THE *SWINTON* SIX: THE IMPACT OF *STATE v. SWINTON* ON THE AUTHENTICATION OF DIGITAL IMAGES*

Catherine Guthrie**
Brittan Mitchell***

I. INTRODUCTION

"[T]he machine does not isolate man from the great problems of nature but plunges him more deeply into them."[1] Nowhere is this more apparent than in the struggle between rules of law and scientific and technological advances. Our court system's response to this challenge is scrutiny and adaptability, two traits evidenced by the ebb and flow of requirements for authentication of digital images.

This Article examines the evolution of authentication requirements for digital images, with particular emphasis on the impact of *State v. Swinton*.[2] Part II of this Article provides an overview of digital images as well as the general rationale for their authentication. Part III reviews past statutory and common law rules for establishing the authenticity of such evidence. Part IV summarizes *Swinton*, a 2004 case from Connecticut which represents a major development in this area of law. Part V applies the holding from *Swinton* to a new type of digital evidence, virtual autopsies, in a theoretical context. The Article concludes in Part VI.

** Catherine Guthrie is a graduate of Stetson University College of Law and an active member of The Florida Bar. She is currently working for the National Clearinghouse for Science, Technology and the Law as a Research Attorney.

*** Brittan Mitchell is a graduate of Stetson University College of Law and an active member of The Florida Bar. She was an employee of the National Clearinghouse for Science, Technology and the Law during the authorship of this paper.

1. Antoine de Saint-Exupéry, *Wind, Sand, and Stars* 43 (Lewis Galantière trans., Harcourt, Inc. 1967).

2. 847 A.2d 921 (Conn. 2004).

II. DIGITAL IMAGING AND THE NEED FOR AUTHENTICATION

The technical definitions associated with digital imaging, as well as the related equipment, are addressed in this part of the Article. The alteration, analysis, benefits, and drawbacks of digital imaging are also discussed. The section concludes with a discussion of the rationale for heightened standards of authentication for this type of evidence.

A. Definition of Digital Imaging

Digital imaging[3] refers to images which are collected, generated, enhanced, preserved, or analyzed, in binary format.[4] The purpose of a digital imaging processing system is to uncover information stored in the digital images.[5] Binary digits, which are also known as bits, are the smallest piece of data that a computer

---

3. The following quote provides some insights into the historical context of digital imaging:

> Image enhancement technology was developed during the late 1960s and early 1970s for the [National Aeronautics and Space Administration (NASA)] space program. . . . Due to the weight and power limitations of spacecraft, it was impractical for NASA to use state-of-the-art camera systems on unmanned craft. The cameras used produced somewhat degraded photographs. Image enhancement reverses the degradation . . . and thereby improve[s] the sharpness and image contrast of the photograph . . . [by] eliminat[ing] background patterns and colors.

Id. at 937 n. 22 (internal quotation marks omitted) (quoting Paul C. Giannelli & Edward J. Imwinkelried, *Scientific Evidence* vol. 2, § 25-6.1 (3d ed., LEXIS & Supp. 2003)); *see also State v. Hayden*, 950 P.2d 1024, 1026 (Wash. App. Div. 1 1998) (noting that "the technology used to enhance photographs of latent prints evolved from jet propulsion laboratories in the NASA space program to isolate galaxies and receive signals from satellites"); Richard Bernstein, Student Author, *Must the Children Be Sacrificed: The Tension between Emerging Imaging Technology, Free Speech and Protecting Children*, 31 Rutgers Computer & Tech. L.J. 406, 408 (2005) (tracing the history of digital imaging even further back to cave drawings and Disney movies).

4. "Generally, data forensics is the collection, preservation, analysis, and presentation of evidence found on electronic devices." Gail M. Cookson & Carole Longendyke, *Data Forensics*, 29 Md. B.J. 66, 66 (Jan./Feb. 2006); *see also* Intl. Assn. for Identification & L. Enforcement/Emerg. Servs. Video Assn. Intl., Inc., *Forensic Imaging and Multi-media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), and Forensic Video (FV)* 68 (2006) (available at http://www.theiai.org/guidelines/iai-leva/forensic_imaging_multi-media_glossary_draft06.doc) (defining "digital evidence" as "[i]nformation of probative value that is stored or transmitted in binary form") [hereinafter *Forensic Imaging and Multi-Media Glossary*].

5. Imaging Research, Inc., *Evaluating Image Analysis Systems*, "Image Analysis Equipment," http://www.imagingresearch.com/applications/evaluating.asp (accessed May 18, 2007).

is able to process.[6] Images are made up of pixels, which are "code[s] consisting of bits of information representing a specific color, intensity, and location."[7] One court has analogized pixels to dabs of paint in a pointillist painting.[8] Computers store these digital representations on a rectangular grid known as a bitmap.[9]

Most commonly, digital images take the form of videos and photographs. Such images are generated in one of two ways. First, digital cameras can be used to create digital images.[10] Digital cameras electronically record and store photographed images in a digital format rather than on traditional film.[11] Specifically, "the light entering the lens of the digital camera is reflected off a sensor that records the data in binary form and stores it in a file."[12] Secondly, scanning traditional film negatives or photographs into a computer also generates digital images.[13] Scanners are "input device[s] that move[ ] a light-sensitive electronic device across an image-bearing surface, such as a page of text or photographic negative, to convert the image into binary digits that can be processed by a computer."[14] Other digital imagery, including x-

6. Penney Azcarate, *Digital Imaging Technology and the Prosecutor*, 34 Prosecutor 26, 26 (Feb. 2000).

7. *Id.*; *see also Swinton*, 847 A.2d at 935 n. 15 (citing *U.S. v. Grimes*, 244 F.3d 375, 378 n. 4 (5th Cir. 2001)).

8. *Swinton*, 847 A.2d at 935 n. 15 (citing *Grimes*, 244 F.3d at 378 n. 4).

> A pixel is the smallest discrete element of an image. . . . It is a set of bits that represents a graphic image, with each bit or group of bits corresponding to a pixel in the image. The greater the number of pixels per inch, the greater the resolution. A rough analogy to painted art is that a pixel is the same as each colored dab of a pointillist painting.

Id. (quoting *Grimes*, 244 F.3d at 378 n. 4).

9. Azcarate, *supra* n. 6, at 26. Digital imaging works as follows:

> An initial step in digital[-]image processing is the transformation of image features (density, color, position) into discrete digital values. This transformation process is known as digitization. During the digitization process, the continuous spatial extent of the image is broken into discrete spatial elements which are stored in a memory bank (image memory) within the image processor. A single "picture element" in image memory is a pixel. With the location and density or color of each pixel digitally coded, image processing becomes a matter of "number crunching."

Imaging Research Inc., *supra* n. 5.

10. Azcarate, *supra* n. 6, at 26.

11. *See Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 67 (defining "digital camera").

12. Christopher J. Buccafusco, *Gaining/Losing Perspective on the Law, or Keeping Visual Evidence in Perspective*, 58 U. Miami L. Rev. 609, 614–615 (2004).

13. Azcarate, *supra* n. 6, at 26.

14. *Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 208.

rays, animations, simulations, charts, graphs, and models, are generated with more advanced technology such as radiological equipment and specialized computer-software programs. In general, any image that is created through digital processes may be categorized as "computer-generated."[15]

Once the images are in digital format they can be electronically stored, transferred, altered, and analyzed. Storage and transferability most often involve legal issues pertaining to discovery and privacy, which are outside the scope of this Article. However the ability to alter and analyze the images directly impacts their authenticity and, thus, merits further discussion.

1. Alteration of Digital Images

Alterations include enhancement, restoration, and compression. Enhancement is any process wherein the image's visual appearance is improved, either through traditional photographic techniques or through nontraditional, computerized methods.[16] Traditional techniques have "direct counterparts in traditional darkrooms" including spotting, cropping, color balancing, brightness and contrast adjustment, burning, and dodging.[17] Nontraditional techniques do not have a "direct counterpart within traditional silver-based photography," are not as well established in the forensic community, and, thus, are more susceptible to challenge.[18] Examples of such computerized techniques include random noise reduction, pattern noise reduction, color processing, nonlinear contrast adjustments, and linear filtering.[19]

---

15. Computer-generated evidence may be either routinely prepared business records or evidence generated in anticipation of litigation. The computer-generated evidence that this Article will focus on includes the forms that are prepared in anticipation of litigation. *See infra* nn. 260–267 and accompanying text. Note that some courts' interpretation of the phrase computer-generated evidence might be broader than that of practitioners in the field. See the definition of "Detection of Image Creation" in Scientific Working Group on Imaging Technology (SWGIT), *Guidelines for the Imaging Practitioner*, "Section 14: Best Practices for Image Authentication" 4 (2007) (available at http://www.theiai.org/guidelines/swgit/guidelines/section_14_v1-0.pdf).

16. SWGIT, *Guidelines for the Forensic Imaging Practitioner*, "Section 5: Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System, Version 2.0" (2006) (available at http://www.theiai.org/guidelines/swgit/guidelines/sec5_2_20060109.pdf).

17. *Id*.

18. *Id*. at 3.

19. *Id*. at 3–5; *see also Nooner v. State*, 907 S.W.2d 677, 686 (Ark. 1995) (observing

Restoration refers to processes that totally or partially remove defects created by a known source, such as a blur or defocus, from an image.[20] These reparative techniques include blur removal, geometric restoration, color balancing, warping, and gray-scale linearization.[21] However, the amount of defect limits the possibilities of the restoration process in that completely lost data cannot be replaced.[22]

Compression refers to processes that reduce the size of data image files, which are normally quite large, such that they require less storage space.[23] The techniques used for this form of alteration are called lossy compression and lossless compression.[24] Certain images, particularly those that have already been compressed, should not be subjected to this form of alteration because data may be lost during the process.[25]

2. Analysis of Digital Images

The two main types of digital-image analysis are quantitative image analysis and cognitive image analysis. Both quantitative and cognitive analysis fall under the heading of Forensic Image Analysis, which "is the application of image science and domain expertise to interpret the content of an image and/or the image itself in legal matters."[26] Digital-image analysis may be utilized in both civil and criminal litigation.

---

that contested photographs were enhanced by increasing and improving levels of brightness and contrast).

20. SWGIT, *supra* n. 16, at 5; *see also Global Interprint, Inc. v. Burton*, 2003 WL 22093837 at **3–4 (Cal. App. 1st Dist. Oct. 10, 2003) (involving testimony by a photo image restoration expert that damaged images could be repaired digitally).

21. *See* SWGIT, *supra* n. 16, at 6–7 (defining and explaining the purpose of these reparative techniques).

22. *Id*. at 5.

23. *Id*. at 7.

24. *Id*. In *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), the court observed that while lossy compression "achieves its reduction in file size by eliminating some of the data in the file being compressed . . . it seeks to do so by eliminating data that is imperceptible, or nearly so, to the human observer." *Id.* at 313 n. 107. On the other hand, lossless data compression ensures that "the recovered image is identical to the original." *Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 148.

25. SWGIT, *supra* n. 16, at 8.

26. *Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 100.

Quantitative image analysis (QIA) is a process wherein measurable data is extracted from an image.[27] Typically, QIA is automated through the combination of computer hardware and software.[28] Specific QIA techniques include colorimetry,[29] photogrammetry,[30] photometry,[31] and image authentication.[32] Accurate size measurements depend on whether the digital image was properly calibrated and whether the exact pixel spacing was known.[33] For example, "if a circular object in an image includes 314 pixels, and the area covered by a single pixel is one square

27. *Id.* at 193.

28. Imaging Research, Inc., *supra* n. 5; *see generally* Dennis Hetzner, *Quantitative Image Analysis, Part 1 Principles*, 2(4) Tech-Notes 1–5 (1998) (available at http://www.buehler.com/application_support/tech_note_pdf/vol2_issue4.pdf) (discussing QIA and the history of image analysis systems).

29. Colorimetry is "[t]he quantification of the color of an object." Sci. Working Groups on Digital Evid. & Imaging Tech., *SWGDE and SWGIT Digital & Multimedia Evidence Glossary* 4 (2006) (available at http://www.theiai.org/guidelines/swgit/swgde/glossary_v2-0-1.pdf) [hereinafter *Digital & Multimedia Evidence Glossary*]; *see e.g. In re G.B.*, 2003 WL 22327191 at *2 (Tex. App. Amarillo Oct. 10, 2003) (using the testimony of an expert in colorimetry to explain the color changes in the context of drug testing).

30. Photogrammetry is the science involving methods, techniques, and analytical procedures used to make accurate measurements of distances and/or sizes of objects from photographic images. *Digital & Multimedia Evidence Glossary*, *supra* n. 29, at 10–11; *see e.g. Chapman ex rel. Estate of Chapman v. Bernard's Inc.*, 167 F. Supp. 2d 406, 421–422 (D. Mass. 2001) (discussing the reliability, as a scientific field, of photogrammetry (also termed photo-scaling)).

Ikea Center Urban Renewal, L.P. v. AFI Food Services Distributors, Inc., 2006 WL 463547 at **12–13 (N.J. Super. Ch. Div. Feb. 24, 2006) demonstrates the variety of approaches taken by experts in photogrammetry. *Ikea Center* was a case dealing with a contested easement. The existence of an "asphalt apron" on a specific date was determinative of the rights of the parties under the easement. *Id.* at *2. Two experts in photogrammetry testified in the trial as to the existence of the asphalt apron. The first expert used visual analysis and logical reasoning to deduce whether the asphalt apron existed on the date in question. *Id.* at*12. Although the court was impressed with the expert's credentials, it was not persuaded by the expert's opinion. *Id.* The second expert in photogrammetry took a more mathematical approach termed "supervised classification of a picture." *Id.* at *13. The expert analyzed "the pixels in each picture by assigning a color to a pixel and then [statistically] reviewing the entire picture against [his assignment]." *Id.* This mathematical calculation assisted him in formulating his opinion on the existence of the asphalt apron. *Id.* Interestingly, the court was similarly unpersuaded by this approach. *Id.*

31. Photometry is "[t]he measurement of light values of objects in an image." *Digital & Multimedia Evidence Glossary*, *supra* n. 29, at 11.

32. Image authentication is "the scientific examination process used to verify that the information content of the analyzed material is an accurate rendition of the original data by some defined criteria." *Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 122.

33. SWGIT, *Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System*, *Version 1.2*, in Forensic Sci. Communs. vol. 5 (Jan. 2003) (available at http://www.fbi.gov/hq/lab/fsc/backissu/jan2003/swgitdigital.htm).

millimeter, then one can conclude that the area of the object is 314 square millimeters."[34] Cognitive image analysis (CIA) is a process wherein visual information is extracted from an image.[35] In other words, the data is extracted from an image by the viewer's visual inspection of the image, rather than by a computer.

B. The Benefits and Popularity of Digital Imaging in the Forensic Context

There are numerous reasons why digital images are beneficial to forensic and legal practitioners, beginning with the fact that digital images can be collected with great speed, ease, and efficiency.[36] Investigators can photograph evidence at the scene, review the results, and, if the picture is unsatisfactory, immediately re-shoot the image before the setting is disturbed.[37] They also avoid having to carry dozens of rolls of film with them—a single memory card can hold hundreds of photographs.[38] Another advantage is that, unlike film, digital images do not need to be developed in expensive chemical laboratories by trained technicians.[39]

Once captured, the images can be promptly transferred via electronic mail, saved onto disks and CDs, stored in computer hard drives, and added to searchable databases.[40] These characteristics are particularly beneficial in multi-agency investigations where several parties need access to the same information. They also reduce the number of procedural steps associated with the preservation of chain of custody.[41] Further, the paperless aspect of

34. *Id.* "Similarly, if the distance between the adjacent pixels in an image of a document is 0.02 inches, and the length of the document is 340 pixels, then it must be 340 times 0.02, or 6.8 inches long. These examples do not consider perspective distortion." *Id.*

35. *Digital & Multimedia Evidence Glossary*, *supra* n. 29, at 4.

36. Azcarate, *supra* n. 6, at 27.

37. *Id.*; *see also* James I. Keane, *Prestidigitalization: Magic, Evidence and Ethics in Forensic Digital Photography*, 25 Ohio N.U. L. Rev. 585, 588 (1999) (describing the convenience of digital photography).

38. John Roark, *Forensic Photography: The Pros and Cons of Going Digital*, http://www.forensicfocusmag.com/articles/3b1feat2.html (Nov. 2003).

39. Azcarate, *supra* n. 6, at 27.

40. *Id.*; *see also* Theresa Rubinas, *File Cabinets: A Thing of the Past?* 25 Leg. Mgmt. 50, 50 (Jan./Feb. 2006) (indicating that digital imaging technology improves firm productivity because employees are able to access those images from practically any location).

