BORN DIGITAL IMAGES AS RELIABLE AND AUTHENTIC RECORDS

by

JESSICA ELAINE BUSHEY

B.A., The University of British Columbia, 1992

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARCHIVAL STUDIES

in

THE FACULTY OF GRADUATE STUDIES

Library, Archival and Information Studies

THE UNIVERSITY OF BRITISH COLUMBIA

August 2005

ABSTRACT

In recent years, the long-term preservation of digital records has received increasing attention. Several research initiatives have focused upon the challenges presented by the preservation of digital photography. They have primarily addressed issues related to continuing access to accurate and authentic images. These initiatives are aware of the fundamental difference between preservation of analogue photographs and preservation of digital photographs. While the key factors allowing for digital preservation are media stability and technological interoperability, central to the scholarly discourse is the changing role of the *creator* (i.e., the photographer), who is becoming responsible for performing the functions traditionally carried out by the *preserver* (i.e., archivist).

This thesis contributes to such discourse by investigating the creation, use, and preservation of born digital images as reliable and authentic records.[i] It does so by studying existing literature in the archival-diplomatic, legal, and photographic fields; analyzing the results of a survey of the recordkeeping activities of digital photographers; examining existing best practices and standards, especially as regards metadata schemas for digital photographs; and comparing the findings of these research activities with protocols for record authenticity. This study reaches several conclusions. First, an interdisciplinary approach to the topic of digital preservation should incorporate the concerns of both creators and preservers. Second, although photographers are concerned about the reliability and authenticity of their born digital images, they should be informed of the conceptual and

i. The term "born digital image" refers to a digital image that never physically existed before becoming a digital file. The most common example is an image created with a digital camera. An existing photograph or document that is scanned or digitally photographed to create a digital file is not considered to be born digital but to have been digitized and would be referred to as a digital image, not a born digital image.

methodological thinking that supports best practices for creating, maintaining, and preserving reliable and authentic records. Third, current standards and best practices promulgated by the digital imaging community are a solid foundation on which it is possible to build a trusted recordkeeping system. Fourth, contemporary archival diplomatics provides a valid measurement of the effectiveness of existing standards to document the identity of born digital images and attest to their integrity over time. Lastly, strategies to ensure the reliability and authenticity of born digital images should be developed on the basis of the requirements of the creator's operating environment.

TABLE OF CONTENTS

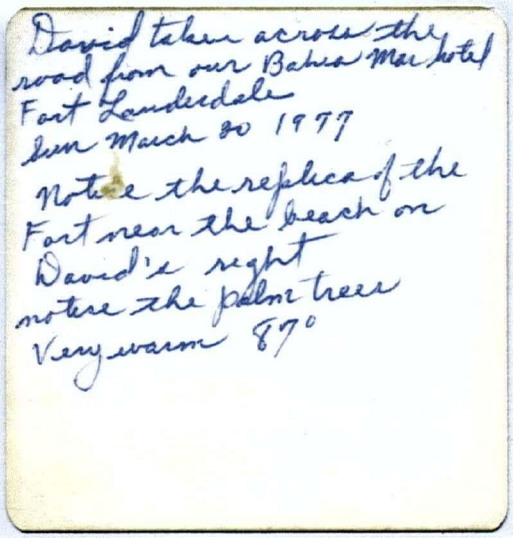
LIST OF TABLES

LIST OF ABBREVIATIONS

CAPIC	Canadian Association of Photographers and Illustrators in Communications
CCD	Charge-coupled Device
CD	Compact Disc
CJS	Criminal Justice System
CMOS	Complementary Metal Oxide Semiconductor
CMY	Cyan Magenta Yellow
COTS	Commercial-off-the-Shelf
DVD	Digital Versatile Disc
EPUK	Editorial Photographers United Kingdom & Ireland
ERMS	Electronic Records Management System
Exif	Exchangeable Image File Format
FREA	Federal Rules of Evidence Act
IAI	International Association for Identification
IIM	International Interchange Model
IMI	Institute of Medical Illustrators
IMS	Image Management Software
InterPARES	International Research on Permanent Authentic Records in Electronic Systems
IPTC	International Press Telecommunications Council
ISO	International Standards Organization
JEITA	Japan Electronics & Information Technology Industries Association
JPEG	Joint Photographers Expert Group
NPPA	National Press Photographers Association
PDF	Photoshop Draw File
PPOC	Professional Photographers of Canada
ProDIG	Professionals Using Digital Imaging
PSD	Photoshop File (Native Format)
RGB	Red Green Blue
SAA	Stock Artists Alliance
SOP	Standard Operating Procedure
SWGDE	Scientific Working Group on Digital Evidence
SWGIT	Scientific Working Group on Imaging Technology
TIFF	Tagged Image File Format
TPW	Toronto Photographers Workshop
UEEA	Uniform Electronic Evidence Act
UREA	Uniform Rules of Evidence Act
XML	Extensible Mark-up Language
XMP	Extensible Metadata Platform

ACKNOWLEDGEMENTS

I would like to thank my grandmother, Doris Vincelette for diligently documenting our family history and revealing the true power of metadata long before the digital epoch.



Grateful acknowledgements are made to my thesis advisor, Luciana Duranti for providing me with the opportunity to pursue an interdisciplinary thesis that combines both my interests in photography and archival studies. Her tireless assistance throughout the research and writing of this thesis should be lauded.

I would like to extend my appreciation to my thesis committee, Manuel Piña, Sidney Fels, Francesca Marini and the Chair, Judith Saltman. Each of you provided me with thoughtful commentary that stems from your areas of expertise and resulted in improving and expanding the breadth of my thesis.

A great deal of my research for this thesis stemmed from my activities with the InterPARES 2 Project. Throughout my two years as a graduate research assistant with InterPARES 2 I have had the pleasure of working with Marta Braun. I would like to thank

her for always responding to my e-mails and phone calls, regardless of what time zone or country she was in.

There were so many moments during the research and actual writing of this thesis when I had to rely on the generosity and skills of others. In particular I would like to thank Diana Breti for her exacting edit, Greg Kozak for his book loans, guidance, and encouragement, Randy Preston for being my Excel Guru, and Seth Dalby for reviewing my first chapters, providing important feedback, and never tiring of discussing the concepts of reliability and authenticity.

At the final stages of writing this thesis I gained important insight from my cousin Anthony, a true scholar through and through, and relied upon Dr. Marilyn Antonucci's sound advice. I wish to thank both of them for picking-up the baton and helping me finish the race.

In closing, I would like to thank my parents, Jeanne and Richard, and my sister Sarah for their emotional and financial support, which has made everything in my life possible, including this thesis. I am deeply indebted to Cameron Andrews for his limitless love and for being the best Masters Coach in the world.

INTRODUCTION

This thesis studies the creation and maintenance of images that are produced and maintained in the digital environment and makes recommendations that will ensure the production of reliable images capable of being preserved over the long term as authentic records, notwithstanding the obstacles presented by media fragility and technological obsolescence. My interest in this topic emerges from my research as a graduate student research assistant with the International Research on Permanent Authentic Records in Electronic Systems: Experiential, Interactive and Dynamic Records Project (InterPARES 2).[1] My experience as a professional photographer and my coursework in archival studies at the University of British Columbia have provided me with a basis for investigating the issues linked to the creation, use, and preservation of images as reliable and authentic records.

This study was sparked by a research assignment to create an annotated bibliography on the concepts of accuracy, reliability, and authenticity as understood by photography scholars in relation to digital photography. I discovered a basic lack of sources about the topic, and this motivated me to pursue further research. Reviewing the scarce available literature, I was also struck by the inconsistency of the terminology, particularly with regard to the definition of born digital images, due to the fact that professional photographers and art theorists are utilizing what could be defined as an "analogue mindset" to describe new forms

---

1. InterPARES 2 was initiated in 2002 as an international and interdisciplinary exploration into the issues related to the creation and maintenance of accurate and reliable records and the long-term preservation of authentic records in the context of artistic, scientific, and e-government activities. InterPARES2, "Project Summary," (2004), http://www.interpares.org/ip2/ip2_index.cfm (accessed March 12, 2005).

The InterPARES 2 Project is built upon the findings of the first InterPARES project (1999-2001), which explored the long-term preservation of authentic records created and/or maintained in digital form. Its focus was on the records created and/or maintained in databases and document management systems in the course of administrative activities. InterPARES1, "Project Summary," (2001), http://www.interpares.org/ip1/ip1_index.cfm (accessed March 12, 2005).

of visual representation whose characteristics would be more accurately expressed using terminology from the digital environment. For example, the most commonly used terms to refer to images that are born digital are "digital photography" and "electronic photography," which are inaccurate and misleading as they may refer to digitized analogue material as well as to material created by cameras that offer automated functionality. To avoid further confusion, this thesis will use the term "born digital images" to refer to images produced, maintained, and used in a digital environment.

The major challenge presented by this thesis stems from the author's desire to reconcile her experiences as a photographer who uses digital technology with her knowledge of archival studies and, more specifically, of contemporary archival diplomatics.[2] The goal, then, of this study was to define both conceptual and methodological requirements and practical strategies for the creation, management, and preservation of born digital images as reliable and authentic records. In order to reach this goal, it was necessary to go beyond what is generally discussed in the literature about photographers' current approaches to record keeping in the digital environment. Thus, a survey was designed that focuses on the record-keeping practices of professional photographers using digital technology.

The survey addressed the following questions: (1) What kinds of digital records do photographers produce? (2) What are the assumptions of photographers about future access to their records? (3) What is the nature and variety of digital materials used by photographers?

---

2. Diplomatics emerged in the seventeenth century as a body of concepts and methods that aimed to determine a record's authenticity for legal purposes. Over the centuries, it has evolved into a modern discipline called archival diplomatics, which aims to evaluate the authenticity of contemporary electronic records, including those in electronic form. Authenticity Task Force, "Part One: Establishing and Maintaining Trust in Electronic Records," in *The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project,* ed. Luciana Duranti, 23-25 (San Miniato, Italy: Archilab, 2005).

Question 1 reflected my expectation that photographers use a variety of file formats for production that meet their business and creative needs first and their preservation needs last. Question 2 reflected the expectation that, although photographers are aware that born digital images are more vulnerable than analogue photographs, they have accepted and in some cases adopted the term "archival" as synonymous with long-term preservation, when realistically the longevity of optical storage media and printing papers is yet to be accurately determined. Question 3 reflected the expectation that photographers use a variety of hardware devices, software applications, file formats, and metadata schemas to create their digital images and manage them as collections.

To obtain answers to the three research questions a quantitative survey approach was chosen that utilized a Web-based questionnaire, and various analytical instruments developed by the InterPARES project to gather knowledge in a deductive way were adopted for the analysis of the responses.[3] The theoretical framework for this study is rooted in the work of the InterPARES project, specifically the integration of archival and diplomatic principles and methods, while the information framework is constituted by literature and practical studies on photography, archival theory and methods, and jurisprudence.

Until very recently, most archival literature on photographs focused on the nature of analogue materials and on the role of context to discover meaning; management and preservation of electronic records; and on methods for digitizing archival photographs for preservation and access purposes. Lately, a second wave of archival literature has expanded the scope of research into photographs as electronic records and their reliability and authenticity, but they have not provided those who make photographs with the criteria that

3. Design of the Web-survey was informed by, Don A. Dillman, *Mail and Internet Surveys: The Tailored Design Method,* 2nd ed. (New York: John Wiley & Sons, Inc., 2000); Duranti, *Long-Term Preservation.*

define and determine these characteristics. In addition, the authors of this literature treat born digital images as visual sources without having first gathered an understanding of their *documentary form* and reproduction requirements.[4]

There are several ways in which the investigation carried out by this thesis and its findings may be significant. However, they are directed primarily to two groups of potential users. The first group is represented by preservers, such as archivists and collections managers and museum and art gallery curators, who are interested in the nature of born digital images and in the way in which they can be protected by preservation procedures. The second group is constituted by record creators, such as photographers and digital technicians and the organizations employing them, who are interested in current methods and future strategies for creating, using, managing, and maintaining born digital images as reliable and authentic records throughout their lifecycle. The findings of this thesis also help to make them understand the importance of born digital images as business assets that have long-lasting value and require special handling to remain accessible and functional in the future.

The first chapter provides an overview of the literature that explores the concepts of reliability, authenticity, and originality in regard to photography. The three areas addressed in the literature review constitute the interdisciplinary foundation of this thesis: the archival-diplomatic field, the legal field, and the photography field. This literature review is intended to present the historical treatment of photography as a source of visual documentation and to lay the foundation for current theories and practical approaches regarding born digital images as reliable and authentic records of business and cultural activities. This chapter also includes

4. Documentary form refers to the rules of representation that articulate the content of a record, its administrative (i.e., organizational structure of the creating body) and documentary context (i.e., the collection in which the image belongs and its internal structure) and its authority. Authenticity Task Force, "Appendix 1: Template for Analysis," in *Long-Term Preservation,* ed. Luciana Duranti, 198-199 (San Miniato, Italy: Archilab, 2005).

a discussion of existing practices in the photographic industry that are aimed at creating, using and maintaining born digital images as reliable and authentic records.

The second chapter presents the data collected by the survey of the record-keeping practices of photographers using digital technology. More specifically, it includes an overview of the research problem, the research questions, the rationale and significance of the study and its limitations, and the findings. The findings are divided into two sections: (1) Creation & Use, which refers to the actions of photographers that affect the reliability of the records: and (2) Preservation & Transmission, which refers to the actions of photographers that affect the authenticity of the records. This structure reflects the procedural phases in the life cycle of a born digital image and relates the functions of the creator to manifestations of documentary form.

The third chapter discusses current standards for digital image metadata and best practices for establishing and implementing standard operating procedures for the creation, use, and preservation of digital imagery. Both these standards and best practices were discovered as a result of the analysis of the qualitative information provided by survey participants. The analytical framework of this chapter is based on research instruments produced by InterPARES research, which include the "Metadata Schema Registry," a database intended to facilitate the categorization and characterization of existing metadata schemas, and the "Benchmark and Baseline Requirements," which support the presumption of authenticity of electronic records and the production of authentic copies for preservation purposes.[5] This chapter tests the current methods for documenting information about born

5. The template for the metadata schema registry is provided in Ann Gilliland-Swetland, "Setting the Stage: Defining Metadata," in *Introduction to Metadata: Pathways to Digital Information 2.0,* ed. Murtha Baca. (Los Angeles: Getty Information Institute, 2000),

digital images against archival criteria for managing records in a reliable and authentic manner.

The fourth chapter discusses in detail the relationships among the benchmark and baseline requirements developed by InterPARES, the procedures and controls identified by the survey, and, existing standards and guidelines, for the purpose of outlining a coherent and strategic overview of the life cycle of born digital images and the actions of creators and preservers. Recommendations for creators and preservers resulting from the analysis of these relationships are listed at the end of the chapter and focus on strategies that support record authenticity.

The concluding chapter assesses the achievement of the research goal of this thesis and discusses the key issues drawn from the data analysis and application of standards and practices against archival criteria. The implications of these findings are considered and further research is recommended.

---

http://www.getty.edu./research/conducting_research/standards/intrometadata/2_articles/index.html (accessed June 24, 2005).

The benchmark and baseline requirements are available in Authenticity Task Force, "Appendix 2: Requirements for Assessing the Maintaining the Authenticity of Electronic Records," in *Long-Term Preservation,* ed. Luciana Duranti, 210-214 (San Miniato, Italy: Archilab, 2005).

CHAPTER ONE

A discussion of born digital images as reliable and authentic records has to begin with an examination of the historical development of the concepts and their relationships. A survey of photographic literature containing commentary on the concepts of accuracy, authenticity, and reliability revealed three areas in which the concepts are defined and discussed in relation to photography:[6] the disciplines of diplomatics and archival science, which provide the theories that are the foundation of this thesis; the legal discipline, which establishes how photographs and digital images are to be assessed as evidence in court proceedings; and the photographic discipline, which interprets their trustworthiness as manifestations of reality partly on the basis of its own theory and partly as a reflection of legal and other social requirements.

The evolution of ideas regarding the treatment of photography provides the foundation for current approaches to image creation and preservation in the digital environment. The examination of the concepts and the terminology used to express them within each discipline provides an opportunity to compare and contrast and to reconcile differences in order to gain a clear understanding of what constitutes a reliable and authentic born digital image.

This chapter is divided into sections corresponding to these three disciplines.

---

6. The survey was undertaken by the author as part of her research in the context of the InterPARES 2 project. A literature review produced ten articles, which were selected for their exploration of the concepts of authenticity, reliability, and accuracy in regard to photography. See Marta Braun and Jessica Bushey, "Article Summaries from the Digital Photography Bibliography," (InterPARES 2, June 30, 2004). http://www.interpares.org (accessed May 15, 2005). This summary document is contained within the restricted area of the InterPARES 2. Web site; however, aspects of it will be incorporated into a future publication.

Archival-Diplomatic Disciplines

Since its first articulation in 1681, diplomatics has aimed at determining "the authenticity of documents, for the ultimate purpose of ascertaining the reality of rights or truthfulness of facts represented in them."[7] The discipline has traditionally studied individual medieval administrative documents issued by sovereign authorities in order to determine their authenticity for legal purposes and their authority as sources. In 1998, Luciana Duranti introduced this system of ideas to the North American archival community and re-elaborated diplomatics, thereby providing the impetus for its application to modern and contemporary documents in both the paper and electronic environment for the purpose of identifying and communicating their true nature. In essence, Duranti presented the analytical system of diplomatics as a universal method for determining the trustworthiness of public and private *records* despite ongoing changes in record-making and record-keeping technology.[8]

A holistic understanding of the knowledge developed to address the creation and preservation of records requires incorporation of the concepts and methods of diplomatics into the discipline of archival science, the theory and methods of which aim at acquiring and maintaining physical and intellectual control over aggregations of records.[9] In the last two decades, the challenges digital technology has presented to the design of effective record-keeping systems have led to such an integration for the purpose of defining the conceptual requirements for creating and preserving authentic and reliable records in the electronic

---

7. Luciana Duranti, *Diplomatics: New Uses for an Old Science* (Lanham, MD and London: SAA, ACA, Scarecrow Press, 1998), 45.

8. A record is any document created (i.e., made or received and set aside for further action or reference) by a physical or juridical person in the course of a practical activity as an instrument and byproduct of it. See Authenticity Task Force, "Part One: Establishing and Maintaining Trust in Electronic Records," in *Long-Term Preservation*, ed. Luciana Duranti, 21 (San Miniato, Italy: Archilab, 2005).

9. Archival science looks at records as aggregations, whereas, diplomatics looks at records as individual items. See Luciana Duranti, Terry Eastwood, and Heather MacNeil, *Preservation of the Integrity of Electronic Records*, Vol. 2, *The Archivist's Library* (Dordrecht: Kluwer, 2002), 10-11.

environment.[10] Digital technology has not only increased the number of records being made and distributed; it has also provided more opportunities for them to be created haphazardly, to be mismanaged and even permanently lost. Thus, these requirements are needed to guide governments who pursue on-line initiatives for service delivery, such as taxation and licensing; for businesses that require and store vast quantities of sensitive client information in electronic databases; and for any number of individuals who use personal computers to create and distribute their information and intellectual property in digital form. The authenticity of the records created cannot be presumed, given the manipulability and vulnerability of digital information, the fragility of the media, and the problem of technological obsolescence; therefore, archivists must revisit traditional strategies for creating reliable and accurate content, preserving authentic records over time, and verifying authenticity to develop conceptual requirements for electronic records that assist in shaping the future of record -making and record -keeping.[11]

Diplomatic authenticity is the trustworthiness of a record as a record, rather than as information. Accordingly, an authentic record is what it purports to be and has not been altered or tampered with since being *set aside*.[12] An authentic record possesses both *identity* and *integrity*. Identity is the whole of the unique characteristics that distinguish one record from another, that is, of its attributes, such as the persons concurring in its creation (i.e., creator, author, writer, originator, addressee), the date(s) a record was created (i.e., made, received, and set aside), the date(s) it was transmitted, the indication of the subject or action,

10. Duranti, *Diplomatics: New Uses for an Old Science,* 21.

11. Duranti, 20.

12. To set aside a record is to file it, and keep it as a part of one's *fonds*. The fonds is the whole of the records that a physical or juridical person naturally accumulates by reason of its activities and as byproducts of them. See Duranti, Eastwood, and MacNeil, *Preservation of the Integrity of Electronic Records*, 16.

and the expression of the *archival bond*, which links it to other records.[13] Integrity is the quality of being whole and unaltered. A record has integrity if it is intact, sound, and able to convey the message that was intended by its author. The integrity of a record is protected through procedures exercising control over transmission, maintenance and preservation, and documentation of a trusted *chain of custody*.[14] To verify the authenticity of a record, one must verify its identity and its integrity.[15]

Contrary to common assumptions that equate authenticity with originality, diplomatics considers originality as a separate concept. Originality relates to the state of transmission of the record and refers to its degree of perfection. A record can be transmitted as a draft, an original, or a copy. The characteristics of an original record are primitiveness, completeness, and effectiveness: an original is the first record to be made (i.e., primitiveness), it includes all required formal elements (i.e., completeness), and it is capable of reaching the consequences intended by its author (i.e., effectiveness). Completeness and effectiveness are referred together as perfection. Its form endows a record with perfection. The manifestation of a record exhibits various degrees of completion, which are reflected in its form. Diplomatics is concerned with originality and the state of transmission because they are part of the grounds on which the trustworthiness and authority of a record are assessed.

---

13. The archival bond refers to the interrelationships between a record and other records resulting from the same activity. The archival bond comes into being when the record is filed, or set aside, an act which in the paper environment had a physical nature and in the electronic environment has an intellectual nature such as assigning a classification code to a record within the recordkeeping system. The archival bond is not external to the record but an integral part of it and provides expression of the *documentary context*. The documentary context of the record refers to the fonds to which a record belongs and its internal structure. Ibid., 19-22.

14. The chain of custody refers to the succession of offices or persons who have held recorded materials from the moment they were created. This succession of custodians must be trustworthy, which means that they must have no reason to alter the records under their care, or to allow others to alter them. See Duranti, *Long-Term Preservation,* 49.

15. Authenticity is not to be confused with authentication, which is a declaration of authenticity made by a juridical person or a person entrusted with the authority to make such a declaration at a specific point in time. It is an authoritative statement added to a record and attests that the record is authentic. See Ibid., 22.

The *states of transmission* of a photograph can be exemplified as follows.[16] An analogue photograph begins its existence as a film negative (or positive in the case of transparency film.) The film is endowed with primitiveness, being the first instance in an order of transformations; however, in this form, a photograph is not capable of achieving the author's intent (unless such intent is to deliver the film to the addressee for whom it is destined), and thus, it cannot be used and is not effective. Further actions of enlargement and development, and several manifestations of form such as prints with varying contrasts and cropping are part of the necessary process to produce a final photograph. The first print is the first instantiation of the photograph (i.e., the one endowed with primitiveness) that is complete and capable of producing the effects intended by the author, that is, the original. The by-products of the process leading up to the photographic print are considered drafts and are valued as documentation of the creative process culminating in the original but are not recognized as the definitive document since they are generated for the purpose of correction. Any photographic prints made at the same time, and destined for the same purpose, as the original print are originals as well. In this context, the concept of the original embraces both primitiveness and plurality. If multiple prints are made after the first set of complete and effective prints, they are copies in the form of the original. Copies are reproductions of an existing photograph in any state of transmission; therefore, there may be copies of drafts and copies of originals. Copies of originals are identical to and indistinguishable from them and are termed copies in the form of original and have the same effects as the originals.[17] There are many other types of copies depending on the purposes for making the copy and therefore

16. The states of transmission refers to a document's genetic process, as well as the ways it is handed down to future generations. See Duranti, *Diplomatics: New Uses for an Old Science,* 48 n32.

17. The verb forms of copy and reproduction are synonyms; however, in this thesis, the noun forms of these two words are treated differently, with copy being the result of the reproduction process.

on its characteristics. The photocopy is an example of an imitative copy, which reproduces the content and the form of the original but makes clear in its presentation that it is a copy. Diplomatic analysis of copies focuses on the relationship among the copies and between the copy and the original.

Reliability is a concept quite distinct from that of authenticity. Reliability is defined as the trustworthiness of a record as a statement of fact and refers to the *accuracy* of its content.[18] Reliability is ascertained through an examination of the completeness of the form of a record; the author's competence, which is the author's authority and capacity to issue such record; and the procedures exercising control over its creation. With photography, and every record, a standardization of the rules governing the process of creation and handling would increase its reliability. An example of such standardization is the procedure for creating a passport photograph, in which the content is strictly prescribed and then verified through the attestation of a qualified signatory. The photograph must conform to a particular size and must present an accurate visual representation of a person; otherwise, it is rendered ineffective. Of course, the purpose and expected use of a photograph determines the necessity and degree of procedural controls over its creation and maintenance over time. The functional purpose of a passport is to provide accurate identification of a person and regulate passage across international borders. The requirements for a record's reliability are directly related to the legal and regulatory context in which the persons concurring in its formation operate and its intended uses, as demonstrated by this example of the genesis of a passport photograph.

18. Accuracy refers to the precision of a record's content: it contributes to its completeness and is thus a part of reliability.

Inspired by the application of the diplomatic concepts of authenticity, originality, and reliability to the contemporary record-keeping environment initiated by Duranti, archivist Joan M. Schwartz published an article exploring the ability of diplomatics to reveal the true nature of analogue photographs.[19] In her article, Schwartz discusses the concept of originality of the state of transmission in relation to photographic negatives and prints. In her analysis, she contrasts the diplomatic definition of the original with past approaches taken by the archival community, and in the process she isolates the original's characteristic of primitiveness from completeness and effectiveness and equates originality with uniqueness, an interpretation that conflicts with the diplomatic approach to originality, which allows for primitiveness and plurality. This undermines her effort, as it is the presence of all three characteristics that determines the state of transmission of a photograph as an original. However, her attempt demonstrates the necessity of analyzing the characteristics of originality without elevating one quality over another. The strength of Schwartz's article lies in her argument that archival photographs are too often presented in publications and displays as decontextualized historical documentation, coupled with textual records as mere illustration, regardless of a *shared provenance*.[20] Schwartz demonstrates that photographs are created with the intent to convey messages, and too often their true meaning as records is obscured by their manner of dissemination and their valuation based solely on content.[21] Schwartz embraces diplomatics as an analytical tool for revealing the evidential value of

---

19. Joan M. Schwartz, "'We Make out Tools and Our Tools Make Us': Lessons from Photographs for the Practice, Politics, and Poetics of Diplomatics," *Archivaria* 40 (Fall 1995): 40-74.

In addition to Schwartz, archivist Lorraine O'Donnell published an article that focused on the nature of family snapshots and utilized a diplomatic framework. See Lorraine O'Donnell, "Towards Total Archives: The Form and Meaning of Photographic Records," *Archivaria* 38 (Fall 1994): 105-118.

20. Shared provenance refers to the records as byproducts of the activities of the same creator (individual, family or organization). Richard Pearce-Moses, *A Glossary of Archival and Records Terminology* (Chicago, IL: The Society of American Archivists, 2004) http://www.archivists.org/glossary/index.asp (accessed April 7, 2005).

21. Schwartz, "We Make Our Tools," 44.

photographs as records, referring to the context of the photograph provided by its origin, function, and the activities of its creator. By emphasizing context, Schwartz redirects the focus of contemporary archival practice away from her perceived fixation on content towards an analysis of the circumstances of a photograph's creation, use, and preservation. Her arguments are important because archival photographs are valued as authentic sources, and it is the duty of the preserver (i.e., archivist) to arrange and describe them in a manner that makes evident their identity and protects their integrity.

Legal Discipline

The history of the legal admissibility of photographs as reliable and authentic records informs current disputes regarding the challenges digital images present to the rules of visual evidence. During the late nineteenth century, the general acceptance of the veracity of the photograph began to falter as artistic applications of photography became more prominent and revealed the ability to alter an image through camera optics and darkroom techniques. As a result, the photograph's capacity to be used as direct evidence rapidly diminished and a photograph began to be considered hearsay and required human testimony to authenticate it.[22] Since the turn of the nineteenth century, statutory and common law evidence rules have allowed photographs to be introduced as evidence of facts related to legal proceedings, albeit with increasing controls over their admissibility.[23]

Evidential value in the legal sense refers to the usefulness of something to prove or disprove a fact. Relevance and authentication are the principal requirements for admitting a

---

22. See Thomas Thurston, "Hearsay of the Sun: Photography, Identity, and the Law of Evidence in Nineteenth-Century American Courts," *American Quarterly Online,* (2001), http://chnm.gmu.edu/aq/photos/index.htm (accessed April 9, 2005).

23. Photography's first mention occurs in Luco v. U.S., 64 U.S. 515 (1859), where a group of signatures, genuine and disputed, were examined in a single photograph. Ibid.

photograph into evidence. Authentication amounts to a testimony by a photographer or other qualified witness that the photograph is accurate in its representation of fact, and it is what it purports to be.[24] This authentication is based on a verification of authenticity, that is, on the process of establishing a correspondence between known facts about the photograph and the various contexts in which it has been created and maintained and the proposed fact of its authenticity.[25] A photograph that is offered as a general representation of physical objects in order to support a statement requires nominal proof of accuracy and minimal verification of authenticity, whereas a photograph offered as representation of handwriting, or certain objects in which the perspective is in question, requires a testimony that specifies the circumstances under which the photograph was taken such as the type of equipment, the method used to develop the negative and print the photograph, and possibly the competency of the photographer.[26] In the case of forensic photography, in which fingerprints are presented as an enlargement, or the contrast of a print is adjusted to accentuate footprints or bloodsplatter, the photographic process, that is, the alterations and operations performed during the process of creating the final print must be described by a criminologist for the court to determine whether it was a trustworthy process.[27] In these cases, the accuracy of the content of the photograph is sought through knowledge of the procedures over its creation. Eventually the legal system established that a photograph without testimonial sponsorship proves nothing.[28]

In the United States, in an effort to clarify the rules of evidence and create a doctrine that would supplement local regulations regarding the admissibility of photographs and

---

24. Porter v. Buckley., CA3d NJ 147 F 140 (1906).
25. Duranti, Eastwood, and MacNeil, *Preservation of the Integrity of Electronic Records*, 24.
26. Cunningham v. Fair Haven & W.R. Co. 72 Conn 244, 43 A 1047 (1899).
27. DeCamp v. United States 56 App DC 119, 10 F2d 984 (1926).
28. DeCamp v. United States (1926).

documents, the rules of evidence for both criminal and civil cases were codified as the *Federal Rules of Evidence Act* (FREA)[29] and the *Uniform Rules of Evidence Act* (UREA).[30] Since their enactment, both acts have been revised to reflect changes in society and the law, such as the introduction of new methods of communication. The process of revision requires some explanation in order to (1) provide a greater understanding of how the acts respond to new case law, (2) lay the foundation for an analysis of the rules regarding photographic evidence, and (3) explain how a discussion of the process of authentication and identification of photographs and the issue of originality and admissibility of duplicates reveals the structure underlying the FREA and UREA and the cultural expectations shaping their approach to photographs as reliable and authentic records.

The acts were promulgated while photography was predominantly an analogue process and output. At that time photographs were presumed dependable due to the assumption that a change in the information presented would be susceptible to detection through visual inspection. Technological developments in law enforcement are rapidly changing methods of gathering evidence and presenting it in legal proceedings; however, many of the rules regarding the admissibility of visual evidence still rest on assumptions made on the basis of analogue photography. An example is the *best evidence rule*,[31] which

---

29. The Federal Rules of Evidence (FRE) were adopted by order of the Supreme Court of the United States of America on November 20, 1972. The FRE Act (FREA) was enacted with amendments by Congress to take effect on July 1, 1975. The FREA is a federal statute that is not intended to preempt state law, but to supplement it. United States Government, *"Federal Rules of Evidence,"* (Washington, DC: US Government Printing Office, January 2, 2001).

30. The Uniform Rules of Evidence (URE) was drafted by the National Conference of Commissioners on Uniform State Laws in 1953; however, it was considered radical and was not adopted by all of the state jurisdictions. The URE Act (UREA) was revised in 1974 and modeled after the FREA. In 1999, the UREA was enacted. The most recent revisions and amendments to the Act occurred in 2005.

31. The Best Evidence Rule, also known as the Original Document Rule, requires that the original photograph be presented in order to prove its contents and be admitted into evidence. If for some reason the original is not available, the absence must be explained. If the explanation falls under the exceptions to the rule, then a copy or an oral testimony will be accepted in place of the original photograph.

requires that the original photograph be presented as evidence. Traditionally the negative or first print would be presented; however, in the digital environment, this requirement is open to interpretation since one could argue that the original digital image disappears as soon as it is saved for the first time onto a hard drive or removable medium such as a compact disc (CD).[32] The UREA was updated in 1999 to include definitions of terms and to facilitate greater interoperability with the FREA and, in many ways, the revised rules reflect the attempts of the legal community to address the digital environment and provide guidance.

A close reading of the definitions in Article X, Rule 1001 reveals a lack of precise terminology in defining the limits of photographs, digital images, and computer-generated records.[33] This suggests interpretations of the rules that are ineffective in discriminating between requirements for analogue photographs and digital images. A photograph is defined as "a form of a record which consists of a still photograph, stored image, X-ray film, video tape, or motion picture." The meaning of "stored image" is not explained; however, an image is defined as "a form of a record which consists of a digitized copy or image of information." It is unclear from this explanation if a born digital image would be considered an image or if the term only applies to information that has been translated from analogue to digital (i.e., digitized). Furthermore, the inclusion of the term "image," albeit qualified, in the definition of photograph is confusing. Would a photograph that is digitized exist as both a stored image and a photograph? If so, which document is the authoritative one? In the same definition, an original is equated with "a printout or other perceivable output of a record of images stored in a computer, if shown to reflect the images accurately." An advisory note to this definition explains that the status of an original photograph is strictly reserved for the negative;

32. The claim rests on the fact that an original digital file must be "copied" to memory in order to save it for future use/reference.

33. Unif. R. Evid. 1001 (1999).

however, practicality and common usage require that any print from the negative be regarded as an original.[34] There is no discussion of the nature of digital information and its challenges to the concept of the original and requirements of an original. Throughout Article X, the terms duplicate, copy, and print are used somewhat interchangeably, yet duplicate is the only term defined. A duplicate is "a counterpart in the form of a record produced by the same impression as the original, from the same matrix, by means of photography, including enlargements and miniatures, by mechanical or electronic re-recording, by chemical reproduction, or by another technique that accurately reproduces the original."[35] It is unclear what aspect of the original is being reproduced accurately, since documentary form is altered by any act of enlargement.

