **Concepts of identification.** Unless distinguishing features can clearly be observed from the CCTV images, identification of individuals is highly problematic. There are issues regarding general morphological descriptions of features and how these observations can be considered as discrete identifying features.

Another method of determining the identity of persons of interest depicted in CCTV footage may be the recognition by persons who know the accused from suitable CCTV images. Several papers from psychologists testing people's skills in identifying persons from images have indicated that, if the person is known to the viewer, the accuracy is relatively high. From a circumstantial evidence perspective, clothing can also provide distinctive features including checked patterned clothing and stitching orientation; rips and tears; random splashed paint from the result of clothing worn during painting; clothing with random patterns like tie-dying and acid-washing; stitching errors and patterns; and the combination of clothing outfits (shoes, pants, shirt, glasses, hat, jewellery, etc). Other data associated with the accused around the same location and time, including location of mobile phone or iPad through GPS; phone calls or text messages triangulated from the cell towers; and other CCTV footage showing car registration plates; clothing of persons of interest while withdrawing from ATMs or making petrol station purchases with a credit card, can all assist when combined with other identifying considerations.

SELF-INCRIMINATING EVIDENCE FROM PHOTOGRAPHS

The increase in image-making within contemporary society has also led to the increase in people taking images that could be self-incriminating. A recent phenomenon witnessed with cameras installed in mobile phone devices is the change from taking images of the world looking outwards, to turning the camera on to ourselves and taking a self-photograph, or what is known as a 'selfie'.

The value of self-incriminating images is linking the image via the device (for example, a mobile phone or computer) to the incident by supporting information sourced from the metadata. Images taken from digital cameras often have >>

> Most CCTV camera placement is considered from the perspective of security personnel monitoring crowd behaviour rather than for forensic identification, and offers poor resolution, which produces very little facial detail for identification.

information pertaining to that image embedded into the digital file. The metadata could provide useful corroborative evidence including date, time, place using GPS co-ordinates and details of the device. Images posted on social network sites and/or stored on mobile phone devices are certainly an area that investigators can search for incriminating image-based evidence. 'Trophy photographs' taken by the perpetrator or by accomplices to the criminal activity can also be a source of incriminating evidence.

In child exploitation cases, the metadata information can prove highly valuable. Establishing the location where the images were taken could provide information to investigators and the date could assist in determining the age of the victim at the time the offence took place. Sophisticated child exploitation networks would eradicate any incriminating metadata, but less sophisticated operators may not be aware of this type of evidence.

On occasions, accidental self-incriminating evidence may be present within the pictorial elements of the image. This type of evidence may involve information sourced in the background or details that could lead to the identity of the offender. An example of this type of evidence was recently witnessed in a child exploitation case where a relative of the victims was identified by the photographs he took while he assaulting the young victims with his fingers. During a forensic examination of images sourced from a seized computer, several close-up images showed the ridge detail of the offender's fingertips. These highly resolved images of the fingerprint matched the accused and a guilty plea was quickly obtained as a result of these self-incriminating images. This evidence was not discovered, however, until a robust forensic triage of the images was conducted by imaging experts. The analysis of images by forensic experts is not well understood or properly supported by agencies. The often misconceived notion is that images speak for themselves.

Another type of self-incriminating image has occurred in recent insurance claim cases. When the insured is requested by the insurer to provide evidence that the claim

items actually existed by way of receipts or photographs, images are taken by the insured using their phone device and emailed to the insurer. In recent cases, the metadata in the digital image file has indicated that the photographs were taken after the time of the alleged incident, generating discrepancies in the insured's claim. The GPS data may also indicate where items are kept.

CONCLUSION

Technological advancements in digital imaging technology, the inclusion of cameras in mobile phones, the ease of transmitting images across digital media platforms, and the proliferation of CCTV surveillance cameras have all resulted in a significant increase in our capacity to produce images. This has led to redefining communication practices within contemporary society, which in turn has had a considerable impact on the justice system. There are fundamental gaps in our current understanding of how images, when used as evidence, can affect and influence decision-makers; be inappropriately used as a way to infer evidence rather than be validated by forensic concepts; and be supported by useful and accurate descriptions or analysis.

Images can, however, provide worthwhile intelligence during an investigation: certain details of events; simplistic documentation; self-incriminating evidence and tools for investigators to gain admissions or guilty pleas. Images when used as evidence should be properly scrutinised for reliability of the actual evidence, and should not be admissible unless appropriate forensic evaluations have occurred. Images as evidence should always assist the proceedings by providing an accurate representation of the facts without relying on inferences from the jury. ∎

Notes: 1 J Good, (2011) 'How Many Photographs Have Been Taken?' from Ancestory.com, http://blog.1000memories.com/94-number-of-photos-ever-taken-digital-and-analog-in **2** *Ibid.* **3** *Ibid.* **4** Facebook (2012), *Newsroom: Photos and Video*, http://newsroom.fb.com/content/default.aspx?NewsAreaId=21. **5** G Porter, (2007), 'Visual Culture in Forensic Science', *Australian Journal of Forensic Sciences*, 39:2, pp81-91. **6** G Porter, M Kennedy, (2012), 'Photographic Truth & Evidence', *Australian Journal of Forensic Sciences*, 44:2, pp183-92. **7** G Porter, (2011), 'A New Theoretical Framework Regarding the Application and Reliability of Photographic Evidence', *International Journal of Evidence & Proof*, 15:1, pp26-61. **8** G Edmond et al, (2009), 'Laws Looking Glass: Expert Identification Evidence Derived from Photographic and Video Images', *Current Issues in Criminal Justice*, 20:3, pp337-77. **9** *Ibid.* **10** A Dale, (2013), 'I Saw Her Die', *The Daily Telegraph*, November 6, p7. **11** *Morgan v R* [2011] NSWCCA 257.

Dr Glenn Porter *is the academic course adviser (Forensic Science), University of Western Sydney (UWS), School of Science and Health. As a forensic photographer, he previously worked for the Australian Federal Police. He is chief investigator for the new Photographic Evidence Research Laboratory (PERL) at UWS and regularly gives presentations on images as evidence, in addition to carrying a casework load as an imaging expert.* **EMAIL** *g.porter@usw.edu.au.*