41. Roark, *supra* n. 38.

digital evidence reduces costs associated with administrative assistance, copying, and file storage.[42] As these costs are decreasing, the quality of the images and cameras is increasing. One study revealed that "[h]igh-resolution digital cameras can capture approximately 16 million different colors and can differentiate between 256 shades of gray."[43]

The images can also be modified and analyzed through computerized processes. This kind of detailed information can be critical for generating police leads, reconstructing scenes, verifying alibis, and identifying perpetrators. For example, an enhancement specialist can modify the brightness and contrast of an image, even a moving image, to clarify details such as a license plate number.[44] Arrest photographs can be enlarged to reveal unique features like tattoos and scars,[45] and images of fingerprints can be magnified to expose arches, ridges, whorls, loops, and even skin pores.[46]

Over the past few years digital imaging equipment, including cameras, scanners and software programs, has become more and more accessible to both laypersons and forensic personnel due to decreased prices and increased market competition.[47] Some re-

42. Rubinas, *supra* n. 40, at 50.

43. Azcarate, *supra* n. 6, at 27. Even though digital cameras are improving in quality, they still have not caught up to film in terms of color range. See "Advantages of Silver-based Film Cameras in Field Applications" in Scientific Working Group on Imaging Technology (SWGIT), *Guidelines for the Imaging Practitioner*, "Section 3: Guidelines for Field Applications of Imaging Technologies in the Criminal Justice System" 2 (2001) (available at http://www.theiai.org/guidelines/swgit/guidelines/section_3_v2-3.pdf).

44. *See State v. Clark*, 2002 WL 31895162 (Wash. App. Div. 2 Dec. 31, 2002) (demonstrating how a digital image can be enlarged to enable police officers to read license plate numbers).

45. *See* Mich. St. Police, Press Release, *State's Photo Database Exceeds One Million Images* (April 27, 2006) (available at http://www.michigan.gov/msp/0,1607,7-123-1586_1710-142044--M_2006_5,00.html) (reporting that the Michigan State Police's digital image database, containing mugshots, scars, marks, and tattoos, "has surpassed the one million images mark, making it a more powerful investigative tool for law enforcement").

46. *U.S. v. Llera Plaza*, 188 F. Supp. 2d 549, 572 (E.D. Pa. 2002) (commenting that "[n]o one doubts that fingerprints can, and do, serve as a highly discriminating identifier, and digital photographic enhancement and computer databases now promise to make fingerprint identification more useful than ever before").

47. Buccafusco, *supra* n. 12, at 614. "In under a decade, digital cameras have landed in just over half of the [United States'] 110 million households. That penetration could reach 55 to 60 percent [in 2006] and top out at around 70 percent by 2009, analysts say." Ben Dobbin, *Aim, Shoot, Farm Out Prints*, Seattle Times C1 (Feb. 23, 2006); *see also* Harry Wessel, *Fujicolor's Orlando Plant to Lay Off 64 Workers, Close*, Orlando Sentinel C3 (Apr. 13, 2006) (describing the closing of film plants caused by the popularity of digital alterna-

ports claim that sales of traditional camera film are declining annually by twenty-five percent—much faster than anticipated and at such a rate that film cameras will be "all but dead within a couple of years."[48]

Examples of this trend abound in law enforcement. For instance, in 2001 the Seattle Police Department began a program to replace all of its traditional patrol car cameras with wireless, digital technology.[49] The Oregon State Police's forensic laboratory went "all digital" around 1999.[50] Even police departments in smaller cities such as Elmurst, Illinois[51] and Murray, Utah[52] have implemented digital imaging.

As the popularity of this technology surges upward among the general public and law enforcement, it cannot help but overflow into America's courtrooms.[53] More and more attorneys are utilizing digital images to support and illustrate their arguments in front of both judicial and administrative panels.[54] This trend is documented in numerous articles[55] and in both civil and criminal

---

tives).

48. Charles Arthur, *Digital Photography: How the Digital Revolution Is Shaking Up the Photo Industry*, Indep. 3 (Nov. 18, 2005).

49. Hector Castro, *Police Cars Get Digital Cameras; Seattle Department First to Use New Wireless Capability*, Seattle Post-Intelligencer Rept. B1 (Dec. 18, 2004). The wireless capability "enables officers to download the images from their patrol cars directly to the precincts." *Id*.

50. Brian Bergstein, *Digital Photography Poses Thorny Issues for Justice System*, USA Today (Feb. 7, 2004) (available at http://www.usatoday.com/tech/news/techpolicy/2004-02-07-crime-images_x.htm).

51. City of Elmhurst, *Police Department General Information*, http://www.elmhurst.org/elmhurst/police/generalinfo.asp (accessed Aug. 13, 2007).

52. Murray City Police Dept., *2006 In Car Video Recording Program*, http://www.murray.utah.gov/police-department-home.asp?id=11 (accessed May 17, 2007).

53. James H. Rotondo, David B. Broughel & Edgar B. Hatrick, *Digital Images: Don't Blink or You Will Miss Them*, 23 Prod. Liab. L. & Strategy 3, 3 (Mar. 2005) (noting that "[a]s the use of digital photography has become commonplace, so too are digital photographs being increasingly offered as evidence").

54. *Id*.; *see also* Edward A. Hannan, *Computer-Generated Evidence: Testing the Envelope*, 63 Def. Counsel J. 353, 362 (1996) (commenting that "[d]esktop portable computers now bedeck courtrooms like dandelions in May and, like dandelions, their number, use and application continue to grow").

55. *See e.g.* Linda Miller Atkinson, *Persuasive Evidence for Digital Juries*, 2 ATLA Annual Conv. Ref. Materials 1537 (July 2003) (discussing how technology is making a lawyer's research efforts more efficient, comprehensive and economical); Bruce L. Braley, *Using Technology to Sharpen Your Message without Losing Your Mind*, 1 ATLA Annual Conv. Ref. Materials 255 (July 2004) (reporting that software developers are marketing legal presentation software "to give trial lawyers the ability to create and present high-impact visual images"); Benjamin B. Broome, *Demonstrative Evidence: A Tutorial from an*

cases.[56] It is further evidenced by the development of the "e-courtroom"—a courtroom that contains advanced electronic equipment such as multiple high-resolution monitors, projectors and screens, high-resolution video cameras, video annotation devices, and high-quality sound systems.[57] The availability of these technological capabilities supports and encourages the use of digital-image evidence.[58]

The reliance on pictorial exhibits is not surprising considering that jurors tend to focus primarily on visual, rather than oral,

---

Expert—Tips on Using Stock Medical Demonstrative Evidence, 2 ATLA Annual Conv. Ref. Materials 1479 (July 2005) (indicating that digital technology has allowed attorneys to obtain stock medical demonstrative evidence for a more economical price than they could in the past); Joseph A. Desch, *Digital Imaging in Document Intensive Litigation*, 68 J. Kan. B. Assn. 7 (May 1999) (commenting that state and federal courts are rapidly becoming "computerized"); Sam Guiberson, *Digital Media as Evidence and Evidence as Media*, 19 Crim. Just. 57, 58 (2004) (arguing that technologically competent advocates have an advantage with jurors because digital media "[stimulates] the mind with changing input from many senses, each alternatively primary and then secondary, all repeating and thereby reinforcing, a common message"); Daniel E. Harmon, *National Institute for Trial Advocacy Publishes Guide Books on Using Courtroom Technology*, 21 Law.'s PC 12 (Nov. 1, 2003) (noting that lawyers are using not only computers but an array of technological hardware in the courtroom); Shelley Watts, *Technology Creates Winning Visual Evidence*, 36 Tr. 68 (Sept. 2000) (listing the advantages of a digital courtroom presentation and arguing that such presentations are practically indispensable in order to keep jurors' attentions from waning).

56. *See Verizon Directories Corp. v. Yellow Book USA, Inc.*, 331 F. Supp. 2d 136, 137–138, 142 (E.D.N.Y. 2004) (describing categories of computer-generated pedagogical devices and determining that such devices should, subject to a few exceptions, be admitted as evidence); *State v. Hayden*, 950 P.2d 1024, 1028 (Wash. App. Div. 1 1998) (holding that the trial court did not err in admitting digitally enhanced photographs in a murder case, as the validity of digital imaging has been generally accepted as reliable by the scientific community).

57. Winton Woods, *Firms Take Courtrooms to the Next Level*, 37 Ariz. Atty. 46 (Apr. 2001); *see also* Nicole De Sario, Student Author, *Merging Technology with Justice: How Electronic Courtrooms Shape Evidentiary Concerns*, 50 Clev. St. L. Rev. 57, 60–62 (2002–2003) (describing the plush technological innovations built into a federal courtroom in Ohio); Stacey A. Rowcliffe, *The Digital Courtroom: How to Use This New Trial Media Tool If It's Available at a Courthouse Near You*, 26 Mont. Law. 30 (Dec. 2000) (describing a courtroom in Montana featuring a built-in computer monitor in the witness box that enables the witness to electronically mark the screen to clarify his or her testimony); Stetson U. College of L., Press Release, *Stetson College of Law Builds Model Courtroom for the Elderly and Disabled* (Tampa Bay, Fla., Sept. 23, 2005) (available at http://www.law.stetson.edu/communications/news.asp?id=206) (introducing a courtroom that features refreshable Braille displays, electronic gates and a multi-lingual software speech synthesizer and translator). Pictures of a courtroom incorporating some of this technology can be viewed online. *See* Stetson U. College of L., *Eleazer Courtroom*, http://www.law.stetson.edu/EleazerCourtroom (accessed Aug. 13, 2007).

58. For one court's detailed description of the use of computer-generated exhibits in court, see *Verizon*, 331 F. Supp. 2d at 138–139.

evidence.[59] One study designed to measure information retention among jurors showed "that jurors were able to recall sixty-five percent of the evidence presented three days earlier if the evidence was presented through a combination of oral and visual evidence."[60] However, when purely oral evidence was presented, the jurors could only retain about ten percent of the information.[61] Jurors are probably more likely to retain data presented in a visual format because such information is easier to understand.[62] For instance, an accident reconstructionist may wish to reference a picture of the scene of a car crash rather than orally describing exactly how the automobiles were positioned. As one author noted, these images do more than "add 'sparkle' to cases"; rather, "they are simply necessary to explain the complexities of the case."[63]

C. The Drawbacks

Digital imaging is not without its detractors. For one thing, certain consumers, such as smaller police departments, may have difficulty keeping current with the ever-changing world of digital electronics.[64] Also, despite constant technological advances, the quality of digital-image resolution is still considered inferior to that of traditional film cameras.[65] Users complain about the amount of time it takes to obtain multiple exposures with digital

59. John Selbak, Student Author, *Digital Litigation: The Prejudicial Effects of Computer-Generated Animation in the Courtroom*, 9 High Tech L.J. 337, 360 (1994).

60. *Id.*; *see also* Adam T. Berkoff, Student Author, *Computer Simulations in Litigation: Are Television Generation Jurors Being Misled?* 77 Marq. L. Rev. 829, 829 (1994).

61. Selbak, *supra* n. 59, at 360; *see also* Berkoff, *supra* n. 60, at 829 (noting that it is more comfortable for jurors to be able to "sit back and watch" a multimedia presentation than it is for them to digest a "tiresome and confusing string of statistics and facts").

62. Fred Galves, *Where the Not-So-Wild Things Are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance*, 13 Harv. J.L. & Tech. 161, 167–168 n. 15 (2000).

63. *Id*. at 168–169.

64. However, at least one court has specifically allowed for the use of older digital enhancement software even though newer technologies were available. *See e.g. U.S. v. Seifert*, 351 F. Supp. 2d 926, 927–928 (D. Minn. 2005) (admitting into evidence a digitally copied and contrast-enhanced analog tape over an objection that the tape did not sufficiently record the surveillance images).

65. *See* Jill Witkowski, Student Author, *Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images*, 10 Wash. U. J.L. & Policy 267, 269 n. 6 (2002).

equipment.[66] There is usually a several second delay between the time the light sensor adapts to the desired image and the point where the flash is triggered.[67] There is also a delay between the time the first image is taken and the time when another image can be taken.[68] The second delay is caused by the processes necessary to digitize, compress, and save the captured image.[69] These interruptions can be particularly problematic for persons attempting to capture action photographs, as may be useful in an undercover, or "sting," operation.[70]

The security of storing sensitive or confidential images on an Internet-accessible computer also raises concerns.[71] Such files may be accidentally or intentionally viewed, and possibly even modified, by unauthorized third parties, including computer maintenance personnel[72] and hackers.[73] In fact, there are several opportunities for this kind of corruption as well as for basic technical malfunctions. Problems may arise related to data entry, hardware, software, output, execution of the instructions, and general user error.[74] Thus, "[o]ne of the greatest advantages of digital photography—the reduction of a photographic image to an electronic file, can also be a great disadvantage."[75]

Critics are additionally concerned with the potential for juror prejudice and photographic trickery.[76] In other words, the "persuasiveness and manipulability"[77] of digital imagery are as much a detriment as they are a benefit. As previously discussed, jurors tend to retain and understand visual evidence more than oral evidence.[78] This leads to the often debated yet still controversial

66. Roark, *supra* n. 38.
67. *Id*.
68. *Id*.
69. *Id*.
70. *Id*.
71. David Hricik, *The Speed of Normal: Conflicts, Competency, and Confidentiality in the Digital Age*, 10 Computer L. Rev. & Tech. J. 73, 88 (Fall 2005).
72. *Id*. at 95.
73. *Id*.
74. 57 Am. Jur. 3d *Proof of Facts* § 7 (2000).
75. William W. Camp, *Practical Uses of Digital Photography in Litigation*, Ann. 2000 ATLA-CLE 1463 (July 2000) (explaining that "[e]lectronic files can be lost, damaged, or accidentally erased—perhaps more so than traditional 35 mm negatives").
76. Buccafusco, *supra* n. 12, at 620.
77. *Id*.
78. Selbak, *supra* n. 59, at 360; Berkoff, *supra* n. 60, at 845–846.

question of whether jurors place the appropriate value on visual evidence or whether they are unduly influenced by such material. While proponents of digital technology argue that laypersons are "increasingly immune to confusion by the encroachment of technology into heretofore primitive communication zones such as the jury room,"[79] others disagree. For instance, one scholar wrote that because they "are especially prone to believe evidence that is presented visually, regardless of its veracity[,] . . . juries may discard common sense when confronted with computer evidence, and instead accept as proven fact whatever the computer proposes as the calculated result of the outcome."[80]

The fact that the imagery itself may be intentionally or unintentionally altered compounds this problem. Digital photographs are much easier to modify, particularly in terms of time and skill, than traditional images.[81] Digital alteration does not require advanced training, equipment, or software.[82] Digital-camera users arguably have a greater opportunity to modify photographs because they usually process the images themselves, rather than utilize the services of a professional print developer.[83] Such digital modifications are also hard to detect,[84] especially because

> [u]nlike traditional cameras, which produce one negative, digital cameras create an electronic file from which the image can be generated. Because the image file contains a finite set of ones and zeros, exact copies of the image file can be made with no loss of image quality between generations. Thus, it is impossible to determine which image is a first generation image and is therefore the "original." The lack of an "original" for comparison with the offered image reduces the opportunity to verify that the image has not been altered or has only been altered in an acceptable manner, thereby increasing the likelihood that changes will not be discovered unless the proponent of the image reveals them.[85]

79. *Verizon*, 331 F. Supp. 2d at 142.
80. Buccafusco, *supra* n. 12, at 620 (quoting Selbak, *supra* n. 59, at 339).
81. Witkowski, *supra* n. 65, at 271.
82. *Id*.
83. *Id*.
84. *Id*.
85. *Id*. at 272–273 (internal citations omitted). Law enforcement is aware of this issue and continues to develop compensatory strategies. *See generally* SWGIT, *Guidelines for the*

The fact that it is difficult, if not impossible, to identify modifications presents unique challenges to proponents of digital imagery. It also heralds the need for heightened standards of admissibility of such evidence, particularly in the context of authentication.

D. The Need for Authentication

Most of the drawbacks associated with digital imaging technology relate to one key issue—the reliability of the images and the processes used to create them.[86] Opponents of such evidence often argue that both judge and jury are misled and distracted by high-tech, graphic exhibits. However, according to at least one court, "[t]he suggestion that trials are turning into legal smoke and mirror laser shows, lacking real substance, has no merit where the court exercises appropriate control."[87] Such control comes in the form of authentication.[88] In other words, attorneys who wish to introduce this kind of evidence will need to establish that the digital image is in fact what it purports to be.