Forward thinking and the desire to bring the legal community up to date with practices employed in the current record-creation and record-keeping environment led to the *Uniform Electronic Evidence Act* (UEEA) in 1998. The act was a response to the need for admissibility of "any form of information in an electronic record, whether figures, facts or ideas."[36] The act was updated in 2002 and replaced the requirement of originality of individual records with the requirement of integrity of the electronic system containing the records, using standards to demonstrate the system's reliability and authenticity. The UEEA puts the burden of proving the authenticity of an electronic record in a legal proceeding on the person seeking to introduce it and states that proof of the integrity of the electronic system ensures the integrity of the individual record. This new rule places greater emphasis on the manner in which the record is created, used, and maintained and incorporates the contexts that generate a digital image. In this manner, system reliability becomes a substitute

34. Transport Indemnity Co. v. Seib, 178 Neb. 253, 132 N.W. 2d 871 (1965).
35. Unif. R. Evid. 1001 (1999).
36. Electronic Evidence Act, 2nd Session, 58th General Assembly (Revised 2002).

for record reliability. To prove system reliability and make evident the chain of custody, standard procedures for creation, receipt, and use of records must be documented; access privileges of individuals must be clearly designated with password protection; and audit trails to reveal any and all changes made to the records must be in place.[37] This approach is reflected in the Canadian Rules of Evidence regarding the acceptance of reproductions of records in place of the original records if certain procedural safeguards, established by the Canadian National Standards Board, have been met.[38] By requiring proof of compliance with standard operating procedures as a characteristic of a reliable record-keeping system, evidence laws are making explicit the importance of established procedural guidelines that emphasize accountability and implement an operational framework predicated on transparency to demonstrate the reliability and authenticity of digital images as legal evidence.

In recent years, imaging technology has improved in quality and dropped in price, and there has been a marked increase in computer literacy among the general public. Consequently, the assumption that image alterations are detectable, or that seamless manipulation is only the purview of experts, is no longer a valid stance. Additionally, the proliferation and diversity of digital devices capable of image capture and transmission, such as cell phones, introduce the possibility of a far greater range of image types and image creation processes whose admissibility in a court of law must be determined. Efforts made by the forensic community to address the admissibility of digital images may be found in online

---

37. These requirements are also aspects of compliance with Article IX, Rule 901, in the Federal Rules of Evidence for Authentication and Identification. Michael Kennedy, "Legal Issues: General Rules of Evidence for Authentication and Identification," *Journal of Imaging Services* (2002), http://www.dsasolutions.com (accessed May 20, 2005).

38. Donald S. Skupsky, "Legal Standards for Records and Information Management Programs," *ARMA Records Management Quarterly,* (July 1994), http://www.findarticles.com/p/articles/mi-_qa3691/is_199407/ai_n8716186 (accessed June 10, 2005).

journals and professional forums. Steven Staggs presents guidelines for ensuring digital image admissibility that reflect the definitions and requirements outlined in the FREA.[39] The first recommendation is to establish department policies regarding digital image use, documentation of a chain of custody, image security, and access to images. The next step is to implement these policies as standard operating procedures. In regard to the issue of the original in the digital environment, Staggs suggests preserving the digital original in its capture format, that is, the original file format. If the digital original is not copied onto removable media for storage and is instead held on a shared hard drive, access privileges are recommended that reflect user groups with defined competencies for viewing, altering, and deleting image files. Lastly, Staggs recommends implementation of file-naming conventions that identify originals and surrogate files as separate from one another. Efforts by the forensic community to define and develop guidelines and best practices for the creation, use, and preservation of reliable and authentic born digital images highlight the nascence of legal regulations specific to digital representation.

Photographic Discipline

"The Work of Art in the Age of Mechanical Reproduction," written by Walter Benjamin in 1935, addresses the role of photography as an art form within the critical frame of political and economic movements that value the qualities of reproduction and consumption over uniqueness and ritual.[40] In his examination of the nature of photography as a product of mechanical reproduction, Benjamin explores the meaning of originality and its

39. Steven B. Staggs, "The Admissibility of Digital Photographs in Court," *Crime Scene Investigator,* (2001), http://www.crime-scene-investigator.net/admissibilityofdigital.html (accessed June 23, 2005).

40. Walter Benjamin, "The Work of Art in the Age of Mechanical Reproduction," in *Illuminations,* ed. Hannah Arendt, trans. Harry Zohn, 217-247 (New York: Shocken Books 1969).

relationship to authenticity. He equates originality with an art object's unique existence, which is determined through an examination of the changes in the ownership of the object and its physical medium. Ownership is traced through the location of the original, and changes are reflected in its movement as it is exchanged from one owner to another. The physical medium is identified by chemical analysis, and the effects of time are determined scientifically through physical inspection.[41] Benjamin asserts that in the reproduction of photographs through mechanical means, a mass number of copies can be quickly produced and widely disseminated, activities that destroy the ability to trace an object's history through change in ownership or physical medium. The removal of the photograph from its original context through mechanical reproduction interferes with the art object's *historical testimony*.[42] This places the mechanically produced photograph in direct conflict with Benjamin's metaphysical concept of authenticity: "The authenticity of a thing is the essence of all that is transmissible from its beginning, ranging from its substantive duration to its testimony to the history which it has experienced."[43] Thus, as the link between the object and its origin is destroyed through mass reproduction and distribution, the photograph's unique existence is replaced by a plurality devoid of the capacity to act as historical testimony. Benjamin asserts that originality is a prerequisite of authenticity, and therefore there can be no such thing as an authentic photographic "print" because its duplicity is a foil.[44]

To support his claim, Benjamin explains that historically, the first function of the art object was in the service of ritual. This was expressed through religious ceremonies that cultivated respect for the inherent aura of an unapproachable idol, often depicted in a

---

41. Ibid., 220.

42. Benjamin uses the phrase "historical testimony" to refer to art's capacity to act as evidence of changing phenomena or past actions. Walter Benjamin, Ibid., 221.

43. Ibid.

44. Ibid., 224.

painting or statue. Art was attributed with the uniqueness of the phenomenon and gained cult value. Later, the secularization of art replaced ritual with authenticity. Authenticity became equated with the genius of the maker and the uniqueness of the creation.[45] Connoisseurship determined the value of art instead of religious fetishism. The following advent of mechanical reproduction replaced authenticity with reproducibility. Therefore, the value of photography became instilled in its capacity for dissemination and the experience of a phenomenon was substituted by a representation of reality as shown through the camera's mechanical eye. In effect, the photograph started to be seen as altering our perception of time and space by presenting the viewer with a referent devoid of context. Art galleries, magazines, and post cards favoured the photograph for its immediacy and its disembodiment. The hegemony of connoisseurship was leveled by the democracy of the multiple.

The explanation presented by Benjamin regarding the evolution of art and its shifting value creates a timeline in which photography and its technological infrastructure are placed in the position of transforming the very nature of art and, by implication, challenging the Victorian structures of social morality and class hierarchies. Benjamin observes that the public's response to conventional art is uncritical enjoyment, whereas its response to a truly new art form is to criticize it with aversion. His observation actually predicts the initial public response to the integration of digital technology into photographic practice and the skeptical introduction of born digital images as a prevalent form of visual culture.

Starting in the early 1980s in the fields of science and communications, the production and transfer of digital images began to replace functions previously performed by traditional analogue photography. The increasing use of digital images in news media raised

---

45. Benjamin offers this explanation of the concept of authenticity in his notes at the end of his essay. Ibid.

concerns regarding editorial decisions to alter images and quickly led to investigations into the boundaries between image processing and outright deception. As a result, new terminology developed to assist in identifying digital imagery and to distinguish analogue photographs from their digital counterparts.

At the same time, discussions about visual representation emerged that contrasted the trustworthiness of analogue photography with the potential for deception posed by digital imagery. An expression of this argument is found in the title and work of William J. Mitchell's *The Reconfigured Eye: The Visual Truth in the Post-Photographic Era.*[46] Mitchell begins by comparing how digital and analogue information are created and received. He describes the nature of digital representation as "discrete," referring to how a digital image is composed of separate pixels that are perceived from a distance to be continuous. These pixels represent distinct values that may be calculated and replicated exactly. Digital information is characterized by its seamless and rapid manipulation of content for reuse, which is made possible by the fact that the mathematical values assigned to each pixel can be altered without detection. In contrast, analogue representation is a continuous spectrum that is characterized by permanence (alterations are easily detected) and uniqueness (a physical original exists for comparison). Mitchell asserts that in addition to its structure, the analogue photograph's correspondence with reality endows it with truthfulness. Furthermore, analogue photography relies on a mechanical apparatus to accurately represent the objects in front of the lens as evidence of that reality; in so doing, Mitchell likens photography to a causal process based on physical and chemical forces, rather than an intentional one. He attributes the intentional process to digital imagery, which involves incorporating multiple digital

46. For the purpose of this thesis, the chapter "Intention and Artifice" is explored in depth. See William J. Mitchell, *The Reconfigured Eye: The Visual Truth in the Post-Photographic Era* (Cambridge: MIT Press, 1994), 23-56.

devices for input and output, is less reliant on standardized procedures, and is more heavily influenced by the artistic intent of the creator.[47] On this basis, the meaning of a digital image is not determined by a correspondence between reality and its representation.[48] Therefore, the "truth" of a digital image must be evaluated using a different set of principles. Mitchell attempts to demonstrate that a digital image could not be a true record of the real by contrasting its content with its context. He presents a method of testing the authenticity of a digital image by establishing the image's provenance (time and date created), the authority and trustworthiness of the originator, the accuracy of the process, and the chain of transmission.[49] This information is in turn, measured against other testimonies of historical evidence. In effect, Mitchell's observation confirms that the techniques of digital simulation and visualization are changing the idea of representation and its association with truthfulness as a correspondence between image and object.[50] By this conclusion, Mitchell establishes the need for documentation about an image in order to verify its authenticity.

Unlike analogue photographs, the authenticity of which Mitchell asserts is established by examination of the "original negative" and the reliability of the printing process, digital images challenge the concept of originality in their capacity for endless replication and require a different method of examination to prove authenticity. Whereas the film emulsion of a negative can be examined for proof of tampering and factual correlation with the photographic print, this is not possible in the digital environment. Instead, an indicator of

---

47. Ibid., 31.

48. The correspondence theory of truth has two systems, a representing system (the photograph) and a represented system (the natural world) and a correspondence between the two systems. Truth is determined by correspondence between the photograph and reality. The photograph presents a visual depiction that corresponds to reality and thus it is true because it does so. See Ibid., 24.

49. Ibid., 43-49.

50. Coherence with a set of beliefs is the test of truth. The truth of a digital photograph consists in its coherence with a specified set of propositions, not with the existence of a unitary extrapictorial reality. Consistency between what one knows about a specific situation and what is visually depicted in the digital photograph may lead to a truth claim if no contradictions occur. See Ibid., 36.

alteration may be located in the time and date stamp attached to a digital image.[51] Mitchell suggests that the traditional distinction between originals and copies is made on the basis of a hierarchy that derives from the primacy of the negative to create derivatives and the distinctly inherent loss of quality with each copy made. Artists wanting to control or limit the reproduction of analogue photographs may destroy the negatives, thereby increasing the value of the existing prints and reasserting the primacy of the negative as the original. In part, the value of analogue photography rests in its capacity to be owned and controlled, whereas Mitchell identifies the value of digital imagery with its capacity to be manipulated and shared.[52] Without an authoritative original, the digital image is divorced from the concept of authorship and functions as an entirely new graphic construct that may be used for many of the same purposes and in many of the same contexts as traditional analogue photographs, but without the characteristics of stable form and content. In so doing, digital images challenge traditional assumptions about the relationship between visual representation and the truth.

Along the same lines, art theorist Lev Manovich explores the threat posed by digital imagery to traditional notions of visual truth; however, he arrives at a different conclusion.[53] Manovich asserts that digital images break away from traditional visual representation while at the same time reinforcing it. Issues posed by digital images and attempts to develop criteria to assess their reliability and authenticity contribute to and shape the discourse on the

---

51. Mitchell also asserts that the time and date stamp of an image file is dependent upon the system hardware with which it is saved. Therefore, errors may occur, or intentional alteration by a person with a degree of technical expertise may change this characteristic of provenance. Ibid., 51.

52. The type and degree of manipulation allowed by digital photography is the key difference between digital and analogue. Mitchell recognizes that the ability to manipulate a digital image file without producing any evidence of change challenges its reliability. "Image files are ephemeral, can be copied and transmitted virtually instantly, and cannot be examined (as analogue negatives and positives can be) for physical evidence of tampering." Ibid.

53. Lev Manovich, "The Paradoxes of Digital Photography," in *Photography after Photography: Memory and Representation in the Digital Age,* ed. Amelunxen Hubertus, Stefan Inglhaut, and Florian Rotzer (Sydney: G&B Arts, 1996), 57.

role of context to determine meaning. The power of context to alter the meaning and reception of visual representation is an ongoing theme in the study and practice of art. Manovich reflects on the use of manipulation in *photomontage* in the early nineteen hundreds as a method of investigating the concepts of authenticity and originality in relation to imagery.[54] Juxtaposing readily available visual sources as the content of photomontage, that is, creating a purposive assemblage of disparate contexts, generates new meaning and, in turn, makes one question the authority and authenticity of visual representation. It is recognized that the disruptive power of photomontage lies in its construction, which jeopardizes the concepts of originality, reliability, and authenticity.[55] In so doing, photomontage links the notion of originality and the primacy of creation with authenticity and questions the construction of meaning through mediated images. The discourse initiated by post-war artists using photomontage as a method for re-interpreting the authority of the visual image is continued in current explorations into the ways digital technology disrupts the notion of the original. Of course, the diplomatic and legal perspectives on this issue are that a photomontage is a new image, with its own originality and authenticity.

Existing Practices

The fact that digital images are presented in the same context or, increasingly, as substitutes for analogue photographs in the fields of medicine, photojournalism, and the criminal justice system makes the assurance of their reliability and authenticity an ethical and

54. Photomontage refers to the technique of combining multiple photographs into a composite image.

55. Sources for early photomontage were derived from magazines and newspapers intended for consumption. The images were selected and assembled within an arbitrary frame to challenge the authenticity of art. Timothy Druckery, "From Dada To Digital: Montage in the Twentieth Century," *Aperture* (Summer: 1994), 4-7.

legal issue. Photojournalists, forensic photographers, and medical illustrators must be conscious of the ways digital images mimic traditional photographs in their delivery and reception of visual information. In the absence of a label identifying visual content as either digital or analogue, efforts to control the creation and reproduction of digital images and ensure their reliability and authenticity have therefore emerged through industry-specific best practices, guidelines, and ethical codes. The following discussion explores current initiatives that aim to redress the challenges to reliability and authenticity presented by the creator's use and maintenance of digital images in the fields of law enforcement and photojournalism.

The development of a body of knowledge in forensic science regarding the creation, handling, and storage of digital information began in 1995 and has grown steadily in the past decade.[56] The increasing use of digital information, in particular digital images, to assist and in some cases perform the activities of law enforcement has created a need for international and national organizations to produce guidelines and standard operating procedures to ensure that digital images can be assessed as accurate, reliable, and authentic evidence.[57] The Scientific Working Group on Digital Evidence (SWGDE) is a North American group consisting of representatives from federal crime laboratories and state and provincial law enforcement agencies. SWGDE has focused on producing guidelines for the handling and exchange of digital evidence, and has worked with the Scientific Working Group for Imaging Technologies (SWGIT) to develop guidelines for good practices in the use of imaging technologies within the criminal justice system. Together they have authored "Recommended Guidelines for Developing Standard Operating Procedures," "Guidelines and Recommendations for Training in Digital & Multimedia Evidence," and "Proficiency Test

56. Mark M. Pollitt, "Report on Digital Evidence," in *13th INTERPOL Forensic Science Symposium* (Lyon, France: INTERPOL, 2001), 2.

57. Ibid., 2.

Program Guidelines." SWGIT has proposed two draft best practices, "Documenting Image Enhancement" and "Practitioners of Forensic Image Analysis."[58] The goal of these publications is to facilitate the integration of imaging technologies and systems within the criminal justice system and to provide guidelines for the capture, storage, processing and analysis, transmission and output of digital images according to legal standards set for the admissibility of visual evidence. The 2002 "Guidelines for the Use of Imaging Technologies in the Criminal Justice System, Version 2.3" proposed methods for ensuring the reliability and authenticity of digital images as evidence.[59] This document will be discussed at length in Chapter 3.

The field of photojournalism has also experienced rapid technological growth and is reliant on the accuracy, reliability, and authenticity of its digital images as sources. Editorial and documentary photographers are part of the larger telecommunications industry that provides information on a global scale. The need to create and maintain reliable and authentic digital images for news reportage has provided the impetus to update existing ethical standards and improve the integrity of information transfer across wireless networks. The National Press Photographers Association (NPPA) adopted the "Digital Manipulation Code of Ethics" into the "NPPA Code of Ethics" in June, 1995, in an effort to address the public's growing suspicion of digital images.[60] The code states that "[a]s journalists we believe the guiding principle of our profession is accuracy; therefore, we believe it is wrong

---

58. All documents are available as PDF downloads from the International Association for Identification Website. See Scientific Working Group on Imaging Technology, "Documents," (International Association for Identification, http://www.theiai.org/swgit/index.html (accessed April 17, 2005).

59. SWGIT, "Guidelines for the Use of Imaging Technologies in the Criminal Justice System" V.2.3," International Association for Identification (2002). http://www.theiai.org/swgit/ (accessed May 28, 2005).

60. National Press Photographers Association, "Digital Manipulation Code of Ethics: NPPA Statement of Principle," *Business Practices*, http://www.nppa.org/professional_development/business_practices/digitalethics.html (accessed March 11, 2005).

to alter the content of a photograph in any way that deceives the public."[61] In addition to content, photographers working in the digital environment are learning the necessity of retaining the context of a digital image to assist editorial decisions to alter images for publication. These decisions risk disturbing the essential relationship between content and context and thus destroy the reliability and authenticity of the image as a record of a real event. Furthermore, this brings into question the authenticity of the digital image as a visual source.

The International Press Telecommunications Council (IPTC), established in 1965 as a consortium of major news agencies and news industry vendors, develops and publishes technical standards for the interchange of news data.[62] With the advent of multimedia Web exchange, the IPTC recognized the need to link the textual information describing a digital image (i.e., metadata) with the image data itself. In 1991, they introduced the Information Interchange Model (IIM) as a metadata and binary structured framework to handle the transmission of digital resources of all types.[63] Simply put, when a digital image is transmitted from the photographer to the news service bureau, an envelope of information identifying the type of data, the file format, its context and content is virtually wrapped around the image and transmitted as one self-explanatory entity. This technique enables pertinent editorial and technical information to accompany the digital image during its transmission, such as the image title, date created, author, location, copyright, and descriptive caption. The IPTC metadata initiatives, along with standards such as the Exchangeable Image

---

61. Ibid.

62. The first approved news exchange standard was in 1979, the "IPTC 7901." See "The IPTC-NAA Standards," Controlled Vocabulary.com, http://www.controlledvocabulary.com/imagedatabases/iptc_naa.html (accessed March 12, 2005).

63. IPTC, "Information Interchange Model," IPTC (2005), http://www.iptc.org/IIM/ (accessed March 12, 2005).

File Format (Exif) promulgated by the Japan Electronics & Information Technology Industries Association (JEITA),[64] are examples of approaches to documentation that may be used to link digital image content with its context and make evident a record's attributes of identity and integrity. In turn, preservers may utilize this documentation at a later date to support a presumption of the record's authenticity.

Conclusion

In general, the archival, legal, and photographic disciplines bear similarities in their understanding of the concepts of reliability and authenticity. Reliability is viewed as the trustworthiness and accuracy of the content of a photograph. The reliability of a photograph is determined through analysis or review of the controls over the procedures of creation and use and the competency and authority of the persons involved in these activities. Diplomatics and the law both address reliability as the trustworthiness of a record as a statement of fact and allow for the assumption that records are reliable so long as they continue to be used by their creator in the usual course of business. The accuracy of content is approached in the arts as a direct reflection of the methods employed in the creation of the photograph. Traditional assumptions about the verisimilitude of the analogue photograph inherent in its mechanized processes of creation are being revisited in light of digital imagery. Regardless of the fact that the computer and the camera are both machines, the conservative view of analogue photography as "objective," and therefore reliable, is made on the basis of the photographer acting as a passive operator of the mechanized camera and the correlation between reality

64. Japan Electronics and Information Technology Industries Association, "Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.2," JEITA (2002), http://www.exif.org (accessed June 3, 2005).

and the photographic referent. In contrast, the processing capabilities of digital cameras and image software programs offer edit operations that are far beyond the capabilities of traditional darkroom techniques and camera optics; therefore, the born digital image is viewed as a fabrication of reality and "subjective" at best. All three disciplines address the nature of digital information and its capacity for seamless manipulation and endless replication as a threat to established procedures and methods for establishing the reliability and authenticity of a visual source. In affirming this, they recognize that digital imagery introduces and in some cases re-engages the discourse on the role of context in visual representation and cultural communication.

Authenticity is equated with trustworthiness of the image as an object in both diplomatics and the arts. Diplomatics breaks authenticity down into identity and integrity, which are demonstrated by attributes of the record that provide essential information about the photograph and about the procedural controls over its use and maintenance. Legal requirements for authenticity focus upon providing documentation that attests to the integrity of the digital image and provides the identity of individuals involved in its creation, handling and maintenance, which are expressed through documentation such as evidence of a chain of custody. Policies and standard operating procedures are recommended by agencies that operate within legal and regulatory environments as controls that are able to ensure digital images will be admissible. Criticism of digital imagery from within the arts community has centered on its capacity for limitless replication and seamless alteration as a threat to record identity and integrity. In some respects, the advent of digital technology has re-engaged many of the earlier discussions about the effects of photography on the evolution of artistic practice.

The similarities between Mitchell's approach to verifying the authenticity of born digital images and the legal requirements for authentication and identification presented in Article IX, Rule 901 of the Federal Rules of Evidence provide valuable insight into the attributes of image identity and integrity. A basic set of conceptual requirements is presented that includes capturing information about the context of image creation, use, and preservation and providing documentation that reveals a chain of custody. A trusted chain of custody or knowledge of a photograph's custody over time is understood as a method of ensuring its integrity in both the analogue and digital environment. The evolution from authenticating one record to establishing the integrity of the electronic record-keeping system as proof of the authenticity of all digital images held within it reveals the progression of the law as it responds to new technologies in communication.[65]

The commonality found among the disciplines in regard to the concepts of reliability and authenticity is not evident in their understanding of originality and what constitutes the difference between an original and a copy. The role of the original in photography is generally understood by all three disciplines as residing in the characteristic of primitiveness (i.e., the first instance of the captured image, be it analogue or digital), but it is here that the similarities end. Diplomatics and the law make allowance for the possibility of multiple originals, which are made at the same time, are complete, and are capable of fulfilling their intended use. The arts are more reticent to accept the notion of plurality as an attribute of the original, choosing instead to focus on uniqueness. The analogue original refers to the film and the print is a numbered multiple in a series or edition. Much of the criticism about the lack of "truth value" in digital imagery stems from the absence of an original for the purpose

65. Electronic Evidence Act.

of comparison. The law has a broad interpretation of the digital original and the prevailing notion is that if an original digital image does exist, it should be preserved for purposes of comparison. Therefore, the law recognizes the existence of a digital original. The literature that discusses current legal requirements for original digital images is critical of the terminology and categorization of photographs, images, and computer records. In general, a more rigorous approach to defining digital imagery and requirements for its admissibility are encouraged within the legal community.

This chapter has shown how the literature on photography treats the concepts of reliability and authenticity and how existing standards address them within specific industries such as law enforcement. Photographic representation is shaped by the techniques selected by creators to fulfill purposes that are determined by the functional origin of the photograph. The way photographers actually deal with creating digital images to achieve business purposes requires closer examination. Therefore, Chapter 2 presents an analysis of the record-creating and record-keeping habits and routines of photographers, and will provide a greater understanding of the procedures they use for the creation, management, and preservation of digital images as reliable and authentic records and of their awareness of the dangers presented by technological obsolescence.

CHAPTER TWO

This chapter discusses the results of a Web-based questionnaire surveying the record-keeping practices of photographers who use digital technology. Conducted under the auspices of InterPARES 2, the survey explores how photographers are creating, using and preserving digital images. Prompted by a lack of information regarding the documentary procedures and business practices of photographers working in the digital environment, the survey contributes a new perspective to the discourse on the evolution of photographic representation and the trustworthiness of digital images. Analysis of the resulting data will assist in determining whether photographers are creating digital images as reliable records and are managing and preserving these images in a manner that ensures their authenticity for the long term.[66]

Survey Methodology

The development of the survey was initially based on the hypotheses that (1) photographers keep their digital images for re-use and reference, (2) they are not generally concerned with authenticity and reliability, and (3) they have not begun to grasp the challenges to continuing access and long-term preservation presented by the use of proprietary digital systems and by technological obsolescence.

An iterative research design was predicated on the exploratory nature of the research topic and the lack of existing sources specific to the integration of archival and diplomatic

66. A future activity of InterPARES 2 will be communication of the research findings within the photographic and archival communities to aid in the development of management methods for digital images that implement controls over creation, use, and preservation to overcome the threat posed by the digital environment to the reliability and authenticity of photographic representation.

concepts with photographic practice. A review of archival and photographic literature revealed a handful of sources addressing the concepts of reliability and authenticity in regard to analogue and digital images; in addition, these sources were theoretical in nature and did not provide methodologies for creating born digital images as reliable records and ensuring their authenticity throughout preservation.[67] The prevailing assumption contained in the literature is that digital images are not as trustworthy as their analogue counterparts and are therefore destabilizing the authoritative status of the photographic document; yet, the arguments used to support these claims do not rest on actual photographic practice in the digital environment. The result of these discussions is a wealth of theoretical speculation that does not offer any solutions.

The overarching research method identified as the best one for gathering rich data – which could provide insight into the photographers' work practice and their complex view of digital imagery – was qualitative. A Web-based survey was deemed the most effective and efficient method of collecting data, based on the presumption that photographers using digital technology to create and manage their images have a relatively high degree of computer literacy, technical expertise in the operation of mechanical systems, and access to, as well as experience with, the Internet. The survey targeted photographers who are known to create digital images and use digital technology to manage and store their images, such as photographic artists who incorporate digital technology into their practice and law enforcement officers currently working with forensic digital image processing. In addition,

---

67. The InterPARES 2 decision to launch a Web-based survey was made on the basis of research that contributed to the "Bibliography of Digital Photography," the "Annotated Bibliography of Digital Photography" and the "Literature Review of Digital Photography (Authenticity, Accuracy and Reliability)." These are documents contained in the restricted area of the InterPARES 2 Web site, but will be made public in the near future. The Web-based survey, "Record-Keeping Practices of Photographers using Digital Technology" received the Certificate of Approval: B04-0526 from the Behaviour Research Ethics Board at the University of British Columbia on August 20, 2004.

the purposive sample targeted professional online forums and photographic association Web sites that foster a community of photographers using digital technology, such as the National Press Photographers Association, Stock Artists Alliance and the Professional Government and Military Photographers of Canada.[68] By posting the invitation to online newsletters and professional forums, the potential participants increased to approximately 14,500 and included photographers from North America and the United Kingdom.[69] The Web-based survey method made it possible to contact a large number of professional photographers working in a variety of business contexts and operating within different regulatory frameworks. The total number of responses to the survey was 402.[70] Respondents were located in the United States, Canada, Great Britain and Ireland.[71] They were professional photographers working with digital technology in fields that included photojournalism, fine art, commercial studio, medicine, military and government, geology, astronomy, forensics and law enforcement.[72]

Interested photographers were required to complete and submit an electronic consent form before gaining access to the questionnaire. The "Informed Consent Information Letter" stated that participation was limited to professional photographers using digital technology, and defined the objectives of the survey, which were to obtain qualitative and quantitative

---

68. The administrative and technical officers of each professional association granted permission to post invitations to their membership list, and in many cases they did the actual posting of the invitation themselves. A complete list of participating organizations and institutions is located in Appendix A, "Survey: List of Participating Organizations," 128.

69. Numbers are based on association membership tallies; however, it is impossible to know for certain how many photographers are currently receiving association information on a regular basis.

70. The total number of respondents for each question is recorded in the upper right-hand corner of each chart and percentages are shown with bar graphs. See Appendix C, "Survey: Questions & Charted Responses," 131.

71. See Appendix A, "Survey: List of Participating Organizations," 128.

72. See Question 1 in Appendix D, "Survey: Selected Textual Responses," 147-149.

data on photographers' use and knowledge of digital technology.[73] The survey was contextualized within the larger research goals of InterPARES 2, mainly the investigation of problems surrounding the reliability, authenticity, permanence, and accessibility of digital records.

The questionnaire was designed for maximum usability, with 33 multiple-choice questions and boxes for optional additional commentary. The inclusion of text boxes for each question and a request at the end for additional information regarding photographic record-keeping practices in the digital environment resulted in the discovery of industry-specific best practice guidelines and a greater understanding of individual work habits and routines. The questions were formulated to gather information regarding the principles and procedures that contribute to the creation, use, and preservation of digital images as reliable and authentic records; however, the terms "reliability" and "authenticity" were omitted from the survey to avoid confusion resulting from individual and disciplinary interpretations of their meaning.[74]

The immediate and virtual nature of online interaction and e-mail communication required a follow-up e-mail one month after the first invitation to remind candidates to participate in the survey before the established deadline.[75] This proved to be an effective method of increasing participation.

The responses to the questionnaire were transmitted across the Web and collected within a database that was securely operated by the InterPARES 2 designated technical co-

---

73. See Appendix B, "Survey: Informed Consent Information Letter," 129.

74. The conceptual basis of the questionnaire was founded on the findings of the InterPARES 1 project. See Duranti, Eastwood, MacNeil, *Preservation of the Integrity of Electronic Records.*

75. If a person does not respond immediately to an electronic invitation it may be assumed that the daily inundation of electronic communiqué will obscure recent items. The layouts of most e-mail applications make it onerous to review electronic messages more than one week old. The survey was posted online for two months, starting September 15th, 2005 and terminating on November 13, 2005.

ordinator.[76] The collected data was output in Excel spreadsheets, which were used to organize and analyze survey responses. Data analysis was conducted on the basis of qualitative techniques such as tallying the responses to each multiple-choice question and expressing these numbers in percentages and examining the additional textual responses for categories and themes.

Survey Findings

This report on the results of the survey is divided into two broad sections that address issues contributing to the reliability and authenticity of digital images. The first section explores actions and procedures that affect the reliability of a digital image. Discussed in this section are the different types of file formats and software applications that photographers use for the creation and management of their born digital images, the concept of "original" and its characteristics in the digital environment, and the analysis of individual work habits and institutional practices. Both the quantitative and qualitative survey data are used to interpret the series of decisions and actions that guide the creation and use of digital images as reliable records. The second section explores actions and procedures that affect the authenticity of a digital image. Discussed in this section are the steps taken by photographers to store and preserve their digital images and the security measures they take to protect images during transmission. The critical role of metadata, and its essential contribution to establishing the reliability and proving the authenticity of a born digital image, is dealt with in both sections because metadata are generated at different stages throughout the life cycle

76. Web-based surveys require a computer programmer to create interactive web pages with programmed language, in this case, ColdFusion (CFML). ColdFusion is a *Macromedia* product that allows web pages to interact with databases.

of a record. Metadata elements are organized into a schema that defines and delivers digital image structure, content, and meaning. The application of metadata to a digital image file is controlled by the structure of the schema. There are many types of metadata schemas that provide a variety of information about digital records. The schema itself is composed of metadata elements that define specific characteristics of a record such as the name of the author, the date and time of creation, and so on.[77] Further explanation of the informational structure of digital image metadata, the functional purpose of metadata, and existing metadata standards for digital images will be presented later in this chapter.

The survey indicates that most photographers are aware of the issues of media fragility and technological obsolescence; however, their decisions regarding creation, management, and preservation are determined by their business needs and their artistic intentions, which lead to choices that may place the longevity of their digital images at risk. The photographic profession has embraced the transition from analogue to digital in response to clients' growing expectations for faster turnaround times, creative innovation, and remote transmission. Because of this situation, photographers concentrate on the active stages of an image's lifecycle and avoid addressing its long-term needs. Most photographers describe their practice as completely digital, allocating the use of analogue film to the occasional personal project.[78] Even among photographers who identify their practice as a hybrid of digital and analogue, the bulk of the images are born digital with only a small percentage of analogue images that are eventually digitized.[79] Most photographers are aware of the fragility

---

77. Technical Advisory Service for Images, *Metadata Standards, Schemas and Specifications,* http://www.tasi.ac.uk/advice/delivering/metadata.html (accessed June 30, 2005).

78. Out of 389 respondents to Question 2, 69% produce images by using a completely digital process. See Appendix C, "Survey: Questions and Charted Responses," 131.

79. Thirty-one percent produce images in a hybrid practice. Ibid. Additional comments revealed a commonality within hybrid practice, which is that 90-95% of the images are born digital and 5-10% are

of digital media and the vulnerability of the digital environment in which they work, but they lack confidence in the methods and procedures they use to protect their digital assets. Many of the respondents posed comments that were, essentially, asking for advice. This is especially true of freelance photographers who do not operate in structured environments such as institutional settings and are not directly regulated by a specific industry. Most photographers have not lost valuable digital image files through software or hardware obsolescence; however, many of them have experienced problems accessing early text-based documents and are currently implementing preservation actions to prevent the loss of their image files stored on digital media. In most cases, preservation decisions are made ad hoc and determined by financial constraints and time limitations.

Survey Findings: Creation and Use

Initial decisions made by photographers during in-camera capture determine the quality of the digital image data. The ability to *re-purpose* a digital image to fulfill more than one creative objective is determined by the choice of file format at the time of capture.[80] Although standardized file formats exist, such as the Joint Photographers Expert Group (JPEG) and the Tagged Image File Format (TIFF), many photographers risk the future usability of their digital images by selecting proprietary file formats, such as RAW, for initial capture.[81] The RAW format refers to the unprocessed or "raw" digital image data in the

---

digitized from analogue sources. See Question 2 in Appendix D, "Survey: Selected Textual Responses," 150-151.

80. To re-purpose something, in this case a digital image, refers to the process of using an image more than once, either in part or as a whole, for another purpose. Software programs with special image processing tools enable photographers to edit and seamlessly combine multiple images into one final composite image or to crop and divide a single image into multiples.

81. Out of 389 respondents to Question 3, 49% capture in JPEG and 29% capture in RAW. See Appendix C, "Survey: Questions and Charted Responses," 132.

camera before applying any in-camera settings such as compression, white balance settings, and colour calculations. Photographers refer to RAW as the camera file format that accurately represents the scene information received by the pixel sensors inside the camera. Thus, a digital image in RAW format is the image that contains the largest amount of unprocessed information possible. The RAW digital image file is likened by photographers to the in-camera analogue negative before chemical development. In cases where photographers use RAW format to capture the scene digitally, the RAW file is equated with the original image and treated as such throughout subsequent procedures for use and preservation.[82] An original digital image is identified as the first instantiation of the data captured by the camera's photosensitive detectors, using charge-coupled device (CCD) or complementary metal oxide semiconductor (CMOS) technology.[83] The technical process of digital image capture relies upon a light source to react with a photosensitive surface of the CCD or CMOS to form a visual representation.[84] In many ways it is similar to the analogue process of light reacting with chemicals on an emulsified film surface to produce a latent image, which will later be processed into a photographic print.

RAW and JPEG are the two most common file formats captured in-camera by photographers.[85] JPEG is the standard file format for newspaper photography: many of the photographers who participated in the survey identified themselves as photojournalists who capture the JPEG file format in-camera and transmit it along with its metadata to the news

---

82. Out of 375 respondents to Question 8, 71% consider the camera image file to be the original and additional comments identify the RAW format as the file format associated with the camera image file. Ibid., 134; Question 8 in Appendix D, "Survey: Selected Textual Responses," 153-156.

