Digital Photos and Confessions

"[O]ur society is going digital. Like it or not, we're becoming a digital culture." [1]

The digital revolution has had a huge impact on law enforcement. Digital technology now controls police dispatching, 911 systems, and radio communications. It is also used to create, store, and access rap sheets, crime reports, fingerprint records, booking photos, composite drawings, and DNA data.[2]

More recently, law enforcement agencies have been converting to digital recorders for taking statements from suspects and witnesses, and to digital cameras for taking pictures of crime scenes and other things. As noted in an FBI publication, "More and more agencies are choosing digital capture systems to eliminate the need for film-based imaging systems. The potential for budgetary savings and the ability to deliver images faster continue to drive more law enforcement agencies toward a conversion to digital imaging."[3]

Another advantage to digital is the quality. Discussing digital photos, one court noted, "The advantage of digital photographs, rather than analogue film photographs is that digital photography can capture approximately 16 million different colors and can differentiate between 256 shades of gray. Digital photographs work with light sensitivity, just like film photographs, except the computer uses a chip and a hard drive in place of the camera's film."[4]

Because digital cameras and recorders are used specifically to obtain evidence that can be presented in court, some officers and prosecutors have asked whether they can expect problems when they seek to have digital photos and statements admitted into evidence. The question is especially pertinent because more and more people are walking around with cell phones that can shoot, store, and transmit digital photos and even videos.[5] It is inevitable that some of these people will be taking pictures of crimes in

---

[1] John Paul Walter, *Going Digital,* Presentation to St. Louis University (2003). NOTE: The University of California reports that 93% of all information generated in 1999 was generated in digital form. Source: Kenneth J. Withers, *Electronic Discovery: The Challenges and Opportunities of Electronic Evidence,* Address at the National Workshop for Magistrate Judges (July 2001).

[2] DEFINED: "A digital system uses numbers to represent a concrete object or an abstract idea. Digitization is the process of transforming the object or idea into a numerical code. The baseline of digital technology is a coding system with only two numbers—1 and 0 . . . " *Digital Technology Made Simpler*, Paul Conway, Head, Preservation Department, Yale University Library (2002).

[3] FBI, *Forensic Science Communications* (2000) Vol. 2 Number 4, "Legal Ramifications of Digital Imaging in Law Enforcement" by Erik C. Berg, Forensic Services Supervisor, Tacoma Police Department.

[4] *Washington* v. *Hayden* (1998) 950 P.2d 1024, 1028. NOTE: While these statistics are impressive, the process has improved greatly since 1998. ALSO SEE *U.S.* v. *Capanelli* (2003) 257 F.Supp.2d 678, 679 ["In this case, the voice recordings were made using a digital recording device which enables law enforcement agents to record several hours of conversations on memory chips, thereby vastly expanding the recording capability over the 'body of wires' of yesteryear. The chips can hold and store the recordings. The contents can subsequently, by use of computer software designed for the purpose, be transformed into CDs or audio tapes."]; *Wall Street Journal* (April 22, 2004) p. A6 ["Kodak's Net Soars As Its Focus Shifts To Digital Lines."].

[5] "Camera phones are cropping up everywhere . . . . Sales of the camera-equipped mobile phones rose fivefold last year to 84 million, surpassing even sales of digital cameras for the first time." *Wall Street Journal* (April 29, 2004).

progress, perpetrators, and other things that will be of interest to officers, prosecutors, judges, and especially jurors.

In light of the importance of this issue and the widespread use of digital technology, one might expect to find lots of cases in which the admissibility of digital evidence has been challenged in court. Actually, there are very few. This might seem odd at first but, as we will explain, it makes sense when you consider that digital technology had proven itself reliable long before prosecutors ever attempted to use it in court.

Digital reliability

If digital technology were deemed a "new scientific technique," neither digital photos nor statements could be admitted into evidence unless prosecutors could prove the technology had acquired "general acceptance by the scientific community."[6] This would be a costly and time-consuming proceeding.