Authentication not only establishes the general reliability of evidence, but also axiomatically helps to ensure a fair trial by excluding untrustworthy or "doctored" evidence. Admission of such faulty evidence may otherwise violate a party's rights, particularly under the Confrontation Clause of the Sixth Amendment, which states that "[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be confronted with the witnesses against him . . . ."[89] This essentially refers to a criminal defendant's Sixth Amendment right to show jurors that his opponent's evidence is unreliable, or, in other words, to confront the evidence and show it may not be what it claims to be.[90]

Imaging Practitioner, "Section 13: Best Practices for Maintaining the Integrity of Digital Images and Digital Video" (2007) (available at http://www.theiai.org/guidelines/swgit/guidelines/section_14_v1-0.pdf).

86. *See infra* nn. 272–275 and accompanying text (discussing eight areas where the reliability of computer-generated evidence may be called into question).

87. *Verizon*, 331 F. Supp. 2d at 142.

88. The different types of permissible authentication are described by Federal Rule of Evidence 901. *See also Black's Law Dictionary* 142 (Bryan A. Garner ed., 8th ed., West 2004) (defining authentication as "the act of proving that something (as a document) is true or genuine, esp. so that it may be admitted as evidence . . . .").

89. U.S. Const. amend. VI.

90. *See e.g. Crawford v. Washington*, 541 U.S. 36, 61–62 (2004) (holding that the Con-

It is important to note that authentication is not the only evidentiary obstacle facing computer-generated digital images. Issues pertaining to privacy, scientific evidentiary standards, disclosure,[91] discovery, hearsay,[92] and the Best Evidence Rule[93] may also create hurdles for digital imaging techniques. However, these issues are not within the direct scope of this Article.

III. HISTORICAL OVERVIEW OF THE RULES OF AUTHENTICATION

While the previous Part addresses the reasons *why* the digital imaging process should be authenticated, this Part describes *how* courts have attempted to do so. The first Section reviews the

---

frontation Clause mandates that the reliability of evidence be tested through the procedural process of cross-examination).

91. *See e.g. Clark v. Cantrell*, 529 S.E.2d 528, 536–537 (S.C. 2000) (explaining how issues of timely disclosure may affect the court's analysis for admissibility under concepts of fairness and prejudicial effect).

92. *See e.g. U.S. v. Harris*, 55 M.J. 433 (App. Armed Forces 2001) (addressing the amount of evidence necessary to deem pictures captured by digital imaging authentic, reliable, and therefore admissible when such evidence is challenged as hearsay).

93. The Best Evidence Rule, set forth in Federal Rules of Evidence 1001–1008, establishes a preference for original material when dealing with a "writing, recording, or photograph." Fed. R. Evid. 1002. However, the Rule also provides for situations where duplicates are permissible. Fed. R. Evid. 1003.

A federal district court admitted a digitally enhanced surveillance tape as an appropriate duplicate in an arson criminal trial. *Seifert*, 351 F. Supp. 2d at 926. The defendant only partially challenged the enhancement process; he did not challenge the changing of the analog tape to digital images, the slowing down of the images to real time, or the deleting of images from the tape that were irrelevant to the underlying criminal charge. *Id*. at 927. However, the defendant did object to the remaining processes that the enhancement specialist undertook, including: (1) circling an image; (2) enlarging that particular image to "fill the screen"; and (3) adjusting the image by highlighting the "walking figure" by altering the image's brightness and contrast. *Id*. The court stated that the Best Evidence Rule permits the admission of duplicates—"mechanical or electronic rerecording[s]"—as long as the duplicate reproduces the original in an accurate fashion, is authentic, and is circumstantially fair. *Id*. In reaching its conclusion that the digitally enhanced video was admissible as a fair and accurate rendition of the original video stream, the court viewed the before and after versions of the tape. *Id*. at 928. The court also listened to the testimony of the enhancement specialist, that although he altered the contrast and brightness of the digital images, he did not alter the respective relationships of shading on the image. *Id*. Instead he "simply 'moved' the brightness relationship on the scale, increasing the light's intensity while maintaining the image's integrity." *Id*. Therefore, the court held that the digitally enhanced video was admissible as a duplicate under the Best Evidence Rule. *Id*. In dicta, the court referred to the testimony of the enhancement specialist, indicating that updated versions of the enhancement software that tracked the technician's digital alterations would be preferable in forensic settings because it would allow the court and opposing counsel to verify the steps made during duplication and enhancement. *Id*. at 927 n. 2.

relevant statutory requirements for authentication. The second Section describes the two most popular common law approaches for authenticating evidence derived from digital processes, with a particular emphasis on imaging.

A. The Legislative Authority for the Authentication of Digital Images

Federal Rule of Evidence 901 states that "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[94] This concept of authentication and identification is "a special aspect of relevancy."[95] Although there are ways for the parties to forgo the analysis required for authentication,[96] authentication is usually a logical and necessary step.[97]

Rule 901(b) provides ten illustrations of the proper methods of authentication. A few of these examples include the following: (1) the testimony of a knowledgeable witness; (2) a review of distinctive characteristics in context of the circumstances; and (3) an evaluation of the contested process or system.[98] Although arguments have surfaced using all of these methods as forms of proper authentication for digitized evidence, this Article will demonstrate the superiority of the method of authenticating computer-generated images through factors that focus on the process or system through a comparison of the two primary judicial approaches.[99]

The majority of the states' authentication evidentiary standards parallel the federal statutory language, even though the illustrations and committee commentary may vary slightly from state to state.[100] Even in jurisdictions where the evidentiary code

94. Fed. R. Evid. 901.

95. Fed. R. Evid. 901(a) advisory comm. nn.

96. *Id*. The examples listed in the committee's notes include requests for admissions and pre-trial conference. *Id*.

97. *Id*.

98. Fed. R. Evid. 901(b).

99. "Process or system" is specifically defined in Federal Rules of Evidence 901(b)(9).

100. An example of a possible deviation from the federal rule is found in Alabama's committee commentary, which specifically adopts the "process or system" approach for the authentication of results of computer processes. Ala. R. Evid. 901(b)(9) advisory comm. nn. Florida and Alaska represent states that opted to list the illustrations from Federal Rule

does not have a specific rule related to authentication or identification, the common law principles of reliability and relevancy will dictate the appropriate evidentiary handling of difficult issues.

B. Common Law Reflections on Digital Imaging Technology and its Predecessor Technology

This Section reviews two dominant trends in the authentication of digital imaging. The first trend deals with the relaxation of judicial scrutiny of electronic evidence. The analysis stems from a review of the standards applied to pre-digital imaging technologies such as non-digital photographs, video recordings, and sound recordings. The second trend deals with the development of authentication standards that focus on input, processing, and output. This analysis focuses on digital imaging techniques as a form of computer-generated evidence.

1. Judicial Scrutiny

A historical analysis of the application of authentication principles reveals that multiple forms of electronic evidence were initially subjected to strict admissibility standards.[101] However, as both society and the judiciary became more familiar with the specific type of evidence, courts gradually relaxed the degree of information necessary for legal authentication.[102] This Section will examine how this trend developed through its application to areas that pre-dated digital imaging technology. Then, this Section will

---

of Evidence 901(b) in the commentary portion of the rule rather than in the rule itself. Fla. Stat. § 90.901; Alaska R. Evid. 901; *see* Appendix (listing multiple states' statutory references for their authentication standards).

101. *Swinton,* 847 A.2d at 946 (citing *Cunningham v. Fair Haven & Westville R.R. Co.,* 43 A. 1047, 1048–1049 (Conn. 1899) and *Dyson v. N.Y. & New England R.R. Co.,* 17 A. 137, 139 (Conn. 1888) (representing the courts' hesitancy in allowing photographic evidence without proper authentication)); Mark A. Johnson, Student Author, *Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?* 75 Marq. L. Rev. 439, 448–450 (1992) (analyzing caselaw regarding the strict standards initially applied to computer-generated records); *see also* Witkowski, *supra* n. 65, at 276–277 (citing *State v. McKeever,* 169 F. Supp. 426, 426 (S.D.N.Y. 1958), *rev'd in part on other grounds*, 271 F.2d 669 (2d Cir. 1959) (referring to the seven *McKeever* factors for sound recording authentication)).

102. Witkowski, *supra* n. 65, at 280 n. 53 (quoting in part Charles C. Scott, *Photographic Evidence* vol. 3, § 1297 (2d ed., West 1991)) (attributing the relaxation of standards for video recordings to the "widespread social, cultural, and technological acceptance of the medium").

review how courts are inappropriately applying this trend to novel forms of digital imaging technologies and processes.

a. Non-Digital Evidence

The traditional photograph is an appropriate starting point for an analysis of authentication standards prior to digital imaging. In the late nineteenth century and early twentieth century, many courts exhibited a general hesitancy towards the introduction of photographs as evidence.[103] This hesitancy displayed itself in the form of who could testify and what was included in that testimony.[104] For example, a United States Supreme Court case from 1900 affirmed a lower court's admission of the enlarged photograph because the photographer authenticated the photograph by testifying regarding the process used and the final outcome of the enlargement methodology.[105] However, by the middle of the twentieth century, the burdensome nature of authenticating a photograph had changed.[106] Courts relaxed the need for the photographer's testimony about the process and outcome and instead only required a witness to testify that the photograph was a "fair and accurate representation" of the contested object or scene.[107]

---

103. One court described the general hesitancy towards admitting photographs as follows:

> When photographs first began finding their way into judicial trials they were viewed with suspicion and received with caution. It was not uncommon to place upon the offering party the burden of producing the negative as well as the photograph itself, and of proving that neither retouching or other manual or chemical intervention was reflected in the proffered print.

U.S. v. Hobbs, 403 F.2d 977, 978 (6th Cir. 1968); *see also Cunningham*, 43 A. at 1049 (providing an analysis of a sliding-scale approach for the admission of photographs in which the level of scrutiny applied varied with whether the photograph was used to demonstrate a minor issue or whether it was related to a pivotal issue).

104. *E.g. Hobbs*, 403 F.2d at 978 (stating that the party who altered the photographic evidence had the burden of proving its accuracy).

105. *U.S. v. Ortiz*, 176 U.S. 422, 430 (1900).

106. *Hobbs*, 403 F.2d at 978.

107. *See e.g. Lowery v. Ill. Cent. Gulf R.R.,* 356 So. 2d 584, 585 (Miss. 1978) (noting that the introduced photographs were testified to by qualified individuals as being "fair and accurate representations" of the photographed location); *Nyce v. Muffley,* 119 A.2d 530, 532 (Pa. 1956) (stating that a photograph must be verified through the testimony of either the photographer or another sufficiently knowledgeable person that the photograph "fairly and accurately represents" the reproduced object or place).

One court described the shift in scrutiny regarding authentication standards for traditional photographs as follows:

This fair and accurate standard, which may be attested to by any witness, has gained widespread judicial acceptance as the current authentication standard for traditional photographic images.[108]

The "silent witness theory" has also developed as an alternative approach to authenticating traditional photographs.[109] This theory allows "photographs to substantively 'speak for themselves' after being authenticated by evidence that supports the reliability of the process or system that produced the photographs."[110] The silent witness theory originated in an early twentieth century case from Iowa.[111] The prosecution sought to admit an "x-ray photograph" to demonstrate the location of a bullet lodged near the victim's spine.[112] The defendant objected and argued that the x-ray was not admissible because no witness had personally seen the bullet and could testify that the picture was accurate.[113] The court took note of the skill level of the individual who took the x-ray and then, by judicial notice, recognized that photographs had independent value apart from the testimony of the witnesses.[114] The court allowed the x-ray photograph to enter as direct evidence.[115]

Whether a court applies the fair and accurate standard or the silent witness standard, the judicial standard is significantly more relaxed than the judicial hesitancy that marked the infancy

> Concerning any photographic operation only the most scholarly expert could testify as to the manner in which the original image is transmitted through the lens of the camera to the emulsion on the film or plate, the development of the latent image, the printing by a contact or projection process, and concerning the chemical procedures involved. Even where an occasional qualified witness may be available to testify as to such details such testimony would obviously be irrelevant and immaterial. What is material is what the rankest box camera amateur knows, namely that he "gets" what he sees. We thus come full circle to the judicial test . . . as being whether the proffered photograph is an accurate representation of the scene depicted.

Hobbs, 403 F.2d at 978–979.

108. *See* Witkowski, *supra* n. 65, at 280 (noting that, absent "evidence of tampering," the court typically applies the fair and accurate standard).

109. *E.g. Harris*, 55 M.J. at 438 (applying the silent witness theory standards to automated cameras).

110. *Id*. (quoting in part *McCormick on Evidence* vol. 2, 15–16 n. 15 (John W. Strong ed., 5th ed., West 1999)).

111. *State v. Matheson*, 103 N.W. 137 (Iowa 1905).

112. *Id*. at 138.

113. *Id*.

114. *Id*.

115. *Id*. at 139.

of photographic imaging. This pattern of cautiously decreasing judicial scrutiny is also true for traditional video[116] and sound recordings.[117] This trend is appropriate in these more traditional forms of electronic evidence because judges and jurors are more familiar with the underlying types of evidence.[118]

b. Digital Imaging Technology

The previous Section introduced the judicial movement towards relaxed authentication standards for the traditional forms of electronic evidence. This Section will explore the danger of inappropriately applying the traditional authentication standards to novel forms of digital and computerized evidence. Even though broad judicial discretion and relaxed standards for authentication are acceptable for forms of evidence that courts have routinely

---

116. *See Harris*, 55 M.J. at 438 (noting that "[a]ny doubt as to the general reliability of the video cassette recording technology has gone the way of the BETA tape."). One author has observed as follows:

> In fact, strict foundational requirements for video recordings "are now almost universally rejected as unnecessary. This departure from the strict foundational requirements for video evidence is a product of "the judicial system's growing familiarity with video evidence, and the widespread social, cultural, and technological acceptance of the medium.

Witkowski, *supra* n. 65, at 280 n. 53 (internal citations omitted).

117. In the instance of sound recordings, the *McKeever* factors were introduced in the late 1950s. *See* Witkowski, *supra* n. 65, at 276 (citing *McKeever*, 169 F. Supp. at 430). The seven *McKeever* factors are as follows:

(1) That the recording device was capable of taking the conversation now offered in evidence.
(2) That the operator of the device was competent to operate the device.
(3) That the recording is authentic and correct.
(4) That changes, additions or deletions have not been made in the recording.
(5) That the recording has been preserved in a manner that is shown to the court.
(6) That the speakers are identified.
(7) That the conversation elicited was made voluntarily and in good faith, without any kind of inducement.

McKeever, 169 F. Supp. at 430.

However, by the 1970s courts began abandoning the factors in favor of more discretion for the trial court. The Fifth Circuit reduced the authentication standard to a four-factor test and emphasized that the factors were guidelines and not a strict elemental test. *U.S. v. Biggins*, 551 F.2d 64, 66 (5th Cir. 1977). This relaxation of the strict elemental test was again reiterated by the Fourth Circuit in *United States v. Branch*, 970 F.2d 1368, 1371–1372 (4th Cir. 1992). For a more detailed analysis of authentication standards for sound recordings, see Witkowski, *supra* n. 65, at 276–279.

118. *See* Witkowski, *supra* n. 65, at 281 (referring to the general increase in computer usage and the corresponding liberalization of authentication standards for computer-generated evidence).

admitted, the digitized versions of these types of evidence should not be afforded the same degree of laxity.[119] Nonetheless, courts have often failed to recognize the effects that computer-generated processes may have on the underlying evidence. In *Almond v. State*,[120] the Georgia Supreme Court failed to recognize the implications of the digitizing process and held that digital photographs should be authenticated using the same principles applied to still-camera photographs.[121] The record indicated that the prosecution had authenticated the digital photographs through testimony that the pictures were "fair and truthful representations of what they purported to depict."[122] However, the defendant in this murder case argued that the trial court committed error in admitting these digital photographs.[123] Noting that the standard of review was abuse of discretion, the Court indicated that it was "aware of no authority . . . for the proposition that the procedure for admitting pictures should be any different when they were taken by a digital camera."[124] This holding set forth the dangerous but common precedent that digital versions of routinely accepted traditional evidence do not require additional scrutiny despite the fact that they are the result of new technological processes.

