

Digital Photography as Legal Evidence

Contents:

Part I: Introduction

Part II: The Nature of Digital Photography

- Section 1: How Computers Store Information
- Section 2: How a Digital Photograph is Captured
- Section 3: How a Digital Image May Be Altered
- Section 4: Why Digital is Different From Analog

Part III: Existing Approaches to Photographic and Computer Evidence

- Section 1: Photographs as Evidence
- Section 2: Computer Data as Evidence
- Section 3: Can Existing Doctrine Be Applied to Digital Photographs?

Part IV: Responding to the Problem of Digital Photography

Part V: Conclusion

Notes

Digital Photography as Legal Evidence: You Won't Believe Your Eyes!

It is common knowledge that as to such matters, either through want of skill on the part of the artist, or inadequate instruments or materials, or through intentional and skillful manipulation, a photograph may not only be inaccurate but dangerously misleading.

Cunningham v. Fair Haven & Westville R. Co. (1899) (1)

The future is not some harebrained scheme of the digital Information Highway or something. It's a step-by-step progression of enhancing photography using digital technology.

George Fisher (Chairman, Eastman Kodak Co.) (2)

Part I: Introduction

The art of photography, although still quite young, (3) is entering a period of radical transition. Computer technology now allows photographers to capture, store, and display digital images without the use of film or paper. (4) With this capability comes a great deal of opportunity, and some foreseeable risk -- at any point in this process, the image may be degraded or altered, intentionally or accidentally. (5) Although the integrity of visual evidence has always been open to question, as noted by the court in Cunningham, (6) statutory and common law evidence doctrines developed in response to the problem, and photographs are now routinely admitted into evidence in both criminal and civil trials. (7) Digital photography, however, is fundamentally different from conventional photography. (8) It seems appropriate, as digital imaging becomes more common and more affordable, to ask whether existing safeguards in the rules of evidence are well suited to verify the integrity of visual evidence captured and stored in digital form.

Any discussion of digital photography must begin with some understanding of the technical

issues raised. Part II of this Note comprises an abbreviated overview of how digital images are captured, stored, and manipulateded. It goes on to argue that the unique quality of digital photography results from its hybrid nature -- part photograph, part computer data. Each of these fields has generated a body of evidence doctrine independently, and so Part III will provide a brief review of those doctrines as they exist presently. It will be argued that neither doctrine is entirely adequate to address the foreseeable danger of negligent or fraudulent misuse of inaccurate images. Part IV offers suggestions to assure the integrity of visual evidence presented in court.

A few terms must be defined at the outset. Digital photographs, as the phrase will be used here, are visual records captured and stored in a digital form without the use of film or paper; the term is meant to suggest a contrast with conventional photographs (i.e., those created by means of chemical film). (9) Digital images are any visual data stored in a format which may be used by a digital computer; all digital photographs are digital images, but so are conventional photographs "scanned" into a computer, as well as other visual records such as X-rays, sonograms, infrared images, etc. (10) Finally, visual evidence describes images offered in court as real (not demonstrative) evidence that a particular scene or image once existed materially as portrayed. Visual evidence may include still or live action records, in either digital or conventional form. (11)

Part II: The Nature of Digital Photography

Digital photographs exist only as digital data. (12) Unlike conventional photographs, no film or paper are employed in their capture or storage. (13) Although they may ultimately be displayed in a printed form, it is not necessary to do so -- they can just as easily be displayed on a monitor screen (14) --or, there need never be an analog representation (15) of the scene or image.

Section 1: How Computers Store Information

A digital computer is essentially nothing more than a collection of switches. (16) It is thus limited to expressing one of two logical states -- on or off, true or false -- with each switch. A modern computer derives its power from the ability to open or close each switch in a tiny fraction of a second, and from the ability to open or close one switch in response to the position of another switch. These characteristics provide the computer with the features that make it most useful: speed and programmability.