83. Bruce Fraser, "Understanding Digital Raw Capture," Adobe Systems Inc. White Paper (2004), http://www.adobe.com (accessed May 24, 2005).

84. Simply put, the reaction between the light and the CCD triggers a process of repeating electrical charges that are converted to digital information and stored in the camera's memory, either internally or on an external device such as a memory stick.

85. Out of 389 respondents to Question 3, 49% capture in JPEG and 29% capture in RAW. Appendix C, "Survey: Questions and Charted Responses," 132.

agency.[86] JPEG is an open standard, which means that its specifications are available to the public, and it is cross-platform operable, which means that the image and its metadata should remain intact when they are transmitted across systems and software applications.[87] The drawback to the format is its use of *lossy*[88] compression, which enables it to be transmitted quickly but makes it less than desirable for purposes beyond newspaper publication and online dissemination. The problem posed by lossy compression is that the image does not retain as much detail or bit-depth after being compressed in this manner.[89]

Photographers who do not operate within the news industry, or who are working on personal projects, capture their digital images as RAW files. The RAW specification is proprietary, determined by each camera manufacturer, and requires conversion software to transform the encoded sensor information into a RAW image file. Unlike JPEG, which is captured in-camera using the existing camera settings, the RAW sensor data are captured as unprocessed grayscale information that must be converted to red, green, blue (RGB) or cyan, magenta, yellow (CMY) to create a colour digital image.[90] The conversion process (i.e., an algorithm) that transforms the sensory information into colour representation is different for each make and model of camera and is proprietary. The purpose of the conversion is to allow

---

86. Out of 371 respondents to Question 1, 57% identified themselves as photojournalists. See Appendix D, "Survey: Selected Textual Responses," 147-149.

87. The details of digital image metadata transmission will be discussed at length in Chapter 3.

88. Lossy compression is an algorithm that removes irrelevant data or information that makes little difference to the perception of the image by the human eye. Lossy compression may reduce the image file size to 10% of its original size without distortion; however, the compression is irreversible and the information is permanently discarded. See Technical Advisory Service for Images, *"File Formats and Compression,"* http://www.tasi.ac.uk/advice/creating/fformat.html (accessed June 20, 2005).

89. The bit-depth of a JPEG file is a maximum of 8 bits per colour channel (i.e., red, green, and blue). This value is a measurement and controls the amount of luminosity and colour available for image presentation. In comparison, RAW format provides 16 bits per colour channel, which offers a 48-bit image capable of representing billions of colours. See Michael Reichmann, "Understanding Bit Depth," *The Luminous Landscape,* (2005), http://www.luminous-landscape.com/tutorial/bit-depth.shtml (accessed July 5, 2005).

90. Cameras that capture RAW data use a *colour filter array* (CFA) to convert the grayscale information into colour representation. This is a complex conversion that incorporates metadata about the filter device and the sensory capture settings to enable interpolation of colours. Fraser, "Understanding Digital," 2.

photographers more creative flexibility; however, no standard specification for RAW exists, which means that it is determined by each manufacturer. Therefore, RAW image files contain the pixel information (i.e., the image), the setting metadata (i.e., information automatically captured about the technical settings of the camera), and metadata specific to the arrangement of the colour filters on the sensors, which is proprietary to the camera manufacturer and may be encrypted. This last category of metadata may be quite extensive depending upon the manufacturer; however, it is difficult to determine its extent since this information is not made public. This has resulted in numerous problems with interoperability between commercial software applications and their ability to recognize and read the range of RAW file formats, especially as new cameras are released. If the RAW image file is downloaded to a software application that does not recognize and cannot read that particular RAW metadata specification, the image may not be rendered accurately according to its colour presentation, saturation, and luminance. Additionally, the image's accompanying metadata may be stripped away. The stripping away of digital image metadata, or the loss of certain metadata elements because the metadata schema is not recognized and properly read, presents a serious threat to the identity and integrity of a digital image. The proprietary RAW format presents a risk to the reliability and authenticity of digital images to be saved for the long term. The fact that the RAW specification is privately owned and controlled by individual camera manufacturers causes additional problems for the accurate rendering of digital image originals in the future, because the technical specifications for the photosensitive detectors (i.e., CCD and CMOS) are protected by intellectual property laws. Nevertheless, professional photographers attest to RAW as the best format for the digital original on the basis that it is the first instantiation of the data and provides the photographer

with a greater range of creative potential.[91] Therefore, it is fundamental to the reliability of digital images to establish a protocol for metadata writers and readers to guarantee that metadata remain linked to the image throughout workflow processes. Metadata facilitate the essential function of identifying images for retrieval within digital image collections.

Control over the digital image in-camera capture process is critical to a photographer's professional practice because it is at this stage that technical and descriptive metadata are attached to, or embedded within, the image.[92] In the course of this discussion it will become clear that the image and the metadata are both methods of presenting information and rely on one another to fully communicate the functional context of an image. Therefore, the capture of as much relevant metadata as possible is a key component of the procedure of creation of digital images. The two broad types of metadata are technical and descriptive. Technical metadata refer to the mechanical settings automatically recorded by the capture device. Descriptive metadata are the explanatory notes that define contextual information supporting the digital image and that are input manually (i.e., voice or touchpad) by the photographer at either the time of capture or soon thereafter.

Analysis of metadata elements ascertains the identity and integrity of the digital image, which attest to an image's authenticity.[93] Metadata that relate to the identity of an image include the names of the persons participating in its creation (i.e., author, addressee,

---

91. Adobe Systems Inc., has recently released the *Digital Negative Specification (DNG),* an open file format that acts as a universal RAW. The DNG contains RAW image data and metadata; however, the metadata contains all the information a RAW converter will need to convert the data even if it has never seen the file format before. In this way, the DNG can be used in conjunction with any sensor design and can be the default RAW format. Adobe is encouraging photographers to adopt the DNG and convert their existing proprietary RAW file formats into DNG files to increase the interoperability and cross-platform support of their digital images. Adobe Systems Inc., "Introducing the Digital Negative Specification," Adobe Systems Inc., (2004), http://www.adobe.com/products/dng/pdfs/dng_primer.pdf, 2.

92. Different file formats link the image to its metadata in different ways. JPEG and RAW embed the information and TIFF writes it as an annotation in the header of the file.

93. Reliability is provided by the existence of the metadata (completeness) and the control over the creation process. Analysis of metadata only attests to authenticity.

writer, originator, creator), its date and time of creation (e.g., made, received, saved to file, stored), its subject or the action it participated in, and its formal and technical characteristics (e.g., orientation, pixel resolution). Metadata that relate to the integrity of an image include information on its custody, which includes the procedures and controls exercised on it by the creator and subsequent preservers throughout its life cycle. Additional metadata may be added to the image throughout its lifecycle to assist in documenting any changes made to the image or to the metadata; however, the challenge is to maintain the metadata and the digital image as one entity throughout changes made to file format and transmission between applications and operating systems.

From a preserver's perspective, by assigning metadata to a digital image at the moment of creation the creator formalizes and makes explicit the act of saving the image (i.e., setting it aside) as a record for future action or reference. Once the link between the digital image and its metadata is established they must be managed as a whole. Metadata may be stripped from an image by accident or on purpose; therefore, it is important to be aware of the risks and make decisions on the basis of established protocols and universal standards. When the images are downloaded from the camera for further processing or for long-term storage, the attached metadata should be recognized, read, and written by external hardware and software in order to persistently link them with the related image.[94] Most photographers (and the organizations in which they work) maintain quality control over the digital image capture process by establishing procedures and spot checks of digital image files by recording the operational settings of their equipment. The last control includes calibrating

94. In the case of photojournalists, the JPEG captured in-camera may be transmitted directly to the news agency via the server without undergoing any further processing. Commercial photographers, forensic scientists using digital imaging and artist projects commonly require further image processing such as basic edit operations or explicit manipulations made possible with image software, most notably *Adobe Photoshop*.

devices according to standardized colour spaces and then checking that these calibrations are supported consistently and accurately across all devices through daily operator tests.[95] Organizations and institutions that receive digital images from several photographers rely upon established protocols and assigned responsibilities to ensure that digital images are consistent and complete, thus guaranteeing the reliability of the digital images created by different photographers in a variety of contexts. A substantial number of photographers work alone; therefore, the procedures and controls they establish under their own directives need to withstand professional and legal scrutiny.[96] Attaching sufficient metadata to an image assists in establishing its identity and integrity over time by providing evidence of procedural controls made explicit through attributes of the record.

Unlike analogue photographs, which can be physically browsed, digital images must be retrieved using a computer in order to view them. The act of retrieval creates the need for information about the images themselves to be captured and made recognizable. File naming and version control are the first steps in managing digital images, and most photographers use a systemized approach that includes the identification of each image, (i.e., name, date, version), file logs, and hierarchical folders.[97] File naming and creating hierarchical folders enable photographers to uniquely identify digital images and make evident the relationships between them. After in-camera capture, photographers commonly copy the digital master to compact disc (CD) or digital versatile disk (DVD) and create a digital surrogate to function as a working copy that will undergo alterations with image processing software. As indicated

95. Out of 381 respondents to Question 9, 90% utilize one or more methods of quality control over the digital image capture process. See Appendix C, "Survey: Questions and Charted Responses," 135.

96. Out of 372 respondents to Question 10, 78% do not produce images with collaborators. See Ibid.

97. Out of 392 respondents to Question 7, 62% utilize one or more methods of file management to differentiate between versions of digital images. Ibid., 134.

by survey responses, the most common file formats for digital surrogates are JPEG and TIFF.[98]

A small percentage of photographers favour the Adobe Photoshop file (PSD) because the file retains the editing functionality of the image software program of the same name. This means that PSDs have the capacity to save digital images as layers each time an alteration is made to the file.[99] This method enables photographers to save a history of their processing actions that reveals each alteration made to the digital file, such as cropping or the application of a filter. A history of sequential changes is saved along with the image file as evidence of the techniques or operations used to alter the image. By saving an image in layers, reversal of the image processing operations without permanently affecting the image is always an option. The ability to track changes is a desirable feature for legal and creative needs and one of the main reasons listed by photographers for keeping working files, regardless of format.[100] Additional reasons for keeping working files are to ensure access to the image files so they can be re-located and re-used and to maintain files as evidence of work procedures and business routines (i.e., documentation.) With the exception of law enforcement, a field in which documentation of image processing must be recorded to support further image analysis, industry guidelines do not require photographers to produce a draft copy for inspection; however, retaining these drafts assists photographers in re-purposing particular images for other creative ventures and provides them with a visual explanation of how an image evolved from concept to final production.

---

98. Out of 396 respondents to Question 4, 44% produce JPEG and 37% produce TIFFs. See Ibid., 132. Eight percent of respondents provided additional comments that identified PSD. See Question 4 in Appendix D, "Selected Textual Responses," 151-152.

99. TIFF and JPEG require image layers to be flattened before saving in these particular file formats.

100. Out of 375 respondents to Question 11, 76% keep draft digital images during the working process. Of that group, 34% keep working files as a form of notation to reveal the way in which a digital image was compiled and manipulated at different stages in its creation. See Appendix C, "Survey: Questions and Charted Responses," 136.

In addition to preferring and relying upon proprietary file formats, photographers use proprietary software programs for image processing. Nearly every photographer who responded to the survey uses a commercial-off-the-shelf (COTS) software application to display, edit, and manage digital image collections.[101] They are aware that these products are proprietary, and yet there is a widespread belief that these programs will be supported in the future. The issues of continuing support and interoperability between system platforms and software applications are critical when one considers that the image software most commonly used by photographers for image processing, regardless of their business context, has been versioned 9 times in 14 years.[102] A growing number of image management software (IMS) databases designed for managing and delivering images and their associated metadata are readily available on the consumer market for professionals and amateurs wishing to gain varying degrees of control over their digital image collections. The level of image management offered to the user depends upon individual needs (i.e., personal or business). The degree of procedural controls and automation offered depends on the IMS manufacturer and the software version. Many IMS provide a range of automated workflow solutions; store, search, and retrieval tools; and audit functionality to assist photographers and organizations to manage their digital image collections.[103] In general, IMS are proprietary programs that cater to the individual photographer who works in a specific functional context. The more expensive IMS may appear to mimic electronic record management systems (ERMS);

---

101. Out of 386 respondents to Question 6, 98% use commercial-off-the-shelf imaging applications. See Ibid., 133.

102. The imaging application Adobe Photoshop was released in 1991 and its latest version 7.0.2 is now incorporated into Photoshop Creative Suite (CS) 2.0. See Adobe Timeline, http://www.adobe.com/aboutadobe/pressroom/companyprofile.html.

103. Many of the additional comments provided by photographers to Question 6 regarding commercial-off-the-shelf (COTS) products identified a variety of image management software.

however, they do not offer the degree of access control and security measures that provide system integrity.

At the end of a project the majority of photographers save their digital images as JPEGs and/or TIFFs.[104] These are both de facto standards for image file formats that provide photographers with the capacity to write a variety of technical and descriptive metadata. A small percentage of photographers also save digital images in RAW format, which usually functions as their original or "master image file." It is common practice to save two versions, the in-camera image as the digital master and the final image after image edit operations have been applied. Retaining both the original and the final image for comparison is standard procedure for digital images that have undergone image processing and are being used as evidence in a court proceeding.[105] An understanding of the types of digital image formats that photographers create, use, produce, and maintain clarifies the need for a system that manages digital image collections. The use of metadata and file-naming conventions to make evident the functional relationships among the images and to preserve their identity and integrity for the long term is essential. While the implementation of select IMS contributes to the reliability of digital images by automating actions into workflow processes that reflect the documentary and business contexts, many photographers use simple software that presents folder views of digital images. These interfaces are essentially screen displays that allow users to view and search for images using the information directly in the image file itself. The option of assigning more substantial metadata to images to describe the content and context may not be supported by these simpler IMS applications. It must be remembered that most photographers are relying on proprietary software programs to create and manage their

104. See Question 17 in Appendix C, "Survey: Questions and Charted Responses," 139.
105. Staggs, "Admissibility of Digital Photographs."

digital images. This is especially troubling since a component of advanced IMS is control over access and maintenance of digital images no longer held within the active system, through indexing and cataloguing tools, which bears directly on the authenticity of a digital image.

Survey Findings: Preservation and Transmission

The majority of photographers set aside a digital master for preservation purposes after downloading the in-camera file formats (e.g., JPEG and RAW) or at the end of a project (e.g., JPEG and TIFF). Technical metadata are automatically generated for each image upon capture and located in its file header (TIFF) or embedded (JPEG/RAW). The most common method of preserving digital images and their metadata for the long term is to copy the original digital file and/or the final digital file to a CD and DVD.[106] Photographers do not limit their preservation decisions to this approach alone; decisions are made when choosing digital capture devices, file formats, naming conventions for image versioning, and software programs on the basis of their characteristics and capabilities.[107] Most photographers rely on their own knowledge and the recommendations they receive from others to shape their preservation procedures.[108] They are aware that the longevity of CDs and DVDs is yet to be determined and that media fragility along with technological obsolescence of file formats may hamper accurate rendering of their stored digital images over the long term. In response,

---

106. Out of 366 respondents to Question 13, 80% always move their digital images onto CD and/or DVD for long-term storage and 17% preserve processed images of superior quality or value that are a result of the working process; but this latter activity is not systematic. See Appendix D, "Survey: Selected Textual Responses," 156-157.

107. Out of 358 respondents to Question 16, 98% utilize one or more of these choices, with the majority of photographers focusing upon storage media for image preservation. See Appendix C, "Survey: Questions and Charted Responses," 138.

108. Out of 371 respondents to Question 14, 45% rely on their own knowledge, 35% receive recommendations from others and fourteen percent follow institutional guidelines. Ibid., 137.

more than half of photographers take active measures to protect their digital image files from becoming obsolete, outdated, and irretrievable.[109] Prevalent measures involve making back-up files of digital images and copying them onto CD and DVD and then refreshing optical storage media on a regular basis. Updating files to newer versions (i.e., migration) and printing digital images onto a paper medium are two alternative methods aimed at preventing loss and corruption of digital images due to media fragility and technological obsolescence.[110] Photographers are aware that the preservation of digital images involves monitoring and maintenance; yet the task of overseeing large accumulations is daunting and requires photographers to divide their time between creating and preserving, an effort that not all are willing to make. Many photographers do not equate preservation activities with immediate financial return.[111]

From the perspective of the preserver, ensuring the integrity of digital images is not simply limited to their transfer onto storage media; it involves demonstrating a secure work environment evident through access controls and measures taken to protect image files from destruction. Less than half the photographers surveyed indicated that they apply security measures to protect their digital image files from access and accidental destruction.[112] Among the minority that does apply security measures, most maintain their images offline, which is achieved by saving images onto CD, DVD, or an external drive.[113] Storing offline digital image files at an off-site location such as a third-party server and remote storage under lock

---

109. Out of 347 respondents to Question 20, 56% protect their images from becoming obsolete, outdated and irretrievable. Ibid., 140.

110. Out of 195 respondents to Question 21, 48% back up their files, 26% refresh media and 10% update files and print out hard copies. Ibid., 141.

111. See Question 21 in Appendix D, "Survey: Selected Textual Responses," 157-158.

112. Out of 341 respondents to Question 29, 58% do not apply security measures. Appendix C, "Survey: Questions and Charted Responses," 145.

113. Out of 144 respondents to Question 30, 66% store images offline; of this group, 15% store their offline images in an off-site location. Ibid.

and key further strengthens this degree of security. Photographers who work in institutional settings rely on separate organizational divisions, such as a designated department or office for handling the master image files, and on established protocols to protect the stored images from unauthorized access and accidental destruction.

Metadata are one method of protecting digital images transmitted outside of the individual workspace. Nearly all photographers attach metadata to their digital images to identify the image content, its functional context, and the legal rights and restrictions surrounding its use.[114] The range of metadata elements captured by photographers depends on the type of digital capture device, the metadata required by industry regulations, and the intended purposes of the images. Ongoing developments in digital image metadata are aimed at standardizing metadata elements across schemas to ensure that accurate and consistent metadata are written and read regardless of the capture device, file format, software, and hardware used to generate, edit, and store images.[115] Photographers understand the role of metadata in ensuring that they are properly credited for their work, that the digital image is presented accurately, and that their images can be proven to be theirs; however, how to permanently link metadata to the digital image when it is transmitted outside of the personal work-space is not widely understood. Discussions about *semantic* and *syntactic interoperability* are isolated to computer scientists and information professionals.[116]

---

114. Out of 351 respondents to Question 28, 99% of photographers record information about their digital images. See Appendix D, "Survey: Selected Textual Responses," 158-160.

Ninety-five percent of respondents want their images accurately displayed and properly credited to them. Ninety percent of respondents think it is important that their images can be proven to be theirs. See Questions 22 & 23 in Appendix C, "Survey: Questions and Charted Responses," 141-142.

115. Metadata initiatives have been launched by the Digital Imaging Group (DIG-35), Adobe Extensible Metadata Platform (XMP) in cooperation with the IPTC/NAA- IIM metadata standard, the NISO Z39.87: Technical Metadata for Digital Still Images and its Data Dictionary, and the Japan Electronics Industry Technological Association's (JEITA) Exchangeable Image File Format (Exif) for digital still images.

116. Murtha Baca, ed., *Introduction to Metadata: Pathways to Digital Information 2.0,* (Los Angeles: Getty Information Institute, 2000),

Semantic interoperability refers to methods for identifying and displaying metadata in a common programming language for the purposes of providing and promoting metadata discovery and data sharing across applications, systems, and community boundaries. Syntactical interoperability refers to the development and implementation of rules and protocol for exchanging metadata properties associated with a digital image file. Syntax for metadata exchange will be discussed in Chapter 3 in regard to current metadata initiatives involving Adobe Systems Inc. and the International Press Telecommunications Council.

Most photographers are aware that transmitting their digital images outside of their personal workspace may lead to unauthorized use. However, there is a consensus that existing protection methods are preventative, not protective. When photographers transmit their digital images to clients, they rely on digital watermarks, copyright registration, and metadata to alert users to the ownership and usage rights associated with each image.[117] Transmission of digital images is common practice for photojournalists and they are required to follow industry protocol, which specifies the use of open standard formats such as JPEG or TIFF with attached IPTC metadata elements to prove the identity and integrity of each digital image. In the exchanges between photographers and their clients the transfer of digital images may be regulated by contractual agreements that explicitly state the terms and penalties for unauthorized use or alteration of images.

The unregulated environment of the Internet is an additional matter.[118] When photographers mount their digital image collections onto the Web (which half of respondents

---

http://www.getty.edu/research/conducting_research/standards/intrometadata/index.html (accessed June 20, 2005).

117. Out of 144 respondents to Question 25, 30% use digital watermarking, 22% register the copyright and seventeen percent attach important information in metadata. See Appendix C, "Survey: Questions and Charted Responses," 143.

118. Out of 354 respondents to Question 26, 56% make their images available via a Web page. Ibid.

do) they manage access to these digital images using IMS with a dynamic online publishing component, the operation of which they oversee as administrators. Photographers also provide access to their images through vendor management packages that offer custom-built image management databases that are operated by a third party.[119] Depending upon the software functionality, the image's metadata are read to facilitate the access and retrieval of images within electronic systems. The database harvests the metadata attached to each digital image, and when users enter a keyword search for a particular image or set of images the software application locates the corresponding metadata and retrieves the related image from within the system. Access to the images within these systems may be regulated by password controls for different user groups. Photographers who choose to build their own online forums for their digital images collections populate the file header with usage and copyright information and display screen-resolution images only as protective measures.[120] Protecting images from unauthorized use is an ongoing challenge for photographers and Web masters. The majority of digital image collections online includes a statement of copyright and usage restrictions on every page of the website to inform users that penalties for unlawful use do exist and may be enforced. For most photographers, the issue of unlawful use is both economic and ethical. For this reason, a large proportion of professional photographers trust their digital image display and dissemination to stock agencies or the Web management division of their news organization or institution. This relieves individual photographers of the burden of pursuing copyright infractions.

Photographers are not aware of international organizations that are involved in the inspection and approval of technology supporting the digital imaging industry nor digital

119. Ibid.

120. Out of 198 respondents to Question 27, 31% use databases, 26% are vendor managed, and 24% use file header information. Ibid., 144.

image-related standards published by the heritage sector.[121] They are, however, aware of industry-specific standards and best practices that guide the creation, use, and preservation of digital images in regard to their business context and specific work environment. Many of the suggestions made in the comments section of the questionnaire pointed towards industry initiatives and association publications that are followed within the photographic community but are not known to archivists and collections managers. The overwhelming majority of photographers would be willing follow a standard for digital image creation and file maintenance to ensure the longevity of their digital images if it were applicable to their practice (i.e., if it were useful and did not disturb existing workflow), inexpensive, and not time consuming.[122]

By establishing technical standards, the likelihood of sustained compatibility, interchangeability, and commonality among digital image file formats, software applications, and operating systems is far greater, and this would benefit photographers working in the digital environment and digital collection managers such as archivists. A review of industry initiatives, best practices, and standard operating procedures for guiding photographers working with born digital images will be explored in the next chapter and mapped against conceptual requirements developed by the InterPARES Project for ascertaining the reliability and authenticity of electronic records.

---

121. Out of 349 respondents to Question 31, 73% are not aware of the standards and guidelines promoted by the U.S. National Information Standards Organization (NISO), Object ID, Research Libraries Group's Preservation Metadata Elements, Categories for the Description of Works of Art, the International Organization for Standardization and the British Standards Institution. Ibid., 146.

122. Out of 340 respondents to Question 32, 96% said they were willing to adopt a standard and they provided additional commentary on the parameters of adopting such a standard. See Appendix D, "Survey: Selected Textual Responses," 160-161.

Conclusion

The survey provided the opportunity to gather valuable information regarding the record-creating and record-keeping practices of professional photographers working with digital technology. Reflecting upon the initial hypotheses led to the following conclusions:

1. Photographers keep their digital images for re-use and reference, as demonstrated by their choice of in-camera file format and the fact that they keep multiple versions of a digital image, including the working drafts, to enable selection and use of a multitude of instantiations to serve undetermined future needs.
2. Photographers are generally concerned with authenticity and reliability, as proven by the routine capture of metadata and population of file information headers for digital originals and their surrogates, quality control procedures and routine preservation procedures that incorporate a measure of security; yet, it should be noted that methods to protect digital images during transmission could be improved.
3. Photographers have begun to understand the challenges to continuing access and long-term preservation presented by the use of proprietary digital systems and technological obsolescence, as revealed by their habits of saving digital images in more than one file format, refreshing digital media, and upgrading older file formats to operate on newer versions of image applications; by their willingness to adopt a standard for image creation and preservation; and by their eagerness to participate in the survey.

The fact that the majority of survey respondents identified the context of their photographic practice as artistic is interesting since it was assumed at the outset of the survey that the established procedures for producing reliable and authentic digital images would be typical of photographers working in scientific and government contexts, not artistic.

In the next chapter, a discussion of the two standard metadata schemas for digital images the Exchangeable Image File Format (Exif) and the International Press Telecommunications Council's Information Interchange Model (IPTC-IIM) and a review of SWGIT guidelines and best practices will serve to clarify the relevant actions and elements of such approaches that contribute to born digital images as reliable and authentic records.

CHAPTER THREE

Approach

The findings derived from the analysis of the qualitative survey data suggest the importance of exploring the standards, best practices, and guidelines followed by members of the *imaging community* in the creation, use, and preservation of born digital images.[123] This chapter discusses two current metadata schema standards used by photographers and supported by vendors and examines their efficacy for ensuring the reliability and authenticity of born digital images. Additionally, it presents the guidelines and best practices concerning procedures for the use of digital images and imaging technologies in the criminal justice system, and more specifically their role in establishing documentary procedures, that is the rules governing the making of a digital image as a reliable record and maintaining its identity and integrity over time and space. By focusing on current technological and procedural methods used by photographers to generate and maintain digital images as reliable and authentic records, this chapter intends to provide a clearer sense of what is considered a reliable and authentic born digital image.

This chapter also addresses the roles of the photographer as a creator and as a preserver in relation to the chain of preservation, which is the system of controls that extends over the entire life cycle of the digital image. The overall purpose of this chapter is to demonstrate that selection of an appropriate metadata schema and the establishment of standard operating procedures support the creation and maintenance of accurate and reliable born digital images that fulfill creative and business needs, and that authenticity is protected

123. The imaging community is composed of photographers who use digital technology and vendors who create digital image processing software and hardware.

by the use of methodological controls that can be verified by documentation throughout the life cycle of the records.

Overview of Metadata Schemas

As communicated in the report on the survey results, photographers record and retain metadata about their digital images for the purposes of managing access to their images, protecting them from alteration when they are transmitted outside the personal workspace, and providing key information to fulfill business functions.[124] In the context of these and other business activities, metadata contribute to the identification and classification of images, their proper storage and preservation, and control over their distribution and exploitation. To be useful, metadata must be retained and made accessible (i.e., coupled) along with the digital image they relate to throughout the image's life cycle. The effectiveness of metadata for image discovery and delivery is dependent on the choice of capture device(s), image file format(s), and software application(s) used to support (i.e., write and read)[125] the information contained in the schema throughout all instantiations of the digital image that are manifested in the professional workflow of an individual, a business, or several businesses. Photographers should consider hardware and software capabilities for

---

124. See Questions 24-28 in Appendix C, "Survey: Questions and Charted Responses," 142-144.

This chapter focuses on the contribution of metadata to the reliability and authenticity of digital images. While the technical details of how metadata are embedded within different image file formats and communicated across technological systems are mentioned as they relate to issues of syntactic and semantic interoperability, this is not a discussion of system architecture or programming languages. Simply put, metadata are non-pixel information embedded and stored in "containers" in the image file. David Riecks, e-mail message to author, May 9, 2005.

125. To write metadata refers to the capacity of devices, hardware, or application software to output information about a digital image. To read metadata refers to the capacity of devices, hardware, or application software to directly read information about a digital image located in the file header or embedded in the file and use it to accurately reproduce the image (virtually and in hard copy.) Japan Electronics and Information Technology Industries Association, "Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.2," JEITA (2002) http://www.exif.org (accessed June 3, 2005).

writing and reading digital image metadata prior to the act of image capture, otherwise they risk choosing equipment and programs that may not support compatible metadata schemas. This results in inoperable files and irretrievable images. Ideally, the selected metadata schema(s) should fulfill the purpose of identifying the digital images in the context of the creative and business activities in which they participate and their end uses. Metadata are an important part of the system of controls photographers implement to ensure that the identity (i.e., the immediate context of creation and manner in which the image has been handled and maintained) and the integrity (i.e., the state of an image being complete and unaltered) of the image remain evident across time and space.

The digital camera is currently the most prevalent digital image capture device; however, cell phones and personal data assistants (PDAs) now incorporate imaging technologies to facilitate the capture, display, and transmission of digital images as part of their communication packages. The results of these developments are an expansion of the digital image market and a diversification in image file formats and their accompanying metadata, which complicates attempts by photographers to create, manage, and maintain images as platform-independent standard formats. As methods for digital capture increase and image formats become more varied, the ability to locate and retrieve stored images efficiently and accurately becomes more challenging. Approaches to providing standardized metadata and enabling interoperability across imaging technologies present a viable solution to many of the problems posed by the rapid expansion and variable nature of the digital imaging environment.

The metadata schemas developed by the Japan Electronics and Information Technology Industries Association (JEITA) and the Information Press Telecommunications

Council (IPTC) are the results of efforts aimed at creating metadata specifications that are written to standard image file formats for the purpose of platform-independent exchange. As part of the analysis of standard metadata schemas used by photographers, categorization of the schemas into type(s), and of their elements into groups identified by specific characteristics, will assist in determining the audience and application for each schema and will facilitate a comparison between the two metadata standards in wide use by professional photographers and supported by commercial software vendors; the Exchangeable Image File Format (Exif) and the International Press Telecommunications Council's Information Interchange Model (IPTC-IIM).[126] The methods and products of the InterPARES' Description Cross Domain research team inform the selected analytical approach. Its "Guidelines for Analysis of Metadata Schemas" and the "Metadata Schema Registry"[127] recommend compiling details of the major elements in a metadata schema to provide a sense of the general purpose for which the schema has been developed and its intended community, as well as an assessment of the schema's usefulness for record keeping, which is its ability to contribute to the process of making and maintaining accurate, reliable, and authentic images as evidence of creative and business activities.[128]

There are five broad types of metadata; administrative (i.e., metadata used in managing and administering images), descriptive (i.e., metadata used to describe or identify images), preservation related (i.e., metadata used in the preservation management of images), technical (i.e., metadata related to how a system functions or an image behaves), and use

126. See, Gilliland-Swetland, "Setting the Stage."

127. These documents are contained in the restricted area of the InterPARES Web site, but are to be made public in the near future.

128. Joanne Evans and Lori Lindberg, "Describing and Analyzing the Recordkeeping Capabilities of Metadata Sets" (paper presented at DC2004: International Conference on Dublin Core and Metadata Applications, Shanghai, China, October 12, 2004), 1. Available online at http://www.siderean.com/dcconf/.

related (i.e., metadata documenting the use of an image). Within each type of metadata there are specific metadata elements that exhibit certain characteristics: the source (i.e., internal or external), method of creation (i.e., automatic or manual), nature (i.e., lay or expert), status (i.e., static, dynamic, long-term, or short-term), structure (i.e., conform to a standard or unstructured), semantics (i.e., conform to standard vocabulary or uncontrolled), and level (i.e., aggregate or item).[129] This framework will be used to analyze the two metadata schemas mentioned above and assess their functionality.

Exif Schema

In 1995, the Japan Electronics and Information Technology Industries Association (JEITA), a trade organization, developed Exif as a standard metadata schema for "digital still camera images."[130] The aim of the Exif metadata standard is to foster and provide compatibility among image file formats and interoperability between capture devices and image software applications. The current Exif Version 2.2 specifies metadata for JPEG and TIFF (some RAW data files can incorporate a container for Exif) and is currently written by most digital cameras and read by the majority of image processing software on the consumer market. The Exif schema is technically structured in different ways depending upon the type of image file format the metadata is attached to, JPEG or TIFF; yet, the elements are anticipated by software applications and accessed according to established protocols that present the schema information in a consistent and persistent manner. As long as both

129. Gilliland-Swetland, "Setting the Stage."

130. The standard was first published in 1995 by Japan Electronics Industry Development Association (JEIDA), but has undergone several revisions. JEIDA changed along with the standard, merging with the Electronic Industry Association of Japan (EIAJ) to form JEITA. Exif Version2.2. was approved in 2002 and amended in 2003. See JEITA, "Exchangeable Image."

The Exif standard is closely linked with the Design Rule for Camera File Systems (DCF), an industry standard since 1999 that shares the same goals of interoperability as Exif and is treated as a companion.

systems (i.e., hardware and software) support the information model promoted by Exif, the metadata are properly exchanged and retained along with the digital image. The standardization of metadata exchange depends upon meeting two criteria: whether it can be read and whether it can be written. Metadata should have an established protocol for exchange so that multiple devices and applications may read the information. In this way, metadata may be approached as a two-part process, and the protocol for both aspects needs to be explicitly stated and recognized by all vendors.

The following is an explanation of the Exif schema using the language of the schema.[131] The schema is divided into elements that are represented by metadata tags, which are machine-readable labels assigned to define data. Standard Exif metadata tags are version (i.e., schema version), image data characteristics (i.e., colour space information), image configuration (i.e., image compression, pixel width and height), user information (i.e., manufacturer notes and user comments), date and time (i.e., date and time of original data), picture taking conditions (e.g., exposure program, shutter speed, aperture, subject distance, light source, flash mode, metering mode, lens focal length, white balance, digital zoom ratio, sharpness, saturation), a unique image ID, and copyright information.[132] The information in these tags is written and read by most devices, hardware, and software applications; however, only version, image data characteristics, and image configuration are "mandatory" for support, which means hardware and software that is compliant with the Exif schema must write and read the information in these tags. The remaining tags are "recommended" or "optional," and support for them is not guaranteed. Additional metadata that define the geospatial positions system (GPS) of an image, such as the longitude and latitude of a

131. See Tables, "Exif Schema," 162.
132. JEITA, "Exchangeable Image."

location, is "optional." Therefore, this metadata may be used by the photographer to capture important information about the image, but the elements are not recognized in protocol exchange as part of the mandatory schema structure and may be stripped from the image during transmission or conversion from one file format to another. This highlights the issue of metadata exchange protocols between devices and applications.

The application of the InterPARES framework to the analysis of the Exif schema and its major elements supports the claim that the schema may provide digital image file compatibility between imaging devices such as cameras and imaging software for personal computers. The schema functions as technical metadata that documents both the digital camera system used to capture the image and the settings that define how the digital image behaves and is represented. This information is presented in a structure that is defined by established transfer protocol and is anticipated by systems and applications. The source of the metadata is internal, as they are generated by the camera system at creation and automatically captured; therefore, the schema is "read-only" and should persist with the digital image throughout workflow operations. Read-only metadata that are automatically generated by the system are very reliable because they do not require manual input by the photographer, and a great effort and expertise would be necessary to intentionally alter them. The Exif schema also includes administrative metadata; however, these metadata elements are optional, such as copyright, date and time of the original and digitized images. Capture of recommended and optional metadata depends on the device used and its capability to write additional information to the image file.