Another example of the improper application of traditional standards to digitally enhanced technology is *United States v.*

---

119. One author has described the differences between traditional and digital photography, and the evidentiary issues arising from these differences, as follows:

> Like the introduction of photography in the mid-nineteenth century, digital evidence creates evidentiary issues that lawyers and judges are unaccustomed to dealing with. Recent advances in microchip processing speed have dramatically increased the applications of computers for creating and manipulating images, and general improvements in computer technology have reduced the cost of hardware and software to the point where digital technology is widely available to the public. In fact, the need to address evidentiary issues of digital media is perhaps more compelling than it originally was for photography, where the means of production remained beyond the reach of the public for many years.

Buccafusco, *supra* n. 12, at 613–614 (internal citations omitted).

120. 553 S.E.2d 803 (Ga. 2001).

121. *Id*. at 805.

122. *Id*.

123. *Id*.

124. *Id*.; *see also Macaluso v. Pleskin*, 747 A.2d 830, 837 (N.J. Super. App. Div. 2000) (holding that computer-generated images of x-rays could be authenticated by testimony of the doctor who took the x-rays that the x-rays were a "fair and accurate depiction" even though the doctor could not testify about the computer process and the doctor did not participate in the digitization of the x-ray photograph).

Calderin-Rodriguez,[125] a 2001 Eighth Circuit case. The defendant argued on appeal that the foundational safeguards were not satisfied for the digitally enhanced sound recordings.[126] The Eighth Circuit cited the seven factors for the authentication of sound recordings and noted that none of the factors required that the witness understand the workings of the underlying technology.[127] Instead, the foundational factors simply required evidence that the machine was capable of functioning.[128] In deeming the digitally enhanced recordings admissible, the court continued,

> [w]e see no distinction between the foundation required for the tape recorder and that for the digital enhancement program, which, from the point of view of a listener, simply improves the quality of the recording. If the capacity for digital enhancement were built into the tape recorder itself, rather than a separate step being required, the admissibility of the resulting tapes would clearly be governed by *McMillan*. There is nothing in the use of this separate device that should change our analysis.[129]

The failure to review computer-generated evidence more strictly than its traditional predecessors is erroneous. Equally inappropriate is the assumption that all forms of computer-generated evidence are alike. As the *Swinton* Court later wrote,

> [T]he appearance of computer[-]generated evidence in our courts is becoming more common. Not only can we not anticipate what forms this evidence will take, but also common sense dictates that the line between one type of computer[-]generated evidence and another will not always be obvious.[130]

Both approaches ignore the fact that different kinds of digital evidence have different properties, such as alterability, that can se-

125. 244 F.3d 977 (8th Cir. 2001).

126. *Id*. at 986.

127. *Id*.; *see also supra* n. 117 (listing the seven *McKeever* factors for the authentication of sound recordings).

128. *Id*.

129. *Id*. (citing *U.S. v. McMillan*, 508 F.2d 101, 104 (8th Cir. 1974) (referring to the *McKeever* factors)).

130. *Swinton*, 847 A.2d at 938.

riously affect their reliability. This ignorance reveals premature judicial laxity. Such inattention is particularly significant in the context of visual imagery—evidence which studies have proved is dangerously seductive to juries.[131] Although such laxity can be explained by the general rise in America's use of digital equipment, it cannot be excused.

Courts should be hesitant toward new forms of digital evidence, and this hesitancy should translate into increased scrutiny in the analysis of authentication and other evidentiary foundations. In the dissenting opinion in *Perma Research and Development v. Singer Co.*,[132] Judge Van Graafeiland of the Second Circuit expressed the policy behind judicial cautiousness when dealing with digital evidence.[133] The *Perma* plaintiff built a case centered on expert testimony that resulted from computerized experimentation.[134] However, the plaintiff's computer expert would not testify as to the "proprietary" programming steps that he employed.[135] The district court and the majority of the appellate court found that the computerized evidence was still admissible.[136] However, Judge Van Graafeiland disagreed and opined that the trial court's ruling was "prejudicially erroneous."[137] In his dissent, Judge Van Graafeiland wrote the following comments on the policy of applying strict judicial scrutiny to newer forms of digital evidence:

> As courts are drawn willy-nilly into the magic world of computerization, it is of utmost importance that appropriate standards be set for the introduction of computerized evidence. Statements like those of the District Judge that a computer is "but calculators (sic) with a giant 'memory' and the simulations the computer produces are but the solutions to mathematical equations in a 'logical' order" represent an overly-simplified approach to the problem of computerized proof which should not receive this Court's approval. Al-

131. *See supra* nn. 59–63 and accompanying text (discussing studies of juror recall and how such findings have influenced the use of visual evidence in court).

132. 542 F.2d 111 (2d Cir. 1976).

133. *Id.* at 124–125 (Van Graafeiland, J., dissenting).

134. *Id.* at 124.

135. *Id.*

136. *Id.*

137. *Id.*

> though the computer has tremendous potential for improving our system of justice by generating more meaningful evidence than was previously available, it presents a real danger of being the vehicle of introducing erroneous, misleading, or unreliable evidence. The possibility of an undetected error in computer-generated evidence is a function of many factors: the underlying data may be hearsay; errors may be introduced in any one of several stages of processing; the computer might be erroneously programmed, programmed to permit an error to go undetected, or programmed to introduce error into the data; and the computer may inaccurately display the data or display it in a biased manner.[138]

Judge Van Graafeiland then encouraged judicial cautiousness when dealing with computer-generated evidence.[139] He then explained the policy behind stricter foundational requirements for such evidence as follows:

> [A] court should not permit a witness to state the results of a computer's operations without having the program available for the scrutiny of opposing counsel and his use on cross-examination. Moreover, such availability should be made known sufficiently in advance of trial so that the adverse party will have an opportunity to examine and test the inputs, program and outputs prior to trial. Long before the age of computers, the law was established that an expert witness might refer to records such as elaborate mathematical calculations, if, but only if, such records were made available for inspection by opposing counsel and thorough cross-examination thereon was permitted. Because of the computer's "ability to package hearsay and erroneous or misleading data in an extremely persuasive format" this rule should be strictly adhered to whenever expert testimony is predicated upon specially prepared computerized calculations or simulations. It is a mistake to liken the program of a computer to human calculation, because the program directs the performance of tasks that humans would not attempt, in a manner that they would not elect. An error in programming can be repeated time after time, and simulation with

138. *Id*. at 124–125.
139. *Id*. at 125.

> an incorrect program is "worse than worthless." For this reason, programming requires great accuracy, more than that needed in other types of engineering.[140]

That particular comment not only clarifies the need for stricter scrutiny, but it also mentions the importance of inputting, programming, and outputting. These three elements provide the basis of a second, more active approach towards authenticating computer-generated evidence.

C. Input, Processing, and Output as Helpful Guideposts in the Authentication of Digital Imaging Technologies

Many authentication factors and judicial movements have surfaced during the lifespan of digital evidence. This Section will discuss the constructive use of the three main components of the computer process—the input, the processing, and the output—to develop fundamental guidelines for the authentication of digital imaging and computer-generated evidence.[141] The incorporation of these three guideposts into authentication standards for digital imaging technologies comprises the second trend. This review will provide examples from the non-digital and digital technologies.

1. Non-Digital Evidence

The concept of properly authenticating the input, process, and output of electronic evidence existed prior to the digital era. A perfect example is a previously referenced case dealing with photographic images, *United States v. Ortiz*.[142] This 1900 United States Supreme Court case affirmed a lower court's admission of

140. *Id*. at 125–126 (internal citations omitted).

141. These three factors are reflected in the language of the Federal Rules of Evidence, which allow for authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." Fed. R. Evid. 901(b)(9). Processing can be defined as "any activity that transforms an input image into an output image." *Forensic Imaging and Multi-Media Glossary*, *supra* n. 4, at 124. Input can be defined as "[t]he terminals, jack or receptacle provided for the introduction of an electrical signal or electric power into a device or system" and output as "the means by which an image is presented for examination or observation." *Id.* at 128; *Digital & Multimedia Evidence Glossary*, *supra* n. 29, at 8; *see also Telex Corp. v. IBM Corp.*, 367 F. Supp. 258, 274 n. 25 (N.D. Okla. 1973) (defining input and output in the context of electronic data processing systems).

142. 176 U.S. 422 (1900).

an enlarged photograph because the photographer authenticated the photograph by testifying to the process pursued and to the final outcome of the enlargement methodology.[143]

These three guideposts—input, process, and output—may also be analogized to the foundational factors that were applied in the authentication of sound recordings.[144] Courts authenticated the input by assuring that the "operator of the device was competent to operate it" and that the "conversation . . . was made voluntarily and in good faith."[145] The courts authenticated the process by questioning whether the "the recording device was capable of taking the conversation."[146] Finally the court reviewed the output by reviewing the trustworthiness and accuracy of the recording, identifying the speakers, evaluating the manner of preservation manner, and verifying that "changes, additions or deletions have not been made."[147]

Utilizing factors that review the input, processing, and output procedures has provided helpful checks and balances for courts to assure that evidence has been properly authenticated. The need for these guidelines is even more overwhelming when dealing with digital imaging technologies.[148]

2. Digital Imaging Technologies

The first trend focused in part on the inappropriate use of judicial laxity towards digital imaging technologies; however, not all courts have openly accepted the introduction of digitized evidence. A few jurisdictions have adopted a more analytical stance, choosing instead to examine the processes and systems that generate such evidence.[149] This trend encourages the judiciary to focus specifically on the input of data into the computer system,[150]

143. *Id.* at 430.

144. For a discussion of the factors applied to sound recordings, see *supra* note 117, which lists the seven *McKeever* factors and reviews the historical trends in the application of these factors.

145. *McKeever*, 169 F. Supp. at 430.

146. *Id.*

147. *Id.*

148. This heightened need for factors examining input, processing, and output is justified because of the differences between traditional and digital photography. *Supra* n. 119.

149. *E.g.*, *Am. Oil Co. v. Valenti*, 426 A.2d 305 (Conn. 1979) (examining all stages in the generation of digital evidence to determine whether such evidence was admissible).

150. *Gosser v. Commw.*, 31 S.W.3d 897, 903 (Ky. 2000) (commenting in dicta that

the processing of the computer system, and the output produced by the computer system.[151]

The Court in *American Oil Co. v. Valenti* provided an early example of recognizing the importance of using standards that reflected a clear analysis of the input, processing, and output for computer-generated evidence.[152] The Connecticut Supreme Court encouraged courts to be cautious in finding a sufficient foundation for computer-generated evidence because of the possibility of errors and malfunctioning in the "input procedures, the data base, and the processing program."[153] Since the evidence in *American Oil* was a routinely prepared business record and not prepared in anticipation of litigation, the Court did not require strict scrutiny for the foundational requirements.[154] However, the opinion did define the importance of the judiciary's focus on the authentication factors of input, processing, and output when dealing with computer-generated evidence.

Almost two decades later, in *Bray v. Bi-State Development Corp.*,[155] the Missouri Court of Appeals faced the challenge of defining the proper identification standards for computer-generated evidence prepared in anticipation of litigation.[156] In *Bray*, the plaintiff alleged that the defendant, a parking garage owner, failed to light his garage adequately, causing the plaintiff's slip-and-fall injury.[157] The plaintiff appealed an adverse jury verdict and argued that the trial court abused its discretion in allowing a

"where a [computer-generated] diagram purports to contain exact measurements, to be drawn to scale, etc., then testimony as to how the data was obtained and inputted into the computer would be relevant and could be necessary to the admission of the diagram"); *see also Commercial Union Ins. Co. v. Boston Edison Co.*, 591 N.E.2d 165, 168 (Mass. 1992) (recognizing that the accuracy of the input is important in determining the admissibility of computer modeling programs).

151. Output may be defined as "the information as produced by the computer in a useful form, such as a printout of tax return information, a transcript of a recorded conversation, or an animated graphics simulation." *Swinton*, 847 A.2d at 942–943; *see also* Gregory P. Joseph, *A Simplified Approach to Computer-Generated Evidence and Animations*, 156 F.R.D. 327, 332–334 (2004) (providing checklists for the analysis of input, processing, and output); *see also* 57 Am. Jur. 3d *Proof of Facts* § 7 (explaining the use of input, process, and output as valid means of authenticating computer-generated evidence).

152. 426 A.2d 305 (1979).

153. *Id*. at 310.

154. *Id*. at 311.

155. 949 S.W.2d 93 (Mo. App. 1997).

156. *Id*. at 97.

157. *Id*. at 95.

computer-generated chart on the issue of lighting.[158] The defendant's expert witness was a civil engineer who had participated in the development of the garage's lighting scheme.[159] The expert testified as to the purpose of the software program, and that while he was capable of manually performing the calculation, it would be impractical because it would be a "tremendous amount of hand calculations."[160] In addition, the expert testified that although he did not personally prepare the exhibit, it was normal within his field to rely on the assistance of the manufacturer's representatives to produce the computer printout.[161] However, he had personally provided the input variables, and he was able to explain to the jury the process that the computer software utilized in generating the result.[162] Finally, the expert testified that he personally verified the computer's printout by testing actual light samples within the garage.[163] The plaintiff argued that this testimony did not establish a proper foundation for the defendant's software program; however, the trial court admitted it into evidence.[164]

The *Bray* court indicated the need to look to other jurisdictions for guidance because the Missouri courts had not yet established a guideline for the authentication of computer-generated evidence prepared in anticipation of litigation.[165] The court then analyzed the three factors that were initially outlined in a Massachusetts case: "(1) The computer is functioning properly; (2) The input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party, so that they may challenge them); [and] (3) The program is generally accepted by the appropriate community of scientists."[166] The court found that although these factors were helpful in providing a starting point for the authentication analysis, the factors were far from complete.[167] However, the court indicated that the majority of courts

158. *Id.*
159. *Id.* at 96.
160. *Id.*
161. *Id.*
162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.* at 97. For further discussion of computer-generated evidence prepared in anticipation of litigation, see *infra* notes 260–267 and accompanying text.
166. *Bray*, 949 S.W.2d at 97 (citing *Commercial Union*, 591 N.E.2d at 168).
167. *Id.* at 99.

have failed to provide a list of factors for the authentication of computer-generated evidence prepared in anticipation of litigation.[168]

Many other courts will also be forced to look to other jurisdictions for persuasive judicial analysis on authentication standards for digital imaging and other forms of computer-generated evidence. This is because such evidence has often gone unchallenged in courtrooms across America.[169] Even when the computer-generated evidence is challenged, many cases remain unpublished.[170] This information gap created the perfect opportunity for the Connecticut Supreme Court in *State v. Swinton*[171] to review the reported judicial opinions and the legal commentary, and then to create a synthesized analysis of the legal standards necessary for the authentication of digital imaging evidence.

IV. STATE v. SWINTON

In May 2004, the Connecticut Supreme Court set forth a comprehensive, fifty-four page opinion on the foundational requirements for evidence that was either generated or altered by a computer.[172] It is this case that will likely provide the guiding light for our nation's courts as they develop more exacting guidelines for the authentication of new technologies, especially digital imaging.[173] This Part first reviews the facts of the case. Then, it examines the court's legal analysis and holding. Finally, it concludes with a discussion of post-*Swinton* caselaw.