But digital technology is not "new." More to the point, it would be a gross understatement to say it has been "accepted" by the scientific community. The scientific community is utterly dependent on it. And so do judges and lawyers, although admittedly to a lesser extent.

Consider this: If a defense attorney were to file a motion to suppress a digital photo or confession on grounds the technology was "new," "unproven," or "unreliable," he would probably have typed his motion on his reliable digital computer, and would have printed out a perfect hard copy on his dependable digital printer. It is also likely that the judge who would hear the motion would probably research the issue by logging on to a digital legal resource service such as WestLaw or Lexis, and that the judge probably relies on digital technology to send and receive e-mail, record and access voicemail, watch movies, surf the internet, and pay bills.

Worse yet (from the attorney's perspective) virtually everyone knows that digital technology is the backbone of highly complex and critically important operations including NASA space flights, global positioning satellites, air traffic control, military defense systems, cell phone networks, and even some complex micro surgery. For these reasons, defense attorneys will seldom launch a serious attack on the reliability of digital technology.

There is, however, a legitimate legal issue that prosecutors must contend with. It is known as "authentication."

Authentication

Digital photographs and recordings are classified as "writings" in the Evidence Code which means they must be "authenticated" before they can be admitted into evidence.[7] This simply means that prosecutors must present "sufficient" evidence that the photo or recording is an accurate reproduction of what was photographed or recorded.[8]

---

[6] See *People* v. *Kelly* (1976) 17 Cal.3d 24; *People* v. *Leahy* (1994) 8 Cal.4th 587, 604; *People* v. *Pizarro* (2003) 110 Cal.App.4th 530, 541, fn.4.

[7] See Evidence Code § 250 [recorded statements and photographs are "writings"]; Evidence Code § 1401(a) ["Authentication of a writing is required before it may be received in evidence."]; *People* v. *Mayfield* (1997) 14 Cal.4th 668, 747 ["To be admissible in evidence, an audio or video recording must be authenticated."]; *O'Laskey* v. *Sortino* (1990) 224 Cal.App.3d 241, 249 ["(A) tape recording is a 'writing' and must therefore be authenticated before it can be received into evidence."].

[8] See Evidence Code § 1400 ["Authentication of a writing means (a) the introduction of evidence sufficient to sustain a finding that it is the writing that the proponent of the evidence claims it is or (b) the establishment of such facts by any other means provided by law."]; Federal Rules of Evidence, rule 901(a) ["The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in

In most cases, this is not a contested issue. Sometimes, however, defense attorneys will fight the introduction of digital evidence, claiming it might have been altered. Although this could be a legitimate issue, it is usually just a desperation ploy. In any event, prosecutors must deal with it.

It is, of course, widely known that digital photos can be modified electronically without leaving any tell-tale signs. This was graphically demonstrated at a meeting of the Federal Computer Investigations Committee in which federal agents and prosecutors were shown a digital photo of a dead body on the floor of a room. The photo showed a bloody chest wound and a handgun on the floor across the room. On the wall above the victim's body, the following words were scrawled in blood (presumably the victim's): *I'll kill again. You'll never catch me.*

After everyone had studied the photo, an agent went to work on it. Using commercially available software, he started rearranging its digital structure. When he was done, he had, (1) removed the killer's words from the wall, (2) closed the chest wound and cleaned up the blood, (3) put a small hole in the victim's temple, (4) added a tickle of blood at the hole, and (5) put the gun in the victim's hand. The photo now "proved" the victim had committed suicide.

This was pretty dramatic. But don't forget that many, maybe most, types of evidence can be altered. Film-based photos can be altered,[9] statements can be edited, documents can be scanned and modified.