The computer stores and processes information in the form of numbers. Those numbers are expressed in binary notation, (17) because a binary digit (or bit) includes only a one or a zero. It is thus an easy matter to assign "one" to describe the state of a closed switch and "zero" to an open switch. Unless a piece of information can be reduced to a numerical expression (that is, digitized), it may not be stored or processed by a computer. (18)

Ingenious methods have been devised to digitize information that one might not think of as numeric by nature. For instance, the English alphabet has been translated into a standard code known as ASCII. (19) Each letter, upper case and lower case, as well as each punctuation mark, each numeral, and some common characters (such as carriage returns and line feeds) is converted into a number between 1 and 256. Any member of the ASCII set may be expressed in a number no longer than eight bits (or one byte). (20) Much more sophisticated techniques must be employed in the digitizing of complex information, such as sound recorded on a digital compact disk. (21)

When not actively processing information, a computer may store it for future use in one of two ways: (22) the information may be stored for short periods of time in random access memory (RAM), or it may be stored indefinitely on a magnetic or optical digital medium (such as a floppy disk or CD-ROM). (23) Regardless of the physical location of the information, however, it remains nothing more than a collection of numbers. (24)

One characteristic feature of digital information, not shared by analog media such as

photography, (25) is that it may be reproduced at will without becoming degraded. (26) For instance, a photocopy of a document is of noticeably lower quality than the original, and a photocopy of the photocopy is worse still. In contrast, if the document existed in digital form, it could be copied freely. Each copy would be indistinguishable from the original, as would each copy of a copy. (27) Furthermore, if the original document is altered in any way -- for instance, the author of the document performs some editing and replaces the original file with the edited file -- the previously made copies remain, absolutely faithful to an original that no longer exists.

Section 2: How a Digital Image is Captured

Just as information such as text or sound can be digitized, so can visual data. A scene or image may be mapped to a grid, and each discrete cell assigned a numerical value defining the average shade and intensity of color of the area contained within the cell (or pixel). (28) Greater visual detail may be rendered in two ways: the scene or image may be mapped to an extremely fine grid, resulting in high spatial resolution; (29) or each pixel may represent a relatively large amount of digital information, resulting in a reproduction having superior tonal resolution, or color depth. (30) The price paid for such detail is in the sheer volume of the information required to express it. (31)

A digital image may be created by "scanning" a photograph or other analog image into a computer programmed to digitize the image, (32) or it may be captured with a digital camera. A digital camera might look very much like a conventional camera, (33) but the method by which the scene or image is recorded is fundamentally different. A sensing apparatus within the camera corresponds to the pixel grid of the desired image, and calculates the numeric value assigned to each pixel. (34) The digital information can then be recorded directly, with no need to create an analog representation of the image.

The genesis of digital imaging technology is difficult to date with precision. Some authorities set the date at 1957, (35) others as much as ten years later (36) or thirty years earlier (37) -- depending on what point in the evolution of digital imaging is seen as defining the "beginning." In any event, it is probably fair to say that digital photography as discussed here dates back to 1981, when Sony released the Mavica, "the first consumer level electronic camera that used a solid state chip instead of film to record images." (38) It was at this point that anyone, using commercially available tools, suddenly developed the ability to create a photographic image without first creating a traditional, "original" negative or print. Today, digital cameras capable of capturing a reasonably high quality image are available for under \$1000, (39) and models producing professional quality output may be had (albeit for substantially more money). (40) These prices are sure to plummet in the near future, however, as manufacturers (most notably, Eastman Kodak) anticipate bringing digital cameras to the market for only a few hundred dollars in the next several years. (41)

Section 3: How a Digital Image May Be Altered

Ten years ago, an article in the magazine *Whole Earth Review* predicted "the end of photography as evidence of anything." (42) More recently, a student Note in *Rutgers Computer & Technology Law Journal* declared that "a picture is worth a thousand lies." (43) These comments are prompted by yet another characteristic feature of digital data -- the ease with which they may be altered or manipulated. Indeed, many photographers make use of digital imaging technology specifically because the image is manipulable; examples include NASA scientists enhancing images transmitted from satellites, (44) or a commercial photographer removing unwanted elements from an advertisement. (45)

Because digital data consists of only numbers, information may readily be added, removed, or replaced. (46) Any such corruption of the original data is likely to occur in one of three contexts: it may be accidental, it may be intentional but innocent, or it may be fraudulent. Accidental alteration might result from a variety of causes -- for example, a magnetic disk on which data is

stored might be placed too near a powerful magnetic field (such as that generated by some computer monitors). (47) The effects of accidental alteration are likely to be catastrophic, and it is difficult to imagine what evidentiary problems could follow beyond those commonly raised by destroyed documents.