A. Factual Background

The defendant in the case, Alfred Swinton, was convicted and sentenced to sixty years in prison for the murder of twenty-eight-year-old Carla Terry.[174] Terry was last seen alive around 2:00

168. *Id.*
169. Azcarate, *supra* n. 6, at 28.
170. *See id.* (identifying only one published opinion on the issue).
171. 847 A.2d 921.
172. Molly McDonough, *Enhancing Rules for Digital Data: Connecticut's Top Court Lays Down the Law on Computer-Modified Evidence*, 3 (21) ABA J. E-Report (May 28, 2004).
173. *Id.*
174. *Swinton*, 847 A.2d at 927, 932.

a.m. on January 13, 1991.[175] Approximately three hours later, her partially dressed body was discovered wrapped in a brown garbage bag in a snow bank.[176] Paramedics tried unsuccessfully to revive the young woman and she was pronounced dead at a local hospital.[177]

The state deputy chief medical examiner, Edward McDonough, concluded that manual strangulation caused her death.[178] In addition to bruises and scratches on the victim's head, neck, and body, McDonough detected and photographed crescent-shaped contusions on each of her breasts.[179] He identified the contusions "as being consistent with bitemarks"[180] but, at the time, could not determine whether they were inflicted at or near the time of death.[181] McDonough conferred with a forensic odontologist,[182] Lester Luntz, who agreed that the bruises on the victim's breasts were indeed bitemarks.[183] Luntz made molds of the defendant's teeth pursuant to a warrant; however, it was not until five years after Luntz's death that another forensic odontologist, Constantine Karazulas, examined the molds.[184] Karazulas concluded that the defendant had made the bitemarks at or about the time of death.[185]

Circumstantial evidence also weighed in favor of the defendant's guilt, including brown garbage bags and various articles of the victim's clothing found in and around the defendant's home and car.[186] Additionally, police discovered a single edition of a newspaper in the defendant's residence dated the day that Terry

175. *Id*. at 927.
176. *Id*.
177. *Id*.
178. *Id*.
179. *Id*. at 928.
180. *Id*.
181. Gus Karazulas, *New Forensic Odontology Tools* 2 (unpublished paper, Conn. St. Police Forensic Sci. Lab, Mar. 28, 2001) (available at http://www.imagecontent.com/lucis/applications/forensics/New%20Forensic%20Odontology%20Tools.pdf).
182. "Forensic odontology is the application of the law to the field of dentistry. It includes the analysis of dentition and bitemarks for purposes of identification." *Swinton*, 847 A.2d at 928 n. 3.
183. *Id*. at 928.
184. *Id*.
185. Karazulas, *supra* n. 181, at 3.
186. *Swinton*, 847 A.2d at 928.

was killed.[187] The defendant also repeatedly made incriminating statements to coworkers and acquaintances.[188]

In June 1991, the defendant was arrested for the crime but the charges were dismissed for lack of probable cause.[189] He was arrested again in October 1998 and subsequently convicted.[190] An appeal to the Connecticut Supreme Court followed, and the Court delivered its opinion on May 11, 2004.[191] On appeal the defendant claimed five points of error;[192] however, the majority of the legal analysis in the opinion addressed the defendant's first alleged error regarding two forms of bitemark evidence.

B. The Contested Bitemark Evidence

The defendant challenged the admissibility of two pieces of evidence: (1) bitemark photographs that were enhanced with Lucis software; and (2) overlay images created with Adobe Photoshop software.[193] Specifically, the defendant claimed that the photographs and overlays, both of which the court categorized as computer generations,[194] were improperly admitted without an adequate foundation.[195] The following two Sections will review the factual background for the testimony related to this claim.

1. Lucis-Enhanced Photographs

During the trial, the State introduced multiple computer-enhanced images of bitemarks based on autopsy photographs.[196] Karazulas provided the original digital photographs and a software program titled Lucis that was used to create the enhancements.[197] The images were enhanced at Lucis' manufacturer's of-

187. *Id*.
188. *Id*. at 928–932.
189. *Id*. at 928 n. 5.
190. *Id*. at 928 n. 5, 932.
191. *Id*. at 932.
192. *Id*. at 927.
193. *Id*. at 932.
194. Regarding the Lucis-enhanced photographs, the court considered the images to be computer-generated because "a computer was both the process and the tool used to enable the enhanced photographs to be admitted as evidence . . . ." *Id*. at 938; *see also id*. at 951 n. 42 (coming to the same conclusion regarding the overlays).
195. *Id*. at 932.
196. *Id*. at 934.
197. *Id*.

fices because the Connecticut police lacked the necessary equipment.[198] Timothy Palmbach, the overseer of scientific services in the state's public safety department, explained the evidence.[199] His qualifications included extensive forensic experience and a master's degree in forensic science.[200]

According to Palmbach, Lucis was created in 1994 for "scientific applications," but specialists also used the program for forensic purposes.[201]

Palmbach discussed how he and Karazulas confirmed the accuracy of the enhancement process outside of the courtroom.[202] First, Karazulas produced a bitemark on his own arm.[203] Then, the two men photographed the mark, enhanced the photograph, and compared the original and enhanced images.[204]

In the courtroom, Palmbach provided an arguably more objective, and definitely less painful, demonstration of the accuracy of the enhancement process for the jury by using his laptop.[205] First, he scanned the original bitemark photograph into his computer, explaining that the scan converted the image into a collection of pixels.[206] Then, he selected a certain section of the image to enhance.[207] Finally, Palmbach defined "contrast ranges" through the manipulation of big and small cursors.[208] This last step allowed him to diminish extraneous layers of contrast and reduce "ultrafine detail" such that the cluttering effects of unnecessary detail were dissipated.[209] Once the cursors were set at particular values, the Lucis software performed a specific algorithm, called "differential hysteresis processing," which enhanced the selected

198. *Id.* at 934–935. Specifically, the enhancements were made at the New Britain, Connecticut offices of Image Content Technologies. *Id.* at 935. For more information about Image Content Technologies, visit the company's website at http://www.imagecontent.com.

199. *Swinton*, 847 A.2d at 934.

200. *Id*.

201. *Id*. at 935. For Palmbach's detailed description of how Lucis enhances detail by narrowing the band of contrast layers in an image, see *id*.

202. *Id*.

203. *Id*. at 935–936.

204. *Id*. at 936.

205. *Id*. at 935.

206. *Id*.; *see also id.* at 935 n. 15 (describing the process of scanning an image as a conversion into pixels, which are best analogized to "each colored dab of a pointillist painting").

207. *Id*. at 935.

208. *Id*.

209. *Id*.

section of the image.[210] The resulting enhanced image appeared in a "one-to-one," or life-size, format.[211]

Throughout his testimony, Palmbach asserted that the enhancement process did not remove or add anything from or to the original photograph.[212] Specifically, Palmbach claimed that the software did not produce any "artifacts," or artificial additions, during the enhancement process.[213] Furthermore, he stated that that he was unaware of any published error rates for the Lucis program.[214]

Although Palmbach spoke extensively about how the Lucis software functioned, he was not technically qualified as a computer programmer, an expert on Lucis, or an expert in software programs.[215] In fact, Palmbach admitted that he did not know how the computer distinguished between layers within an image, the exact details of the algorithm, or how the algorithm sorted through the multiple layers.[216]

2. Adobe Photoshop Overlays

The State also introduced overlays created with Adobe Photoshop wherein images of Swinton's bite pattern were superimposed over photographs of the bitemark found on Terry's breasts.[217] This evidence was offered through the testimony of Karazulas, who was admitted as an expert in forensic odontology.[218] At the time

210. *Id*. at 935 n. 16.

211. *Id*. at 935 n. 17.

212. *Id*. at 936.

213. *Id.* Palmbach defined an "artifact" as "an artificial component . . . [or] something that was never there to begin with." *Id.* at 936 n. 18. More technically, an artifact is "[a] visual/aural aberration in an image, video, or audio recording resulting from a technical or operational limitation . . . [including] speckles in a scanned picture or 'blocking' in images compressed using the JPEG standard." *Digital & Multimedia Evidence Glossary*, *supra* n. 29, at 3.

214. *Swinton*, 847 A.2d at 936.

215. *Id*.

216. *Id*.

217. *Id*. at 946.

218. *Id*. at 946–947. According to a paper that Karazulas authored in 2001, the forensic odontologist has examined over 5,000 bitemarks in his forty-year career. However, he maintains a cautious approach towards odontological evidence. For example, he wrote that out of the 5,000 bitemarks, in his opinion only 150 qualified as evidence. At that point in time he had only made about ten court appearances with regard to such data. Karazulas, *supra* n. 181, at 2.

that Karazulas received the case in June 1998,[219] he was the Chief Forensic Odontologist for the Connecticut State Police Forensic Science Lab, having previously served as an oral surgeon for the Connecticut State Prison System.[220]

Karazulas utilized many comparative techniques to establish that the defendant was the biter in this case.[221] These techniques involved the defendant's dental molds, unenhanced photographs of the marks, and, finally, the Adobe Photoshop overlays challenged in the appeal.[222]

The overlays were generated as follows.[223] First, Karazulas created a wax impression based on the models of the defendant's dentition.[224] The impression revealed the arch of the teeth, gaps between the teeth, the cutting edges of the teeth, and the width and length of each tooth.[225] It also showed the shape of the jaw, which teeth were tipped forward, and which teeth were located farther back in the defendant's mouth.[226] Next, Karazulas placed the defendant's upper and lower dental molds onto a photocopier and printed out a two-dimensional image of the molds.[227] Then, he placed a sheet of paper on top of the photocopied image and, "over a lighted surface, he manually traced out the biting edges of the teeth."[228] Karazulas photocopied this tracing onto a clear piece of acetate, which resulted in a transparent overlay.[229] The overlay depicted the edges of the defendant's teeth and, according to Karazulas, showed multiple unique characteristics, including two tipped incisors, two rotated cuspids, and numerous gaps between the teeth.[230]

---

219. The doctor also performed extensive testing to prove that the bitemarks were inflicted close to Terry's death. Specifically, the doctor showed that the color of the bruises from the bitemarks was similar to that of the strangulation marks and, since deceased bodies do not heal, the two sets of contusions must have been made at or about the same time. Karazulas, *supra* n. 181, at 2–3.

220. *Id*. at 2.

221. *Swinton*, 847 A.2d at 947.

222. *Id*.

223. *Id*.

224. *Id*.

225. *Id*. at 947 n. 35.

226. *Id*.

227. *Id*. at 947.

228. *Id*. at 947–948.

229. *Id*. at 948. Note that some of the additional tracings were made with a computer scanner instead of a copy machine. *Id*. at 948 n. 36.

230. *Id*. at 948 n. 37.

Karazulas then enlisted the help of Gary Weddle, a chemistry professor from Fairfield University.[231] Karazulas told the jury that he instructed Weddle not to modify the original images during the superimposition process.[232] Weddle scanned tracings of the defendant's dentition, enhanced photographs of the bitemark, and unenhanced photographs of the bitemark into a computer.[233] Next, Weddle used the Adobe Photoshop software to superimpose the defendant's bite pattern over the bitemark.[234]

According to Karazulas's testimony, Weddle generated several such superimpositions, or overlays.[235] There were essentially two groups of overlays.[236] The first included overlays wherein tracings of the defendant's bite pattern were superimposed over unenhanced and enhanced, cropped photographs of the bitemark.[237] The State offered two exhibits that fell under this category.[238]

The second group included overlays wherein images of the defendant's actual teeth were superimposed over the bitemark photographs.[239] To create the overlays in this second category, portions of the defendant's dental molds were scanned to create another exhibit.[240] Next, the computer software isolated "the upper layers of the occlusal edges of the molds from the images."[241] Then, a process was used wherein the images of the teeth became more transparent and less opaque.[242] Finally, this translucent image of the defendant's teeth was superimposed over different bitemark photographs.[243] The State offered multiple exhibits in this category.[244]

231. *Id*. at 948. Despite his involvement, Weddle did not testify at trial and, according to the record, no reason was given for his absence. *Id*. at 948 n. 38.

232. *Id*. at 948.

233. *Id*.

234. *Id*.

235. *Id*.

236. *Id*.

237. *Id*.

238. *Id*.

239. *Id*.

240. *Id*.

241. *Id*. at 948. Occlusal edges refer to the grinding or chewing surface of the back teeth. Quality Dentistry, *Dental Terminology*, http://www.qualitydentistry.com/dental/terms.html (accessed Aug. 14, 2007).

242. *Swinton*, 847 A.2d at 948.

243. *Id*.

244. *Id*.

Karazulas used these processes to conclude that the defendant inflicted the wounds found on the victim's breasts.[245] To demonstrate this point, the opinion included several quotes from the odontologist as he testified about the superimposed images.[246] However, it should be noted that Karazulas did not scan the images himself nor generate the superimpositions "[b]ecause he was not familiar with Adobe Photoshop, and was using the program for the first time for an odontological match."[247] However, he did spend about seven to eight hours watching Weddle create the overlays.[248]

C. The *Swinton* Analysis: Authentication of Computer-Generated Evidence

After a thorough examination of the factual predicate of the case, the Court reviewed many alternative arguments and legal theories before announcing the standard for Connecticut courts in determining the authentication of computer-generated evidence.[249] The Court indicated the significance of this legal precedent when it wrote, "[w]hat exactly is required in the context of computer[-]enhanced and computer[-]generated evidence . . . presents an issue of first impression in Connecticut."[250] This Section highlights the important portions of the *Swinton* Court's analysis. In particular, it discusses the following three issues: (1) the importance of a clear understanding of the relevant terminology in the context of computer generations; (2) a six-factor test for authentication, both in general and in the context of the contested bitemark evidence; and (3) constitutional and testimonial considerations.

245. *Id*.
246. *Id*. at 948–949.
247. *Id*. at 948.
248. *Id*.
249. *Id*. at 933. Although the Court started its analysis with the *Daubert* factors, it concluded that *Daubert* was a threshold determination for admissibility and not a catch-all test for all of the evidentiary hurdles. *Id* at 933. In particular, the *Daubert* factors were insufficient for the authentication of computer-generated evidence required by the Confrontation Clause of the United States Constitution and the Connecticut Constitution. *Id*. at 933–934.
250. *Id*. at 934.

1. Understanding the Terminology

The Connecticut Supreme Court had a significant task in properly defining and explaining many confusing concepts, since the *Swinton* case was dealing with issues of first impression. The Court started its analysis by clarifying some of the definitions and evidentiary categories appropriate to computer-generated evidence.[251] Specifically, the Court looked at whether the computer-generated evidence was illustrative or demonstrative in nature.[252] Next, the Court analyzed the differences between the broad categories of computer-generated evidence: business records and evidence prepared in anticipation of litigation.[253] The Court then defined two popular types of evidence prepared in anticipation of litigation: animations and simulations.[254] Finally, the Court highlighted the importance of reliability in the authentication process.[255] This Section reviews these categorical and definitional issues, concluding with the Court's analysis of reliability.

a. Illustrative v. Demonstrative

The Court needed to decide whether the contested computer-generated evidence (the enhanced photographs and the overlays) was illustrative or demonstrative in nature. The State argued that the computer-generated evidence was solely intended to illustrate the expert opinion and that the evidence had no independent evidentiary value.[256] The Court rejected this argument and classified the contested evidence as demonstrative.[257] Definitely, demonstrative evidence is not exclusively intended to illustrate a witness' testimony; instead, it is a "pictorial or representational communication" that is actually integrated into the "testimonial evidence."[258] The simple fact that the record reflected that these computer generations were entered into evidence allowed

251. *Id*. at 936–937.
252. *Id*. at 936 n. 20.
253. *Id*. at 938–939.
254. *Id*. at 937.
255. *Id*. at 942–943.
256. *Id*. at 936 n. 20.
257. *Id*.
258. *Id*.

the Court to conclude that the proper categorization was demonstrative rather than illustrative.[259]

b. Business Records v. Evidence Prepared in Anticipation of Litigation

The parties debated whether the contested evidence should be classified as computer-generated evidence. At the time of this case there was no clear definition of the term "computer-generated."[260] In fact, the Court listed several cases that failed to categorize the underlying evidence as a computer generation even though it would have classified the evidence as such.[261] The Court generically defined computer-generated evidence as evidence that was created using a computer as both the "process and the tool."[262] This broad definition included photographs that were enhanced through the use of a computer.[263]

The Court then split computer-generated evidence into two broad categories: business records and evidence prepared in anticipation of litigation.[264] Computerized business records, a well-recognized hearsay exception, have fewer admissibility issues because the reliability can be "extrinsically established" through a business' reliance on the computer generations.[265] However, computer generations that are created within a potentially adversarial context do not share the same reliability safeguards as com-

259. *Id.* Illustrative evidence is subject to different evidentiary considerations than demonstrative evidence. *Compare* Fed. R. Evid. 611(a) (setting forth a standard of broad judicial discretion with regard to illustrative evidence by allowing the court to exercise "reasonable control over the mode . . . [of] presenting evidence") *with* Fed. R. Evid. 901 (requiring that a predicate of authentication or identification be fulfilled before allowing for admission of demonstrative evidence). In *Verizon*, the court sets forth the six following categories of "Computer-Generated Pedagogical Devices" that it deemed to be illustrative evidence: (1) static images projected onto a larger screen; (2) animations; (3) simulations; (4) computer models; (5) enhanced images; and (6) easel writings or attorney notations made at trial in an automated format. 331 F. Supp. 2d at 137–138. The court also observed that while computer-generated evidence was traditionally considered illustrative, courts are increasingly deeming it demonstrative and, therefore, requiring a showing of accuracy and reliability as a predicate to admission. *Id.* at 141–144.

260. *Swinton*, 847 A.2d at 937.

261. *Id*. at 938.

262. *Id*.

263. *Id*.

264. *Id*. at 939.