Consequently, the defense cannot keep a digital photo or statement from the jury by merely claiming there was a *possibility* it might have been modified. Instead, it must prove it was, in fact, altered or was otherwise inaccurate.[10] And it cannot meet this burden by merely proving there was a possibility of alteration.[11] As the United States Court of Appeals observed, "The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility."[12]

---

question is what its proponent claims."]; *U.S.* v. *Pang* (9th Cir. 2004) __ F.3d __ ["The authentication requirement is satisfied by "evidence sufficient to support a finding that the matter in question is what its proponent claims."].

[9] See Lederer, *Some Thoughts on the Evidentiary Aspects of Technologically Presented or Produced Evidence* (1999) 28 Southwest University L.Rev. 402-3 ["Yet what of a traditional photograph? Are the two image technologies really so very different? Photographs *can* be altered."]; *Kennedy* v. *Florida* (2003) 853 So.2d 571, 573 [discussing digitally enhanced photos of bloody shoe prints and fingerprints the court noted, "Certainly the enhancement of otherwise available evidence is not an innovative scientific theory."].

[10] Evidence Code § 1553 ["A printed representation of images stored on a video or digital medium is presumed to be an accurate representation of the images it purports to represent."].

[11] See Overly, *Electronic Evidence in California* (1999) p. 9-4; United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002) ["The courts have responded with considerable skepticism to such unsupported claims that computer records have been altered. Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record." Citing *U.S.* v. *Whitaker* (7th Cir. 1997) 127 F.3d 595, 602 [allegation of tampering was "almost wild-eyed speculation"]; *U.S.* v. *Bonallo* (9th Cir. 1988) 858 F.2d 1427, 1436 ["The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."]; *U.S.* v. *Glasser* (11th Cir. 1985) 773 F.2d 1553, 1559 ["air-tight security system" to prevent tampering "is not, however, a prerequisite to the admissibility of computer printouts."]; *U.S.* v. *Allen* (6th Cir. 1997) 106 F.3d 695, 700 ["Merely raising the possibility of tampering is insufficient to render evidence inadmissible."].

[12] *U.S.* v. *Bonallo* (9th Cir. 1988) 858 F.2d 1427, 1436. ALSO SEE *U.S.* v. *Tropeano* (2nd Cir. 2001) 252 F.3d 653, 661 ["Authentication of course merely renders the tapes admissible, leaving the

DIGITAL PHOTOS: To authenticate a digital photo, prosecutors must present some evidence that it is an accurate reproduction of that which was photographed.[13] This is ordinarily accomplished by presenting eyewitness testimony that the picture accurately depicts the scene in question.[14] In most criminal cases, the witness will be the officer or technician who took the photo or someone who saw it taken. The witness will then testify that he later examined the photo and determined that it accurately depicted the scene, person, or thing that was photographed. As the Washington Court of Appeals explained:

> To authenticate the photograph of a crime or accident scene, for example, a proponent can call a witness (a) who has personal knowledge of the scene the

---

issue of their ultimate reliability to the jury."]; *U.S.* v. *Salgado* (6th Cir. 2001) 250 F.3d 438, 453 ["The government is not required to present expert testimony as to the mechanical accuracy of the computer where it presented evidence that the computer was sufficiently accurate that the company relied upon it in conducting its business."]. NOTE: If necessary, an expert may be able to give an opinion that the data had not been altered. See *U.S.* v. *Rearden* (9th Cir. 2003) 349 F.3d 608, 613 ["(Video effects expert) testified that in his opinion, the images transmitted by Rearden had not been manipulated in any manner. He indicated that they had not been composited (which involves the altering of images by, for example, transferring the head of one person to the body of another) or morphed (which in Jones's view involves the creation of an intermediate image from two other images)."].