Intentionally manipulated images, however, are another matter. There are a number of commercially available software packages (48) which allow the user to remove elements from an image, rearrange the elements of an image, or add elements to an image. (49) Even subtle details such as color, (50) contrast, (51) light, (52) and shadow (53) may be adjusted. A photographer or editor might want to manipulate an image for an innocent reason; National Geographic magazine, for instance, created a controversy by moving Egyptian pyramids closer together in a photograph so that the scene would look aesthetically pleasing on the magazine cover. (54) Few evidentiary problems are raised by intentionally manipulated images, so long as a witness is available and willing to testify that the scene has been edited. (55) If, however, someone were to intentionally manipulate an image for fraudulent purposes, the same tools used by the conscientious photographer may be applied to the task of perpetrating that fraud -- and there is no easy method of detection. (56)

Section 4: Why Digital Is Different From Analog

Of course, the possibility of misrepresentation by visual image is not unique to digital photographs. As noted in the introduction, suspicion of photography did not develop in this century. From simple techniques such as choice of film, lighting, exposure interval, lens -- or more simply, posing or staging (57) -- to sophisticated darkroom editing and collage procedures, (58) photographers have had opportunities to manipulate images virtually since the camera was invented. Even a photograph that was not intended to be misleading may in fact be misleading. (59) Courts have (on occasion) identified the danger, and rejected photographic evidence on the basis that it could not be proved to portray what its proponent claimed. (60) Still, relevant photographs are rarely excluded. (61) It also remains true that, as a society, we continue to grant a strong presumption that a photograph is solid evidence that a particular scene or image once existed materially as portrayed. (62)

In this manner, photography is quite different from previously known, subjective visual arts such as drawing or painting. "If a painting represents a subject, it does not follow that the subject exists nor, if it does exist, that the painting represents the subject as it is." (63) On the other hand, "[a] photograph is a photograph of something In other words, if a photograph is a photograph of a subject, it follows that the subject exists" (64) At some level, a photograph has to at least begin with an image which was nothing more than a reflection, a record of light mirroring the subject, and physically reacting to film in predictable ways. There is always an original. (65)

Digital images may be as detailed as conventional analog photographs, and if printed on photographic paper, may be indistinguishable from conventional photographs to an observer. (66) More importantly, however, digital images resemble conventional photographs in that they are internally consistent. (67) If a photograph shows three automobiles, for example, and the highlights on the surfaces of two automobiles are consistent with the sun being to the left of the scene, but the highlights on the third vehicle indicate that the sun is to the right of the scene, the picture will not "look right." It may require some study (if the alteration is particularly subtle), but eventually the eye will discern the inconsistency. The fraud will become evident.

Of course, a very skillful fraud might never be detected. If there was no obvious need for anyone to examine a particular photograph closely enough, the photograph would likely be presumed accurate. There is an evident risk in making this presumption about any photograph, but it is not a serious one. The skill and equipment necessary to create a good forgery is considerable; even more so to create a virtually perfect forgery. (68) It is possible that a photograph has been manipulated so seamlessly that the deception will go unnoticed, but it is not

very probable.

Until fairly recently, the same improbability applied to most digital images, as well. Hardware and software for the capture and editing of visual data was expensive and exotic. (69) Now, however, it is becoming increasingly affordable and common. It is also (especially in the case of software) becoming easier to use. Only a few years ago, creating a convincingly altered digital image required the efforts of a specialist using sophisticated equipment; now it can be easily accomplished by a hobbyist with a home computer. (70) And, after the data file replaces the original in the computer's memory, there need not be any indication that another "original" ever existed.