265. *Id*.

puterized business records.[266] Therefore, the *Swinton* Court aimed to provide guidance on authentication issues for computer generations that were prepared in anticipation of litigation.[267]

c. Animations v. Simulations

Within the category of evidence prepared in anticipation of litigation, some jurisdictions choose to divide such evidence into the two following subcategories: animations and simulations.[268] The *Swinton* Court found that "[t]he evidence at issue in the present case does not fall cleanly within either category,"[269] and therefore decided to "reserve judgment on the validity of these two categories of computer[-]generated evidence, as such, and withhold [its] agreement as to the merits of this bifurcated approach."[270] The Court felt that one standard that focused on reliability would be sufficient for this category of computer-generated evidence, and it disagreed with suggestions that "mischief" would result from the failure to differentiate between simulations and animations.[271]

d. Reliability

Although the Court had difficulty finding judicial opinions on point, the Court turned to statutory law and caselaw from a variety of jurisdictions that were analogous in some degree to the underlying issues in *Swinton*.[272] In looking at the cases, the Court

266. *Id*.

267. *Id*.

268. *Id*. at 937. The *Verizon* court defined animations as

> moving pictures. The computer allows otherwise static images to be "shown in rapid succession to create the [illusion] of motion." The graphics are often crude or oversimplified. Animations are not intended "to recreate or simulate an event."

331 F. Supp. 2d at 137–138 (internal citations omitted). *Verizon* defined simulations as

> [c]omputer functions [that] allow the user to simulate actual events—or, more properly, the opinion of the creator as to the nature of the events. Most simulations are detailed and realistic. The recreated computer image of the event can be manipulated. It can be portrayed from different angles or from the viewpoints of different witnesses. A common use involves the recreation of accidents.

Id. at 138.

269. *Swinton*, 847 A.2d at 937.

270. *Id*. at 937 n. 21.

271. *Id*. at 945.

272. *See id*. at 938–942 (listing and analyzing caselaw from other jurisdictions as well as discussing the federal rules).

primarily focused on the degree of reliability that the various tests offered because the Court found that reliability was a central focus in the authentication process.[273] The Court made specific note of the following eight areas where reliability could be problematic when dealing with computer-generated evidence: (1) the underlying data; (2) the inputting of the data into the computer system; (3) the hardware of the computer; (4) the software on the computer (i.e., the programmed instructions); (5) the processing of the instruction (i.e., the transformation of the input into the output—usually by calculating, transforming, sorting, storing, and/or retrieving the data); (6) the output itself; (7) the security controls that manage computer access; and (8) human errors that may occur during input, processing, or output.[274]

After reviewing the important definitions related to computer-generated evidence and having a clear understanding of the "watchword" principle of reliability,[275] the Court was prepared to announce a factorial list for the authentication of computer-generated evidence.

2. Authentication Principles: In General and as Applied

The Court analytically announced an authentication standard for computer-generated evidence. The Court then applied these factors to the two pieces of contested evidence: the Lucis-enhanced photographs and the Adobe Photoshop overlays. This Section reviews the six authentication factors and the Court's related precautionary concerns. It also examines the factors as the Court applied them to the contested evidence.

---

273. *Id*. at 942.

274. *Id*. at 942–943 (citing Robert Garcia, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. Rev. 1043, 1073 (1991)). Reliability concerns regarding computer-generated evidence are often summarized with the axiom "garbage in, garbage out," which can be defined as

> [a] computing axiom meaning that if the data put into a process is incorrect, the data output by the process will also be incorrect. In forensic applications this refers to the fact that the ability to enhance an audio file, a photograph, or a video file is limited by the quality of the input file. If the quality of the original multimedia evidence is so poor, it will be impossible to significantly enhance the evidence.

Forensic Imaging and Multi-Media Glossary, *supra* n. 4, at 107.

275. *Swinton*, 847 A.2d at 942.

The Connecticut Supreme Court adopted the following six factors for the authentication of computer-generated and computer-enhanced evidence:

> (1) the computer equipment is accepted in the field as standard and competent and was in good working order, (2) qualified computer operators were employed, (3) proper procedures were followed in connection with the input and output of information, (4) a reliable software program was utilized, (5) the equipment was programmed and operated correctly, and (6) the exhibit is properly identified as the output in question.[276]

The Court stressed the importance of the trial court's discretion while applying these factors.[277] Specifically, the factors were neither intended to lessen the trial court's discretion nor meant as "a mechanical, clearly defined test with a finite list of factors."[278] Instead, the factors were anticipated to be helpful guideposts in deciding tough admissibility issues.[279]

After defining the rule of law and expounding on the trial court's discretion in applying the rule, the Court began to apply the rule of law to the following contested digital evidence: (1) the Lucis-enhanced photographs of bitemarks, and (2) the Adobe Photoshop generated exhibits of bitemarks.

a. Lucis-Enhanced Photographs

The first piece of evidence under appellate review was the computer-enhanced images of a bitemark found during the victim's autopsy.[280] As previously discussed, these digital photographs were entered into evidence through the testimony of Palmbach, a forensic scientist.[281] The Court applied the six factors listed above to the testimony of the forensic scientist regarding

276. *Id*. (citing Christopher B. Mueller & Laird C. Kirkpatrick, *Evidence: Practice under the Rules* § 9.16 (2d ed., Aspen 1999)).

277. *Id*. at 943.

278. *Id*.

279. *Id*.

280. *Id*. at 934. *See supra* nn. 196–216 and accompanying text (discussing the factual background and testimony related to the bitemark photographs).

281. *Id*. at 934–935.

the digitally enhanced bitemark photograph.[282] The Court explicitly discussed the first four factors and held that the prosecution sufficiently authenticated the digital enhancements of the photograph of the bitemark.[283]

First, the Court was satisfied that the computer equipment used was standard equipment in the field based on Palmbach's testimony that the Lucis program was "relied upon by experts in the field of pattern analysis."[284] Second, Palmbach's testimony regarding his training and experience as a forensic analyst, coupled with Karazulas' presence throughout the enhancement process, clearly established that a qualified computer operator produced the enhancement.[285] Third, Palmbach provided detailed testimony that the Court found sufficient to establish that proper input and output procedures were followed.[286] Fourth, the Court accepted that Lucis was a reliable software program.[287] This conclusion was based on Palmbach's testimony regarding the program's error-reducing features, as well as Palmbach's personal test of its accuracy by making a known exemplar by subjecting the bitemark Karazulas made on his own arm to enhancement.[288]

Neither of the final two factors was discussed explicitly in the opinion.[289] In totality, however, the record reflected that Palmbach provided sufficient detail in his testimony to properly authenticate the Lucis-enhanced photograph.[290]

b. Adobe Photoshop Overlays

This second portion of the Court's opinion dealt with Karazulas' testimony on the odontological evidence "created" through

282. *Id*. at 942–943.
283. *Id*. at 943.
284. *Id*.
285. *Id*. at 943–944.
286. *Id*. at 944.
287. *Id*.
288. *Id*.
289. *See supra* n. 276 and accompanying text (listing the six factors).
290. *Swinton*, 847 A.2d at 944. The Court noted that "[a]lthough [the expert] admitted that the algorithm itself was programmed by someone who 'knows a lot more about computers' than he did, our review of the record reveals that [the expert] had sufficient knowledge of the processes involved in the enhancement to lay a proper foundation." *Id*. at 944–945.

Adobe Photoshop.[291] His testimony was based on four levels of bitemark comparison: (1) molds that demonstrated unique characteristics; (2) regular photographs that allowed the deduction of the victim and assailant's positioning; (3) a comparison of the molds and the photographs; and (4) Adobe Photoshop-enhanced overlays.[292] It is this last form of evidence that the defendant claimed an insufficient foundation.[293] The Court used the same six factors, but this time came to the opposite conclusion.[294] The Court found Karazulas' testimony insufficient for proper authentication because he was unable to testify to the five following important elements: (1) whether the use of Adobe Photoshop to create overlays was accepted in the odontological field; (2) whether proper protocols had been utilized in inputting and outputting the data; (3) whether Adobe Photoshop was a reliable program when dealing with bitemark identification in a forensic setting; (4) whether the underlying equipment was properly programmed and operated; and (5) the qualifications of the individual who created the overlays.[295]

The Court took issue with this illusory "expert" testimony when it came to the Adobe Photoshop overlays.[296] Although the expert was acknowledged to be an expert in odontological identification, the Court found that he lacked the necessary "computer expertise" to allow the defendant to find answers to questions about the program's reliability on cross-examination.[297] Therefore, the Court held that the trial court acted improperly when it admitted the overlays from the Adobe Photoshop software.[298]

3. Testimonial and Constitutional Considerations

Another issue of first impression on which the *Swinton* opinion provided needed guidance was whether certain qualifications were necessary for the person testifying during the authentication

291. *Id*. at 946; *see supra* nn. 217–248 and accompanying text (discussing the factual background and testimony related to the Adobe Photoshop-enhanced overlays).

292. *Id*. at 947–948.

293. *Id*. at 949.

294. *Id*. at 950.

295. *Id*. at 950–951.

296. *Id*. at 951–952.

297. *Id*. at 952.

298. *Id*.

process.[299] The issue of proper qualifications of an authenticating witness gains importance from the defendant's constitutional right to confront a witness.[300] This Section will review the two arguments presented in the *Swinton* opinion along with the holding of the *Swinton* Court. This Section will also briefly review some of the constitutional issues that arise from the use of an inappropriate witness.

The issue of proper qualifications was first addressed in the *Swinton* opinion during the discussion of the Lucis-enhanced photographs. The defendant argued that the computer-enhanced images should require similar authentication standards to those applied to composite pictures,[301] whereas the prosecution argued that the foundational requirements should be similar to those of photographs.[302] The defendant cited the following authentication standard for composite pictures: "[t]he moving party must present witnesses with firsthand knowledge of how the composite was prepared and of how accurately it portrays that which it is intended to depict."[303] The State disagreed with the defendant's analogy to composite photographs and argued that the standard should be analogous to the following standard utilized for photographs: a "witness competent to verify it as a fair and accurate representation of what it depicts."[304] The State highlighted the fact that the witness does not have to be the actual photographer; therefore, the State argued that the computer programmer should not be a necessary witness for an enhanced photograph.[305]

---

299. *Id*. at 934.

300. A criminal defendant's right to confront the witnesses against him is found in the Sixth Amendment to the United States Constitution. *See supra* nn. 89–90 and accompanying text (discussing the relationship between authentication standards and the Confrontation Clause).

301. Composite pictures can be described as

> pictures that are electronically built up using multiple layers to hopefully produce convincing looking fake pictures. This technique is a computer version of using scissors to cut out parts of one picture to paste into another. It is effectively an electronic version of collage making. Composites are used to supplement a reconstruction wherever authentic visual material is not available.

Loose Cannon Productions, *Composite Pictures*, http://www.recons.com/glossary/composites.htm (accessed May 17, 2007).

302. *Swinton*, 847 A.2d at 936–937.

303. *Id*. at 936 (quoting *State v. Weidenhof*, 533 A.2d 545, 551 (Conn. 1987)).

304. *Id*.

305. *Id*. at 937.

The Court reviewed caselaw where the contested evidence was enhanced and found "that the technician or analyst who testified was the person who had engaged in the enhancement process and was capable of testifying in specific detail as to the process."[306] The Court compared the enhanced-evidence standard to the controlling law for computer-generated evidence in Connecticut requiring the "testimony [of] a person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer."[307] In defining the proper standard for the computer-generated evidence in this case, the Court found that "this standard does not dictate that the *only* person capable of such expertise is the programmer of the software."[308]

The *Swinton* opinion represents a perfect situation where one expert was sufficiently involved in the enhancement and well versed in the details of the underlying program, while the other expert witness was a bystander in the generation process and unable to provide even basic testimony about the workings of the software program. The first expert's testimony was sufficient to authenticate the computer-enhanced evidence even though he admitted that he was not the computer programmer, while the other expert's testimony was not sufficient to authenticate the computer-generated odontological exhibits even though he was an expert odontologist.

The constitutional discussion concluded with a discussion on the distinctions between a constitutional error and an "evidentiary impropriety."[309] The defendant argued that a constitutional error[310] arose from the failure to properly authenticate the Adobe Photoshop exhibit, thereby denying him his right to adequately

306. *Id*. at 941.

307. *Id*.

308. *Id*. According to the SWGIT Guidelines, while "[t]he person who performed the processing is best qualified to testify about the techniques used, there may be occasions where the court will require the assistance of additional subject-matter experts." SWGIT, *supra* n. 16, at 9. These guidelines also detail that photographers, technicians, and analysts are all possible candidates for performing the techniques required for image processing; however, the key is to make sure the person doing the image analysis is properly trained. *Id.* at 9–10.

309. *Swinton*, 847 A.2d at 934.

310. In this case, the right of confrontation was guaranteed by not only the federal but also the state constitution. *Id*.

cross-examine a witness.[311] When the Court reviewed the record it found that the defendant effectively discredited the Adobe Photoshop exhibits through the testimony of his own expert witness.[312] Since the defendant had an opportunity to discredit the Adobe Photoshop software, the trial court's error was evidentiary in nature and did not rise to the level of a constitutional error.[313] Additionally, in light of all the other circumstantial evidence, the trial court's evidentiary error was harmless.[314]

D. Post-*Swinton* Analysis of Computer-Generated or Computer-Enhanced Images

As of the publication of this Article, it has been a little over three years since the May 2004 decision in *Swinton*, and the impact of this significant decision has been relatively minor. Although, at the time of this writing, ten reported cases have referenced *Swinton*,[315] most of the citing cases were about secondary issues unrelated to authentication of digital images.[316] This raises two important questions. First, are courts still allowing computer-generated digital evidence without adequate foundational safeguards in place?[317] Second, are the advocates or the judiciary to blame for the failure to proceed cautiously with digital imaging evidence? An appellate court decision from New Jersey, *Rodd v.*

311. *Id*.
312. *Id*. at 954–955.
313. *Id*. at 955.
314. *Id*.
315. These ten cases are: *Barry v. Quality Steel Prods.*, 905 A.2d 55, 67 n. 17 (Conn. 2006); *St. v. Sawyer*, 904 A.2d 101, 115 (Conn. 2006); *St. v. Carpenter*, 882 A.2d 604, 626, 642, 646 (Conn. 2005); *St. v. Lasaga*, 848 A.2d 1149, 1156 (Conn. 2004); *Emigrant Mort. Co. v. D'Agostino*, 896 A.2d 814, 827 (Conn. App. 2006); *St. v. Kelsey*, 889 A.2d 855, 864 (Conn. App. 2006); *St. v. Hamlin*, 878 A.2d 374, 379 (Conn. App. 2005); *St. v. John M.*, 865 A.2d 450, 458 (Conn. App. 2005); *Rodd v. Raritan Radiologic Assocs., P.A.*, 860 A.2d 1003, 1012 (N.J. Super. App. Div. 2004); *Cmmw. v. Serge*, 896 A.2d 1170, 1178 (Pa. 2006).
316. *E.g. Barry*, 905 A.2d at 67 n. 17 (evaluating the admissibility of traditional photographs and citing *Swinton* for the broad proposition that in order to lay a proper evidentiary foundation, a witness must testify that the photograph is "a fair and accurate representation of the conditions").
317. *See e.g. Almond v. State***,** 553 S.E.2d 803, 805 (Ga. 2001) (holding that the procedures for admitting photographs taken by a digital camera into evidence are the same as those for admitting traditional photographs).

Raritan Radiologic Associates, P.A.,[318] provides some guidance to these intriguing questions.

Six months following the *Swinton* decision, a New Jersey appellate court reversed and remanded a wrongful death jury verdict in a medical malpractice case against a radiologist based on an improperly admitted computer-generated exhibit.[319] The defendant radiologist used a magnifying glass to examine the x-ray images from the decedent's 1997 and 1998 mammograms and found them negative for cancer.[320] In 1997, the defendant found that the calcifications were widely distributed and that none of the calcifications appeared overly suspicious.[321] The defendant suggested that the decedent return in one year for a follow-up appointment.[322] During the 1998 examination, the defendant found that the calcifications were still widely distributed, and he attributed this distribution to a preexisting disease.[323] The decedent's discovery of a lump in her breast led to a diagnosis of cancer in 1999 and eventually her death in 2002.[324]

In an effort to aid the jury in distinguishing the finer details of the x-ray photographs, the plaintiff digitized and super-magnified the selected portions of the contested x-rays.[325] These super-magnified images were then projected on a six by eight foot screen.[326] The defendant objected to the plaintiff's computer-generated exhibit on the grounds of untimely disclosure, inadequate disclosure, and the potential for distortion and confusion.[327] However, the trial judge permitted the use of the exhibit.[328] The judge also denied the defendant's motion for a new trial.[329] The trial judge reasoned that the enlarged x-ray images not only helped the jurors understand the complicated factual scenario,

318. 860 A.2d 1003.
319. *Id*. at 1012.
320. *Id*. at 1006.
321. *Id*.
322. *Id*.
323. *Id*.
324. *Id*.
325. *Id*.
326. *Id*.
327. *Id*. at 1006–1007.
328. *Id*. at 1007.
329. *Id*. at 1008.

but were also an improvement to the entire radiological field as follows:

> The message may get—get out now, that in radiology, and I know the radiologist is under awesome pressure reading these films, that maybe they ought to blow it up like that. . . . [M]aybe the whole industry is negligent. Maybe in this case, something ought to be done . . . maybe this message is gonna get out . . . it seems, to me, to be very simple and very easy to implement, in a radiology group, blowing it up on a screen.[330]

The defendant appealed the adverse trial judgment based on several points of error.[331] However, it is the trial court's errors related to the admission of the unauthenticated computer-generated digital image, coupled with the appellate court's analysis of those errors, that are of importance to the development of stricter standards for the authentication of digital images.