Exif metadata are essentially system metadata that are automatically captured by the camera and that provide information about basic image parameters, presentation, and the

technical "how" of digital image creation. The mandatory metadata elements are static and exist as read-only data. The optional tags such as copyright, picture taking conditions, and unique image ID are dynamic and depend on the read and write capabilities of hardware and software used by the photographer. An analysis of the Exif schema in terms of its record-keeping capabilities shows that it fails to provide descriptive information about digital image context, hierarchical information about relationships between images in an aggregate, and processing history about the image. The schema describes the technical aspects of the image itself and the capture system, but it does not give contextual information regarding external agents such as the client, business activities it supports, management processes or its categorization. To be useful as record-keeping metadata, the Exif schema needs to have all its elements supported by devices, hardware, and software applications. The fact that the schema is recognized as a standard by the imaging industry and written to JPEG (standard) and TIFF (de facto standard) offers a high degree of assurance to creators and preservers that the schema will be viable and operable in the future.

The type of information captured by Exif metadata is useful to photographers as a notational device regarding the technical actions (i.e., camera settings and system parameters) used to generate the image; however, very little of this information is pertinent to an outside user.[133] The ability to accurately search and retrieve one particular image among many in an image collection by utilizing Exif metadata presents a real challenge because the information captured relates more to image creation than to use or functional context. The Exif metadata may be useful as documentation when approached as notes regarding the

133. Recent discussions in the imaging community have centered on reasons for not wanting Exif metadata available to users for viewing. Photographers have asserted that with the aid of Exif metadata, clients could determine the technical "know how" to replicate the capture processes and this presents a threat to the professional practice.

process of creation. In many ways Exif information mimics traditional darkroom notation (e.g., focal length, aperture, shutter speed); therefore, it reveals a great deal about how the image is made and the shooting habits of a particular photographer. If an image requires re-shooting or re-creation, a photographer may refer to his or her Exif metadata attached to the image as a guide. On the whole, the application of the Exif schema for the management and protection of images in a collection is limited. The schema is better suited as a source of technical reference for the photographer than a method for image retrieval and delivery.

IPTC Core Schema

Another widely used metadata schema for digital images is prevalent in the news service bureaus and directly applies to photojournalists. Recent developments in the schema's structure and its method of delivery have made it available to professional and amateur image creators. The Information Interchange Model (IIM) released in 1991 by the International Press Telecommunications Council (IPTC) and the Newspaper Association of America (NAA) is the metadata schema used to transfer a data object, which may be an image file or a combination of text and image, along with its pertinent editorial and technical information. In 1994, Adobe Systems Inc. recognized the IIM metadata structure and enabled users to insert IIM metadata about a digital image into the file format headers of JPEG, TIFF, PDF and PSD files through the "File Info" action in the Adobe Photoshop application.[134] The most recent revision of the IPTC-IIM schema reflects changes in the type of information captured, its structure, and method of exchange. The schema is still used for the purposes of captioning digital images and providing essential information about image content and

134. At this time IIM metadata elements were known as "IPTC headers." See, "'IPTC Core' Schema for XMP, V1.0: Specification," *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005).

context; however, the new specification reflects the growing need for syntactic interoperability to identify and display metadata across systems and applications via a common language such as Extensible Markup Language (XML).[135] The new specification, IPTC Core Schema for XMP Version 1.0 (IPTC4XMP Core1.0) released in 2004, is the result of the IPTC4XMP Working Group, a collaborative effort of the IPTC, Adobe Systems Inc., and the International Digital Enterprise Alliance (IDEAlliance).[136] The new schema incorporates an interchange syntax for the representation of data known as XML, which is provided by Adobe's eXtensible Metadata Platform (XMP) introduced in 2001.[137] XMP is a labeling technology that allows metadata (standard and customized) to be embedded into digital image files and then read by other XMP-enabled software applications. XMP-enabled applications currently recognize and read IPTC Core metadata and its legacy version IIM, as well as the Exif schema. XMP is defined as an "overarching metadata standard" that facilitates the exchange of metadata schemas.[138] Adobe has made the XMP schema an open source that is publicly available and readable by any XML-compliant device, in an effort to encourage metadata support and persistence across applications and platforms and throughout the imaging industry.

---

135. XML is a cross-platform and Internet-enabled implementation language. It is a non-proprietary standard recommended by the World Wide Web Consortium (W3C) for creating special markup languages to describe data. XML facilitates the sharing of data across systems, devices and applications and was first defined in 1998. Its latest version, 1.0, was published February 4, 2004. David Riecks, "Ch.Ch.Changes (with File Info)" Controlled Vocabulary.com, http://www.controlledvocabulary.com/imagedatabases/iptc_naa.html (accessed June 10, 2005).

136. IDEAlliance is a non profit membership organization dedicated to advancing user-driven, cross-industry specifications: best practices: and standards for all publishing and content-driven enterprises. The IDEAlliance is involved in XML technologies, content creation, management and delivery, production workflow, supply management and newsstand distribution. See IDEAlliance, "About IDEAlliance," http://www.idealliance.org/about/.

137. David Riecks, "'IPTC Core' Schema for XMP, V 1.0: Custom Panels User Guide," *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005).

138. Adobe Systems, Inc., "Adobe XMP for Creative Professionals: Metadata and the Creative Suite," Adobe White Paper (2004), http://www.adobe.com/products/xmp/ pdfs/XMP_for_CreativePros2004.pdf, 1.

The following are IPTC Core metadata tags and their attributes:[139] title (i.e., short human readable name such as the filename), keywords (i.e., free text to express the subject of the image content), instructions (i.e., text by the creator for the addressee that ensures accurate reproduction of the image, such as a specific colour space), date created (i.e., time and date the intellectual content was generated; this information may be sourced from existing Exif metadata), creator/byline (i.e., photographer/author), creator's job title (i.e., staff photographer or independent), city, state/province, country (i.e., place shown in image), job identifier (i.e., transmission and routing identifier to assist in workflow), headline (i.e., a publishable synopsis of the image content), provider (i.e., originator of photograph if different from creator), source (i.e., original owner of copyright for intellectual content, such as an agency or an individual), copyright notice (i.e., intellectual property for news image and current owner of copyright), caption/description (i.e., text description of the who, what, and why of the image content), caption/description writer (i.e., person responsible for writing image metadata, typically the photographer), creator's contact information (i.e., mailing address, e-mail, phone, URL), ISO country code (i.e., ISO 3166 compliant), intellectual genre (i.e., type of end use, such as obituary or feature), location (i.e., shown in image), rights usage terms (i.e., legal usage of image in free text), subject code (i.e., controlled eight-digit subject-news code), and IPTC scene (i.e., controlled six-digit scene description for a photograph).

There are different ways to display and access the IPTC Core metadata attached to a digital image file. Any application that is XMP-enabled can read and write IPTC Core metadata, and in the case of Adobe Photoshop applications, the information is located under

139. IPTC, "'IPTC Core' Schema for XMP." See Tables, "IPTC Core XMP Schema," 163.

"File" in "File Info." The most recent Adobe image processing application, Photoshop Creative Suite (CS2) delivers the IPTC Core schema in four "panels" that group the metadata elements under the headings IPTC contact, IPTC content, IPTC image, and IPTC status.[140] The information for each field within the IPTC panels may be shared with *Adobe Photoshop File Info* elements and does not require redundant input. This semantic interoperability initiative is directed at making professional workflow more efficient for photographers by *mapping metadata.*[141] This means that the information entered into the IPTC Core title field is entered once and automatically populates all equivalent metadata elements within different schemas. The panels offer photographers a method of visualizing the relationships between elements within the schema and categorizing them according to an overall function.[142] By grouping the metadata elements according to function and presenting the information in automated profiles ready for data entry, the panels make explicit the link between image metadata, and make explicit the documentary and business contexts in which the image participates. By implementing IPTC Core as a standardized metadata profile, a control is exercised over the procedure for transmitting an image to a news service bureau. This control ensures the accurate and reliable submission of images by photojournalists in a consistent and documented approach.

---

140. David Riecks, "'IPTC Core,'"

141. Metadata mapping is an identification of equivalent metadata elements within different metadata schema. A visual representation of metadata mapping is *crosswalks*, which facilitate semantic interoperability by mapping elements from one metadata schema to another and in effect allow multiple schemas to be searched as if they were one large extensible schema. See Baca, *Introduction to Metadata,* Glossary.

142. The IPTC contact panel presents information regarding the photographer/creator, creator's job title, and contact information. The IPTC content panel is used for visual content information, which includes the headline, caption/description, keywords, subject code, and caption/description writer. The IPTC image panel is used for abstract descriptive information, which includes the date created, intellectual genre, scene, location, city, state, country, and ISO country code. The IPTC status panel is used for workflow and copyright information, which includes the title, job identifier, instructions, provider, source, copyright notice, and rights usage terms. Riecks, "'IPTC Core.'" See Tables, "IPTC Core XMP Schema," 163.

Unlike the Exif schema, the IPTC Core schema is not read-only but has many fields of information that may be changed throughout the lifecycle of the image, depending on the intended purpose and end uses of the image. The IPTC Core schema functions as administrative and descriptive metadata that document the content and context of a digital image and define the legal and regulatory parameters of its use. The schema provides photographers with a method of capturing attributes of the digital image's creation and handling that uniquely identify the image; therefore, it is more effective than Exif for the classification and retrieval of digital images in collections. The photographer may add IPTC Core metadata to an image at the time of creation or when the image is ready for transmission to a news service. The nature of the schema is expert metadata that are created about the digital image's immediate context of creation. Specific fields in the schema must conform to controlled vocabularies developed by news service bureaus such as news codes and ISO country codes, which require familiarity with established journalism protocol. Certain elements within the schema are static such as the creator/byline and date created, which will not change even if the image is re-purposed. Metadata fields such as instructions and caption/description are dynamic and change according to the context in which the image is being presented. Regardless, both static and dynamic information may be altered by the photographer or an authorized person. It is important to note that the IPTC-IIM legacy schema was originally developed for transmitting images, and thus the newer specification, IPTC Core, continues to perform this function and is defined as short-term metadata of a transactional status.

In general, the IPTC Core schema does not have the capacity to present hierarchical levels and relationships within an aggregate or an image processing history that would

provide a greater sense of the documentary context related to the creation and use of the images. The IPTC Core schema is mandatory for photographers transmitting images to a news service bureau. Individual news publications have a set of file-naming conventions that photographers must use. These conventions serve purposes of discovery and delivery of images during management and preservation functions performed by the handling office at the service bureau.[143] Upon receipt of the image, additional metadata are added to the existing IPTC Core and managed with the image as a record of the newspaper held within its record-keeping system. Photojournalists work in a professional environment that expects high volume and rapid turnover; therefore, IPTC Core metadata fulfill specific business needs aimed at the dissemination of reliable images.

As demonstrated, Exif and IPTC Core metadata provide substantial information about the creation of the digital image that contributes to the use of digital images as active and semi-active records; however, the information contained within the schemas may not provide enough identifying attributes for an image to be useful in all business contexts. It is at the initial stage of creation that the identity of a digital image must be established in order for its integrity to be assessed at a later date; therefore, Exif and IPTC Core metadata must capture key attributes of the record such as the date and time of creation, the names of the persons who take part in the creation of the image, the action or matter the image participates in, and the image's archival bond or relationship with other images involved in the same activity. For many photographers, the automatic and manual capture of digital image metadata is part of their documentary procedure for creation and use. All the image's attributes must be expressed in the metadata and attached to the digital image in order to signify it as a

143. Kate Bird, Librarian for the Pacific Newspaper Group Inc., telephone conversation with author, May 27th, 2005.

complete and trustworthy record. If a photojournalist submits a digital image to a news service and the IPTC Core creator/byline field is empty, the image is incomplete and cannot be used until the correct information has been added. An image requires documentation to establish that it is a reliable representation of the circumstances that brought it into being.

Greater concerns arise with the Exif and IPTC Core schema in regard to their ability to contribute to the integrity of an image. When photographers no longer actively use their digital images they are stored on CD and DVD for the long term.[144] As inactive records they no longer participate in business processes and their authenticity may be compromised. In cases where a photographer is responsible for creating and preserving his or her digital images, the identity and integrity can be proven through a simple attestation of authenticity. When the preserver is a successor or a third party such as an archival repository, a presumption of authenticity is made on the basis of knowledge of the prior methods used to protect the images from alteration or manipulation, during transmission and long-term storage. The inactive digital image is authentic if it can be proven to be precisely as it was when it was first made or received and set aside; therefore, the preserver must obtain evidence that key attributes regarding the identity and integrity of the image are explicitly linked to the record, and that procedural controls were exercised throughout the image's life cycle.[145] This chapter has so far discussed the role of metadata in expressing attributes of identity and integrity. The procedural controls over preservation may be made evident through documentation accompanying the digital image, either in human-readable format (i.e., published policies and standard operating procedures) or machine-readable format (i.e.,

144. Out of 386 respondents to Question 13, 80% move their digital images into long-term storage. See Appendix C, "Survey: Questions and Charted Responses," 137.

145. Duranti, Eastwood, and MacNeil, *Preservation of the Integrity of Electronic Records*, 27.

system metadata). Third-party scrutiny of these methods and controls determines whether there is evidence to support a presumption of authenticity.

The "Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records" is a systematic set of criteria developed by the InterPARES project to assess record authenticity.[146] A presumption of authenticity may be made on the basis of known facts about the manner in which a digital image has been created, handled and maintained. A comparison of Exif and IPTC Core metadata against the benchmark requirements can determine whether such standards allow for an inference of authenticity on the basis of how many requirements are met and the degree to which each requirement is met.[147] The number of requirements met and the degree to which they are fulfilled provides the basis of the presumption. Analysis of the Exif and IPTC Core metadata schema against the benchmark requirements determines the degree to which the schemas capture metadata regarding the identity and integrity of the digital image and make explicit the procedural controls in the record-keeping environment.

The benchmark requirements are (A.1) Expression of Record Attributes and Linkage to the Record, divided into (a) essential attributes for identifying an electronic record within the fonds of its creator, which includes the names of the persons concurring in its formation (i.e., the author, writer, originator, and addressee); the name of the action or matter the record participated in; the dates of creation and transmission (i.e., chronological date, received date, archival date, and transmission date); the archival bond, that is, the relationship of the record with previous and subsequent records as expressed by a classification code, a register number, or other unique identifier and indication of attachments and (b) essential attributes

146. Duranti, *Long-Term Preservation,* 209.
147. Ibid., 207.

that allow for an assessment of the integrity of the record, which include the name of the handling office (i.e., the office or person competent for carrying out the action to which the record pertains or participates); the name of the office of primary responsibility (i.e., the office or person competent for maintaining the *authoritative* record)[148]; the annotations (i.e., additions to the record after it is completed); and the indication of technical modifications (i.e., changes in digital encoding or software necessary to reproduce or render the record); and (A.2) Access Privileges (i.e., defining access privileges, maintaining access audit trail), (A.3) Protective Procedures over Loss and Corruption, (A.4) Protective Procedures over Media and Technology, (A.5) Establishment of Documentary Forms (i.e., presentation features, electronic signatures, digital time stamp from Trusted Third Party, special signs), (A.6) Authentication of Records, (A.7) Identification of Authoritative Record and (A.8) Removal and Transfer of Relevant Documentation.[149]

In regard to the benchmark requirements for the expression of record attributes and linkages (i.e., essential information about identity and integrity), the Exif schema (if supported) provides an image with the date of creation (i.e., date and time tag), which fulfills the chronological date requirement but does not address the date of transmission, receipt, or the archival date. The Exif schema does not provide any of the other attributes of identity set forth in the requirements. The degree to which the Exif schema satisfies the benchmark requirements for identity is minimal to none.

The IPTC Core schema has four tags, creator/byline, provider, source, and caption writer, that capture information regarding the persons involved in the creation of the digital

148. Authoritative is used in this context to refer to the record that is considered by the creator to be the official record. See Ibid., 211.

149. Ibid., 210-212.

image; however, the addressee is not represented in a metadata element.[150] The action of the digital image is expressed in free text via the IPTC Core keywords tag or the caption/description tag, the latter of which is used to describe the "who, what, and why" of the image content and is considered the definitive source for anything deemed necessary to the content and context of the image.[151] The IPTC Core date and time tag may be used to document the date of creation; however, it does not provide further information regarding transmission, receipt, or archival date. The requirement for the archival bond is best expressed through a classification code or a file identifier that links the digital image with the images prior and subsequent to it; however, it is unclear whether the IPTC Core job identifier tag would suitably explain the relationship between images of the same shoot; therefore, a more reliable system of expressing the archival bond is presented by file-naming conventions established by the news agency or photographer.[152] The degree to which the IPTC Core schema satisfies the benchmark requirements for identity is adequate. In regard to the requirements for integrity, neither schema captures information regarding procedural controls over the image's handling and maintenance. The degree to which the Exif and IPTC Core schemas satisfy the benchmark requirements for integrity is null.

Benchmark requirements A.2 – A.8, which define the procedural controls over the record's creation, use and maintenance that support a presumption of its integrity, are not

---

150. The lack of a defined tag for the addressee is problematic since the news service's system that receives the submitted digital image and its metadata, captures a timestamp of the receipt but does not capture the person or office of receipt; therefore, there is no evidence of the addressee in either the embedded IPTC Core metadata delivered with the image or in the accrued metadata in the record-keeping system. Kate Bird, Librarian for the Pacific Newspaper Group Inc., telephone conversation with the author, May 27th, 2005.

151. The speed and volume of image receipt and production at a news service bureau necessitates designating one tag to be the definitive location for all the important information regarding the identity of the digital image; this tag is caption/description. Ibid.

152. The newspaper has standard file-naming conventions that all photographers are required to follow when submitting images. The conventions assist in determining the relationships between images of the same shoot. Ibid.

addressed by elements in either metadata schema. The survey results reveal that photographers are using protective methods to prevent loss and corruption of their records, such as saving draft versions of images and removing original image files from the active system, refreshing media, and migrating older file versions; however, none of these actions are documented in Exif or IPTC Core metadata.

The analysis thus far has demonstrated the scope and typology of the Exif and IPTC Core schemas and discussed their contribution to the creation of accurate, reliable and authentic digital images. The responsibilities and actions of the individual photographer have been emphasized throughout the discussion. In organizations, the actions taken by individual photographers or imaging technicians to create and maintain a digital image must be governed by rules to provide organization-wide consistency and to produce images that accurately reflect their administrative and documentary context.

Standard Operating Procedures & SWGIT

An approach to creating, handling, and maintaining digital images as accurate, reliable and authentic records in organizations is found in the *standard operating procedures (SOP)* that establish and maintain an effective enterprise-wide quality system.[153] The Scientific Working Group on Imaging Technology (SWGIT) publishes guidelines and best practices aimed at the law enforcement community that define key elements of a *SOP for* the

153. The Scientific Working Group on Imaging Technology (SWGIT) and the Scientific Working group on Digital Evidence (SWGDE) publish "Guidelines and Recommendations for Training in Imaging Technologies in the Criminal Justice System," to assist organizations in identifying the key skill-sets to ensure personnel is properly trained to operate digital image capture devices and imaging software applications used for enhancement, processing and analysis. All SWGIT/SWGDE documents are available at: http://www.theiai.org/swgit/. PDF Available at: http://www.theiai.org/swigit/guidelines/sec6_1_2_2001_12_06.pdf.

purposes of ensuring the integrity of digital image evidence in the criminal justice system.[154] As a member of the International Association for Identification (IAI), SWGIT is positioned to deliver and receive information about the latest developments in enforcement policies and the judicial process regarding digital imaging technology. The issue of ensuring the integrity of digital images is not limited to law enforcement. SWGIT recommendations are valuable to any creator that requires proof for the purposes of legal admissibility that image operations were part of standard procedures and performed by trustworthy personnel.

SOPs are documents unique to a particular organization or agency and describe the methods and procedures to be followed when performing a routine task or series of operations.[155] The goal of SOPs is to facilitate consistency and quality throughout an organization and to provide evidence of procedures that conform to scientific and legal principles.[156] To be effective, SOPs should be readily available in both human- and machine-readable formats and reviewed annually. Ideally, the use of SOPs ensures that digital images are accurate, reliable, and authentic by making evident the procedural controls over creation, transmission, and preservation.

In 2002, SWGIT made available "Guidelines for the Use of Imaging Technologies in the Criminal Justice System," a document that provides organizations and agencies creating SOPs with terminology to facilitate the use of a common language about digital image technologies; recommendations for the proper capture, storage, processing, analysis,

---

154. SWGIT, "Documents."

155. SWGIT/Scientific Working group on Digital Evidence (SWGDE), "Recommended Guidelines for Developing Standard Operating Procedures," Version1.0 (November 15, 2004) http://www.theiai.org/swgit/. PDF available at http://www.theiai.org/swgit/swgde/sop_guidelines_october_2004_1.pdf

156. This is important in regard to enhanced images as evidence in court proceedings since the enhancement process may be challenged and require compliance with the standard to determine admissibility of scientific testimony established in Daubert v. Merrell Dow Pharmaceuticals Inc., 1993. Erik Berg, "Legal Ramifications of Digital Imaging in Law Enforcement," *Forensic Science Communications* 2, no.4 (October 2000), http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm (accessed June 1, 2005).

transmission, and output of images; and the key elements that must be contained in the formulation of any SOP.[157] SWGIT identifies the key elements that must be included and described in an SOP: the title (i.e., descriptive name of the procedure), purpose (i.e., why, when, and for whom the procedure is intended), equipment/materials/standards/controls (i.e., items required to perform the procedure, such as hardware, software, protective equipment, and their configurations), procedures (i.e., agency-specific step-by-step instructions), calibration (i.e., the instrumentation set-up and calibration to ensure accuracy and reliability), calculations (i.e., mathematical operations applicable to the procedure), limitations (i.e., inappropriate actions, interpretations, or equipment), safety (i.e., potential hazards in the procedure),and references (i.e., internal and external sources regarding the principles behind the procedure and related procedures).[158] All procedures concerning the capture, handling, and preservation of digital images should be governed by the establishment of an agency-specific SOP that conforms to the SWGIT model. The combination of key elements in a SOP with the SWGIT recommendations for image capture, processing, transmission, and preservation facilitate the overarching goal of providing a trusted chain of custody for all images regardless of their end use. An analysis of SWGIT documents reveals a high degree of success in fulfilling the benchmark requirements for assessing the authenticity of a creator's records; however, this was to be expected, since a probable end use for an image generated in the context of law enforcement or forensics is as evidence in a legal proceeding, and it must therefore meet legal requirements for digital image evidence.

SWGIT recommendations regarding how to document the chain of custody of the original image reveal a level of control that contributes to the preservation of a digital image

157. Recommendations are taken from SWGIT, "Guidelines for the use of Imaging Technologies in the Criminal Justice System."

158. Ibid., 5-6.

as an authentic record.[159] The recommended procedure regarding the "Chain of Custody of the Original" identifies two important stages in the handling of the original image; capture and "archiving."[160] In many cases, the admissibility of a digital image as evidence is determined by the chain of custody, and if a trusted chain of preservation cannot be accounted for, the integrity of the image may be challenged. SWGIT guidelines recommend a chain of custody policy for "archiving" images that includes documentation of the identity of the individuals with custody and control over the original image file from the moment of its initial capture to the creation of the "archive image."[161] In order to protect the integrity of the digital image throughout its lifecycle, an audit trail is recommended. Actions to be documented by the audit trail should include case details, description of shots and media used, downloading the data, creation of original image, storage of original image, access to original image, media refreshing, viewing of original image, use of original image in court, and final disposition.[162] The recording of these actions should be accompanied by a date and time stamp. Until the original image is actually destroyed, any person having custody and

---

159. SWGIT defines an original image as "an accurate and complete replica of the primary image." The primary image is "the first instance in which an image is recorded onto any separate media," such as recording an image on a flash card or downloading it from the Internet. SWGIT, "Guidelines for the use of Imaging Technologies in the Criminal Justice System," D4-105, 106.

160. Archiving is defined in the guidelines as the long-term storage of an image. Ibid. SWGIT has a recommended procedure for *Image Capture* that states that the functional context and legal requirements of the image dictate the capture process and its degree of documentation. In some situations, analogue photography is recommended for its superior dynamic range and resolution. The guidelines do recognize that digital cameras offer advantages in the immediacy of image viewing following capture and direct transmission, which they note as providing greater security and control; however, the disadvantages of the digital camera are its dependence upon a power source, limited storage capacity, use of proprietary hardware and software that present possible interoperability issues and the challenge of migrating and accessing legacy file formats once placed into long-term storage. The limitations listed reveal a thorough understanding of the challenges presented to ensuring the integrity of digital images over time and space. See SWGIT, "Guidelines for Field Applications of Imaging Technologies in the Criminal Justice Institute,Version2.3," (2001), 2-4, http://www.theiai.org/swgit/guidelines/sec3_2_3_2001_12_06.pdf (accessed June 1, 2005).

161. The Archived Image is defined as the primary or original image stored on media suitable for long-term storage. See SWGIT, "Guidelines for the use of Imaging Technologies in the Criminal Justice System," D4-105, 106.

162. Scientific Working Group Imaging Technology and Police Scientific Development Branch, "Digital Imaging Procedures V 1.0," International Association for Investigation, (2002). http://www.theiai.org/swgit/ (accessed June 28, 2005).

control over the "archived image" throughout its entire life cycle should be identified in documentation. Disposal schedules are determined for each image according to the type of offence and the sentence handed down as well as the fact that images must be available in the event of an appeal or a retrial.[163] A comparison of the recommended actions to be recorded in the audit trail and the benchmark requirements demonstrates the effectiveness of such actions in fulfilling the majority of the requirements. It also clarifies that both metadata and procedures for documentation are controls enacted by creators over digital image creation, use, and maintenance in which data about images are used for the purposes of record keeping.

SWGIT recommended procedures for "Preserving the Original" are to maintain and store the original image in an unaltered state in its native file format, which is the format in which the image was first captured in-camera. SWGIT supports the use of open standard image file formats for interoperability reasons. As a protective measure the original image file is copied onto CD and DVD. These are recommended by SWGIT for long-term storage because they offer high quality, durability, permanence, reliability, and ease of duplication. It is recognized that storage media may require routine refreshing to facilitate ongoing access to image files. The original image is referred to only in the event of a legal challenge to the integrity of a digital image. There are strict procedures outlining who has the authority to access an original image file and the methods of documenting those persons and their actions. Physical protection of the original image involves proper labeling and documentation of the location of all "archived" images as well as environmental controls and physical protection of image files under lock and key. Related to the file format preferences for

163. Ibid.

original images, the "Guidelines for Compression" recommend avoiding compression because of the risk of losing information and introducing digital artifacts into the image. In cases where compression is necessary, lossless compression is recommended. In the "Recommendations and Guidelines for the Use of Digital Image Processing in the CJS," a thorough discussion of compression is given along with visual examples of the effects of lossy compression used by the JPEG format.[164] The section on "Verification of the Original" states that the individual responsible for the capture of the original image, or an individual present at the time of capture, should verify that the image is a true and accurate representation.

The recommended procedure for "Preserving the Original – Post-Capture Processing" is to make a duplicate image that is an accurate and complete replica of the original image, irrespective of media.[165] The duplicate image is treated as the working image and may undergo *enhancement*, *analysis* and *processing*.[166] The type of image and the enhancement techniques used on the image determine the recommended procedures for "Documenting Image Processing." Techniques akin to traditional darkroom processes such as cropping, dodging, and contrast adjustment are considered standard processing steps, and when the results are "visually verifiable," documentation of these processes is limited to a simple description. Techniques used to increase the visibility of specific details in an image that may alter other image details (i.e., enhancement of latent fingerprints) are also considered

---

164. SWGIT, "Recommendations and Guidelines for the Use of Digital Image Processing in the Criminal Justice System,Version1.2," http://www.theiai.org/swgit/guidelines/sec1_2_3_2002_06_06.pdf, 8-10.

165. SWGIT, "Guidelines for the use of Imaging Technologies in the Criminal Justice System," Version2.1, June 1999, D4-105 & 106.

166. Image enhancement refers to any process intended to improve the visual appearance of an image or to draw out specific features or details within an image. Image analysis refers to the examination and interpretation of the content of an image and the image itself for legal purposes. Image processing refers to any activity that transforms the input image into an output image. SWGDE/SWGIT, "Digital & Multimedia Evidence Glossary," Draft Version1.0, April 2005, 7-9.

standard processing steps; however, documentation of these processes is mandatory and must present the enhancement techniques in sequence in order to facilitate duplication of the process for purposes of image analysis. SWGIT recommends an image processing log be used to document techniques for the purposes of image analysis and "Verification of the Processed Image." The minimum requirements for documenting image processing include identification of the software application used along with its settings and processing parameters. The "Guidelines for Compression" recommend lossless compression for working images that are intended for image analysis. In the event that an image must be transmitted to another agency or another specialist, the guidelines for "Image Transmission" emphasize that selected methods and devices for transmission should ensure that the received image accurately reflects the image as it was before transmission. Selection is made on the basis of security, the integrity of the image during transmission, and technological interoperability between file formats, hardware, and software.

Conclusion

This chapter has argued that the reliability and authenticity of digital images are contingent upon their method of creation, maintenance, custody, and preservation. Proving the reliability and authenticity of digital images requires procedures that make evident in the digital image metadata or in policies and standard operating procedures the actions of creators.[167] It is clear that the end use of an image dictates the type of information recorded about the digital image and the methods of managing it. It is also evident that the actions of creators are not necessarily sufficient to fulfill the requirements set by preservers in order to

167. Duranti, Eastwood, and MacNeil, *Preservation of the Integrity of Electronic Records,* 23-27.

assure future users that the images they are referencing are authentic and reliable. The nature of contemporary photographic practice presents a situation in which photographers work mostly as individuals, following their own set of guidelines, which are determined by routine habits and budgetary allowance; inevitably, they must perform the role and acquire the responsibility of both creator and preserver. The structured environment offered by organizations provides methods for creating born digital images as reliable and authentic records, yet many of these methods are generally beyond the scope of most businesses that are not operating under legal and regulatory restrictions.

The next chapter offers photographers recommendations on the type of information that should be recorded and the methods that should be implemented to ensure the creation, use, and preservation of their born digital images as reliable and authentic records over the long term. The recommendations address degrees of reliability and authenticity in a way that facilitates their application to as wide an audience of creators as possible. Thus, the recommendations may be viewed as a bridge between photographers and archivists.

CHAPTER FOUR

Overview

Creators and preservers are quickly learning that maintaining born digital images for future use requires vigilance and preventive actions throughout the image's life cycle to ensure that the digital files remain accessible, accurate, and authentic. Media fragility and technological obsolescence threaten the authenticity of digital images that are no longer used in the daily business activities (i.e., inactive images) but are retained for operational, legal, and historical purposes. Many of the measures taken by photographers to protect their digital image files from loss and corruption, such as refreshing older media and migrating obsolete file formats, alter the image file and, in effect, change it from what it was when it was first set aside.[168]

Current approaches to record keeping by photographers using digital technology depend on the two different environments in which they operate, the individual and the organizational. The organizational environment requires a greater degree of control over procedures for records creation and maintenance in order to ensure consistency and to provide a measure of accountability. These controls are made evident in documentation such as organizational policies and standard operating procedures, which employees follow whenever they create, transmit, and store digital images in the course of business and cultural activities. Thus, organizations rely on procedural means for protecting the authenticity of their digital images.

168. An authentic record is one that is what it purports to be and has not been altered or tampered with since it was first set aside by its creator.

The individual operating environment presents a situation that is less structured and more self-reliant. For the most part, individual photographers work alone and are responsible for all aspects of their record keeping. The fact that a single operator is responsible for the use and maintenance of the entire body of digital images provides a degree of assurance that the images have not been altered or corrupted since first being set aside; however, whenever digital images are transmitted outside of the original workspace and stored on different hard drives or external media, their authenticity is threatened. Many photographers utilize a range of image management software and metadata schemas to assist them in maintaining control over their digital images. Unless they operate within a specific legal or regulatory framework, photographers do not typically produce explicit documentation about their procedures for protecting the authenticity of their digital images. The information captured by individual photographers about their images is implicit and requires inspection of the records and the record-keeping system to be revealed.

Documentation about the creator's technological and administrative environment is important because it can be used to support a presumption of authenticity about the records. Before inactive records are transferred into archival custody, the preserver appraises them to determine their suitability for preservation. During the appraisal process, the preserver assesses known facts about the records, either implicit or explicit, and on the basis of such facts makes a presumption about the records' authenticity. The preserver bases the presumption of authenticity on the degree to which a set of conceptual requirements is met by the records and the procedures over their creation and maintenance. Although the requirements for records authenticity are generally understood and their conceptual basis is often discussed in a variety of writings, the only systematic set of criteria for assessing

records authenticity has been produced by the InterPARES research project, which has issued "Benchmark Requirements Supporting the Presumption of Authenticity of Electronic Records."[169] Once records are appraised and presumed authentic they are ready for transfer into a record preservation system. During the next stage, the continuing authenticity of the records will depend on the actions of the preserver and the maintenance of the records' authenticity. InterPARES has developed another set of criteria, "Baseline Requirements Supporting the Production of Authentic Copies," that apply to the preserver's procedures for maintaining records over the long term, which involve following rules for the production of authentic copies.[170] To attest to the authenticity of the digital copies, the preserver must fulfill all the baseline requirements.

This chapter discusses (1) the benchmark requirements in relation to digital images and the actions of creators concerning their creation, handling, and maintenance; and (2) the baseline requirements in relation to digital images and the actions of preservers concerning their maintenance. On the basis of this discussion, this chapter makes recommendations and addresses possible actions and strategies for creators and preservers.

Benchmark Requirements

Many photographers currently manage their images using methods that are dictated by time constraints and focused on immediate financial return. As a result, they perceive the necessary procedures to capture adequate documentation about the identity and integrity of digital images for record-keeping purposes and long-term preservation as laborious and expensive. An analysis of the conceptual requirements established by InterPARES and their

169. Duranti, *Long-Term Preservation*, 210-212.
170. Ibid., 213-214.

application to digital images in relation to the procedures for creation, handling, and preservation of digital images can provide an effective measurement of what is being achieved and what needs to be done to create and maintain born digital images as authentic records.

The benchmark requirements address the actions that should be taken by creators during the active and semi-active stages of their record's life cycle. The benchmark requirements are divided into two sections: the first section includes Requirement A.1, which defines the attributes of a record that establish its identity (subsection a) and are the foundation on which its integrity (subsection b) is demonstrated; the second section includes Requirements A.2 – A.8, which define the procedural controls over the records' creation, use, and maintenance that support a presumption of its integrity.[171]

Requirement A.1(a) defines the essential attributes for identifying an electronic record within the fonds of its creator. These attributes include the names of the persons concurring in its formation (i.e., the author, writer, originator, and addressee); the name of the action or matter the record participated in; the dates of creation and transmission (i.e., chronological date, received date, archival date, and transmission date); the archival bond, that is, the relationship of the record with previous and subsequent records as expressed by a classification code, a register number, or other unique identifier; and indication of attachments. The values of these attributes establish the identity of the record; however, they must remain persistently linked to the record and properly managed along with the record to ensure its authenticity. The necessary attributes of a record that allow for an assessment of its integrity, defined in Requirement A.1(b), are the name of the handling office (i.e., the

171. Ibid., 209.

office or person competent for carrying out the action to which the record pertains or participates), the name of the office of primary responsibility (i.e., the office or person competent for maintaining the authoritative record), the annotations (i.e., additions to the record after it is completed), and the indication of technical modifications (i.e., changes in digital encoding or software necessary to reproduce or render the record).