Thus, a digital photograph is like a conventional photograph with respect to the impact it makes on the observer. Because it looks like a photograph, possessing the same level of detail and the same internal consistency, the observer is inclined to react with the same degree of trust. Given these circumstances, it is reasonable to review the doctrine which has developed in response to conventional photography and consider how it might apply to digital photography.

But, no matter how closely a digital photograph resembles a conventional photograph, that similarity does not alter the essential nature of digital images -- a nature which should be recognized when analyzing their admissibility in court. Ultimately, a digital photograph is a collection of numbers, several million digits each reading either "one" or "zero," and this fact unavoidably leads to evidentiary concerns. Courts have gradually begun to develop a doctrine that responds to the problems presented by other types of digital data, and that doctrine ought to be mentioned when discussing the future of digital photography and evidence.

Part III: Existing Approaches to Photographic and Computer Evidence

Section 1: Photographs as Evidence

The principal requirements to admit a photograph into evidence are relevance (71) and authentication. (72) In general, a photograph will be admitted into evidence at the discretion of the trial judge. (73) In rare cases a chain of custody (including custody of the undeveloped film) will be required, (74) or the best evidence rule may be invoked if the photograph is offered for its truth and is the basis of a controlling issue in the case. (75)

The most important of these requirements is authentication. Unless the photograph is admitted by stipulation of the parties, the party seeking to introduce the photograph into evidence must be prepared to present testimony that the photograph is accurate and correct. (76) In most cases, the testimony need not be from the photographer; (77) any witness qualified to testify that a photograph accurately portrays a scene familiar to that witness will suffice. (78) Some courts will rule that a photograph is self-authenticating, (79) or presumptively authentic. (80) If the authenticity of a photograph is challenged, it is usually a question for the trier of fact to settle. (81)

Although these threshold requirements are relatively lax, and photographs are routinely admitted into evidence with little scrutiny, existing doctrine is a reasonable response to the slight risk presented by misleading conventional photographs. An inquiry into relevancy assures that the trial court will at least consider whether a photograph, even if probative, might unduly confuse or deceive the trier of fact. The authentication requirement serves as a check against outright fraud, and the chain of custody requirement applied in particular instances provides additional insurance. Finally, although the Federal Rules allow the introduction of a print made from a negative as an original (rather than a duplicate) (82) in those few cases involving the best evidence rule, (83) even this relaxed application provides some protection. At the minimum, it indicates official recognition that there is (or was) a negative -- a "super-original" which, in accordance with the laws of physics, must bear some logical relationship to any duplicates.

Section 2: Computer Data as Evidence

"The presence of computers has created additional complexities and definitional problems within the accepted rules of evidentiary procedure." (84) To a large degree, these difficulties are a direct result of the very qualities inherent in digital data. As one authority described the problem, "[t]he ease with which electronic impulses can be manipulated, modified, and erased is hostile to a legal system that arose in an era of tangible things and relies on documentary evidence to validate transactions, incriminate miscreants and affirm contractual relations." (85) A judge once made the same point more colorfully: "As one of the many who have received computerized bills and dunning letters for accounts long since paid, I am not prepared to accept the product of a computer as the equivalent of Holy Writ." (86)

Perhaps as a result of these difficulties, courts have been slow to construct doctrines governing the admissibility of digital evidence. What little case law that exists on the subject is based almost entirely on the business records exception to the hearsay rule. (87) Application of the business records exception to computer data must have seemed logical when computers were expensive and owned primarily by large enterprises such as corporations, universities, and governments. Computer data relevant to legal proceedings was likely to be of a sort routinely gathered in the course of the enterprise (such as personnel files or financial records), and thus superficially similar in many ways to the type of evidence giving rise to existing doctrine.