The appellate court highlighted that the plaintiff's malpractice claim focused on an "error in visual observation."[332] Therefore, the appellate court found reversible error because the visual aid potentially distorted the contested images and because the court failed to instruct the jury that the enlarged images were intended for demonstration purposes only, not testimonial purposes.[333] The court found that there was potential for juror confusion when the plaintiff repeatedly argued that the cancerous cluster was obvious from visually inspecting the super-magnified image where the standard of care among radiologists required only visual inspection with a 2.5-power magnifying lens.[334] A reasonable juror might have been persuaded to apply an inappropriate standard of care, one based on a super-magnified image, because of both the court's lack of clear instruction regarding the purpose of the digitized image and the plaintiff's continual focus on the super-magnified image.[335]

---

330. *Id.*

331. *Id.* at 1008–1009.

332. *Id.* at 1010.

333. *Id.* at 1010; *see also supra* nn. 256–259 and accompanying text (explaining the distinction between illustrative/pedagogical evidence and demonstrative evidence).

334. *Id.* at 1011.

335. *Id.* at 1011.

As an important side note, the court also found reversible error based on the plaintiff's use of an expert witness who had not participated in the creation of the digital exhibit.[336] The appellate court was persuaded to follow *Swinton* in holding that the computer-generated digital evidence was distinguishable from its photographic counterparts.[337] This part of the appellate court's opinion focused on who should testify as to the authenticity of the digitized evidence.

The appellate court found that authentication of computer-generated evidence required the testimony of an individual with a sufficient background in the specific computer technology employed to create the evidence.[338] The court illustrated that this was a distinction from authentication rules of photographic images.[339] A cursory review of the plaintiff's expert's testimony revealed several deficiencies. First, the expert did not participate in the creation of the x-ray photograph or the digital projection.[340] Second, the expert was not present during the original x-ray, nor was he present during the magnification/digitization of the x-ray picture.[341] Third, the expert did not offer testimony about the input process (scanning) or the operation of the computer program.[342] Fourth, the expert was basically unaware of any circumstantial events that occurred during the creation of the digitized images.[343] Finally, the expert was unaware of the exact specifications of the final output (actual level of magnification).[344] The expert's inability to properly authenticate the exhibit, coupled with its potentially confusing and unduly influential nature, led the *Rodd* court to reverse and remand the trial court's decision.[345]

Other courts should follow the examples of *Swinton* and *Rodd* and find reversible error when the scrutiny applied to digital evidence lacks the appropriate reliability safeguards. As courts and

336. *Id*. at 1010; *see also supra* nn. 89–90 and accompanying text (detailing the testimonial and constitutional considerations involved in the authentication of evidence).
337. *Id*. at 1011–1012.
338. *Id*. at 1012.
339. *Id*. at 1011–1012.
340. *Id*. at 1011.
341. *Id*.
342. *Id*.
343. *Id*.
344. *Id*.
345. *Id*. at 1012.

advocates begin to recognize the potential for manipulation in digital and computer-generated evidence, the *Swinton* analysis will offer great support not only to advocates in selecting expert witnesses and preparing testimony but also to the judiciary in deciding tough authentication issues. These issues are ripe for judicial analysis because digital photography and computer-generated evidence are quickly replacing more traditional forms of evidence.[346] Although trial courts have generally favored the admissibility of digital evidence,[347] this is not necessarily in the best interests of the truth-seeking process. One scholar said that "[t]here have been relatively few challenges to the use of digital technology as evidence and in most of them the courts have looked at them in a fairly superficial way."[348] Other courts can use the principles outlined in *Rodd* and *Swinton* to adequately assess authentication challenges and to ensure the reliability of digital evidence—a field which continually expands as new technologies emerge.

V. THE SWINTON *SIX APPLIED TO VIRTUAL AUTOPSIES*

As *Rodd* illustrates, the principles enumerated in *Swinton* apply to all forms of computer-generated images, not just photographs or overlays. Thus, *Swinton* can also be applied to virtual autopsies, a promising new development in digital forensics.[349] This Section defines the virtual autopsy technique, including its benefits and drawbacks. Then, the six *Swinton* factors (the "*Swinton* Six") are applied to the virtual autopsy process. This analysis, though purely theoretical, incorporates both practical and testimonial considerations.

346. *See generally* CNN, *Digital Evidence: Today's Fingerprints*, http://www.cnn.com/2005/LAW/01/28/digital.evidence/index.html (Jan. 31, 2005) (examining how digital evidence is becoming increasingly common in criminal trials).

347. CNN, *Digital Evidence Raises Doubts* ¶ 13, http://www.cnn.com/2004/TECH/ptech/02/10/digital.evidence.ap/index.html (Feb. 10, 2004).

348. *Id.* at ¶ 14.

349. *See generally* Jacqueline Flowers, *Virtual Autopsy Provides Cutting-Edge Forensic Identification Techniques*, 163 Armed Forces Inst. Pathology 3 (Spring 2005) (available at http://www.afip.org/images/public/Spring2005.pdf) (describing how the United States military employs virtual autopsies to conduct more accurate research regard combat casualties); Jessica Snyder Sachs, *Why Give a Dead Man a Body Scan?* 265 Pop. Sci. 50 (Oct. 2004) (describing how forensic pathologists in Switzerland use body scanners to conduct virtual autopsies).

A. Definition of Virtual Autopsies

In the most general sense, virtual autopsies are an example of diagnostic radiology, which is itself not a new discipline.[350] The term "diagnostic radiology" refers to the "the study of images of the internal structures of the human body" as applied in criminal and civil law.[351] The use of radiology in the field of forensics began within a few months of Wilhelm Roentgen's initial discovery of x-rays in November 1895 when x-ray images of a bullet lodged in a victim's leg were utilized in the successful prosecution of the shooter.[352] Since that time, radiology has been used in the forensic context to identify bodies via dental records,[353] examine physical evidence,[354] detect signs of abuse,[355] and investigate drug trafficking.[356] Even the United States military has utilized this methodology.[357] Medical examiners in the Department of Defense have used conveyor belts to move war casualties through x-ray scanners to check for shrapnel, bullets, and undetonated explosives.[358]

The legal challenges and guidelines for traditional unaltered radiological evidence, including the rule for authentication, are fairly well established.[359] However, virtual autopsies go a step further than traditional technology by using a sophisticated combination of radiological imaging technologies to generate digital

350. *See generally* B.D. Brogdon & Joel E. Lichtenstein, *Forensic Radiology* ch. 2 (CRC Press 1998) (detailing the discovery of x-rays and their early implementation as exhibits in civil and criminal trials).

351. *Id.* at 4.

352. Victorian Inst. Forensic Med., *Forensic Radiology*, http://www.vifm.org/fpradiology.html (accessed Aug. 14, 2007).

353. *See e.g. State v. Acremant*, 108 P.3d 1139, 1157 (Or. 2005) (explaining that identification of the deceased was made through x-rays).

354. *See e.g. Takeuchi v. Sakhai*, 2006 WL 119749 at *2 (S.D.N.Y. Jan. 17, 2006) (explaining that x-rays of artwork revealed it was not an authentic Rembrandt as its buyer had been led to believe).

355. *See e.g. In re J.P.B.*, 180 S.W.3d 570, 572–573 (Tex. 2005) (explaining that parental negligence was evidenced by x-rays that revealed child's broken ribs).

356. *See e.g. U.S. v. Massey*, 443 F.3d 814, 817 (11th Cir. 2006) (explaining that airport x-rays revealed foreign objects in defendant's pelvic region, which turned out to be heroin packages).

357. Sachs, *supra* n. 349, at 115.

358. *Id.*; Flowers, *supra* n. 349, at 3.

359. *See e.g.* D. E. Ytreberg, *Preliminary Proof, Verification, or Authentication of X-Rays Requisite to Their Introduction in Evidence in Civil Cases*, 5 A.L.R.3d 303, 309 (1966) (explaining that "proof of the accuracy and trustworthiness of the X-ray process in general is usually not required").

reconstructions of corpses that can then assist in the determination of cause and time of death.[360] Specifically, noninvasive postmortem photogrammetric scans, magnetic resonance imaging (MRI), and multi-slice computed axial tomography (MSCT) of the body are assimilated by a computer program into two- or three-dimensional digital images.[361] It is this assimilation, as well as the ability to manipulate the images digitally, that may justify heightened judicial scrutiny and, thus, invoke a *Swinton* analysis.[362]

The virtual autopsy technique is being developed and studied at the University of Bern, Institute of Forensic Medicine in Switzerland under the name Virtopsy®.[363] According to the research group's website, "[t]he aim is to establish an observer-independent, objective and reproducible forensic assessment method using modern imaging technology, eventually leading to [a] minimally invasive 'virtual' forensic autopsy."[364]

From the time the program began in 2000 until September 2004, the Swiss researchers have worked on approximately 110 forensic cases.[365] In January 2005, the Office of the Armed Forces Medical Examiner and the Defense Advanced Research Projects Agency began "incorporating virtual autopsy into the forensic process at the Dover Port Mortuary [in] Delaware. Since the system went online . . . over 200 cases have been examined using the scanner, the only CT-augmented autopsy augmented program in the United States."[366] Then, in September 2005, the Technical Working Group Forensic Imaging Methods (TWGFIM) was

360. Michael J. Thali et al., *Virtopsy—Scientific Documentation, Reconstruction and Animation in Forensic: Individual and Real 3D Data Based Geo-Metric Approach Including Optical Body/Object Surface and Radiological CT/MRI Scanning*, 50 J. Forensic Sci. 428, 438 (2005).

361. *Id.*

362. In *In re J.P.B.*, the court held that x-rays were properly authenticated when a radiologist from the hospital where the x-rays were obtained "testified that while the computer program could be used to crop the x-ray or adjust the brightness and contrast of the image, it could not add to or otherwise alter the x-ray." 180 S.W.3d at 575. The assumption that can be drawn from this holding is that the x-rays would require additional review if the computer that created them could have modified the images as is the case with virtual autopsies.

363. Flowers, *supra* n. 349, at 3.

364. Inst. Forensic Med., U. of Bern, Switz., *Virtopsy*, http://www.virtopsy.com (accessed Jan. 15, 2007).

365. *Id.* at http://www.virtopsy.com/results.htm.

366. Flowers, *supra* n. 349, at 3.

founded to help "achieve reliable and legally approved results" with this technology.[367] Despite these developments this technique has not yet been adopted by the mainstream forensic community in the United States. Therefore, it has not been introduced into the American court system. However, its founders believe that it will become "an acceptable alternative to current practice within [ten] to [fifteen] years."[368]

The process generally begins with a photogrammetric scan of the surface of the corpse.[369] The body is placed face up on the examination table.[370] Button-like reference markers are attached to the skin, digital photographs are taken from various angles, and a computer-guided scan is performed with overhead cameras and a projected grid pattern.[371] These steps are repeated when the body is flipped.[372] The calibrated images are converted into a three-dimensional cyber model of the victim.[373] This model is compared to whatever instrumentality allegedly caused the victim's wounds.[374] For example, if an elderly woman was allegedly run over by an automobile, a three-dimensional model of the corpse and a similarly created model of the car can be brought together in cyberspace to determine whether the car's trunk lid and bumper match up with the wounds visible in the surface scan of the victim.[375]

Next, the corpse is placed in a body bag and sent for an MRI scan.[376] This technology "combines a magnet, vastly more powerful than the magnetic pull of the earth, with radio waves to produce computer-generated images . . . ."[377] These images, which are

367. Inst. of Forensic Med., *supra* n. 364; Technical Working Group Forensic Imaging Methods, *Virtopsy—Technical Working Group Forensic Imaging Methods (TWGFIM)*, http://www.twgfim.com (updated Sept. 16, 2005).

368. Sarah Graham, *Autopsies, No Scalpel Required*, http://www.sciam.com/article.cfm?articleID=000C80AC-07C6-1FCD-87C683414B7F0000& (Dec. 3, 2003).

369. Sachs, *supra* n. 349.

370. *Id*.

371. *Id*.

372. *Id*.

373. *Id*.

374. *Id*.

375. *Id*.

376. *Id*.

377. Samuel D. Hodge, Jr., *A Litigation Primer on Diagnostic Imaging*, 16 Prac. Litig. 7, 14 (Sept. 2005). The MRI process can be further described as follows:

> The MRI is based on the principle that the nuclei in the body's hydrogen atoms act as tiny magnets. When stimulated by the MRI's magnetic field, about one-half of the

generally of soft tissue, organs and bone, appear in astonishing detail.[378] Finally, the body receives a CT scan, which operates as follows:

> A computer refocuses the x-ray beam to create a slice or cross-sectional view allowing a physician to [examine] a specific body segment and all of its contents at the same time. To use a loaf of bread as an example, an x-ray is only able to image the top, bottom, or side of the loaf. The CT scan, however, will cut the bread into slices, and will allow the viewer to examine any desired slice, including the crust and doughy part at the same time. These cross-sections are known as axial views.[379]

Then, the equipment combines these slices into three-dimensional pictures and trained operators manipulate and analyze the images to determine cause and time of death.[380]

B. Benefits and Drawbacks

As one of the most recent developments in forensic radiology, virtual autopsies have several advantages over the traditional autopsy. Virtopsies produce clear, detailed graphics because the organs and injuries can be viewed without obstruction from blood and other internal matter.[381] Also, "there is no beating heart, no circulating blood, [and] no digestive motions to blur [the] images."[382] In the legal context, this means that the images are graphic enough to engage and educate jurors but not gory enough to risk exclusion.[383] It also increases efficiency by allowing coro-

---

> nuclei line up in the direction of the magnetic field and the balance line-up in the opposite direction. These excited nuclei are then exposed to radio waves which cause the "tiny magnets" to change direction resulting in the emission of signals that are utilized to generate the final diagnostic images.

Id.

378. *Id.*; Adéle Jurgens-Ling, *Are Bloodless, Noninvasive Autopsies the Future of Forensic Medicine?* 36 ASRT Scanner 10, 11 (2004).

379. Hodge, *supra* n. 377, at 11–12.

380. Sachs, *supra* n. 349.

381. *Id.* at 54.

382. *Id.* (internal citation omitted).

383. Federal Rule of Evidence 403 provides that "[although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice . . . ." The less graphic the autopsy image is, the less likely an opponent will be able to challenge evidence as too prejudicial.

ners to pre-navigate the corpse, to focus their investigation, and to spend less time on traditional time-consuming techniques. In fact, the level of detail is so exact that specific toolmarks, such as knife marks left in a bone, can be identified through three-dimensional micro-CT scans.[384]

The technology is particularly adept at detecting bullet paths, pockets of liquid, hidden fractures, and trapped gasses that are hard to observe with the naked eye.[385] For example, researchers performed a Virtopsy on a forty-four-year-old male who died while scuba diving.[386] In determining the exact cause of death, the examiners found that "MSCT and MRI were superior to autopsy in the demonstration of distributed gas collections."[387] The gas appeared in the two-dimensional MRI images as small black areas.[388] This type of intangible evidence could easily be lost "as soon as a pathologist slices open a vein or organ to look for it."[389] As a result of the Virtopsy findings, the death was attributed to decompression sickness rather than drowning or external traumatic events.[390]

The non-invasive nature of the technique allows autopsies to be performed that may otherwise be prevented because of personal, cultural, or religious beliefs.[391] After all, the deceased person remains sealed in a body bag during the majority of the Virtopsy process.[392] The lack of incisions also protects examiners from toxic agents sealed within the body.[393] Such biosafety con-

384. Michael J. Thali et al., *Forensic Microradiology: Micro-Computed Tomography (Micro-CT) and Analysis of Patterned Injuries Inside of Bone*, 48 J. of Forensic Sci. 1336, 1338 (2003) (measuring the "distances and angles of the injury in 3D volume dataset . . . to determine the size and shape of the injury-causing knife blade in [a] stab wound[ ]").