[13] See Evidence Code § 1400; *Jones* v. *Los Angeles* (1993) 20 Cal.App.4th 436, 440, fn.5 [authentication of videotape is sufficient "if the proponent makes a showing the videotape is an accurate portrayal of what it purports to be."]; 2 Witkin, *California Evidence* (4th Edition) p. 25 ["To authenticate a photograph, a foundation must be laid by showing that the picture is a faithful representation of the objects or person depicted."]. NOTE: "The standard for authenticating computer records is the same for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. United States Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2002). Citations omitted. ALSO SEE *Almond* v. *Georgia* (2001) 553 SE2d 803, 805 ["We are aware of no authority, and appellant cites none, for the proposition that the procedure for admitting pictures should be any different when they were taken by a digital camera."].

[14] See Evidence Code § 1413 ["A writing may be authenticated by anyone who saw the writing made or executed"]; Federal Rules of Evidence, rule 901(b)(1) [authentication may be made by means of "[t]estimony of witness with knowledge. Testimony that a matter is what it is claimed to be."]; *U.S.* v. *Patterson* (4th Cir. 2002) 277 F.3d 709, 713 ["The necessary foundation for the introduction of a photograph is most commonly established through eyewitness testimony that the picture accurately depicts the scene in question . . . "]; Witkin, *California Evidence* (4th Edition) p. 25 ["The showing must be made by a competent witness who can testify to personal knowledge of the correctness of the representation."]; *U.S.* v. *Rembert* (D.C. Cir. 1988) 863 F.2d 1023, 1026 [insufficient foundation because the witness did not testify "as to the type of camera used, its general reliability, the quality of its product, the purpose of its employment, the process by which it is focused, or the general reliability of the entire system."]; *People* v. *Gibson* (2001) 90 Cal.App.4th 371, 383 ["The law is clear that the various means of authentication as set forth in Evidence Code sections 1410-1421 are not exclusive. Circumstantial evidence, content and location are all valid means of authentication."]; *U.S.* v. *Pang* (9th Cir. 2004) __ F.3d __ ["The proponent need not establish a proper foundation through personal knowledge; a proper foundation can rest on any manner permitted by Federal Rule of Evidence 901(b) or 902. Rule 901 allows the district court to admit evidence 'if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.'"]. NOTES: The foundation for admitting videotapes and films is the same as the foundation for admitting photos. See *Jones* v. *Los Angeles* (1993) 20 Cal.App.4th 436, 440, fn.5. The foundation may also be provided by "expert testimony that the picture was generated by a reliable imaging process." See *U.S.* v. *Patterson* (4th Cir. 2002) 277 F.3d 709, 713.

photo depicts, (b) who has compared the photo to that scene, and (c) who states that the photo accurately portrays the scene.[15]

Photos may also be authenticated by means of circumstantial evidence, such as establishing a chain of custody from the taking of the photo to its arrival in court. This is especially useful when there were no eyewitnesses; e.g., photo of burglary was taken automatically. For example, in *Page* v. *Texas*[16] the defendant robbed a grocery store in which a digital recording system had been installed. At the defendant's trial, a digital video recording of the defendant robbing the store was authenticated by a loss prevention investigator who was not present when the robbery occurred. The investigator testified he arrived at the store shortly after the police did, that he immediately replayed the recording of the robbery for the officers, and that he "produced a still photograph of [the defendant] from the digital recording system and copied the recording of the robbery onto a videotape." He then gave the still photo and videotape to the officers. In ruling the recording was sufficiently authenticated, the court said:

> [The store's investigator] testified that the grocery store's "brand new digital recording system" recorded images from 16 video cameras and automatically saved those images onto a computer hard drive. [He] further testified that he accessed the digital recording system's hard drive shortly after the robbery and reviewed the recording of the robbery with police officers.

DIGITAL RECORDINGS: The requirements for authenticating digital confessions and other sound recordings are the same as those for authenticating taped recordings. Specifically, prosecutors must prove, (1) the identity of the person whose voice is heard on the tape; and (2) that the recording accurately reproduced what the person said.[17] As noted in Witkin's *California Evidence*, "Authenticity of the recording may be established by a person who listened to the oral statements and can testify that the recording is an accurate reflection of them."[18] These requirements must also be met before a transcript of the statement will be admitted.[19]

The most common method of authenticating a recording of a defendant's statement is to call an officer who was present when the statement was made.[20] The officer will

---

[15] *Washington* v. *Jackson* (2002) 54 P.2d 739, 741.