The task of making the attributes and their linkage to the record explicit to the user presents certain challenges for creators of born digital images. A photograph is not like a textual record, which may present the signature of the author and the name of the addressee. Much has been written about photographs being used "out of context" and the detrimental effect this has on their ability to accurately convey the creator's intended meaning. This highlights a photograph's dependence on contextual information to explain its purpose and assist viewers in interpreting the content. In analogue photography, slide mounts, plastic negative sleeves, contact sheets, and the print verso act as physical carriers for, and of, contextual information about the photographic image. As part of the procedures for the making of analogue photographs, creators apply a range of identifying information to their photographs through imprinting services offered by the development lab or by personally inscribing information, textual and numeric, onto a variety of photographic materials. Even amateur "photofinishing" services provide customers with a unique numeric identifier for each film roll and frame, which functions as a reference code to assist clients to locate a specific photograph for enlargement or duplication. Unfortunately, the dynamic and virtual nature of born digital images defies traditional methods of physically affixing a record with its identifying documentation.

Digital media require linkages between the born digital image and its documentation, which may be satisfied in different ways depending on the contexts of the images. Professional photographers currently capture in-camera metadata that provide, at the very minimum, the technical settings used to capture the image, the chronological date, a unique file identifier, and the name of the photographer. This is the basic information that is attached to almost all born digital image files captured by professional and amateur cameras and known as the Exif schema. Photographers establish and implement procedures that attach additional information to the digital images that reflect the documentary and procedural context in which the digital images participate. At the point when the image files are transferred out of the camera or off the memory card, and into image software, photographers implement methods for explicitly stating relationships between images and contextual information about the image, which includes file-naming conventions and the population of "File Info" profiles or IPTC profiles with metadata. In this regard, the attributes of identity and integrity set forth in Requirement A.1 provide an adequate foundation for establishing a basic record profile for born digital images that can be easily modified to accommodate extra information that reflects specific contexts. Once the profile is established and implemented it must remain persistently linked to the digital image throughout the image life cycle.[172] The record profile acts as a reservoir of documentation about the born digital image and retains

172. Diagnostic digital images added to patient case files should have explicitly linked metadata that document the context of image creation and provide a unique identifier. See AHIMA Workgroup on Electronic Health Records Management, "The Strategic Importance of Electronic Health Records Management. Appendix A: Issues in Electronic Health Management," *Journal of AHIMA: American Health Information Management Association* 75, no.9 (October 2004), http://library.ahima.org (accessed May 15, 2005).

all the information necessary to access and manage the digital image as a record of business and cultural activities.[173]

Many photographers criticize current techniques for implementing record profiles because the majority of software applications in use do not allow for the application of record profiles to a batch of image files.[174] Batch actions have the capacity to quickly apply consistent information to a number of image files that participate in the same activity, an action which is recommended for groups or classes of records that must comply with retention schedules determined by the juridical-administrative context. Unfortunately, at this time, batch commands in most image programs are notoriously inconsistent.

There is a wide variety of image software that is used by photographers for record keeping. This software offers a range of viewing and image management functionalities. These applications use information that is automatically and manually captured about the context and content of the digital image. By implementing the record profile as a control over the creation procedure, creators are assured that valuable information about a record's identity and integrity is linked to the record and available for discovery by search functions built into software applications. This is recommended for organizations in which many photographers may be contributing images to a central database or in situations where different departments are responsible for the creation, management and preservation of digital images. A further control may be added that requires population of the record profile in order to save an image into the electronic system.

---

173. The Public Records Office, "Guidelines for Management, Appraisal and Preservation of Electronic Records: Principles," *Electronic Records from Office Systems Programme* (1999), http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm (accessed June 28, 2005).

174. Batch actions are used in contexts that require a single operation or set of information to be applied to a large number of digital images such as all the digital images taken on a particular shooting assignment. See Ken Milburn, "The Ideal Digital Photographer's Workflow, Part 1." *O'Reilly Web DevCenter* (2003), http://www.oreillynet.com/pub/a/javascript/2003/12/17/digital_photography.html (accessed June 21, 2005).

Attributes of integrity defined in Requirement A.1 do not directly apply to the practice of individual photographers who hold responsibility for all record-keeping procedures; however, for accountability purposes, the record profile should include the name of the handling office and the name of the office of primary responsibility even if the information values default to the name of the photographer. In this manner, the digital image and its metadata reflect the provenancial context (i.e., the creating body and its mandate, structure, and functions).[175] By making explicit the persons responsible for its handling and maintenance, the integrity of an image is explained and a framework for accountability is provided.

In the context of an organizational operating environment, the attributes of integrity defined in Requirement A.1 are consistent with the guidelines promulgated by SWGIT for agencies operating within the criminal justice system. Their suggested procedural controls over the creation of digital images intended for use as evidence in the court system adhere to the principle that considers the first captured image as the "master image file."[176] The master file is to be transferred onto external media and labeled the "archival image file," which is designated as the authoritative record. Documentation of the chain of custody is required for all archival image files, and this includes the names of all persons involved in the formation, handling and preservation of the record; chronological date; archival date; and a unique file identifier. Standard operating procedures for image processing and capture of the original image are designed to provide evidence of a chain of custody that can be used as documentation attesting to the authenticity of the digital image file in legal proceedings.[177]

---

175. Duranti, *Long-Term Preservation,* 198.

176. SWGIT, "Guidelines for the Use of Imaging Technologies in the Criminal Justice System V2.3," 3-4.

177. Pollitt, "Report on Digital Evidence," D4-109.

The second set of benchmark requirements, A.2 – A.8, refer to procedural controls over record keeping that support a presumption of integrity. Requirement A.2 prescribes defining access privileges among users that reflect different levels of authority and capacity within the organizational structure. Access privileges offer control over administrative actions for image creation, modification, annotation, relocation and destruction. This requirement is more pertinent to organizations that have multiple users accessing digital image files held within a shared record-keeping system, such as agencies of law enforcement or medical health services.[178] In these cases there are certain classes of records, which are confidential and fall under privacy legislation that must be protected from unauthorized actions. User groups should be defined in organizational policies and implemented through standard operating procedures and the record-keeping system architecture.[179] The limits of administrative, group, and individual workspaces should be established on the basis of user responsibilities and job requirements. Audit trails that document the movements of users within the system should be established to determine the effectiveness of access privileges within the electronic record-keeping system. The establishment of user policies and guidelines that explain roles and responsibilities within the organization is recommended to ensure consistency over digital image creation, handling, and maintenance, and more importantly, to comply with protection of privacy legislation.[180]

With respect to photographers who work alone, most hold responsibility for the administration of their record-keeping system as a byproduct of their operating environment. Image management software (IMS) provides the dynamic "publish to Web" feature, which

178. AHIMA Workgroup, "Strategic Importance of Electronic Health Records Management."

179. Public Records Office, "Guidelines."

180. User groups in hospitals are provided access to certain types and classes of records, and in some cases read-only access may be granted but not the ability to alter or mark a record. See AHIMA Workgroup, "Strategic Importance of Electronic Health Records Management."

enables users to search and retrieve digital images held within an image database located on a personal computer, and should therefore implement access privileges as well.[181] IMS that offers access privileges should include read-only options for public user groups and passwords for clients and administrators.

Requirement A.3 refers to procedures for the protection of records against loss or corruption. The risk of losing digital information due to hard drive failures, computer viruses and media corruption is a reality that individual photographers and organizations working with digital technology must address through the implementation of protective procedures. In general, workflow processes for professional photographers rely on the seamless integration between hardware and software components and across operating platforms, which introduces the possibility of loss and corruption.[182] The frequent reports of crashes and pleas for technical assistance posted by photographers onto professional online forums are evidence of the routine hazard of operating in an electronic environment.[183]

Creators should establish protective measures against loss and corruption and implement them as part of routine operation procedures. Digital images held within active systems (i.e., not on removable media) should be routinely copied along with their metadata and file directory indexes. The massive volume of digital images held by professional photographers require significant storage space; therefore, the use of multiple hard drives is recommended for replicating data as a preventive measure against loss and corruption of stored files. It is recognized throughout the photographic community that back-up copies of software programs and operating system files should always be retained and available for re-installation. As part of a quality assurance program, regular scheduling of automatic system

181. Technical Advisory Service for Images, *Image Management Systems*.
182. Ken Milburn, "The Ideal Digital Photographer's Workflow, Part 3."
183. ProDig, Web forum messages, July 1, 2005. Available from http://www.prodig.org/.

back-ups that recognize and document modifications made to individual image files since the previous back-up are recommended procedures for safeguarding against problems when trying to access image files held within electronic systems.[184]

It is common for photographers to maintain numerous versions of an image file until the final product is completed; therefore, protective procedures against loss and corruption of digital image files should include documentation about back-up procedures that enable photographers to rebuild their files and directories. The documentary context of the records is expressed in the file arrangement and can be quite extensive when multiple versions of image files exist. Therefore, file directory "snapshots" and documentation of indexes are recommended to assist in rebuilding the organization of the documentary context and enabling photographers to mirror their directory configuration prior to back-up.[185]

Closely related to the procedures that protect against loss and corruption of records are the measures intended to counteract the effects of media fragility and technological obsolescence, addressed by Requirement A.4. The vulnerability of records stored on digital media is an issue for both creators and preservers of born digital images. The life span of digital media is difficult to determine and impossible to pinpoint; therefore, records stored for any length of time on external media should be monitored. The frequent use of the term "archival" on the labels of optical media and printing materials provides a false sense of security for users of these products. Analogue photography tolerates a degree of neglect so long as it is physically protected, but born digital images do not. They are machine readable and rely on the use of specific software programs to properly present their content and maintain their context throughout the lifecycle. Technological obsolescence is the endemic

184. SWGIT, "Guidelines for the Use of Imaging Technologies in the Criminal Justice System."

185. Bob Smith, "Re: Mac Backup Stuff," message posted to ProDig Web forum, June 23, 2005. Available from http://www.prodig.org/arch.html.

result of a digital image market propagated by vendors that consistently release new versions and discontinue support for legacy products.

Driven by innovation and demand, the diversity of image file formats and software applications available to photographers for image capture, use, and preservation is expanding. Photographers typically use image formats and applications that are supported by the industry in which they work in. For example, photojournalists submit their images in JPEG format to the news agency; however, they often keep TIFF or RAW files for their personal images collection. In order for any digital images to survive, creators should select open standard file formats for images that are selected for long-term preservation, such as original image files. Additionally, routine refreshing of storage media and migration of image files from obsolete formats to current ones should be used to counteract media fragility and technological obsolescence.[186]

Admittedly, most photographers recognize that their inactive records require monitoring to identify which files or classes of records need migrating and which media need refreshing; however, most have neglected maintenance procedures due to self-imposed time constraints. Prolific shooters, such as photojournalists, are responsible for voluminous collections of images that require a serious investment of time and materials to monitor and maintain over the long term. Unfortunately digital image files cannot survive for a long time without attention; therefore, photographers who continue to ignore issues of fragility and obsolescence place their image collections and their livelihood in jeopardy.

Requirement A.5 prescribes that documentary forms be defined for each type of record. The documentary form refers to the rules of representation that communicate a

186. Electronic Evidence Specialist Advisory Group, "Australasian Guidelines for Digital Imaging Processes, V2." National Institute of Forensic Science (2004) http://www.nifs.com.au (accessed June 23, 2005).

record's content, its administrative and documentary context and its authority.[187] Extrinsic elements of the record are part of the rules of representation that determine the general presentation features of a record (e.g., textual, image, audio) and the specific presentation features (e.g., resolution of image files, bit-depth, colour space). Included among the extrinsic elements of form are features that provide means of authentication and attestations such as electronic signatures, electronic seals, certification by a trusted third party, digital time-stamps issued by a trusted third party, and special signs (e.g., digital watermarks, personal logo), all of which affect the way the record is received and used. The expression of extrinsic elements is essential to the manner in which a born digital image is perceived and interpreted; therefore, any changes made to presentation features (incidentally or intentionally), or the application of measures for protection, effectively alter the digital image and its intended use. The addition of certain extrinsic elements to a record such as special signs and electronic signatures is not recommended for use with original image files since they alter the record.

In addition to extrinsic elements, there are intrinsic elements of documentary form that convey information about the action in which the record participates and its immediate context (i.e., names of persons involved in the formation of the record, chronological date and time of record's compilation, action or matter in which the record participates and geographic origin of the record.) There is an obvious overlap of information captured in the record profile regarding attributes of a record's identity and the intrinsic elements documenting a record's immediate context. Therefore, documentation via the record profile satisfies this aspect of requirement A.5 for digital images.

187. Duranti, *Long-Term Preservation,* 192.

Annotations made to a record after it has been created offer valuable information about the procedure a record goes through.[188] There are different types of annotations made to the record at different times in the administrative process: annotations made during the execution of the record (i.e., priority of transmission, transmission date/time/place, indication of attachments), annotations made during the handling of the business matter (e.g., received date/time, name of handling office, further transmission date/time), and annotations made during the management of the record for records management purposes (i.e., archival date, draft or version number, record item identifier, dossier identifier, class code, registration number and name of the creator). In reference to digital images, the most common annotations are those that are made in the course of executing the record, such as information regarding intellectual property rights.

Many photographers attach information about intellectual property rights to their digital images; however, the methods used vary according to each industry. Indication of copyrights and usage restrictions are typically added by photojournalists to the IPTC Core metadata profile before transmitting a digital image to the news service, thereby generating annotations made in the course of executing the record and of handling the business matter to which the record relates. Photographers who make their digital images available via Web sites, as on line viewing galleries, or for the purposes of stock sales, embed copyright information such as their name or the symbol "©" into the image through the technique of digital watermarking. Essentially, the watermark becomes a part of the presentation of the digital image; it fulfills its intended purpose to impede unauthorized use and is treated as an extrinsic element of documentary form.

188. Ibid., 196-198.

A consideration of the extrinsic elements of documentary form for born digital image files introduces the issue of accurate representation within the digital environment. Documentation about specific presentation features of a born digital image includes data on image resolution, compression, colour space, and bit depth. These elements provide the foundation of visual communication in the digital environment. Current photographic practice, regardless of the industry, distinguishes different documentary forms for the original image file and its working surrogates. Differences include file type, compression, colour space, and resolution. Documentary forms vary according to the intention of the creator and the requirements of the juridical system in which they are generated. It should be noted that generalizations mandating the presence of specific elements of form to support authenticity are not possible.[189]

A recent publication of the *Research Libraries Group*, "Automatic Exposure: Capturing Technical Metadata for Digital Still Images," discusses the importance of technical metadata for documentation of the digitization process and an image's provenance.[190] This white paper does not focus on born digital images; however, it raises the critical issue of how to represent digital image files accurately across time and space. The paper aims to identify what type of metadata is best to capture and retain information regarding the technical properties of a digital image. To do this properly, capture devices must document technical settings in a manner that addresses digital preservation (i.e., software independent). For photographers creating born digital images, this places an emphasis on choosing capture devices and file formats that support technical metadata, which many already do. As

189. Ibid., 216.

190. Research Libraries Group, "Automatic Exposure: Capturing Technical Metadata for Digital Still Images," *RLG DigiNews* (2004), http://www.rlg.org/en/page.php?Page_ID-20462#article1 (accessed June 28, 2005).

discussed in Chapter 3, Exif metadata are automatically captured by the camera or scanner and reflect the hardware settings at the time of capture. The initiative to standardize Exif has been successful, and most consumer and professional cameras embed this information in TIFF, JPEG and some RAW file formats. Most photographers now rely on Exif to capture the camera settings and use the information for purposes of search and retrieval and to enable recreation of a shot from a technical perspective. However, as discussed in 3, technical metadata is not written and read by all devices, hardware, and software applications. In effect, the aim of this whitepaper is to make all elements found within the picture taking conditions of the Exif schema mandatory for all "writers and readers."[191]

In the context of any given juridical system, records creators may be required to meet specific legal standards for digital image authentication. Requirement A.6 defines authentication as "a declaration of a record's authenticity at a specific point in time by a juridical person entrusted with the authority to make such declaration."[192] Institutions that produce digital images for legal purposes provide documentation that attests to the authenticity of the digital image, such as organizational charts, policies, and SOPs that implement audit trails for images.[193] These documents make evident the accountability framework and the procedural context of the digital images. A sample SOP for digital image evidence capture and preservation includes documenting the action, chronological date and time, unique identifier, name and signature of author (i.e., photographer or technician), and certification through a declaration of the authenticity of the image at that time by the

191. The White paper promotes the use of the NISO Z39.87: Technical Metadata for Digital Still Images and its Data Dictionary.

192. Duranti, *Long-Term Preservation,* 216.

193. Staggs, "Admissibility of Digital Photographs in Court."

technician.[194] Alternatively, a certificate signed by the electronic record-keeping system operator attesting to the integrity of the system may be sufficient for legal purposes.[195]

Additional approaches to determine the authenticity of digital images that are promoted in the computer sciences community, are the use of software programs that provide algorithms for encryption and require a "key" to view encrypted images properly, hash functions that calculate and compare digital image bit-streams, and a variety of digital watermarking techniques.[196] Recent developments in encryption technology have been focused on the production of cameras that provide in-camera watermarks at the time of capture.[197] The labour and cost associated with authentication by software should be considered before being adopted. Additionally, encryption methods that alter the image data are not recommended for original image files or images that are intended for visual analysis.[198]

Requirement A.7 prescribes procedures for identifying the authoritative record among multiple copies held within a creator's fonds. Photographers typically implement procedural controls for the capture, transfer, and storage of the authoritative record to ensure that its documentary form is not altered and that its status is protected. Most photographers consider the first captured image file to be the digital original. Procedures for the capture and transfer of the original file to external media are prescribed in SOPs and recognized in legislation

194. Police Central, "White Paper: Suggested Procedures for Preservation of Digital Crime Scene Photographs," *Cop Tales* (1998), http://www.policecentral.com/wp-crimescene.htm (accessed June 10, 2005).

195. House of Lords, *Science and Technology Committee – Fifth Report,* London: HMSO, 1998.

196. Ibid.

197. Paul Blythe and Jessica Fridrich, "Secure Digital Camera," *Digital Forensic Research Workshop* (2004), http://www.dfrws.org (accessed July 2, 2005).

198. Due to its non-reversible distortion, watermarking technology is currently not recommended for forensics, medical or military imaging. Berg, "Legal Ramifications of Digital Imaging in Law Enforcement."

regulating the admissibility of digital images.[199] The archival image is consulted as the authoritative image in any legal situation where a comparative analysis between the original and the processed (i.e., enhanced) version is required by the court. The existence of multiple digital originals is recognized and it is presumed that the "marker" of the image (i.e., person responsible for articulating the content of the record) determines which image is intended to be legally effective.[200]

Alternatively, photographers may designate the final processed image (i.e., that which is edited or enhanced with image software) as the complete and authoritative record. This approach recognizes the final image file as the version most capable of producing the intended effects of the digital image. Photographers often deliver the final image to the client after it has been altered, cropped, and so on, and retain the first captured image for their own record-keeping purposes. This demonstrates that the parameters for an authoritative record are dependent upon legal requirements, the intentions of the creator, and the functional context.

A valuable annotation for the management of digital image versions within collections, which is often overlooked by photographers, is the draft or version number. Photographers often rely on the date/time stamp generated by the computer system to indicate relationships between authoritative and surrogate files with the same name. Methods that are recommended for making the authoritative record evident among multiple copies involve file-naming conventions that include versioning information (i.e., including the term "copy" or "original" in the file title or a numeric indicator such as v.1 or v.2) and classifying

199. Existing procedures for creating a digital image with the intention of using it as legal evidence designate the in-camera image as the primary digital image. House of Lords, "*Science and Technology Committee.*"

200. Ibid.

folders into process-related directories (i.e., establishing a drafts folder). These activities are recognized under Requirement A.5 as annotations made by the creator in the course of managing the record.[201] The recommended procedure for file naming involves establishing a system that is extensible, applicable to both analogue and digital images held within the fonds and software application independent. Once the system is established, it should be applied to all images in the fonds and the file directory should be documented along with any indexes.[202]

Requirement A.8 specifically prescribes the removal and transfer of relevant documentation about inactive records that are scheduled for disposal or transfer to an archival facility. Creators who remove digital image files with the intention of disposal or transfer should gather and include documentation that establishes the identity and integrity of the records and reflects their technological, administrative, and procedural context. Documentation transferred with the records should serve the purposes of identifying the digital images and their contexts of creation and providing evidence of a trusted chain of custody.

Retention and disposal of digital images should be scheduled according to the juridical-administrative context in which they participate; therefore, digital images gathered as evidence in court cases must be maintained and monitored throughout the active and semi-active stages of the case file. When the case is closed and the inactive records reach the limitation of their retention period, digital image files should be disposed of according to established procedures set forth by the institution and legal regulations. If the image file is

---

201. Duranti, *Long-Term Preservation,* 197-198.

202. David Riecks, "Filenaming as a Strategy to Managing Your Assets," Controlled Vocabulary.com (2005) http://www.controlledvocabulary.com/imagedatabases/filenaming.html (accessed June 28, 2005).

destroyed, the image's audit trail is closed and the institution should maintain the documentation.[203]

When inactive records are transferred to the preserver, the threshold between the functions and duties of the creator and those of the preserver is crossed. As demonstrated thus far in this chapter, the benchmark requirements are a valuable tool for assessing the maintenance of the identity of the records and the effectiveness of the procedural controls over their creation, use, and maintenance during their active and semi-active stages, for the purposes of appraising the records and determining their degree of authenticity. Assessment of the authenticity of a creator's records should be performed as part of the appraisal process before records are transferred into archival custody.

Baseline Requirements

The "Baseline Requirements to Support the Production of Authentic Copies of Electronic Records" [204] outline the duties of the preserver and examine the preservation function regarding the reproduction of the creator's records to provide future users with authentic copies for reference and use. The baseline requirements do not concern the actions of the creator; instead, they focus on the procedural controls over the transfer of inactive records into archival custody and the preservation actions taken by preservers following transfer. The following recommendations are intended for preservers, but may be of interest to creators as they are frequently placed in the position of preserving their own records.

The baseline requirements address the functions of managing preservation, which involve maintaining the authenticity of the creator's digital images by implementing controls

---

203. Electronic Evidence Specialist Advisory Group, "Australasian Guidelines."
204. Duranti, *Long-Term Preservation,* 212-214.

over records transfer, maintenance, and reproduction (Requirement B.1); providing documentation of the reproduction process and its effects on the reproduced records (Requirement B.2); and implementing archival description (Requirement B.3). If the baseline requirements are met, the preserver can guarantee that any copies made of the records for reference use are authentic copies and that the information about the preservation function is documented in a manner that lends transparency to the preservation process. Whereas the benchmark requirements are founded on the concept of a trusted record-keeping system, the baseline requirements are based on the concept of the preserver as a trusted custodian.[205] Although photographers are not typically involved in the long-term preservation function, the nature of digital media requires that procedures be put in place in the early stages of the image's life to allow for their continuing preservation and to ensure ongoing access. The baseline requirements introduce aspects of the preservation function that are rarely discussed outside the archival community, such as the need to create authentic copies and to describe the records in their context as interrelated aggregations.

Requirement B.1 prescribes controls over the transfer of digital records into archival custody, which include an integrated management of the entire process and all its procedures, such as the verification of the authority to transfer the records and of the prior assessment of the authenticity of the creator's records. Documentation such as the transfer list and file directories should be transferred with the records and used to assess the completeness of the transfer. Once the records are under the responsibility of the preserver, the maintenance of archival records requires establishing procedural controls that implement access privileges

205. A trusted record-keeping system is a type of system in which there are rules governing the persons authorized to input and retrieve records, the actions that may be taken, and the retention of records and transfer out of the system. A trusted custodian is a physical or juridical person entrusted with independently maintaining the records. Ibid., 48.

over access, use, and the reproduction of the records in the archives, and that are capable of preventing the loss or corruption of records and of protecting the identity and integrity of records from the risks presented by media fragility and technological obsolescence.

An important aspect of the preservation function is the authentic reproduction of the records, which involves establishing, implementing and monitoring reproduction procedures capable of ensuring that the process of making authentic copies does not alter the content or presentation of the records in any way. Requirement B.2 prescribes that documentation should be produced throughout the reproduction process, including information about variations between the record and its reproduction, and that this documentation should be made available to users. Because born digital images depend on accurate presentation to convey their meaning, it is highly recommended that any technical information regarding the reproduction process be attached to the authentic copy. This type of documentation provides users with contextual information that assists in interpreting the record and assessing the preservation function.

Requirement B.3 prescribes that the records be collectively authenticated and their administrative and documentary relationships be perpetuated through archival description.

The application of benchmark and baseline requirements to born digital images, under the guidance of professional preservers would help photographers to take steps towards creating and maintaining born digital images as authentic records. As natural and appropriate, the actions of creators are predicated on business needs and the legal and regulatory environment in which they operate. Therefore, organizations are further along in establishing and implementing standard operating procedures for image management and preservation than individual photographers.

Professional photographers who produce born digital images as employees of organizations or operate in highly regulated industries such as structural engineering, medical diagnostics, military surveillance, georeference mapping, and law enforcement follow guidelines and best practices produced by the professional associations that represent them. Many of the record-keeping initiatives are in response to a perceived lack of exact requirements for the legal admissibility of born digital images, since the terminology used by the Federal Rules of Evidence are not as exact as those working in the digital environment would like.

The metadata standards promulgated by the International Press Telecommunications Council are effective for photojournalists and fulfill some of the identity and integrity requirements defined in the InterPARES project benchmark requirements. The presentation of IPTC metadata in profiles (i.e., automatically generated panels with set elements) is gaining attention in the professional community for their ease and integration into image management software application. This raises the issue of proprietary and industry-specific software being used for the management of born digital image collections. On the one hand, image management software offers individual photographers a measure of procedural control that mimics a record-keeping system and offers them some of the structure inherent in the organizational environment. On the other hand, IMS adds another layer of technological complexity to the process of creating and maintaining born digital images, which invites interoperability problems in the future. On the basis of current record-keeping practices employed by individual photographers in unstructured environments, the survival of records of cultural activities is unlikely.

Recommendations

What follows is a summary of the recommendations discussed in this chapter that should be able to support the creation, use, and maintenance of digital images in a manner that would allow for their long-term preservation.

Recommendation 1

Creators of born digital images should establish a record profile for each and every digital image that is saved. The record profile should include data related to the identity and integrity of the image and remain inextricably linked to the digital image file throughout its life cycle.

Recommendation 2

Creators should establish and implement access privileges into their record-keeping system. Assigning specific authority and capacity to user groups provides control over all procedures involving the creation, use, and maintenance of born digital images. Audit trails should document users' interactions with records. This is a critical component for electronic systems containing born digital images that must comply with freedom of information and protection of privacy legislation.

Recommendation 3

Creators should use standardized file formats and metadata schema for born digital images intended for long-term preservation in order to maintain a degree of protection against incompatibility, corruption, accidental loss, and obsolescence.

Recommendation 4

Creators should make regular upgrades to operating systems and hardware and software components as a preventive measure against technological obsolescence. Professional photographers are on the forefront of technological innovation out of the necessity to remain competitive in their chosen industry. Their reliance on a complex technological base to perform daily image operations and management functions requires planning and preparation to protect images within the collection. Every change in the technology base of their business should be undertaken with the understanding that interoperability among system components, which are likely to be affected as well as any "scripted actions" used in personal workflows to automate processes, may be temporarily disabled. Therefore, creators should maintain documentation about the system infrastructure, file directories, scripted actions, and essential records in the event of temporary or permanent loss as a result of upgrading.

Recommendation 5

Creators should select metadata specifications for their born digital images that are interchangeable, extensible, scalable, and consistent, in order to provide documentation that is viable and interoperable for the long term.[206] Capturing metadata in this manner should assure creators that their born digital image files could be accessed in the future even if the native viewing application becomes obsolete. This is especially critical in regard to technical metadata and the proper presentation of the content of born digital images on future systems.

206. Digital Imaging Group, "Dig35 Specification: Metadata for Digital Images V1.0," International Imaging Association (2000), http://www.i3a.org/i_dig35.html (accessed July 1, 2005).

Recommendation 6

Creators should be able to provide authenticating information about their digital images. Current discussions in the photographic community regarding authentication of born digital images for legal purposes focus on producing written or oral testimony regarding the management and operational procedures applied to the record. Presently there are no legal requirements specific to born digital image security or authentication,[207] although for each digital image submitted as evidence in a court of law it must be possible to establish "who did what when" in order to determine its integrity.[208] The authenticating information provided by the creator should be able to demonstrate the use of secure storage, access privileges, back-up procedures, a chain of custody, and proper training of the person responsible for the maintenance of the images.[209]

Recommendation 7

The creator should designate a person or office of primary responsibility that is given formal competence and authority to maintain the authoritative records. Literature on this topic is isolated to law enforcement agencies in which there is a designated "evidence custodian"; however, recent initiatives suggest the need for a "digital evidence custodian" to oversee the transfer of original digital image files from capture hardware to storage media.[210] In practice, photographers store the authoritative files on external media that may be under lock and key. It is recommended that preservation functions include monitoring storage

---

207. U.S. federal and state case law admit photographs, video, and audio providing they are accompanied by documentary or testimonial support. Ibid.

208. Blythe and Fridrich, "Secure Digital Camera."

209. George Reis, "Digital Imaging Guidelines," *Imaging Forensics,* (2004), http://ww.imagingforensics.com (accessed June 23, 2005).

210. Keith Hodges, "Handling Digital Photographs for Use in Criminal Trials, V1 May 27, 2004," http:www.khodges.com/digitalphoto/ (accessed July 2, 2005).

media and performing procedures for refreshing and migration. These actions should be defined in polices and implemented as part of routine preservation procedures. If applicable, the office of primary responsibility should have as its directive the maintenance and monitoring of specific classes of digital image files to effectively determine their retention and disposition schedules and comply with applicable freedom of information and protection of privacy legislation.

Recommendation 8

Creators responsible for producing authentic copies of born digital image files for preservation purposes should understand the importance of documentary form and presentation features. Current initiatives in the heritage sector are focused on digitization projects that transform analogue media into digital media using presentation targets determined by the intended use of the authentic copies. In contrast, the presentation parameters of born digital images are limited by the choices made at the time of capture by the creator and shaped by the available technology. Therefore, preservers should recognize that documentation about reproduction procedures and the results are just as important as the authentic copy itself, if not more so. Documentation about the effects of the reproduction process add yet another layer of context to the record that must be respected and retained along with the reproduced copy.

CONCLUSION

This study demonstrates the importance of an interdisciplinary approach to ensuring the longevity of born digital images as reliable and authentic records. It is a response to an identified need within the photographic and archival communities to develop a comprehensive understanding of how born digital images are being created, used, and preserved. Its aims were, in part, defined by the goals of the InterPARES research project. Some of the instruments used to learn about the activities of photographers and their records are derived from the collaborative efforts of the InterPARES research team. It is hoped that the findings of this study will inform creators and preservers of digital images about the key concepts and methodologies required for the creation, use, and preservation of born digital images as reliable and authentic records, and will provide practical strategies capable of supporting future actions in this direction.

The literature review undertaken at the outset provided evidence of the commonalities and differences among the archival, photographic, and legal disciplines in their understanding of and approaches to the concepts of reliability, authenticity, and originality in relation to analogue photography and digital imagery. The lack of a consistent vocabulary in which to define and describe born digital images was apparent in all disciplines. In general, literature about the creation and use of digitized images is far more prevalent than writings addressing the concepts and methodologies for creating and preserving born digital images. Also, for the most part, the bibliographic sources that informed this study were found online, and included technical specifications, conference proceedings, and discussions posted on professional forums. The literature review made it clear that more substantial information

about how photographers create, use, and maintain their born digital images as reliable and authentic records was to be acquired elsewhere, especially because this study was meant to provide a comprehensive assessment of born digital images as a new type of record format.

Primary Findings

1. Photographers create the kind of digital record that is best suited for their business and creative needs. In general, photographers produce images in JPEG (open standard) and TIFF (de facto standard) formats for the purposes of transmission, printing, and long-term storage. Draft files are most often saved in the layered PSD format, which allows photographers a sequential history of image processing operations. The preference for RAW files (proprietary) as the image captured in-camera and designated as the digital original is, however, troubling.
2. The general assumption of photographers about future access to their records is that it is only a matter of time before something bad will happen to their images. Most photographers expressed genuine concern for the longevity and operability of their inactive born digital image files. Less than a handful of them think that future technology will be capable of accessing obsolete file formats.
3. The nature and variety of digital materials used by photographers is determined by the contexts in which the images are generated as byproducts of business activities and cultural endeavours.

The findings of the survey on record-keeping practices of photographers using digital technology provided a better understanding of the nature of born digital images and the

activities carried out by photographers operating in a variety of business and cultural contexts. The large number of survey participants significantly enhanced the value of the information provided, which led to the discovery of professional standards and procedural best practices and to a greater sense of the climate in which photographers operate. It is evident from the survey data that photographers are not aware of initiatives promulgated by the heritage community regarding the management and preservation of digital images. As expected, most of them aim to produce digital images that meet the requirements set forth by a particular business context. In so doing, the emphasis of their actions is on the active and semi-active stages of the record's life cycle, and their concerns about digital image storage are limited to the short term. Discussions by the imaging community about long-term preservation are limited to selecting "archival" storage media or printing papers. Regardless of the fact that the photographers who responded to the survey have not yet lost image files due to media fragility or technological obsolescence, they expressed concern and trepidation about the day when their images become inaccessible.

The findings of the survey also reveal that most photographers have developed procedures for the creation of their born digital images that involve designating an original digital image, copying derived images, and saving the original file onto external media for maintenance and long-term storage. In general, storage media such as CDs and DVDs are recommended by best practices, regardless of the business context. Media fragility is addressed by refreshing CDs and DVDs as the most common preventive measure. Unfortunately, the more serious problem of technological obsolescence receives less attention than media fragility. Photographers' reliance on proprietary file formats and software applications, combined with the nature of the technology industry in which

innovation fuels an endless stream of new products and new versions, presents an opportunity for operability issues and data corruption. The situation is further complicated by the incorporation of metadata into digital image files. Initiatives to implement semantic and syntactic interoperability for the purposes of sharing and supporting standard metadata schemas are essential to ensuring the authenticity of digital images. There is no point in capturing metadata or discussing the merits of record profiles if the information is not explicitly and persistently linked to the record throughout its life cycle, regardless of the file format, software application, or operating system. Collaborative efforts within the imaging industry to develop standard protocols for the exchange of born digital images and their metadata recognize the need to cultivate and support standardization.