385. Sachs, *supra* n. 349; *see also* David Ranson, *The Role of the Forensic Pathologist* 23, http://www.vifm.org/attachments/o116.pdf (accessed May 17, 2007) (identifying radiology as "the best technique for identifying some pathological processes in particular pneumothoraces, air embolism and some musculoskeletal injuries").

386. Thomas Platner et al., *Virtopsy—Postmortem Multislice Computed Tomography (MSCT) and Magnetic Resonance Imaging (MRI) in a Fatal Scuba Diving Incident*, 48 J. Forensic Sci. 1347, 1347 (2003).

387. *Id*. at 1351.

388. *Id*. at 1350.

389. Sachs, *supra* n. 349.

390. Platner et al., *supra* n. 386, at 1351.

391. Jurgens-Ling, *supra* n. 378, at 12.

392. Sachs, *supra* n. 349.

393. *See also* Kurt B. Nolte et al., *Biosafety Considerations for Autopsy*, 23 Am. J. Forensic Med. & Pathology 107 (June 2002) (listing exposure to radioactive materials as a

cerns are likely to increase as the threat of bioterrorism and pandemics, such as the bird flu, continue to rise.[394]

The Virtopsy website also boasts that "[t]he present-day descriptive, subjective protocolling of autopsy findings can be replaced by a uniform and observer-independent, objective radiological documentation [that] will substantially increase the quality of the evidence presented in court by experts."[395] Therefore, virtual autopsies are arguably very objective because they utilize a computer, rather than a human, to document the actual condition of the body. Thus, the process negates context effects[396] created by the examiner's expectations, which may arise from discussions with police or from the pathologist's own prior experiences.

A related benefit is that the bodies are "digitally preserved" in electronic format, which offers the advantages of permanency.[397] As one of the founders of the program noted, "[m]urder victims have the unfortunate habit of decomposing."[398] Just like the digital imaging processes discussed throughout this paper, the digital autopsy images can also be easily electronically transferred, duplicated, and stored.[399] This is particularly useful in death investigations wherein multiple parties, such as investigators and attorneys, need to view the autopsy report. Furthermore, the technology permits practitioners to click back and forth between images and merge the internal images with external wounds, allowing operators to virtually peel away layers of skin, connective tissue, and muscle to reveal the skeletal structure.[400] This can clarify how an injury was inflicted. Most coroners do not

danger associated with traditional autopsies).

394. *See generally* Kurt B. Nolte et al., *Medical Examiners, Coroners, and Biological Terrorism: A Guidebook for Surveillance and Case Management*, 53 Morbidity & Mortality Wkly. Rep. 3 (June 11, 2004) (available at http://www.cdc.gov/mmwr/PDF/rr/rr5308.pdf) (discussing the increasing threat of bioterrorism).

395. Inst. Forensic Med., *supra* n. 364, at http://www.virtopsy.com/files/Virtopsy_Basic_Course.pdf.

396. For more information about context effects, see M.J. Saks et al., *Context Effects in Forensic Science: A Review and Application of the Science of Science to Crime Laboratory Practice in the United States*, 43 Sci. & Just. 77 (2003).

397. Sachs, *supra* n. 349.

398. *Id*.

399. CNN, *Virtual Autopsies May Cut Scalpel Role*, http://edition.cnn.com/2003/HEALTH/12/04/virtual.autopsy.ap (Dec. 4, 2003).

400. Sachs, *supra* n. 349.

have this luxury since utilizing traditional autopsy techniques "essentially eviscerate[s] the body."[401]

Finally, the digitalized radiological images, much like digital photographs, are likely to have great influence on juries.[402] As explained in Part II of this Article, jurors tend to retain, understand, and thus prefer visual exhibits over oral or written evidence.[403] If virtopsies become the norm, we may one day have pathologist witnesses digitally dissecting victims on screen in court.[404]

However, this new technology also has its disadvantages. The high cost of the machinery places virtual autopsies out of reach for most coroners.[405] In October 2004, the estimated costs were approximately $100,000 for the photogrammetric devices, over one million dollars for an MRI machine, and $500,000 for a CT scanner, plus the cost of training or hiring the necessary specially qualified radiological technicians.[406] Considering that some coroners' offices have budgets as small as $5,900,[407] it is not surprising that American medical examiners would view virtual autopsies as a mostly theoretical, academic venture.

Virtual autopsies are also unable to diagnose some causes of death.[408] For example, poisoning is hard to detect with this process.[409] Instead, poisoning is better detected by toxicological analysis.[410] It is, thus, unlikely that courts will change their opinion

401. *Id.*

402. *See* Kurtis A. Kemper, *Admissibility of Computer-Generated Animation*, 111 A.L.R.5th 529 (2003) (discussing the potential disadvantages of using computer-generated animation at trial).

403. *See* Selbak, *supra* n. 59, at 360 (noting that jurors were able to remember sixty-five percent of visual evidence and only ten percent of oral evidence); *see also* Galves, *supra* n. 62, at 167–168 (commenting that pictures, rather than words, do a far better job of helping a juror retain an image).

404. Sachs, *supra* n. 349.

405. The expense is so significant that, according to one medical examiner, virtual autopsies must be considered "a big luxury." *Id.*

406. *Id.*

407. *See e.g.* John Miller, *Hicks Unhappy with Coroner's Budget*, Nevada County Picayune (Prescott, Ariz.) (Jan. 5, 2005) (available at http://www.picayune-times.com/showstory.heitml?show=t&k.number=17964&pubname=picayune&headline=Hicks +unhappy +with+Coroner's+budget) (reporting that, in 2004, the Nevada County, Arizona coroner's budget was $5,905).

408. *See* Ranson, *supra* n. 385 (noting that "radiology does not always reveal pathology that is detected at autopsy").

409. Sachs, *supra* n. 349.

410. *See* Crime Library, *Modern Detection Methods*, www.crimelibrary.com/criminal

that "examination to determine poison in a human body [is] the work for expert chemists."[411] Additionally, deaths caused by natural events, such as heart failure or infection, are difficult to diagnose.[412] The Virtopsy technique can identify neither organ color, which may reveal inflammation, nor leaks within the vessel system.[413] The technology also only examines the body and its contents; it does not review all aspects of the condition of the deceased's clothing and skin. These items may contain important clues about the cause of death. For example, gun powder residue on a shooting victim's hands may indicate that the cause of death was suicide rather than homicide. Such residue would not be detected by the radiological equipment. Thus, an initial visual inspection of the body is still required.

As a result of these inadequacies, traditional autopsies still need to be performed to confirm the radiological findings.[414] Even the founders of the Virtopsy process acknowledge that virtual autopsies may better supplement, rather than replace, the classic approach.[415] As one of the program's researchers stated: "What we see with our own eyes will remain the gold standard."[416] Thus, proponents of the technology will have to overcome the critics' cries of redundancy by establishing that this new technique is of such quality and merit to be independently beneficial.

Additionally, the examination process is not entirely automated. As a result, the process may not be as "objective" as proclaimed by its founders.[417] First, the body must be physically moved into various positions, which may include lifting it onto the scanner and flipping it onto its back or front. This process may cause further damage to the corpse, thus altering its condition from what it was at the time of death. Second, operators must use

_mind/forensics/toxicology/10.html (accessed Jan. 15, 2007) (stating that the most current method of diagnosing poisoning is by spectrometry and chromatography).

411. F. M. English, *Qualifications of Chemist or Chemical Engineer to Testify as to Effect of Poison upon Human Body*, 70 A.L.R.2d 1029 (1960).

412. Sachs, *supra* n. 349.

413. Jurgens-Ling, *supra* n. 378, at 13.

414. *Id.* at 13 (noting that "[t]he [Swiss] courts require Dr. Dirnhofer to support all his virtual findings with a classic autopsy").

415. Sachs, *supra* n. 349.

416. *Id.*

417. Inst. Forensic Med., *supra* n. 364, at http://www.virtopsy.com/files/Virtopsy_Basic _Course.pdf.

and adjust complicated protocols to extract images from various kinds of body tissues. This means that there is room for manipulation, either in the form of unintentional error or intentional misconduct.[418] For example, some of the equipment functions by translating "signature vibrations" that emanate from various types of atom nuclei.[419] These vibrations slow down at cooler temperatures.[420] Because corpses are usually stored in refrigerated containers prior to examination, technicians must manually make adjustments to the equipment to compensate for the deceased's lower body temperature.[421]

Another concern is the perceived infallibility of computers. The use of a computer can lull jurors, and even medical and legal professionals, into a false sense of security. As is the case with digital photographs, problems may exist with the system's hardware, software, or output. This issue is particularly worrisome considering the weight that jurors tend to give visual and scientific evidence. Therefore, clear and consistent standards of admissibility are necessary. Although the use of a digital reconstruction to supplement or replace the standard autopsy report has not been directly addressed by the American legal system, the courts have addressed the broader issue of the admissibility of digitally enhanced and computer-generated images in *Swinton*.[422]

C. Application of the *Swinton* Six to Virtual-Autopsy Evidence

As explained above, Virtopsy goes a step further than traditional radiological technology by using a sophisticated combination of imaging techniques to generate digital reconstructions of corpses.[423] It is the computer's assimilation of the radiological scans, as well as the operator's ability to manipulate the images digitally, which may cast doubt upon the reliability of the process, thereby necessitating additional scrutiny. It follows that the standards enumerated in *Swinton* can be applied to the Virtopsy

418. *See supra* nn. 369–380 and accompanying text (detailing the process of conducting a virtual autopsy).

419. Sachs, *supra* n. 349.

420. *Id*.

421. *Id*.

422. 847 A.2d 921.

423. *See generally* Thali et al., *supra* n. 360 (discussing how Virtopsy uses a combination of photogrammetric, CT, and MRI images).

process to determine, theoretically, how courts would authenticate such evidence. The purpose of this analysis is to demonstrate not only the continual expansion of digital forensic evidence but also the flexibility and the applicability of the *Swinton* Six.

The first factor is that the "the computer equipment [must be] accepted in the field as standard and competent and [it must be] in good working order."[424] In the virtual-autopsy context, proponents of the evidence will need to establish two predicates: (1) that persons working in the field of forensic radiology generally use photogrammetric, MRI, and CT scanners; and (2) that the equipment used in the case operated properly and accurately. Unbiased expert testimony or peer-reviewed publications may be used to satisfy the first prong. Testimony from the operators about prior, successful use of the equipment and evidence that the equipment was professionally maintained and serviced may satisfy the second prong. Together these two steps will establish the "routineness" of the process and that the equipment functioned in a normal, reliable manner.

The next *Swinton* factor is that qualified operators must procure the evidence at issue.[425] Although *Swinton* does not generically define what "qualifies" an operator, a safe assumption is that such qualifications will rest largely upon education and experience. Such experience and education will most likely need to involve forensic pathology. It will also be critical that the technicians are trained and familiar with the specific radiological processes related to the analysis of postmortem tissue. Proof of degrees, professional memberships, certification, and licensure may be used establish this element. It will also be equally important that unqualified persons, such as mere "bystanders" like administrative supervisors, do not participate in the generation of the evidence.

The operators will not only have to be qualified, but under the third *Swinton* factor they will also need to follow proper procedures "in connection with the input and output of information."[426] In the context of virtual autopsies, input procedures involve the integrity of both the data entry and the body being au-

424. *Swinton*, 847 A.2d at 942.
425. *Id.*
426. *Id.*

topsied. The output procedures refer to steps taken to analyze the body and determine cause and time of death. Proponents will need to first address this requirement by providing the court with evidence from the Technical Working Group Forensic Imaging Methods (TWGFIM) that there are in fact certain protocols and procedures for the virtual-autopsy process. They may also turn to professional guides, such as operation manuals and handbooks, for support.

The *Swinton* Court clarified that this element may also be established through the clear and consistent testimony of the person or persons who actually created the computer-generated evidence.[427] Therefore, the ideal witness for virtual autopsies will probably be the technician or analyst who actually engaged in the generation of the images and could thus explain the process in detail. This person could testify that the corpse was collected and transported properly and that it was not significantly altered prior to examination. He or she could also explain that the data was accurately converted into a computer format for storage and analysis.[428]

Next, the court will want evidence that the software programs that the operators utilized are reliable as required under the fourth *Swinton* factor.[429] This factor primarily refers to the level of automation in the digital process. There is a direct relationship between the quantity of human interaction with a computerized process and the authenticity of the final outcome. This relationship exists because, for every step that requires human interaction, there is the possibility for intentional or negligent manipulation of data. As discussed before, virtual autopsies are not fully automated because operators must create and implement certain protocols to account for the various types of body tissue.[430] Therefore, courts will likely analyze a software program's capacity and its limitations in light of the possibility for human manipulation. Information about the program's history,

427. *Id.* at 944.

428. It should be noted that, under *Swinton*, a witness' in-court demonstration of the contested digital process would satisfy this factor as well. *Id.* However, it is unlikely that the Virtopsy technicians could take the stand and do the same.

429. *Id.* at 942.

430. *See supra* nn. 369–380 and accompanying text (describing how a virtual autopsy is conducted).

error rates, and reputation will be important in the analysis of this element. Additionally, it will be important to show that the software was secure against unauthorized users. Information about security procedures and access will therefore be relevant to this step in the analysis. Such data may be elicited from outside publications or unbiased, experienced witnesses. The *Swinton* analysis suggests that the computer or software programmer is not the exclusive source of authentication testimony; instead, the proponent may elicit such testimony from any "person with some degree of computer expertise, who has sufficient knowledge to be examined and cross-examined about the functioning of the computer."[431]

The fifth *Swinton* factor requires a proffer of proper programming techniques and operational procedures of the three components of a virtual autopsy: photogrammetric, MRI, and CT scanner.[432] This requirement, much like the first, focuses on the reliability of the hardware used to create the digital images. One way to establish this element is to verify the output of the virtual autopsy through an alternate process. The theory is that if a result can be duplicated, then the process used to create the result is more likely to be reliable. In the context of a virtual autopsy this would mean performing a second, traditional autopsy and comparing the findings. Studies have already been done with such comparisons.[433] Additionally, courts may examine how the equipment was programmed, the qualifications of the programmers, and whether their conduct deviated from accepted technical standards. Furthermore, it will again be important to show that the hardware was secure against unauthorized users.

The final *Swinton* element demands that the radiologic evidence be "properly identified as the output in question."[434] Therefore, proponents must show that the resulting images of the body are actually the "output" of the input and process. To do this, it

431. *Swinton*, 847 A.2d at 942 (citing *Am. Oil Co.*, 426 A.2d at 305).

432. *Id.*

433. *See generally* Michael J. Thali et al., *Virtopsy—A New Imaging Horizon in Forensic Pathology: Virtual Autopsy by Postmortem Multislice Computer Tomography (MSCT) and Magnetic Resonance Imaging (MRI)—A Feasibility Study*, 48 J. of Forensic Sci. 386 (Mar. 2003) (examining the feasibility and practicality of virtual autopsies as compared to traditional autopsies).

434. *Swinton*, 847 A.2d at 942.

must be proven that the output was based on a proper request, this requested output was what was generated, and the output was secure against tampering. Again, the operators can most likely establish these elements through their testimony and records.

As stated above, the preceding analysis reveals not only specific suggestions for authenticating a new and innovative form of digital evidence, but it also demonstrates the flexibility and adaptability of the standards defined within the *Swinton* opinion. Even though the *Swinton* Court reviewed a different form of digital imagery, the basic message remains the same: accurate, functioning equipment and well-trained, experienced personnel are *critical* to the reliability of computer-generated evidence. Therefore, their reliability should be proven, rather than presumed, when digital imagery is introduced in court.

VI. CONCLUSION

As the field of digital imaging progresses and expands, the legal community must ensure that the new technologies bring justice, rather than injustice, into our courts. Attorneys, scholars, and the judiciary should thus pay great heed to not only the *Swinton* holding, but also to the careful attention and analysis that the Connecticut Supreme Court employed when reviewing complicated technical definitions and blurry legal precedent. In light of the threat of manipulation, the *Swinton* Court clung to factors that focused on the reliability of the digitization process while still allowing the trial courts enough discretion to maintain their roles as gatekeepers and factfinders. Although the courts might eventually take judicial notice of the reliability of some digital imaging techniques, the *Swinton* Six will survive as a standard for the continually evolving category of computer-generated evidence.