It is not clear, however, that the business records exception to the hearsay rule can be successfully expanded to govern the admissibility of digital data in the many forms it has grown to take. As a threshold matter, it must be remembered that the hearsay rule (and its exceptions) apply only to statements, (88) or assertions. (89) The ability to store information such as sound or visual imagery in a digital form may foreseeably lead to circumstances in which litigants seek to introduce digitized evidence bearing little resemblance to what are traditionally viewed as "assertions."

Also, the business records exception to the hearsay rule applies only to records gathered in the course of a business or similar activity. (90) "The element of unusual reliability of business records is said variously to be supplied by systematic checking, by regularity and continuity which produce habits of precision, by actual experience of business in relying upon them, or by a duty to make an accurate record as part of a continuing job or occupation." (91) These indices of reliability could reasonably be extended to digital data when computers were expensive rarities; now, however, they are becoming common household appliances. (92)

No matter what doctrine is employed to justify admission of computer data into evidence, if it is offered for its truth and forms the basis of a controlling issue in the case, it must still satisfy the best evidence rule. (93) Pursuing this analysis, courts and legislators have on occasion recognized the unique status of digital evidence. In *King v. State*, (94) the court noted that the impulses stored on magnetic tape (that is, the actual digital data) were useless to a human observer until translated into a readable form, and so the best evidence rule was satisfied if the computer printouts were admitted. (95) The Federal Rules of Evidence go further, defining "any printout or other output readable by sight, shown to reflect the data accurately" as an "original" of the digital record. (96) The similarity between this rule and the rule defining a photographic print as an original is not coincidental; in the Federal Rules, the same rule applies to both photographic prints and computer printouts. (97)

Section 3: Can Existing Doctrine Be Applied to Digital Photographs?

Digital photography presents a profound challenge to the existing rules of evidence. Although a digital photograph may be cosmetically identical to a conventional photograph, it represents an entirely different species of evidence. Because a digital image may be precisely copied at will (until it is printed or displayed on a computer monitor) (98) there exists no way to distinguish a copy from the original. (99) And, because digital data may be copied absolutely perfectly, any discrepancy between two versions of a single digital image is likely (100) to be the result of

intentional alteration, either innocent or malicious. Unless the individual responsible for the alteration is identified, there may be no way to identify which image is derivative of the other.

There is a foreseeable risk, as digital cameras replace conventional cameras in common service, that the foundation requirements applicable to conventional photographs offered in evidence will prove insufficient when applied to digital photographs. The honest testimony of an authenticating witness that an image is a fair and accurate portrayal of a scene may no longer be an adequate safeguard if legal rights or liabilities turn on subtle but material manipulation of individual elements within a scene. The "resolution" of the witness' memory may not be that fine, even if the witness is the photographer. Fraud by conventional photograph was difficult, expensive, and easily detectable; photocollage techniques necessary to add, delete, or relocate scene elements were especially difficult and rarely very convincing. Contemporary technology has made manipulation of digital images easy, inexpensive, and seamless; sophisticated tools for potentially undetectable photocollage effects are a standard feature included with commercial photoediting software. (101) If the photograph was captured by means of a digital camera, there need be no trace that an earlier version of the image ever existed.

Analyzing digital photographs as computer records is equally unsatisfactory. There are serious limitations in the present state of the law, which applies to digital data only to the extent that the data can be compared to traditional business records. Although it may be true that some digital photographs could be analyzed in this manner (for instance, surveillance photographs "asserting" that the individual portrayed has committed a crime, as documented in the photograph) many others could not. For instance, a snapshot purporting to place a criminal defendant some distance from the scene at the time the crime was committed would not be admissible as a business record.

Finally, application of the best evidence rule is an ineffective method to assure the integrity of a digital image. By expressing a judicial preference for originals over copies, the rule presumes that originals are distinguishable from copies -- and ignores the possibility that perfect copies may be more accurate than an edited "original." Worse yet is any incarnation of the best evidence rule which follows the Federal Rules of Evidence in defining a printout (102) as an "original" for purposes of the rule. Although it can not be said with certainty which copy of a digital file is the original, it is quite certain that a printout is not. The logical lapse which defines a photographic print as an original may be excusable when the print by definition must be physically connected to the negative. On the other hand, all that is achieved by printing a digital image is a document bearing a superficial similarity to a photograph, but possessing none of the qualities that make conventional photographs generally trustworthy.