As demonstrated in chapter 3, the standard metadata schemas used by photographers are not adequate to ensure a presumption of authenticity. The schemas are narrow in their scope and do not provide sufficient documentation for the management and preservation of born digital images as authentic records. The comparison of the schemas against InterPARES benchmark and baseline requirements has revealed the usefulness of such requirements as an assessment tool. The exercise resulted in a recommendation to establish and implement a record profile. This profile would be generated at the time of saving an image into the record-keeping system and would capture metadata that make explicit record identity and integrity in perpetuity. The increase in available image management software aimed at the needs of both individual photographers and organizations, along with the improved functionality of image processing software, is offering record-keeping capabilities to creators. These include metadata schemas to describe image files, collections indices, version control through file-naming conventions, transmission protocol for image exchange and online delivery, and file

directories for "archived" off-line images. An increasing number of photographers and organizations are customizing software to incorporate actions and processes into the functionality of the actual application that reflect their documentary and procedural contexts. As a direct result, creators are becoming more aware of the issues involved in responsibly managing digital information as an asset. In effect, they are learning about the function of preservation and the role of the preserver in the electronic environment. This is a vital lesson because born digital images will not survive long enough to become archival sources without the pro active efforts of creators during the early stages of the record life cycle and throughout storage. Therefore, it is highly recommended that InterPARES benchmark and baseline requirements be articulated into standards for born digital images and integrated into commercial software functionality. Certification of vendor products would be made on the basis of compliance with the requirements.

The standard operating procedures defined by SWGIT are valuable templates for organizations that produce records that must meet legal regulations. By providing a documented chain of custody for each digital image, these standard operating procedures implement controls on an organization-wide scale that ensure that digital images meet legal admissibility requirements. Currently, documentation of the steps and phases in the creation, handling, use, processing, and maintenance of digital images is captured in paper forms and logbooks. This approach to record keeping is appropriate for large bureaucratic institutions that function within an accountability framework and a hierarchical culture. The controls established by SWGIT are recommended for law enforcement agencies, medical health services, military surveillance operations, and city engineering departments. Because of their focus on the creation of audit trails for each procedure and rigorous controls over the

creation, handling, and preservation of the original digital images, SWGIT guidelines and their partnered initiatives are recommended for their emphasis on digital image integrity. Further analysis aimed at amalgamating the InterPARES benchmark and baseline requirements with SWGIT guidelines in order to articulate a set of criteria that could be incorporated into an electronic record-keeping system is recommended.

There are currently a number of initiatives in the heritage and arts communities that are exploring concepts and methodologies for preserving digital media and for resource discovery in the electronic environment. These research projects are providing needed information on how to maintain records of value for future use. The InterPARES project and this study are part of the effort to inform creators and preservers of the current situation and to assist them in preparing for the future; however, a question must be raised regarding the effects that this type of "advising" will have on the impartial quality of the records and the objectivity of the preserver. The argument against the involvement of preservers in the active and semi-active stages of a record's lifecycle rests on the belief that creators generate records as natural by products of activities and that any interference from preservers will alter the intent of the creator and corrupt the record's characteristic of impartiality. Furthermore, the traditional role of the preserver as a trusted custodian does not include responsibility for the records before they are inactive and transferred to his or her responsibility for long-term preservation. However, the nature of the electronic environment requires that the expertise of preservers be brought to bear on the entire life cycle of the records to allow the survival of digital information; thus, they have to walk a very fine line between interference with the creation process and support for it in order to ensure that the identity of the images generated will not be altered by their preservation needs.

This study has demonstrated that preservation procedures that were once the sole responsibility of preservers must become part of the preventive measures against corruption and loss that creators incorporate into their creation and maintenance procedures. Ultimately, the longevity of born digital images as authentic records for future use rests on the decisions and actions of creators. Yet the findings of this study make it evident that at this time photographers are simply meeting the minimum requirements set forth by their regulatory environment. With this knowledge, preservers would be remiss if they did not share their unique perspective and their valuable insight with creators, if only for the purpose of explaining the inherent risks of the digital environment. More importantly, it is the responsibility of preservers to describe the relationships between the records within the same fonds and explain the functions of the creator within the universe in which it operates, to ensure the continuing authenticity of the images that will be preserved. Archival description elucidates context and locates the records within a cultural continuum. The challenges of digital technology as a method of documentation and communication necessitate a more central role for preservers and an increased need for archival description to place born digital images into their functional context and reveal their true meaning. The approach taken in this study embraces and encourages multidisciplinary inquiry for the purposes of preserving and making accessible born digital images as authentic sources across communities and on a global scale.

This study is intended to provide a foundation for further research on the nature of born digital images as reliable and authentic records and the record-keeping practices of photographers. The structured and unstructured environments identified in this study as the two typical contexts of photographers' activities present the opportunity for an in-depth

investigation and analysis of their different approaches to born digital images and record-keeping procedures. The InterPARES benchmark and baseline requirements are recommended as a tool for assessing these two environments. They should be used in the context of a case study method of investigation, which is usually very fruitful because it allows participants to explain their processes at length.[211] The case study analysis should include an assessment of the effectiveness of the benchmark and baseline criteria in a real-life setting. Guidelines for creators and preservers should be developed on the basis of this kind of extended research. Guidelines for the creation, use, and preservation of born digital images as reliable and authentic records should be written and disseminated throughout the photographic and archival communities. It is hoped that this will represent a valid step and a point of reference toward such purpose.

211. The qualitative data from the survey questionnaire offered valuable insight into the minds and actions of photographers.

BIBLIOGRAPHY

Aaland, Mikkel. *Digital Photography*. New York: Random House, 1992.

Adobe Systems, Inc. "Adobe XMP for Creative Professionals: Metadata and the Creative Suite." Adobe White Paper (2004), http://www.adobe.com/products/xmp/pdfs/XMP_for_CreativePros2004.pdf (accessed May 15, 2005).

Adobe Systems Inc. "DNG: The Public, Archival Format for Digital Camera Raw Data." Adobe Systems Inc., (2004), http://www.adobe.com/products/dng/main.html (accessed January 10, 2005).

Adobe Systems Inc. "Introducing the Digital Negative Specification." Adobe Systems Inc. (2004), http://www.adobe.com/products/dng/pdfs/dng_primer.pdf (accessed May 15, 2005).

AHIMA Workgroup on Electronic Health Records Management. "The Strategic Importance of Electronic Health Records Management. Appendix A: Issues in Electronic Health Management." *Journal of AHIMA: American Health Information Management Association* 75, no. 9 (October 2004), http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_024672.html (accessed May 15, 2005).

Amelunxen, Hubertus, v., Stefan Inglhaut, and Florian Rötzer. *Photography after Photography: Memory and Representation in the Digital Age*. Munich: G&B Arts, 1996.

Ang, Tom. *Dictionary of Photography and Digital Imaging: The Essential Reference for the Modern Photographer*. London: Aurum Press, 2001.

Baca, Murtha, ed. *Introduction to Metadata: Pathways to Digital Information 2.0*. Los Angeles: Getty Information Institute, 2000. http://www.getty.edu/research/conducting_research/standards/intrometadata/index.html (accessed June 20, 2005).

Benjamin, Walter. "The Work of Art in the Age of Mechanical Reproduction." In *Illuminations*, edited by Hannah Arendt, trans. Harry Zohn, 217-247. New York: Schocken Books, 1968.

Berg, Erik C. "Legal Ramifications of Digital Imaging in Law Enforcement." *Forensic Science Communications* 2, no. 4 (October 2000) http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm (accessed June 1, 2005).

Besser, Howard, and Sally Hubbard. *Introduction to Imaging*. Rev. ed. Los Angeles: Getty Research Institute, 2003.

Blythe, Paul, and Jessica Fridrich. "Secure Digital Camera." *Digital Forensic Research Workshop* (2004), http://www.dfrws.org/2004/bios/day3/D3-Blyth_Secure_Digital_Camera.pdf (accessed July 2, 2005).

Braun, Marta, and Jessica Bushey. "Article Summaries from the Digital Photography Bibliography." InterPARES 2 (June 30, 2004), http://www.interpares.org (accessed May 15, 2005).

———. "Proposal for a Survey of the Record-Keeping Practices of Photographers Working with Digital Materials." InterPARES 2 (2004), http://www.interpares.org (accessed May 15, 2005).

———. "Record-Keeping Practices of Photographers Using Digital Technology." Paper presented at the InterPARES 2 Plenary, Vancouver, BC, February 2005.

———."Survey of the Record-Keeping Practices of Photographers Using Digital Technology." InterPARES 2 (2004), http://www.interpares.org/gs07/login.cfm (accessed October 15, 2004).

Bullock, Alison. "Preservation of Digital Information: Issues and Current Status." *Network Notes* 60 (April 1999), http://www.collectionscanada.ca/9/1/p1-259-e.html (accessed January 10, 2005).

Bushey, Jessica. "Approaches to Born Digital Images in Photographic and Archival Literature." University of British Columbia, 2005.

Camera & Imaging Products Association. "Domestic Council Digital Imaging Standardization Groups." (2002), http://www.cipa.jp/english/hyoujunka/international/digitalimage.html (accessed January 10, 2005).

Cherry, Michael. "Reasons to Challenge Digital Evidence and Electronic Photography." *The Champion* 6 (2003): 43.

Cookman, Claude. "The Evolving Status of Photojournalism Education." Available from ERIC Digest, Item ED477610 (2003), http://www.ericdigests.org/2004-1/status.htm (accessed March 13, 2005).

Cope, Peter, ed. *The Digital Photographer's Pocket Encyclopedia.* Cambridge: The Illex Press, 2002.

Craig, Barbara, and Gordon Dodds. "The Picture of Health." *Archivaria* 10 (Summer 1980): 191–123.

Cross, J. M., Dr. "Nineteenth-Century Photography: A Timeline." *The Victorian Web: Literature, History & Culture in the Age of Victoria, University Scholars Programme Project* (February 4, 2001), http://www.victorianweb.org/photos/chron.html (accessed March 12, 2005).

Curtin, Dennis P. *Short Courses* (2003), http://www.shortcourses.com (accessed January 10, 2005).

De Mul, Jos. "The Virtualization of the World View: The End of Photography and the Return of the Aura." *The Photographic Paradigm* 12 (1997): 44–56.

Depocas, Allain, John Ippolito, and Caitlin Jones, eds. *Permanence Through Change: The Variable Media Approach.* New York and Montréal: Solomon R. Guggenheim Foundation and Daniel Langlois Foundation, 2003.

Deschamps-Marquis, Marie-Hélene. "Influence of Copyright on the Emergence of New Technologies: A North American Perspective." Master's thesis, McGill University, 1999.

Digital Imaging Group. "Dig35 Specification: Metadata for Digital Images V1.0." International Imaging Association (2000), http://www.i3a.org/i_dig35.html (accessed July 1, 2005).

Dillman, Don A. *Mail and Internet Surveys: The Tailored Design Method,* 2nd ed. New York: John Wiley & Sons, 2000.

Dillman, Don A., and Dennis Bowker. "The Web Questionnaire Challenge to Survey Methodologists." In *Dimensions of Internet Science*, edited by Ulf Dietrich Reips and Michald Bosnjak. Lengerich, Germany: Pabst Science Publishers, 2001. http://survey.sesrc.wsu.edu/dillman/papers.htm (accessed May 20, 2005).

Druckery, Timothy. "From Dada to Digital: Montage in the Twentieth Century." *Aperture* (Summer 1994): 4–7.

Duranti, Luciana. "The Challenge of Digital Photography & InterPARES 2." In *Il Monde Degli Archivi*, 4–7. Rome: Pompeo Magno, 2002.

———. *Diplomatics: New Uses for an Old Science.* Lanham, MD and London: SAA, ACA, Scarecrow Press, 1998.

———. "Preserving Authentic Electronic Art over the Long-Term: The InterPARES 2 Project." In *Annual Meeting of the American Institute for Conservation of Historic and Artistic Works.* Portland, OR: American Institute of Conservation, 2004.

Duranti, Luciana, ed. *The Long-Term Preservation of Authentic Electronic Records: Findings of the InterPARES Project.* San Miniato, Italy: Archilab, 2005.

Duranti, Luciana, Terry Eastwood, and Heather MacNeil. *Preservation of the Integrity of Electronic Records. Vol. 2, The Archivist's Library.* Dordrecht: Kluwer, 2002.

Electronic Evidence Specialist Advisory Group. "Australasian Guidelines for Digital Imaging Processes, V2." National Institute of Forensic Science (2004), http://www.nifs.com.au/ (accessed June 23, 2005).

Evans, Joanne, and Lori Lindberg. "Describing and Analyzing the Recordkeeping Capabilities of Metadata Sets." Paper presented at DC2004: International Conference on Dublin Core and Metadata Applications, Shanghai, China, October 12, 2004. http://www.siderean.com/dcconf/ (accessed May 15, 2005).

Evening, Martin. *Adobe Photoshop for Photographers CS2.* Burlington, MA: Focal Press, 2005.

Fraser, Bruce. "Understanding Digital RAW Capture." Adobe Systems Inc. White Paper (2004), http://www.adobe.com (accessed May 24, 2005).

Frey, Franziska, and Sabine Süsstrunk. "Digital Photography-How Long Will It Last?" Image and Visual Representation Group (2000), http://ivrgwww.epfl.ch/ (accessed June 20, 2005).

Giannelli, Paul C., Albert J. Weatherhead, III, and Richard W. Weatherhead. "Overview of Evidence Law." In *Understanding Evidence.* Newark, NJ: Matthew Bender & Company, 2003. http://www.lexisnexis.com/lawschool/study/understanding/pdf/EvidCh1.pdf (accessed April 9, 2005).

Gilliland-Swetland, Ann. "Setting the Stage: Defining Metadata." In *Introduction to Metadata: Pathways to Digital Information 2.0,* edited by Murtha Baca. Los Angeles: Getty Information Institute, 2000. http://www.getty.edu./research/conducting_research/standards/intrometadata/2_articles/index.html (accessed June 24, 2005).

Goodman, Nelson. *Languages of Art.* Indianapolis, IN: Bobbs-Merrill, 1968.

Grundberg, Andy. "Photography in the Age of Electronic Simulation." In *Crisis of the Real: Writings on Photography, 1974-1989,* 222–229. New York: Aperture Foundation, 1990.

Habas, Paula J. "The Ethics of Photojournalistic Alteration: An Integrated Schema of Determinants." Master's thesis, University of Windsor, 1996.

Hodges, Keith. "Handling Digital Photographs for Use in Criminal Trials, V1 May 27, 2004." http://www.khodges.com/digitalphoto/ (accessed July 2, 2005).

House of Lords. *Science and Technology Committee - Fifth Report.* London: HMSO, 1998.

Hunter, Gregory, S. *Preserving Digital Information: A How-to-Do-It Manual.* New York: Neal-Schuman Publishers, 2000.

International Imaging Industry Association. "Power of Metadata Is Propelling Digital Imaging Beyond the Limitations of Conventional Photography." DIG 35 White Paper (1999), http://www.i3a.org/i_dig35.html (accessed Janauary 10, 2005).

InterPARES 1. "Project Summary." (2001), http://www.interpares.org/ip1/ip1_index.cfm (accessed March 12, 2005).

InterPARES 2. "Project Summary." (2004), http://www.interpares.org/ip2/ip2_index.cfm (accessed March 12, 2005).

IPTC. "Information Interchange Model." *IPTC* (2005), http://www.iptc.org/IIM/ (accessed March 12, 2005).

———. "*IPTC Core* Schema for XMP, V1.0: Specification." *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005).

IPTC-NAA. *Information Interchange Model, Version No.4.* Windsor, UK: IPTC-NAA, 1999.

Japan Electronics and Information Technology Industries Association. "Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.2." JEITA (2002), http://www.exif.org (accessed June 3, 2005).

Kennedy, Michael. "Legal Issues: General Guidance on Records Authentication and Identification." *Journal of Imaging Services* 16 (2002), http://www.dsasolutions.com/Legal%20Issues.htm (accessed May 20, 2005).

Kozloff, Max. "Critical Reflections - Photographic Criticism." *ArtForum* (April 1997), http://www.findarticles.com/p/articles/mi_m0268/is_n8_v35/ai_19416257 (accessed May 20, 2005).

The Library of Congress. "America from the Great Depression to World War II: Black-and-White Photographs from the FSA-OWI, 1935-1945." *American Memory* (1998), http://memory.loc.gov/ammem/fsahtml/fahome.html (accessed March 12, 2005).

Lister, Martin. "Photography in the Age of Electronic Imaging." In *Photography: A Critical Introduction,* edited by Liz Wells, 249–291. London: Routledge, 1997.

Lubove, Roy. *The Progressives and the Slums: Tenement House Reform in New York City, 1890-1917.* Pittsburgh, PA: University of Pittsburgh Press, 1962.

Manovich, Lev. "The Paradoxes of Digital Photography." In *Photography after Photography: Memory and Representation in the Digital Age,* edited by Amelunxen Hubertus, Stefan Inglhaut and Florian Rotzer, 57–65. Sydney: G+B Arts, 1996.

Martinez, Cristina Sofia. "Art and Law in the Age of Digital Production." *History of Photography* 22 (Spring 1998): 14–17.

McCarvel, Roderick, T. "You Won't Believe Your Eyes: Digital Photography as Legal Evidence." (1995), http://www.seanet.com/~rod/digiphot.html (accessed January 10, 2005).

Milburn, Ken. "The Ideal Digital Photographer's Workflow, Part 1." *O'Reilly Web DevCenter* (2003), http://www.oreillynet.com/pub/a/javascript/2003/12/17/digital_photography.html (accessed June 21, 2005).

———. "The Ideal Digital Photographer's Workflow, Part 3." O'Reilly *Web DevCenter* (2004), http://www.oreillynet.com/pub/a/javascript/2004/02/24/digital_photography.html (accessed June 21, 2005).

Miller, April. "Exhibiting Integrity: Archival Diplomatics to Study Moving Images." Master's thesis, University of British Columbia, 2001.

Mitchell, William J. *The Reconfigured Eye: The Visual Truth in the Post-Photographic Era.* Cambridge: MIT Press, 1994.

National Press Photographers Association. "Digital Manipulation Code of Ethics: NPPA Statement of Principle." *Business Practices,* http://www.nppa.org/professional_development/business_practices/digitalethics.html. \ (accessed March 11, 2005).

———. "Ethics in the Age of Digital Photography: Credibility." *Self-Training Resources,* http://www.nppa.org/professional_development/self-training_resources/eadp_report/credibility.html (accessed March 11, 2005).

O'Donnell, Lorraine. "Towards Total Archives: The Form and Meaning of Photographic Records." *Archivaria* 38 (Fall 1994): 105–118.

Paul, George L. "The 'Authenticity Crisis' in Real Evidence." *The Practical Litigator* (November 2004), http://www.ali-aba.org (accessed April 9, 2005).

Pearce-Moses, Richard. *A Glossary of Archival and Records Terminology.* Chicago, IL: The Society of American Archivists, 2004. http://www.archivists.org/glossary/index.asp (accessed April 7, 2005).

Pedersen, Diana. "The Photographic Record of the Canadian YWCA 1890-1930: A Visual Source for Women's History." *Archivaria* 24 (Summer 1987): 10–35.

"Photographs and Archives." *Archivaria* 5, (Winter 1977–78): 204.

Police Central. "White Paper: Suggested Procedures for Preservation of Digital Crime Scene Photographs." *Cop Tales* (1998), http://www.policecentral.com/wp-crimescene.htm (accessed June 10, 2005).

Pollitt, Mark M. "Report on Digital Evidence." In *13th INTERPOL Forensic Science Symposium*. Lyon, France: INTERPOL, 2001.

The Public Record Office. "Guidelines for Management, Appraisal and Preservation of Electronic Records: Principles." *Electronic Records from Office Systems Programme* (1999), http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm (accessed June 28, 2005).

Reichmann, Michael. "Understanding Bit Depth." *The Luminous Landscape* (2005), http://www.luminous-landscape.com/tutorials/bit-depth.shtml (accessed July 5, 2005).

Reis, George. "Digital Image Integrity: White Paper." Adobe Systems Inc. (2004), http://www.adobe.com/digitalimag/ps_pro_primers.html (accessed June 24, 2005).

———. "Digital Imaging Guidelines." *Imaging Forensics* (2004), http://www.imagingforensics.com (accessed June 23, 2005).

Research Libraries Group. "Automatic Exposure: Capturing Technical Metadata for Digital Still Images." *RLG DigiNews* (2004), http://www.rlg.org/en/page.php?Page_ID=20462#article1 (accessed June 28, 2005).

Riecks, David. "Ch.Ch.Changes (with File Info)." Controlled Vocabulary.com. http://www.controlledvocabulary.com/imagedatabases/iptc_naa.html (accessed June 10, 2005).

———. "Filenaming as a Strategy to Managing Your Assets." Controlled Vocabulary.com (2005), http://www.controlledvocabulary.com/imagedatabases/filenaming.html (accessed June 28, 2005).

———. "IPTC Core Schema for XMP, V1.0: Custom Panels User Guide." *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005).

Sandomirsky, Janice R. "Toronto's Public Health Photography." *Archivaria* 10 (Summer 1980): 145–155.

Schwartz, Joan M. "'Records of Simple Truth and Precision': Photography, Archives and the Illusion of Control." *Archivaria* 50 (Fall 2000): 1–40.

———. "'We Make Our Tools and Our Tools Make Us': Lessons from Photographs for the Practice, Politics, and Poetics of Diplomatics." *Archivaria* 40 (Fall 1995): 40–74.

Scientific Working Group on Imaging Technologies. "Recommendations and Guidelines for the Use of Image Processing in the Criminal Justice System." *Forensic Science Communications* 5 (January 2003), http://www.fbi.gov/hq/lab/fsc/backissu/jan2003/swgitdigital.htm (accessed May 20, 2005).

Scientific Working Group on Imaging Technology. "Draft - Best Practices for Documenting Image Enhancement V1.1." International Association for Investigation (2004), http://www.theiai.org/swgit/ (accessed June 29, 2005).

———. "Guidelines for Field Applications of Imaging Technologies in the Criminal Justice Institute, Version 2.3." International Association for Investigation (2001), http://www.theiai.org/swgit/guidelines/sec3_2_3_2001_12_06.pdf (accessed June 1, 2005).

———."Guidelines for the Use of Imaging Technologies in the Criminal Justice System V2.3." International Association for Identification (2002), http://www.theiai.org/swgit/ (accessed May 28, 2005).

Scientific Working Group on Imaging Technology and Police Scientific Development Branch. "Digital Imaging Procedures V1.0." International Association for Investigation (2002), http://www.theiai.org/swgit/ (accessed June 28, 2005).

Sitts, Maxine, K. *Handbook for Digital Projects: A Management Tool for Preservation and Access*. Andover: Northeast Document Conservation Center, 2000.

Skopik, Stephen. "Digital Photography: Truth, Meaning, Aesthetics." *History of Photography* 27 (Autumn 2003): 264–271.

Skupsky, Donald S. "Legal Standards for Records and Information Management Programs." *ARMA Records Management Quarterly* (July 1994), http://www.findarticles.com/p/articles/mi_qa3691/is_199407/ai_n8716186 (accessed June 10, 2005).

Sontag, Susan. *On Photography*. Toronto: McGraw-Hill Ryerson, 1978.

Southampton Camera Club. http://www.southamptoncameraclub.co.uk/exhibition.htm (accessed May 10, 2005).

Squiers, Carol, ed. *The Critical Image: Essays on Contemporary Photography*. Seattle: Bay Press, 1990.

Staggs, Steven B. "The Admissibility of Digital Photographs in Court." *Crime Scene Investigator* (2001), http://www.crime-scene-investigator.net/admissibilityofdigital.html (accessed June 23, 2005).

Statistics Canada. *Statistics: Power from Data!* http://www.statcan.ca/english/edu/power/toc/contents.htm (accessed March 21, 2005).

Taylor, Phil. *Digital Photographic Imaging Glossary*. Victoria, BC: Trafford Publishing, 2002.

Technical Advisory Service for Images, *File Formats and Compression*, http://www.tasi.ac.uk/advice/creating/fformat.html (accessed June 20, 2005).

———. *Image Management Systems: Available Software.* http://www.tasi.ac.uk/advice/delivering/ims-software.html (accessed July 1, 2005).

———. *Metadata Standards, Schemas and Specifications.* http://www.tasi.ac.uk/advice/delivering/metadata.html (accessed June 20, 2005).

Thompson, Jerry. "Truth and Photography." *Yale Review* 90, no. 1 (January 2002): 25–53.

Thurston, Thomas. "Hearsay of the Sun: Photography, Identity, and the Law of Evidence in Nineteenth-Century American Courts." *American Quarterly Online* (2001), http://chnm.gmu.edu/aq/photos/index.htm (accessed April 9, 2005).

United States Government. *Federal Rules of Evidence*. Washington, DC: US Government Printing Office, January 2, 2001.

Warburton, Nigel. "Authentic Photographs." *The British Journal of Aesthetics* 37, no. 2 (April 1997): 129–138.

Wombell, Paul, ed. *Photovideo: Photography in the Age of the Computer*. London: Rivers Oram Press, 1991.

World Wide Web Consortium. *Resource Description Framework*. http://www.w3.org/RDF/ (accessed January 10, 2005).

APPENDIX A

SURVEY: LIST OF PARTICPATING ORGANIZATIONS

Canadian Association of Photographers and Illustrators in Communications (CAPIC)

Columbia Street Gallery

Editorial Photographers United Kingdom & Ireland (EPUK)

Institute of Medical Illustrators (IMI)

National Press Photographers Association (NPPA)

Professional Government and Military Photographers of Canada

Professional Photographers of Canada (PPOC)

Professionals Using Digital Imaging (ProDIG)

Stock Artists Alliance (SAA)

Toronto Photographers Workshop (TPW)

US National Institute of Justice

APPENDIX B

SURVEY: INFORMED CONSENT INFORMATION LETTER

Informed Consent Information Letter

Survey of Record-Keeping Practices of Photographers using Digital Technology

Funded by a grant from the Social Sciences and Humanities Research Council of Canada (SSHRC)

You are being invited to participate in a brief study of photographers and their use of digital technology, conducted under the auspices of InterPARES 2. You have been asked to participate in this case study because of your experience and knowledge regarding digital photography and the resulting documentation that ensues. InterPARES 2 is an international research project investigating problems surrounding the reliability, permanence, and accessibility of digital records.

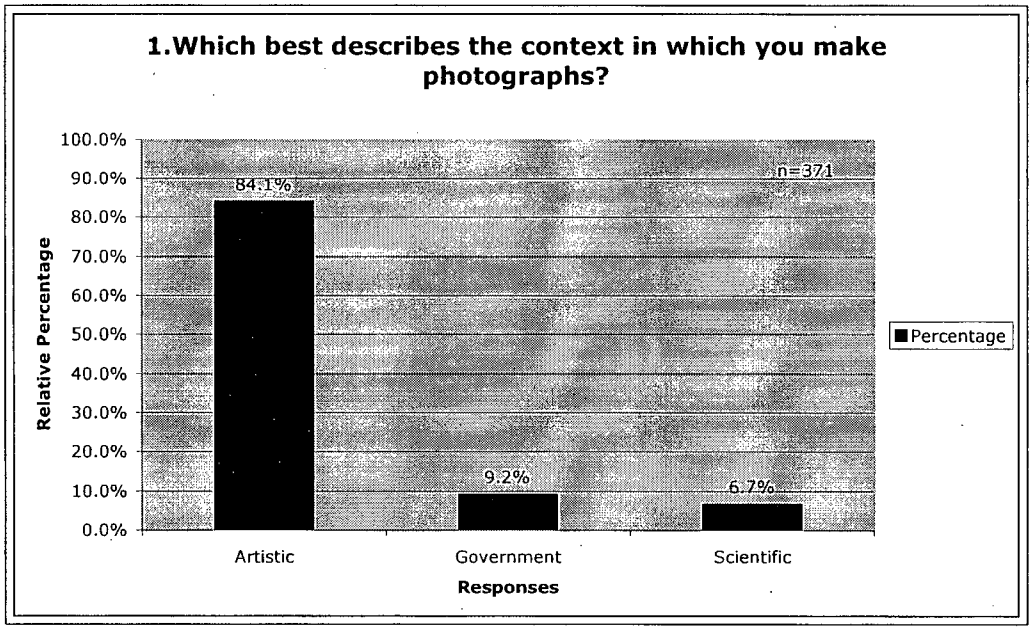
The objective of this particular questionnaire is to obtain some objective data on photographers' use of digital technology. The arts are one of the areas being studied by InterPARES 2 (the others are scientific and government activities) and we are particularly interested in dynamic and experiential documents, that is, documents which may change over time or take on different forms depending on how they are used. One of the longer-term goals of the InterPARES 2 project is to ensure that the records produced will continue to be accessible and reliable in the face of rapid technological change. You are invited to visit the InterPARES 2 website at www.interpares.org/ip2/ip2_index.cfm for more detailed information.

The emailed invitation to participate was sent to a number of photographers whose email is available via their own website or is posted on an affiliated association's website. The managing director of CAPIC gave written consent to post the survey invitation on the weekly online National newsletter.

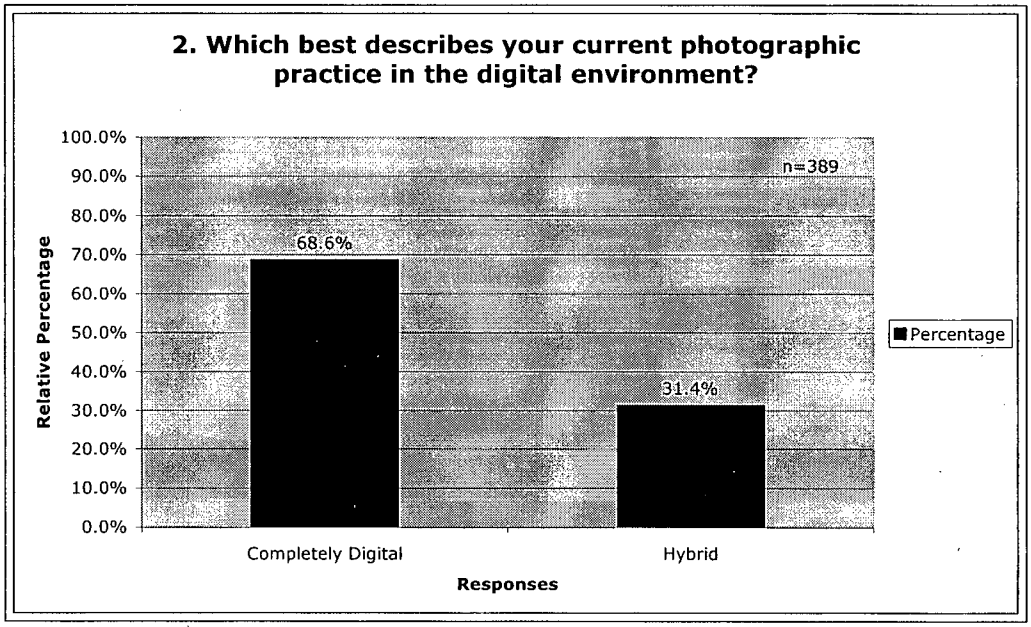
The questionnaire can be completed online in approximately 15-20 minutes. There are no known risks to participants, nor are there any rewards, other than those which may come from looking at one's professional activities in a different light.

APPENDIX C

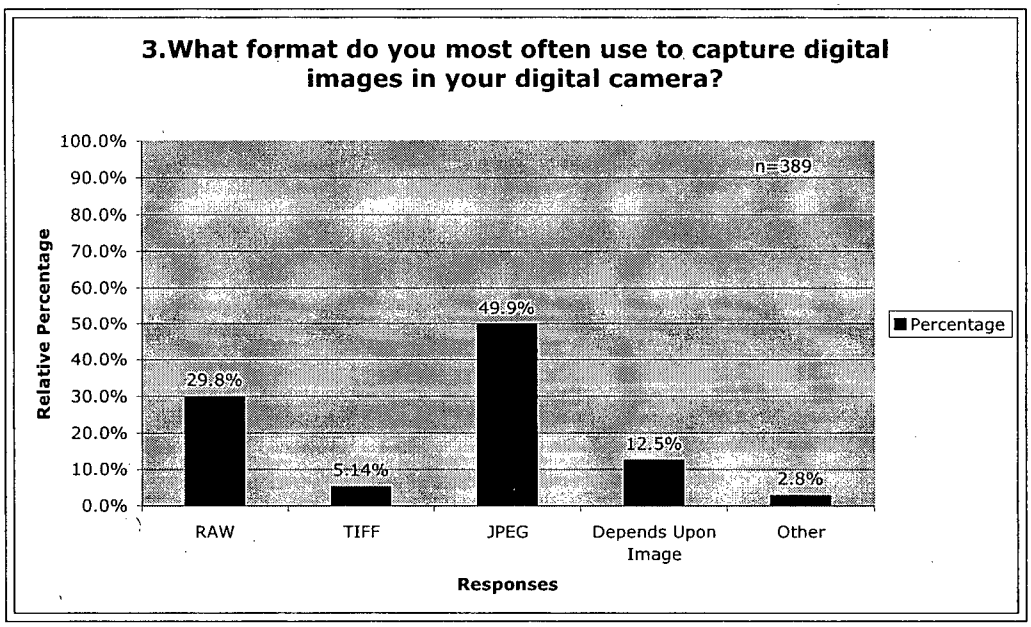
SURVEY: QUESTIONS & CHARTED RESPONSES



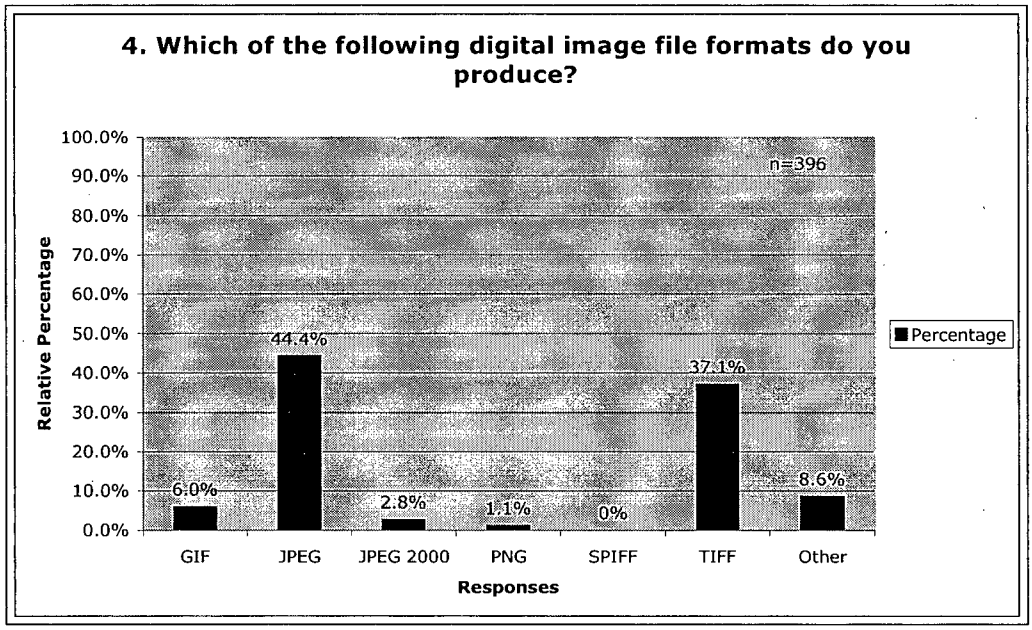
a. Artistic
b. Government
c. Scientific



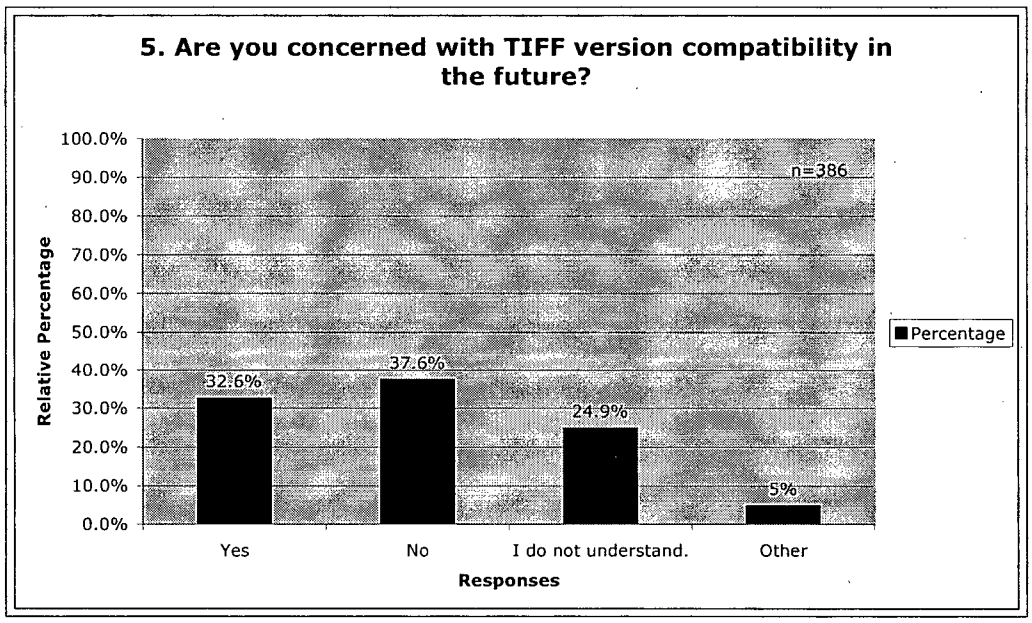
a. Completely digital (i.e., I use a digital camera or digital scanning device, computer program manipulation, digital printing and/or digital display).
b. Hybrid (i.e., I use a mixture of analog and digital technology, such as a film camera image scanned into a computer and manipulated before being printed).