[16] (2003) 125 S.W.3d 640.

[17] See *People* v. *Mayfield* (1997) 14 Cal.4th 668, 747 ["A video recording is authenticated by testimony or other evidence that it accurately depicts what it purports to show."]; *People* v. *Fonville* (1973) 35 Cal.App.3d 693, 708 ["Undoubtedly the usual way of laying a foundation for the playing of a recording is to call one of the participants or a monitor to testify that the conversation was accurately recorded."]; *Washington* v. *Jackson* (2002) 54 P.3d 739, 741-2 ["Just as a proponent can authenticate a photo by 'eyewitness comparison,' a proponent can authenticate a tape recording by 'earwitness comparison'"]; *U.S.* v. *McMillan* (8th Cir. 1974) 508 F.2d 101, 105 ["The standard for the admissibility of an opinion as to the identity of a speaker is merely that the identifier has heard the voice of the alleged speaker at any time." Citations omitted.]; *U.S.* v. *Wells* (8th Cir. 2004) 347 F.3d 280, 288 ["One of the requirements is that the speakers be identified."]. COMPARE *O'Laskey* v. *Sortino* (1990) 224 Cal.App.3d 241, 249 ["There is no way to know whether the tape is what O'Laskey claims it is. No declaration or other sworn testimony of the investigator was offered to describe when, where, how or by whom the tape was made."].

[18] 2 Witkin, *California Evidence* (4th Edition) p. 142.

[19] See *People* v. *Ketchel* (1963) 59 Cal.2d 503, 518 ["(A)s a foundation for its admission, the accuracy of the transcript of a tape recording must first be established."].

[20] See Evidence Code § 1413 ["A writing may be authenticated by anyone who saw the writing made or executed"]; 2 Witkin, *California Evidence* (4th Edition) p. 25 ["The showing must be made by a competent witness who can testify to personal knowledge of the correctness of the representation."]; *U.S.* v. *McMillan* (8th Cir. 1974) 508 F.2d 101, 104-5.

then, (1) identify the defendant in court as the person whose voice is heard on the recording, and (2) testify that he listened to the recording soon after it was made and determined that it accurately recorded what the defendant said.[21] A good example of this is found in *People* v. *Spencer*:[22]

> DA: Was a recording made of the conversation?
> Officer: Yes.
> DA: You have since had an opportunity to hear that recording of that conversation?
> Officer: I have.
> DA: And you heard the recording of that conversation at a time when your own impression of the conversation was fresh in your mind; is that correct, sir?
> Officer: Yes, sir.
> DA: Did the recording fairly and accurately set forth the conversation between you officers and this defendant in its entirety?
> Officer: It did.

A recording may also be authenticated by circumstantial evidence. For example, it may be reasonable to infer that one of the voices on the recording was that of the defendant because he spoke of matters that were "unlikely to have been known by anyone other than [the defendant]."[23]

Like digital photos, digital statements can be altered electronically. But, as noted in the discussion of digital photos, the mere possibility of alteration is not sufficient to prevent admission. For example, when this issue was raised in *U.S.* v. *Tropeano*, the court responded:

> Authentication of course merely renders the tapes admissible, leaving the issue of their ultimate reliability to the jury. [The defense] was free to challenge the tapes' reliability by, for example, cross-examination of the brokers concerning their familiarity with [the defendant's] voice and the tape recording system. Any doubts raised by such a challenge would, however, go to the weight to be given the tapes by the jury, not to their admissibility.[24]