Part IV: Responding to the Problem of Digital Photography

As the conventional photograph goes the way of the horse drawn carriage and the vinyl phonograph record, courts and legislatures will have to establish procedures to assure the accuracy and integrity of visual evidence admitted into legal proceedings. If existing doctrines cannot rise to the task, new doctrines will have to develop.

Some writers have proposed that courts must adopt a new paradigm, rejecting the authenticity of digital photographs as a matter of course. Dartley, for instance, has suggested that digital images be "conspicuously labeled." (103) In this manner, a digital photograph will be accompanied by an implicit warning: the viewer is on notice that the image may not portray what it seems to portray. Unfortunately, this solution falls short in two respects. First, it is not clear who is responsible to attach such a label, or why an individual intent on committing fraud would do so. Second, this suggestion will become much less helpful when digital photographs become the rule rather than the exception. (104)

On the other hand, Guilshan has proposed that digital photographs be properly authenticated only by the photographer, and no other sponsoring witness. (105) Although there is some benefit

to tightening authentication requirements (and it is difficult to disagree with the author's assertion (106) that the self-authentication theory is particularly troubling), this approach seems unlikely to prevail. There is no provision for circumstances in which the photographer is unavailable, (107) or there simply is no photographer. (108) Also, this approach presumes that the photographer is the only person capable of altering an image. As the cases involving unauthorized alteration of computer data (109) illustrate, such a presumption is not necessarily valid.

Finally, it has been suggested that digital photography will inevitably lead to the exclusion of visual evidence entirely. (110) Such an extreme approach does not seem at all likely, however, nor would it be desirable. Justice would not be served by the exclusion of relevant, accurate visual evidence.

Technology can create problems, but it can also be employed to solve problems. Although digital data possesses qualities that give rise to evidentiary concerns, it also possesses qualities that can be applied to meet those concerns. A technical response might, for instance, build upon one last characteristic feature of digital data: it can include, as an integral part, data about itself. (111) It is possible to attach a "digital signature" (112) to a file, encrypted to prevent alteration, (113) verifying that the data has not changed since the attachment was generated. This verification extends to cover perfect digital copies (including the attachment) but belies an altered file, whether it is a copy or the original.

As digital cameras replace conventional cameras, courts and legislatures have the power -- and the responsibility -- to require a stronger showing of authenticity than has been required to date when photographs are offered in evidence. A positive step in this direction would be to exclude visual evidence in the absence of virtually incontrovertible proof of accuracy. A "digital signature" incorporated into the data file would be an easy way to provide that proof. At the very least, digital cameras intended specifically to gather evidence (automated surveillance cameras, or those employed by law enforcement agencies) should be required to include verification technology. Ultimately, it is possible that market forces might lead to the manufacture of digital cameras equipped with data verifying hardware or software as a matter of course. A society which has learned to presume that "seeing is believing" may well prefer image-capturing devices that retain, by design, an assurance of authenticity.

Part V: Conclusion

In only a few decades, computers have evolved from the stuff of science fiction into fixtures of our daily lives. (114) In the course of this evolution, they have begun to influence society in ways that were beyond imagination only a generation ago. As a social institution, the judicial system will have to adapt to the influence of computers if it is to remain responsive in the years ahead. Unfortunately,

[a] risk is run whenever the law places too much reliance upon the past. This risk appears every time a technological change radically transforms society. Law and the judiciary are suddenly caught unaware and are unable to rely upon principles of law that could not have contemplated the technology before them. (115)

If "law and the judiciary" are to effectively address the foreseeable risks suggested by the use of digital photography as evidence in legal proceedings, doctrines of admissibility will have to develop in response to those risks. These new doctrines might incorporate some of the suggestions offered here, or they might take some unanticipated shape. However the courts finally respond, the issue will have to be confronted soon.