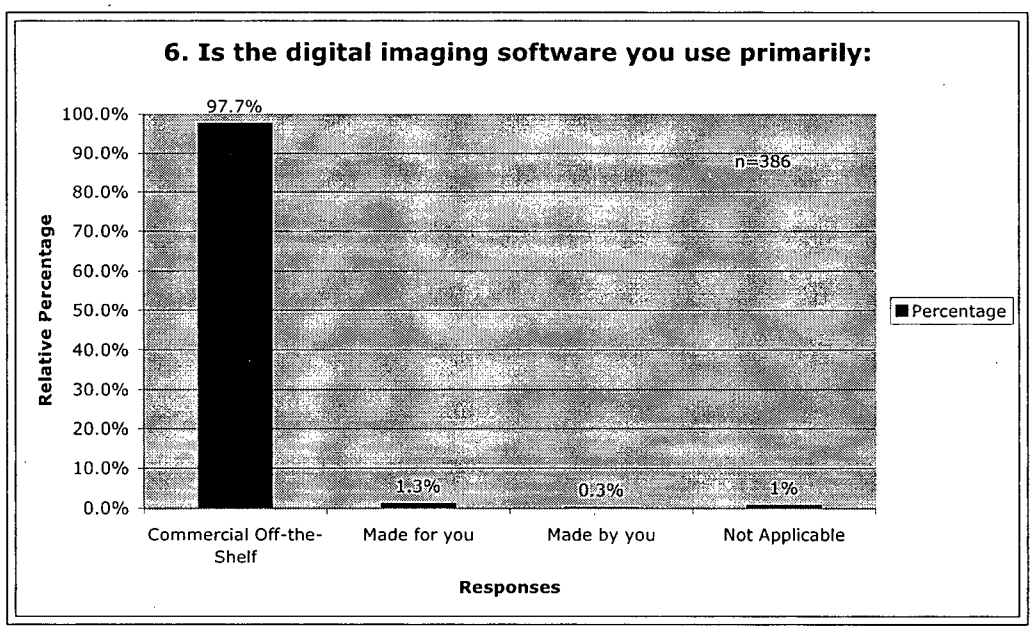
a. RAW
b. TIFF (Tagged Image File Format)
c. JPEG (Joint Photographers Experts Group)
d. Format depends upon image.
e. Other (please explain).



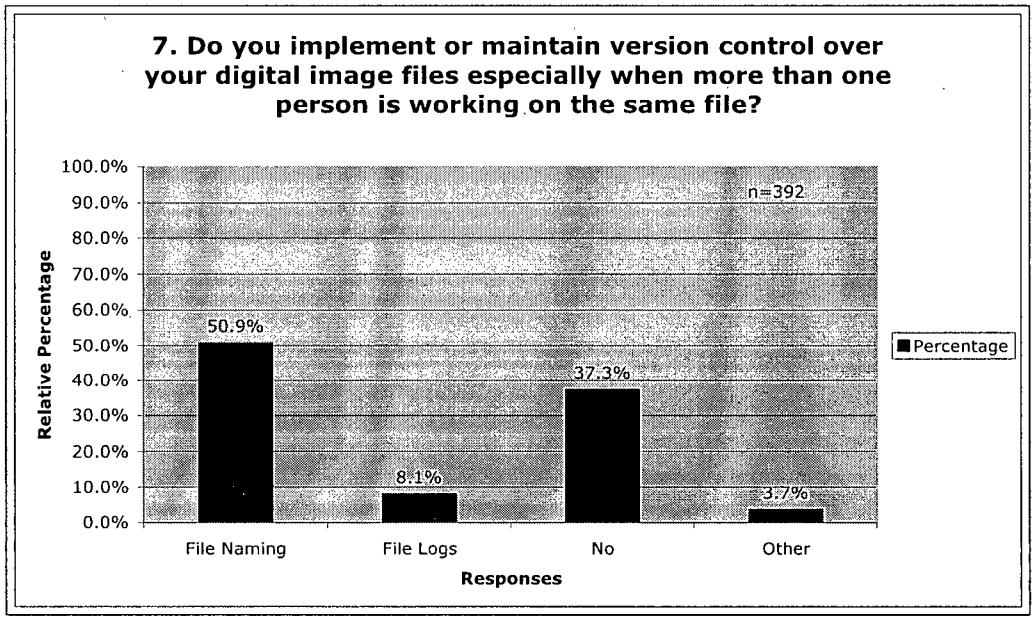
a. GIF (Graphics Interchange Format)
b. JPEG (Joint Photographers Experts Group)
c. JPEG 2000
d. PNG (Portable Network Graphics)
e. SPIFF (Still Picture Interchange File Format)
f. TIFF (Tagged Image File Format)
g. Other (please explain).



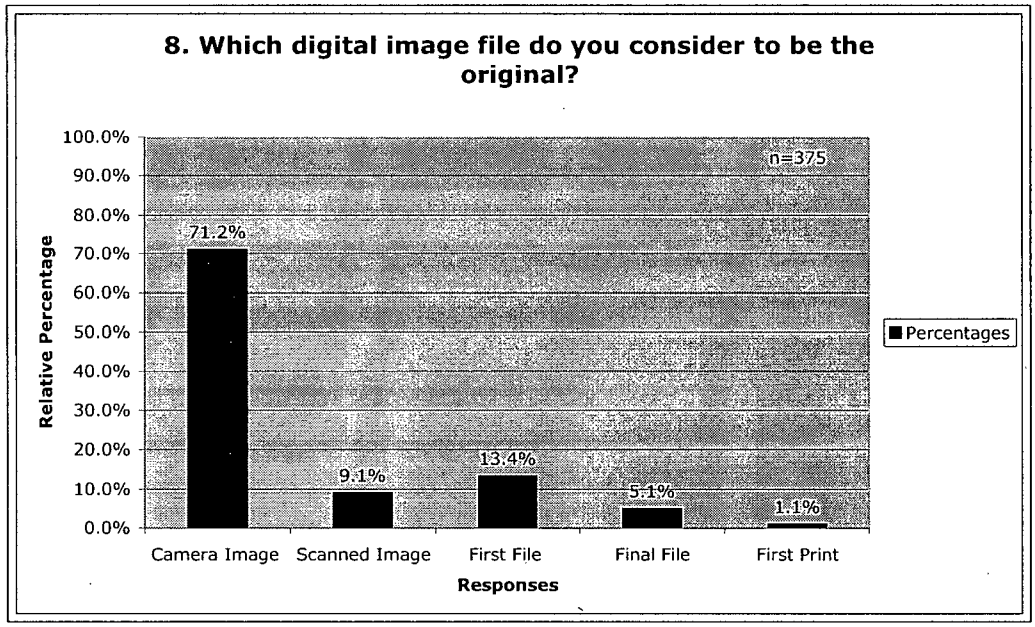
a. Yes
b. No
c. I do not understand the question.
d. Other (please explain).



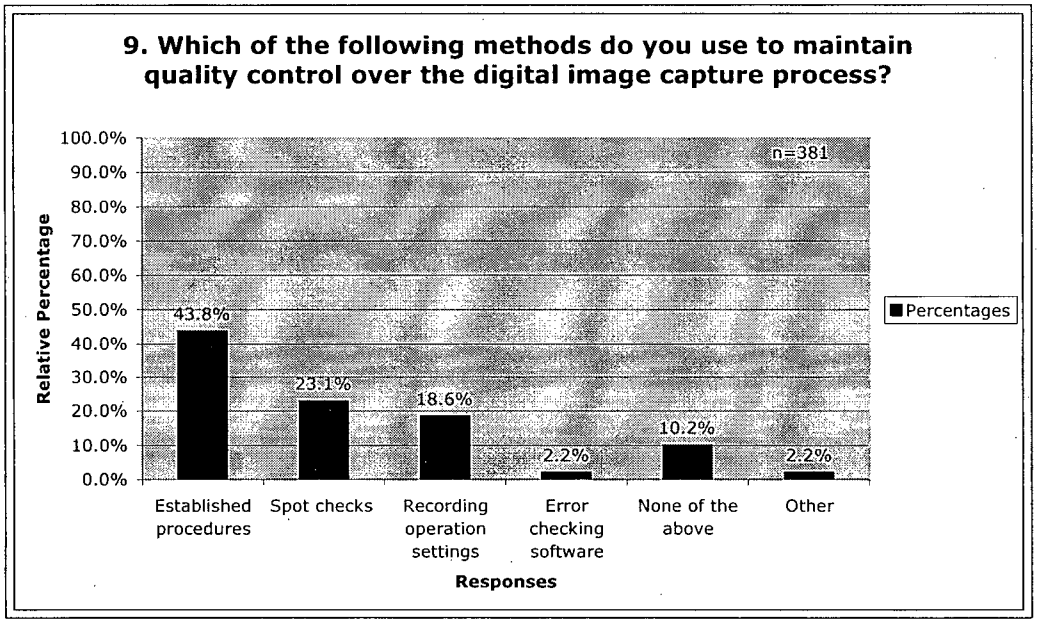
a. Off-the-shelf commercial software.
b. Made for you.
c. Made by you.
d. Not applicable (please explain).



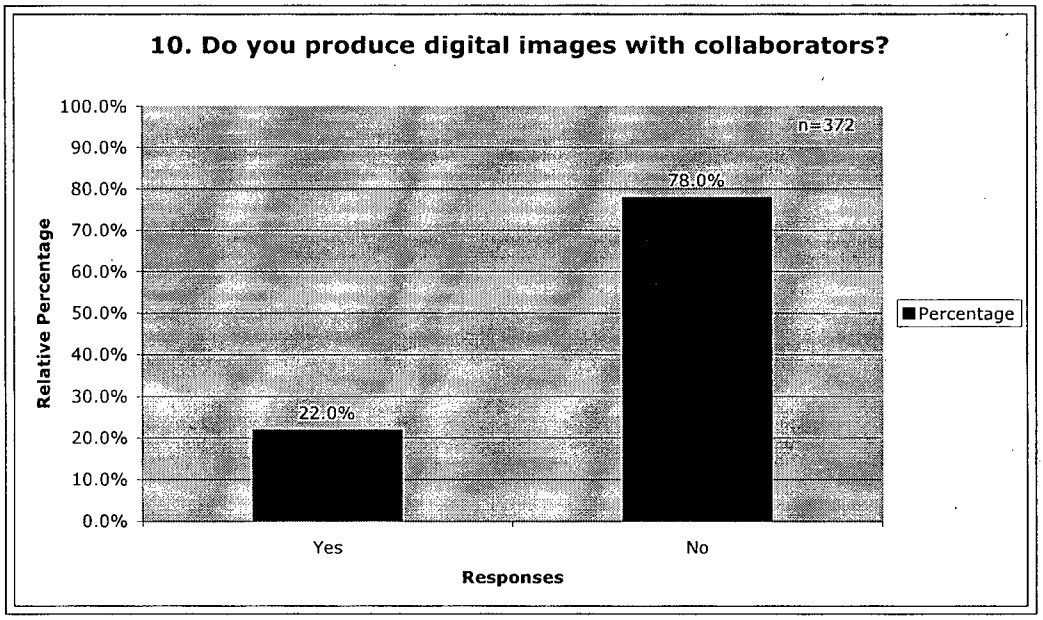
a. Yes, I apply file-naming conventions (e.g., including a version in the file name, such as or imagename.draft.1 or image,name, date, version).
b. Yes, I keep file logs (e.g., a written log, in either a digital format such as an excel spreadsheet or an analog format such as a journal).
c. No, I do not maintain version control.
d. Other (please describe).



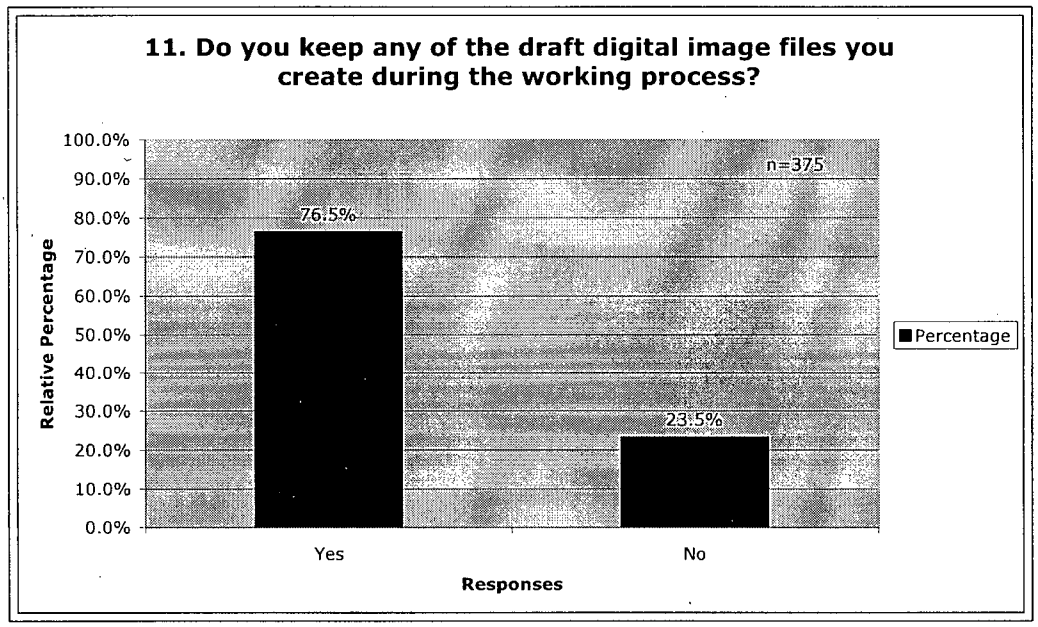
a. The camera image file on the memory card before being downloaded onto a personal computer.
b. The scanned image file before importing into another software program.
c. The first file saved by the software program.
d. The final file saved after completing manipulations and alterations before printing.
e. The first digital print made.



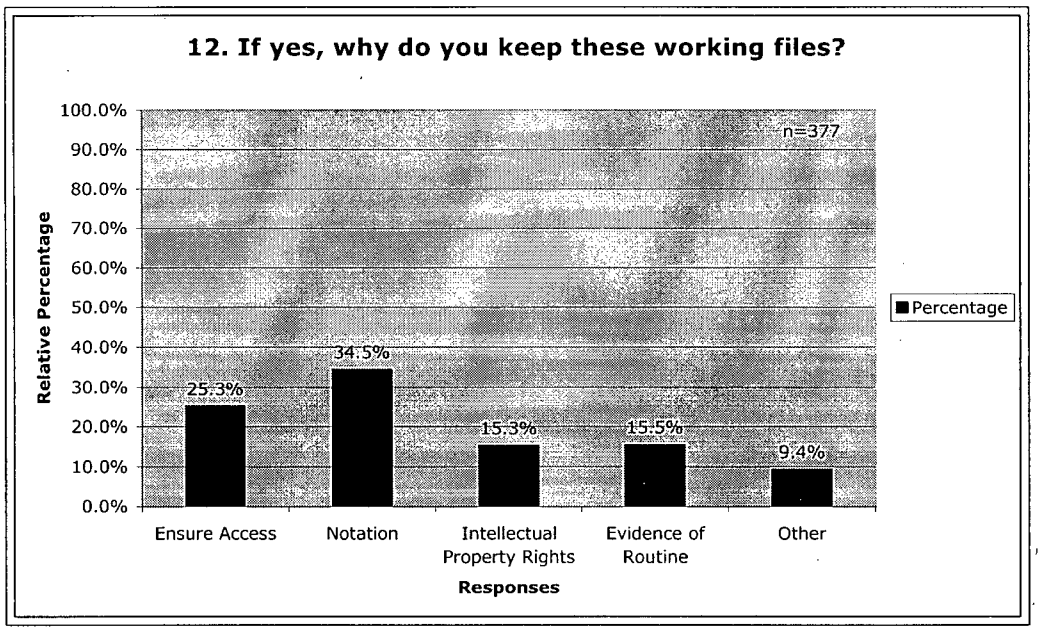
a. Established procedures.
b. Spot checks on digital image files.
c. Recording of operation settings (equipment calibration).
d. Error checking software.
e. None of the above.
f. Other (please explain).



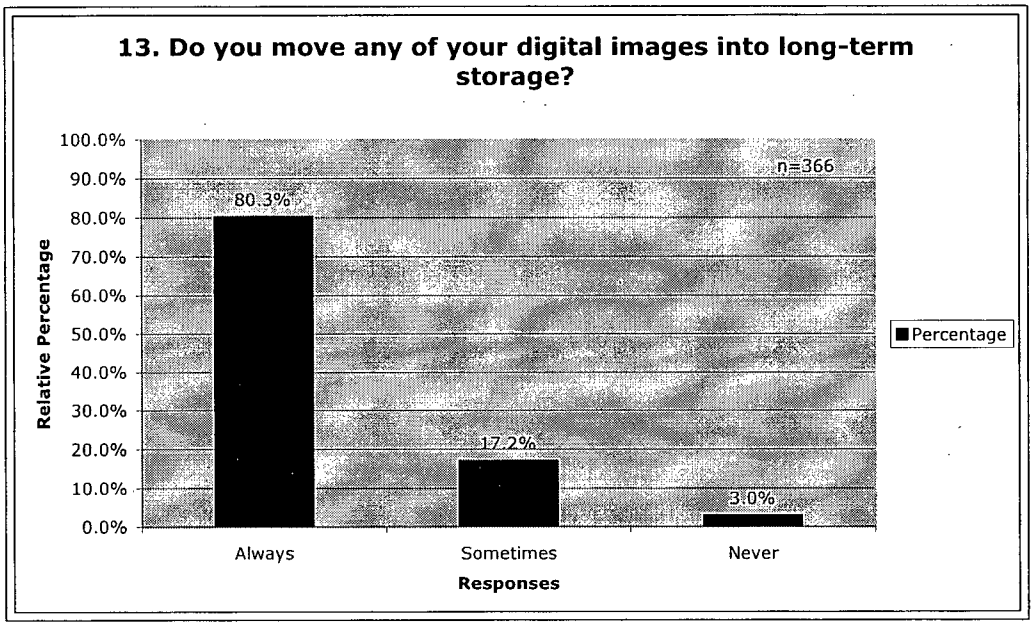
a. Yes
b. No



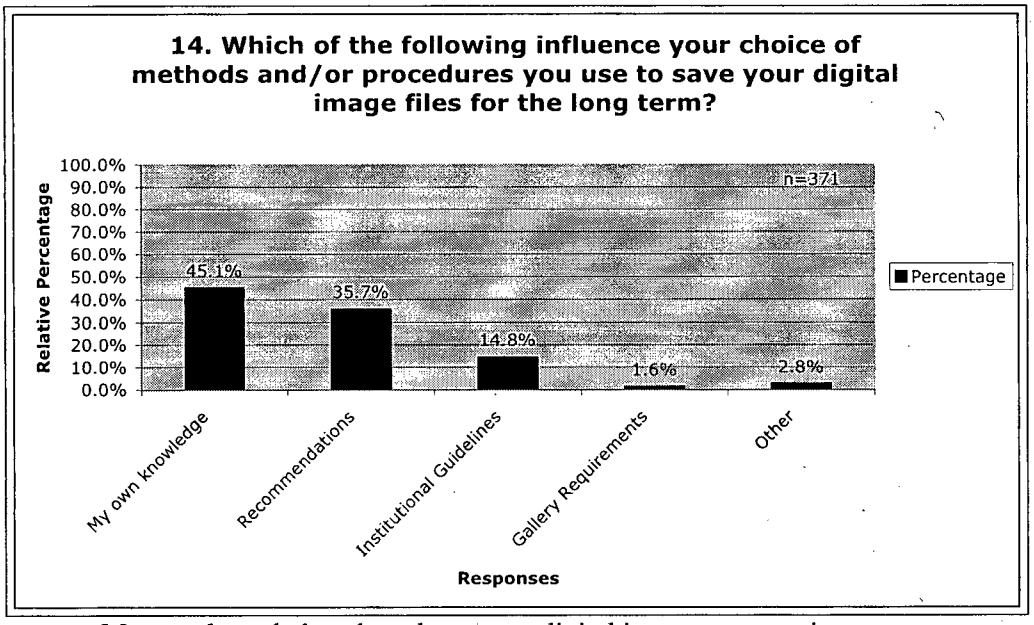
a. Yes
b. No



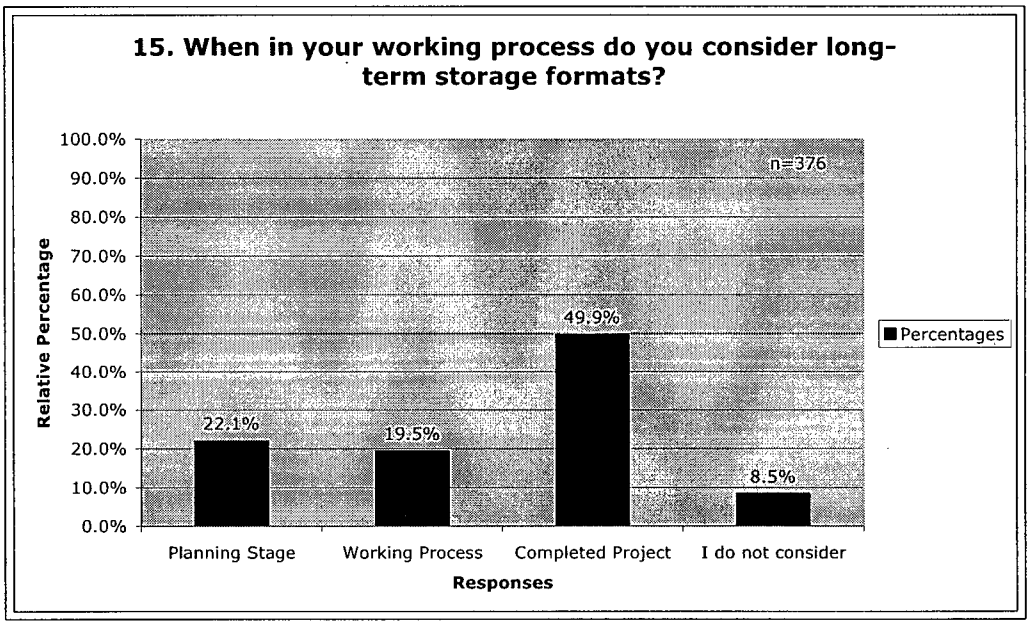
a. To help ensure access, the files can be re-located or re-used by someone else.
b. As a form of notation, to reveal the way in which a digital image was compiled and manipulated at different stages in its creation.
c. To protect intellectual property rights.
d. As evidence of routine work procedures.
e. Other (please explain).



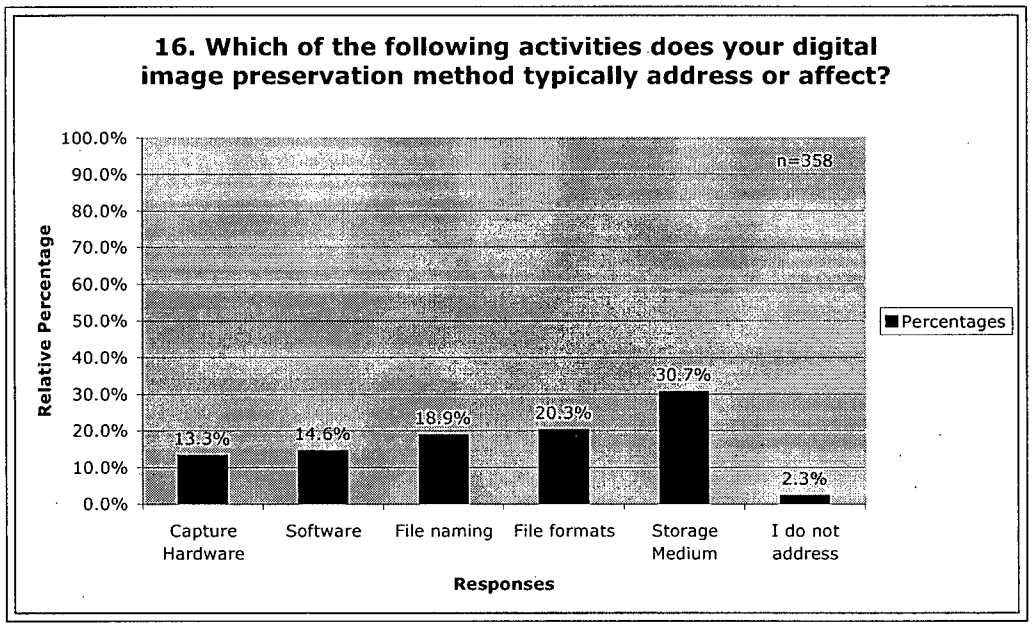
a. Always
b. Sometimes
c. Never



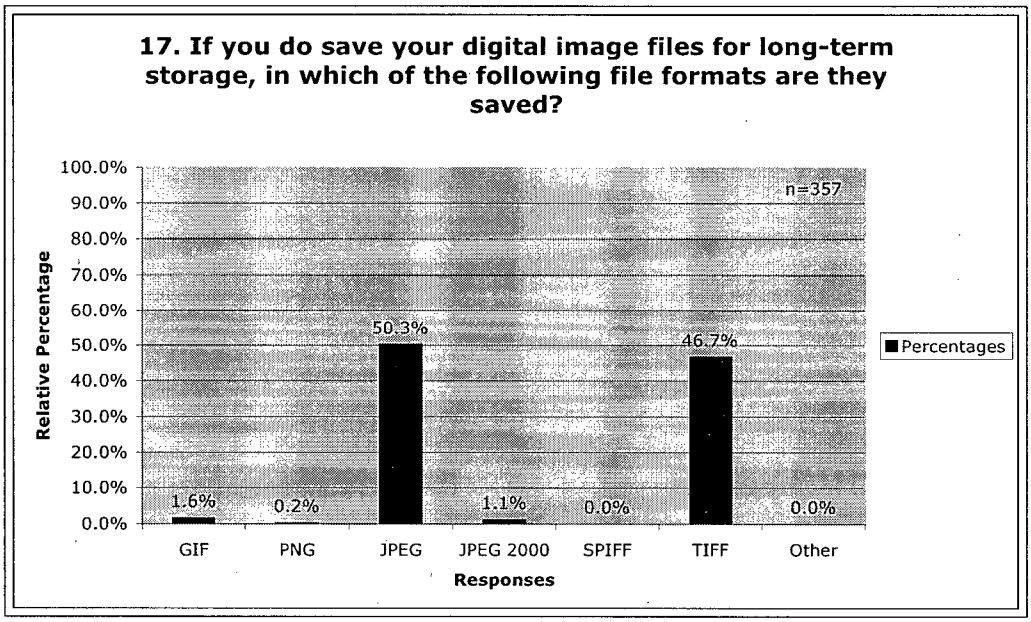
a. My own knowledge about long-term digital image preservation.
b. The recommendations of other colleagues.
c. The preservation guidelines or standards mandated by the institution in which I work.
d. Requirements stated by an art gallery or third party that represents my artistic work.
e. Other (please describe).



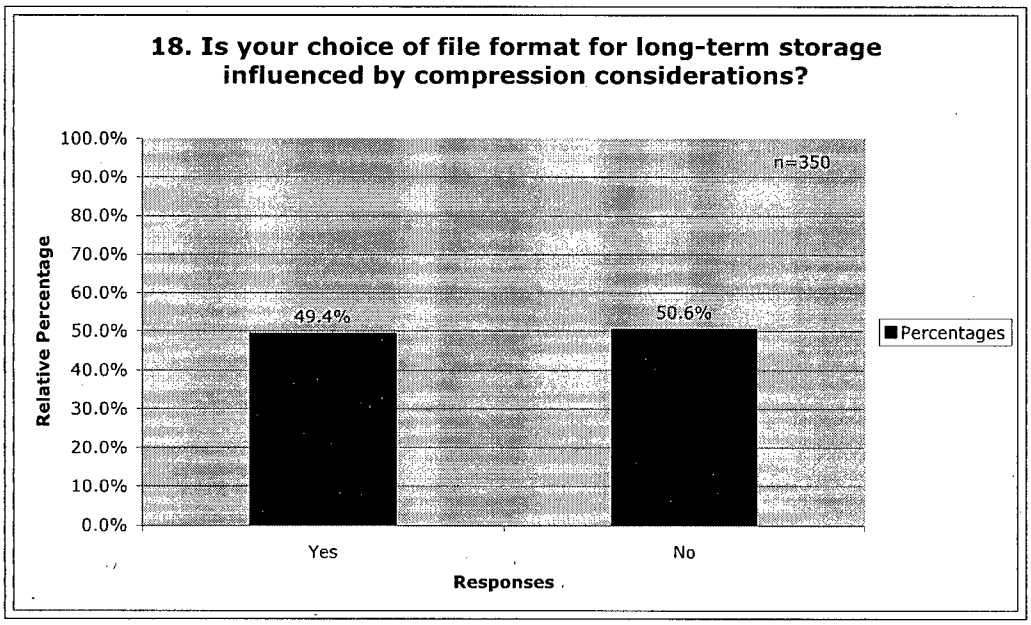
a. At the planning stage of the project.
b. At each stage of the working process.
c. After the project is completed.
d. I do not consider long-term storage formats.



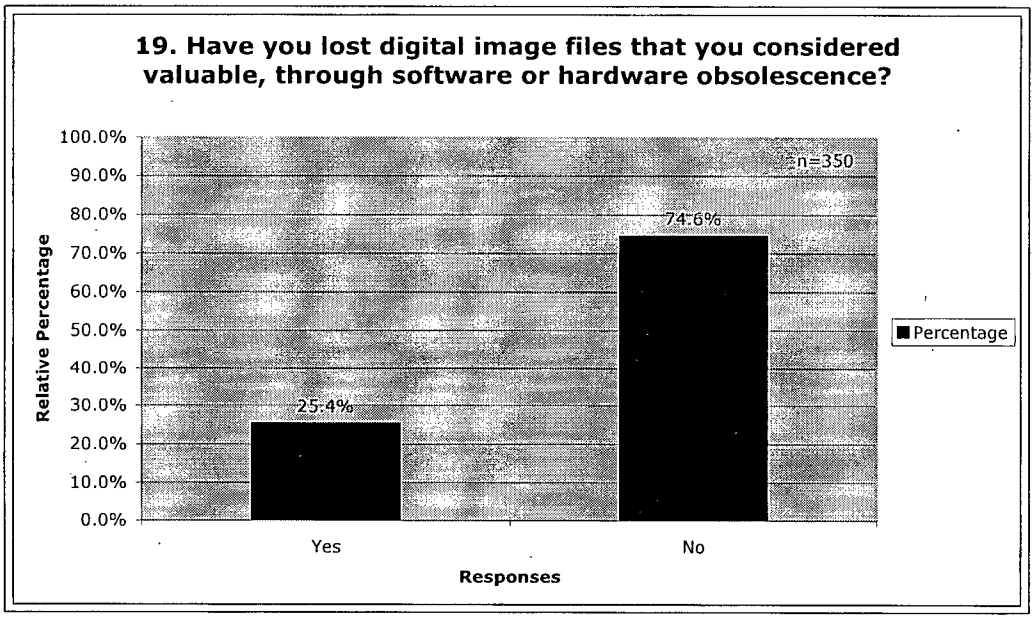
a. Choice of capture hardware (i.e., camera make or type, scanner make or type, computer make or type).
b. Choice of software (i.e., software program attributes).
c. Choice of file naming practices (i.e., naming originals and drafts in a manner that can link them to each other at a later date).
d. Choice of file formats (i.e., choosing the TIFF format for storage).
e. Choice of storage medium (i.e., choosing to store images on external drives, CD, and/or keeping preservation copies in a safe off-site location).
f. I do not address digital image preservation.