---

[21] See 2 Witkin, *California Evidence* (4th Edition) p. 142 ["Authenticity of the recording may be established by a person who listened to the oral statements and can testify that the recording is an accurate reflection of them."]; *Washington* v. *Jackson* (2002) 54 P.3d 739, 741 ["If the tape records human voices, the foundational witness (or someone else with the requisite knowledge) usually must identify those voices."]; Federal Rules of Evidence, rule 901(b)(5) [authentication of a voice recording may be made as follows: "Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker."]; *People* v. *Fonville* (1973) 35 Cal.App.3d 693, 708 ["Undoubtedly the usual way of laying a foundation for the playing of a recording is to call one of the participants or a monitor to testify that the conversation was accurately recorded."]. NOTE: A recording may also be authenticated "by evidence that [it] refers to or states matters that are unlikely to be known to anyone other than the person who is claimed by the proponent of the evidence to be the [speaker]." Evidence Code § 1421.

[22] (1963) 60 Cal.2d 64, 77-8, fn.5. Edited. ALSO SEE *People* v. *Williams* (1997) 16 Cal.4th 635, 662 ["The prosecution laid the foundation for admission of the tape recording when Detective Crews testified that the tape was a record of his conversation with defendant."]; *People* v. *Fonville* (1973) 35 Cal.App.3d 693, 709; *U.S.* v. *Wells* (8th Cir. 2004) 347 F.3d 280, 288; *North Carolina* v. *Rourke* (2001) 548 S.E.2d 188, 191 [911 tape authenticated by 911 employee who testified "that the tape was an exact copy of the digital telephone recording made the night of the incident. He had listened both to the original and to the copy, and testified that they were identical. He identified the voices of 911 emergency center employees on the tape."].

[23] See *People* v. *Fonville* (1973) 35 Cal.App.3d 693, 708-9..

[24] (2nd Cir. 2001) 252 F.3d 653, 661. ALSO SEE *U.S.* v. *Sovie* (2nd Cir. 1997) 122 F.3d 122, 127-8; *U.S.* v. *Capanelli* (2003) 257 F.Supp.2d 678, 680.

Still, officers should take steps to maintain the integrity of digital statements. This can be accomplished in several ways. For example, a department might establish a police that all officers who have taken a digital statement must promptly save it to the hard drive of a departmental computer that is used solely for this purpose. Although the computer might be accessible to all officers in the department who take statements, it could be set up so that no one could access or save a statement-file without a pass code. That way, when it becomes necessary to provide a copy of the statement to a court or defense attorney, officers could testify they reproduced it directly from a protected copy that was made shortly after the statement was taken.[25]

Secondary evidence rule

In the past, the so-called "Best Evidence Rule" governed the admissibility of photos and recordings in California. This meant that, subject to several exceptions, only the original photograph or recording could be admitted. This would create problems with digital photos and statements because the "original" is technically nothing more than a series of electrical impulses.[26]

In any event, the legislature resolved this issue in 1999 when it replaced the Best Evidence Rule with the Secondary Evidence Rule in which a copy of a photograph or recording is admissible unless the court determines there is a genuine dispute as to its accuracy.[27] Furthermore, as noted, there is a presumption that digital photos are accurate and, by logical extension, so are digital statements.[28]

---

[25] NOTE: Another way to protect digital data from alteration is by means of a so-called digital "watermark." A good explanation of this technology can be found at www.surety.com.

[26] NOTE: The legislature confronted this problem as it relates to digital photos "stored in a computer or similar device" by enacting Evidence Code § 255 which provides that the "original" includes "any printout or other output readable by sight, shown to reflect the data accurately."

[27] Evidence Code § 1521(a)(1). ALSO SEE Evidence Code § 255 ["If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'"].

[28] Evidence Code § 1553; *People* v. *Hawkins* (2002) 98 Cal.App.4th 1428, 1450. ALSO SEE Civil Code § 1633.13 [Uniform Electronic Transactions Act: "In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form."].