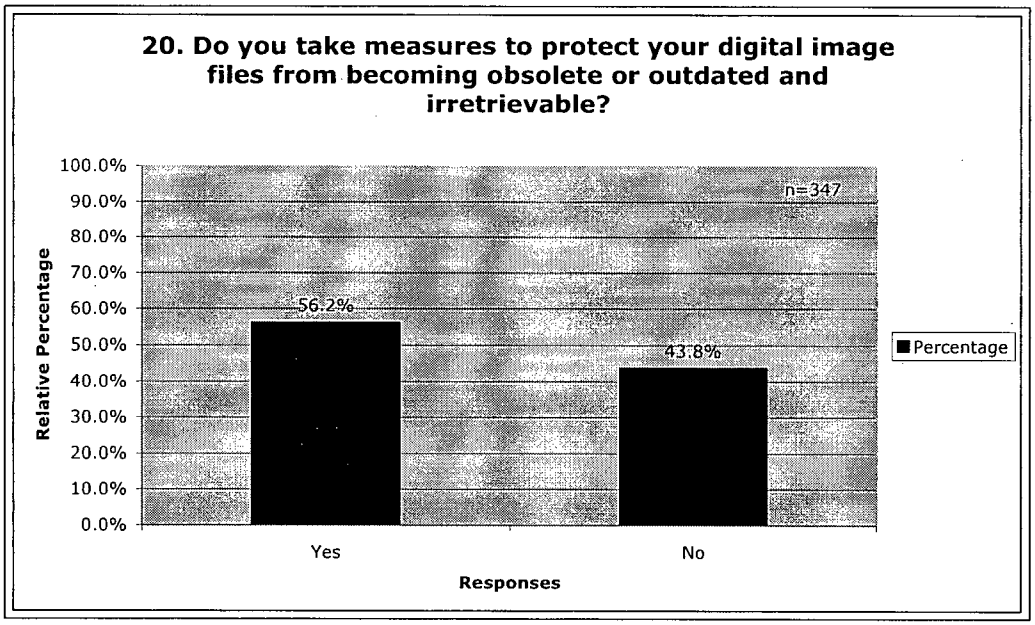
a. GIF (Graphics Interchange Format)
b. PNG (Portable Network Graphics)
c. JPEG (Joint Photographers Experts Group)
d. JPEG 2000
e. SPIFF (Still Picture Interchange File Format)
f. TIFF (Tagged Image File Format)
g. Other (please explain).



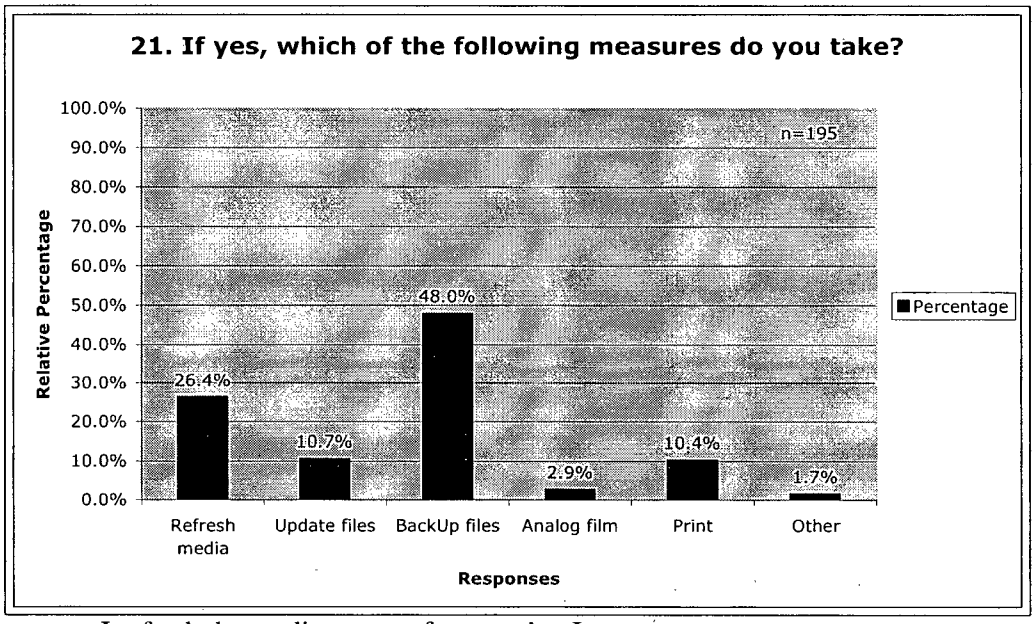
a. Yes
b. No



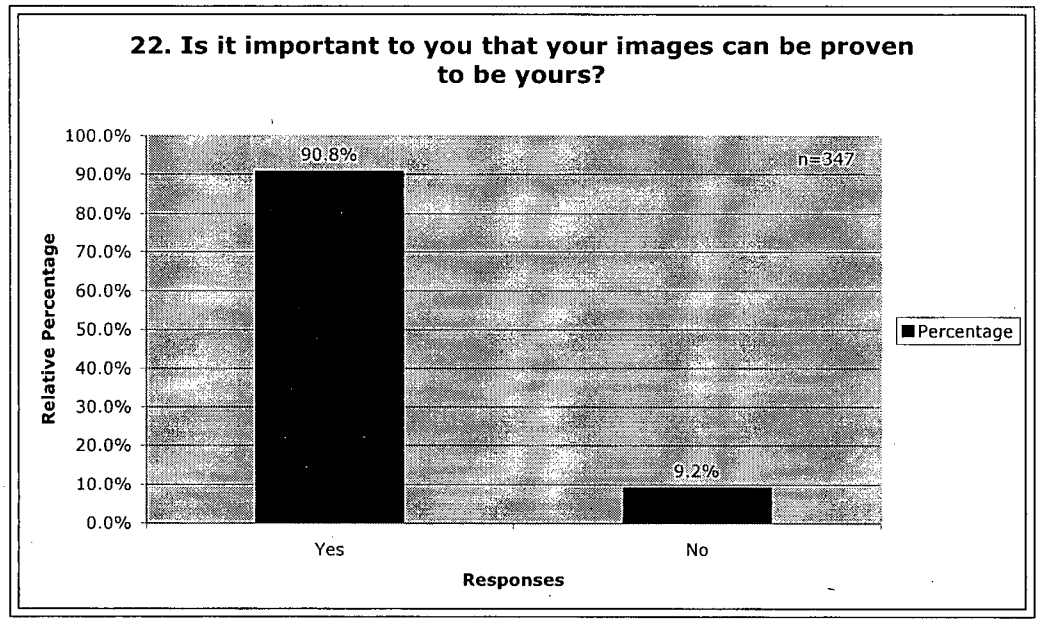
a. Yes
b. No



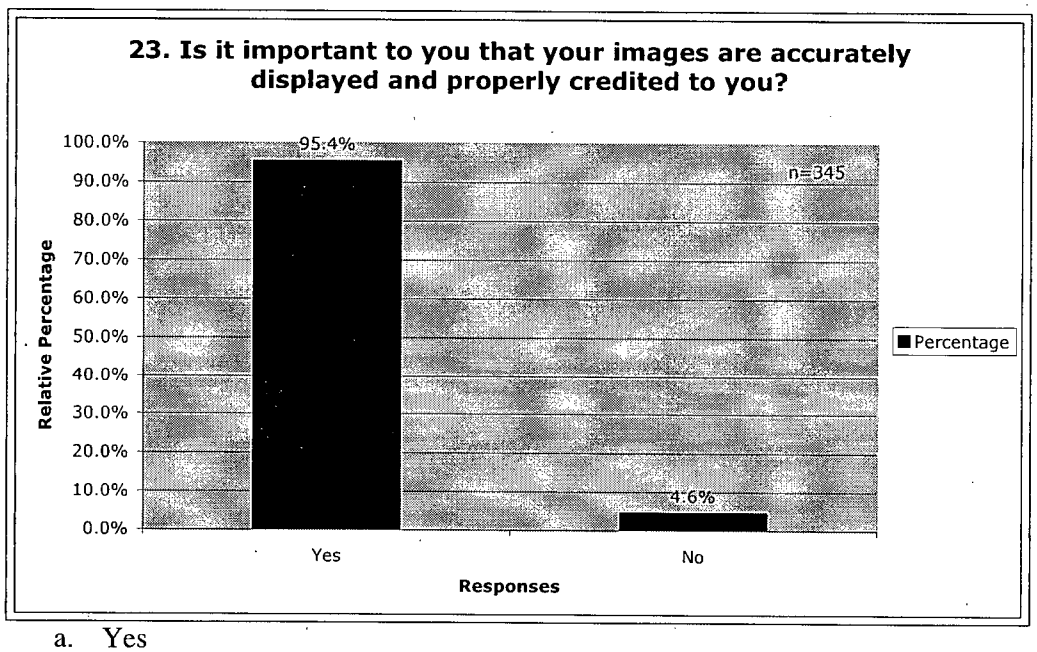
a. Yes
b. No



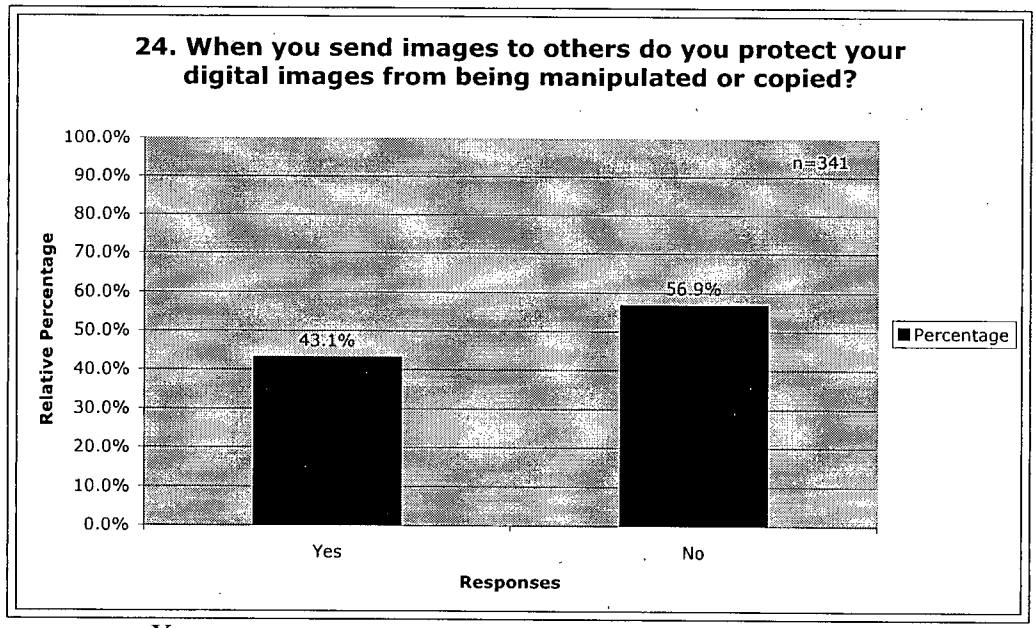
a. I refresh the media storage formats that I use.
b. I update digital image files whenever new software or hardware is implemented.
c. I back up digital image files on another physical medium (i.e., saving files from a drive onto CD).
d. I create analog film versions of the digital image file, such as slides.
e. I print the digital image file.
f. Other (please describe).



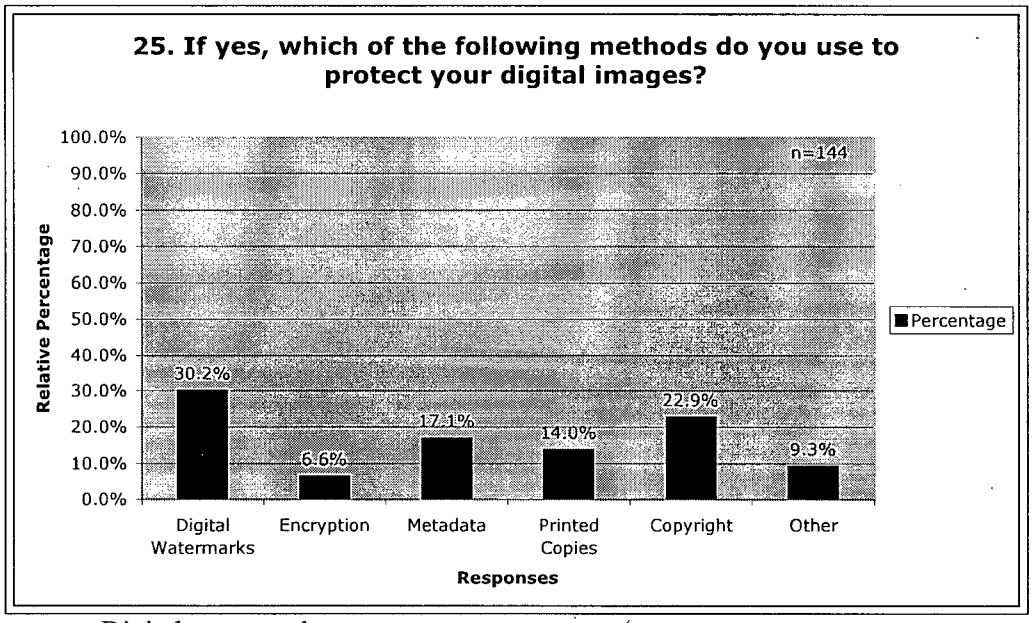
a. Yes
b. No



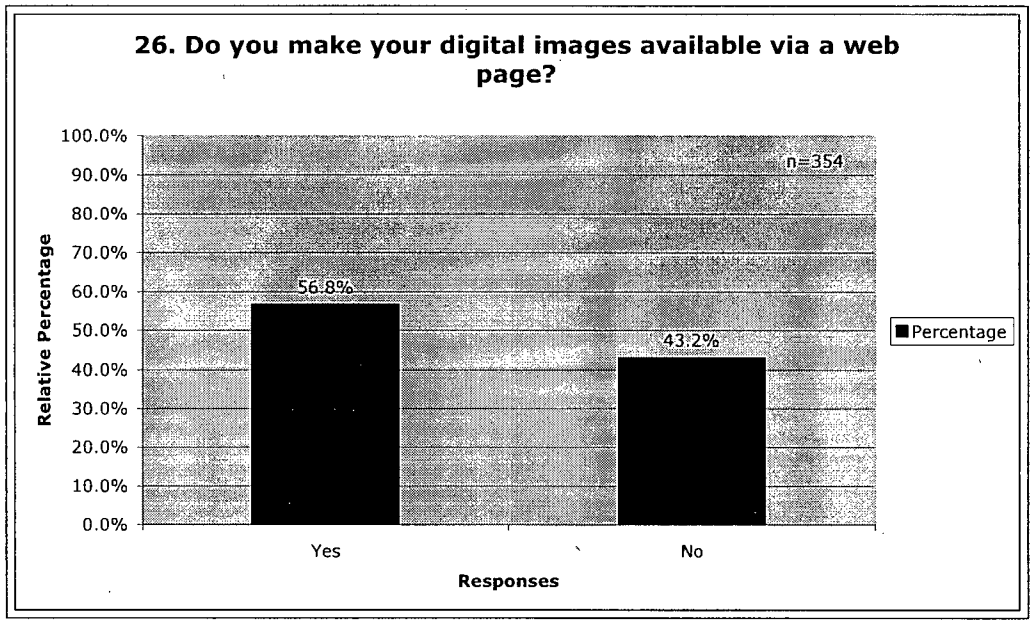
a. Yes
b. No



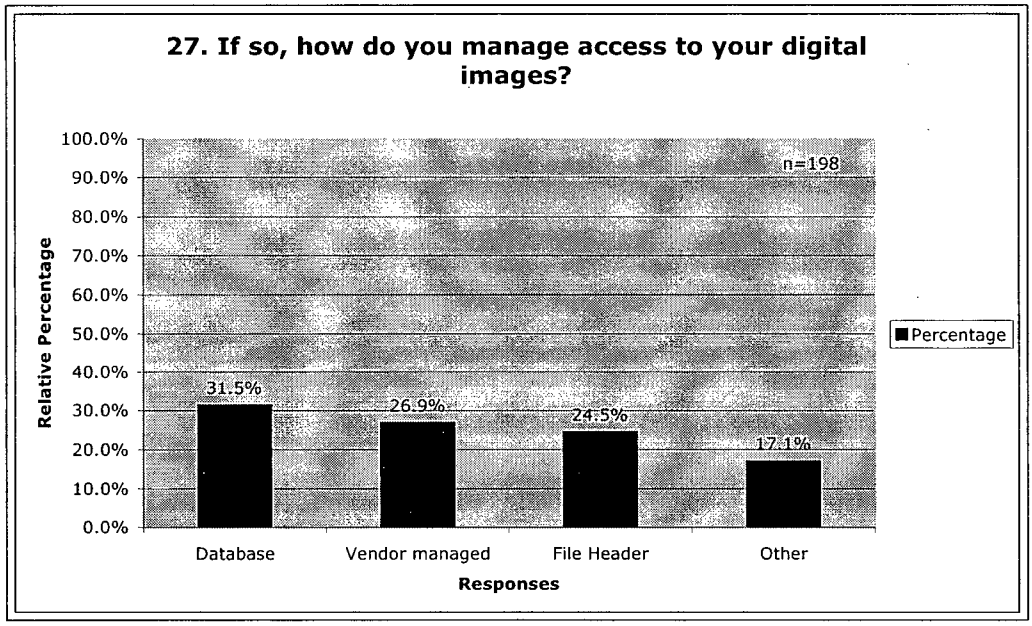
a. Yes
b. No



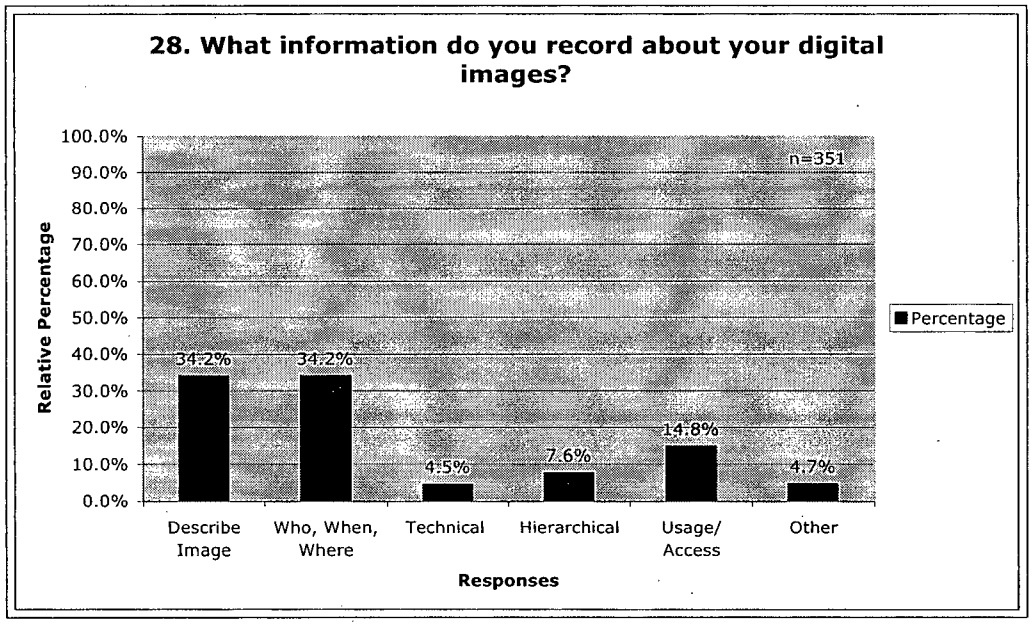
a. Digital watermarks.
b. Encryption (computer algorithms that rearrange the data bits into digital signals in order to prevent reading by unauthorized users).
c. Metadata (structured data about data).
d. Printed copies kept for comparison to digital files.
e. Copyright registration of images.
f. Other (please explain).



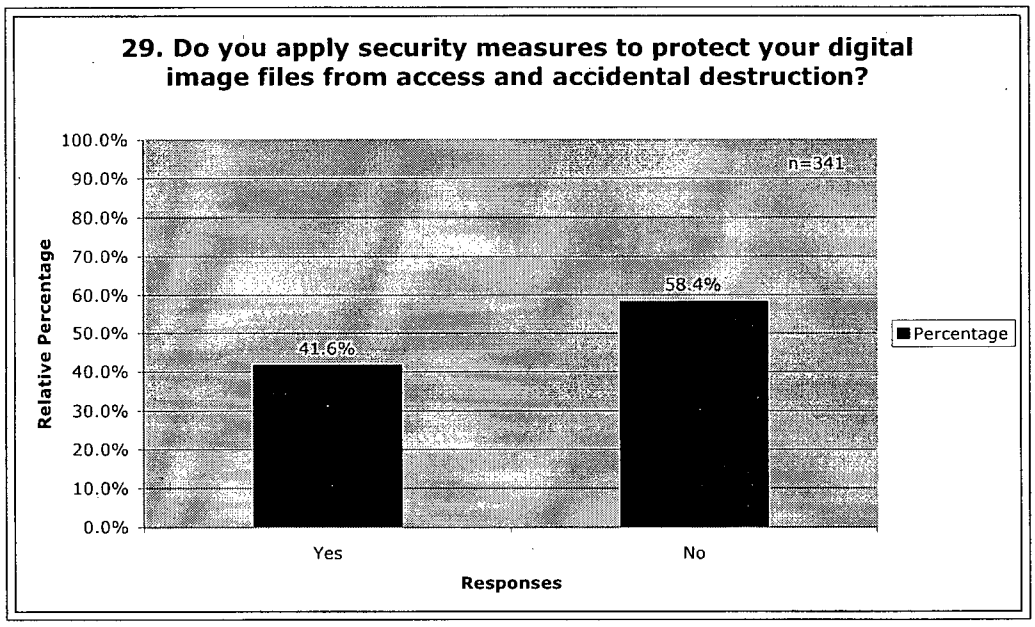
a. Yes
b. No



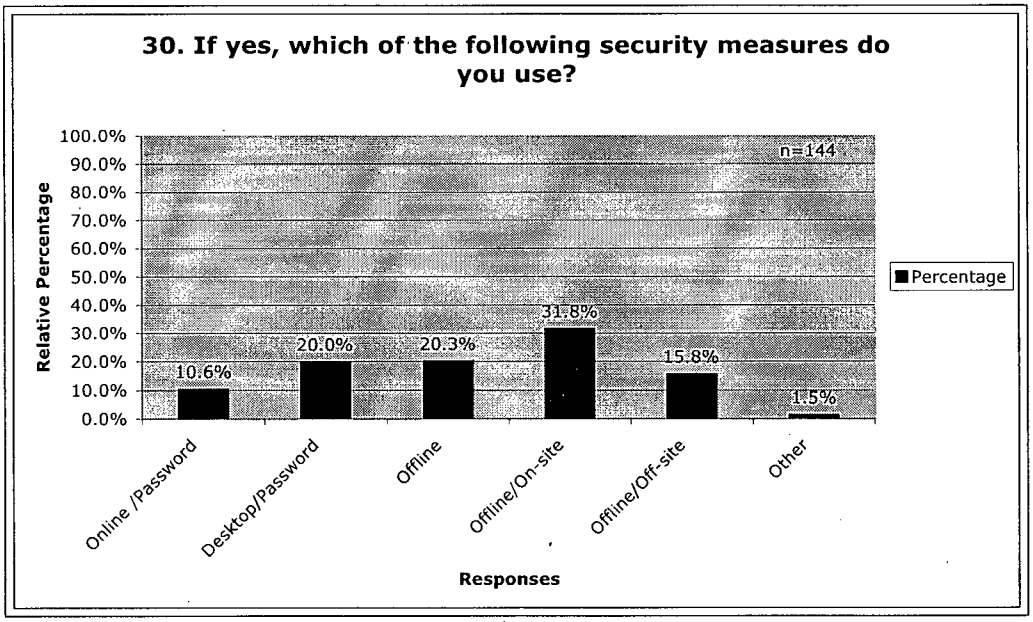
a. I use a database I created to manage all my images.
b. I use a vendor management package that manages access to my images for me.
c. I store information in the header of the digital file itself.
d. Other (please explain).



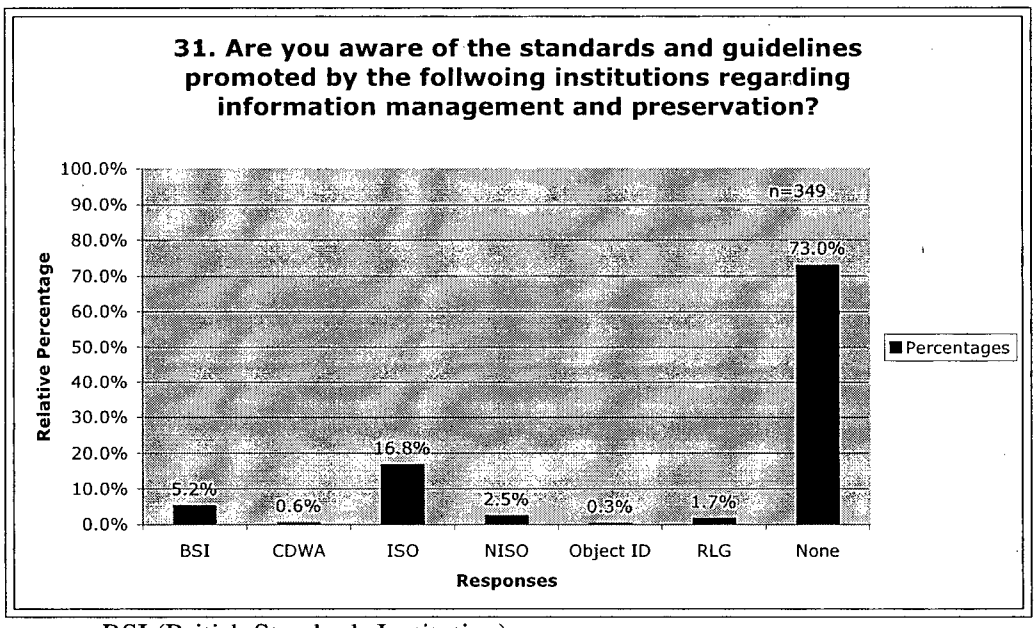
a. Information describing the image itself to allow access and retrieval.
b. Information about who created the images, when and where they were taken, and why.
c. Information about the technical relationships between files, such as software or hardware dependencies.
d. Information about hierarchical relationships, such as an image forming part of a series, or a detail from a larger image.
e. Information about usage restrictions and access.
f. Other (please describe)



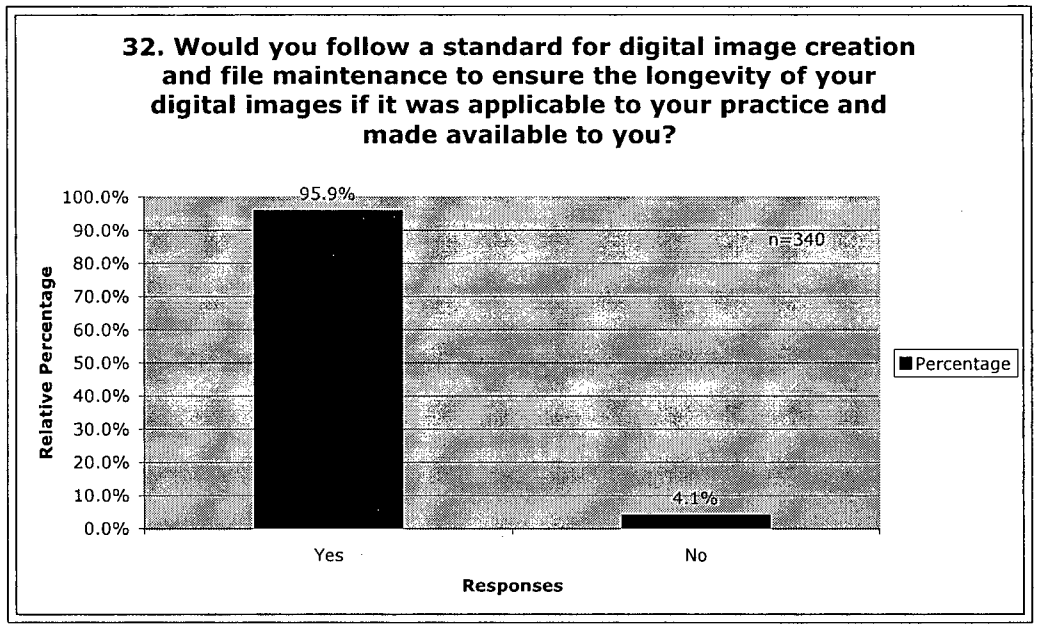
a. Yes
b. No



a. My digital image files are stored online on a network and password protected
b. My digital image files are stored on a personal computer and password protected
c. I have made one or more read-only, offline copies of my digital image files
d. I have stored offline copies of my digital image files in an on-site location
e. I have stored offline copies of my digital image files in an off-site location
f. Other (please explain)



a. BSI (British Standards Institution)
b. CDWA (Categories for the Description of Works of Art)
c. ISO (International Organization for Standardization)
d. NISO (U.S. National Information Standards Organization)
e. Object ID
f. RLG (Research Libraries Group's Preservation Metadata Elements
g. No, I am not aware of any.



a. Yes
b. No

APPENDIX D

SURVEY: SELECTED TEXTUAL RESPONSES

Additional text responses provided by respondents are provided verbatim. The only changes made are to eliminate personal names, email addresses and websites. Where several respondents provided identical answers, these responses have been collapsed and a notation added to indicate how many responses are represented.

Question 1:

1. I'm a photojournalist. (97)
2. Many of my images are scientific in content and artistic in purpose.
3. You forgot commercial style, and editorial style. (14)
4. Also some science.
5. Images of fine art (i.e., paintings, sculptures, art objects), architecture, also medical subjects.
6. In the main I don't consider my work of photographing industrial products to be artistic.
7. Fine Art Photography
8. We also do product photography for other artists and craftspeople.
9. I primarily take photos of or for a client to later paint them in oil paint on canvas. I do not therefore sell photographs per se. I need to catalogue and maintain my photos though.
10. Shoot photos for technical reviews of computer equipment. Published on website.
11. I consider myself a conceptual artist that uses photography among a diverse range of other media in my practice.
12. The categories do not cover my photography field adequately and yet all three cover it in some way. Does that make sense? I am a commercial industrial photographer.
13. Most of what I do I would not classify as Artistic but it is technical, not scientific. Having said that I do Scientific, Artistic and Government work.

14. I'm a newspaper photographer and a Fine Art Photographer.
15. I use digital photography to illustrate books and magazine articles.
16. Commercial photographer specializing in architecture and interiors for commercial clients.
17. Isn't most photography in some way artistic?
18. Commercial, industrial, portrait.
19. Educational.
20. Artistic is the nearest but not a good description of my industrial work.
21. Editorial stock photography
22. Commercial and Wedding/Portrait Photography
23. I work predominately in the documentary as art genre.
24. By the term make you imply create, and as I create an image, no matter what the image, my goal is to create interest through the proper application of artistic techniques. Although I photograph for a city government department.
25. Mostly editorial features based around mountain biking.
26. We are event Photographers and cover all of the above including sport events.
27. I also use photographs for business purposes.
28. For a commercial end use
29. While many photographs I make have an artistic component, the images are made primarily for business reasons: advertising, documentation, etc.
30. I shoot for several small newspapers thus my photos are editorial in nature which can be considered governmental if they are of for example a crime in progress and are subject to court subpoena.
31. I am also involved in documenting current law enforcement trends and actions, which puts me in closer proximity to crime photos.
32. Portrait, Wedding, Events. (3)
33. Weddings, events, and fine art work.
34. Concert and entertainer photography.
35. I am a Corporate Photographer for an engineering firm and do freelance commercial/editorial photography.
36. I am a freelance photojournalist. I do artistic work for exhibits.

37. None of the above really, I create artistically but context is editorial stock.
38. Too narrow a view of who takes photographs.
39. Intelligence and or Evidence.
40. National Health Service Medical Photographer. (9)
41. I am a community college photography and photojournalism professor. I am a former newspaper chief photographer and a former university photographer.
42. Photos are part of the database for the Roman Catholic Archdiocese.
43. The province of Ontario's online digital locations database.
44. Hospital & University
45. Staff appointed University photographer.
46. Central still and digital images storage for the Canadian Forces.
47. Effective, Accurate and Authentic (with reliable and constant means of archiving and retrieval systems) in digital Medical Scientific & Forensic Imaging.
48. Medical Photography, which includes both Clinical (patients and specimens) and non- clinical (PR, Portraiture, Architecture, Reprographics) work.
49. Forensic Science-Government. (5)
50. I use georeferenced digital photos to record excavated surfaces of archaeological deposits.
51. I am the photographer at Queensland Institute of Medical Research. I do all the graphics so a lot of my work is artistic and this is a government organization.
52. Machines take the majority of real scientific pictures.
53. My specialization is astrophotography but I do a considerable amount of work, which can be defined as 'artistic'.
54. Although I work for a government agency, some of the images I take are used for scientific examination.
55. Dental Photography
56. Clients (individuals, companies) commission me to photograph a wide range of subject matter.
57. None of the categories match my photography.

Question 2:

1. But I still produce a few slides.
2. For the last 5 years NO film....
3. Your use of "manipulation" should be thought out better.
4. I may use film for the novelty of it once in a blue moon. I have been trained on both systems, unlike some younger people in the biz, but digital is the fastest and most cost effective.
5. I have aspirations of doing more work with film but my schedule does not really permit it now. I do use film when photographing a wedding but that is infrequent.
6. Went digital in 1999.
7. I still shoot a little bit of film that is eventually scanned, but I am shooting 95% on digital cameras. (6)
8. For work purposes, I use almost entirely digital equipment, from start to finish. I use film for personal photo needs. (6)
9. Additionally I shoot on Medium Format film.
10. The use of manipulation and the term photography should never be used in the same context.
11. I use film very rarely, only when using very long exposures for photos at night when using digital creates too much "noise" on the image.
12. There are still some rare times that I use color negative film or slide film.
13. Changed to a completely digital workflow in July 2004.
14. My work is now about 60% digital and 40% film. I still find there are situations where I have more faith in film.
15. Film is dead for dailies.
16. Some clients prefer film; some are ready for digital.
17. Using mostly digital creation and manipulation with some scanning of older film photographs.
18. I use both digital and film cameras. (6)
19. I am an Irish advertising photographer who is about to make the jump from film to digital workflow.
20. Most new work will be entirely digital format. (5)

21. 95% digital - conventional film used only for specialist retinal photography.
22. At work we are strictly digital, but have film archives over 50 years that are scanned when needed.
23. We also directly capture images using cameras and both film and flatbed scanners. We also work on images sent via email and images from videotape.
24. Film isn't quite dead, though I expect to stop using it for new imaging almost entirely within 5 years.
25. I take pictures on a 4 x 5 camera using 64 Tungsten color film transparencies. I scan them using top quality drum scanners and technicians.
26. But the analogue share is very small, 5-10% at most.
27. Mostly digital but sometimes film and slides depending on the client's needs.
28. I use very little silver based material, small amount of Polaroid and scanning existing 35mm film and prints.

Question 4:

1. I also create files in .swf and .fla formats
2. Other is layered PSD Photoshop native. (44)
3. EPS (Encapsulated Postscript) (8)
4. Photoshop (PSDs) and PDFs (4)
5. Here, our JPEGs are turned into RichTIFFs for use in production. This is an almost archaic format. They are turned into JPEGs for archiving.
6. CPT (Corel Photopaint)
7. All RAW images are migrated to TIFF files for conservation. Some JPEG images are produced for quick viewing and E-Mail purposes.
8. .ai
9. RAW (7)
10. .NEF – Nikon RAW format. (3)
11. I would Use JPEG 2000 if my clients could open it but most couldn't.
12. TIFF - mostly for printing and backup; JPEG - for web.

13. Our current working environment of a four-color newspaper requires the transfer of images to the paginator in EPS format. Primarily, the archived files are JPEG's. We hope to change this system of archival method due to the destructive nature of the JPEG conversion.
14. Video
15. I also make my photos into PSDs in Photoshop if I'm doing any manipulation that requires layering. I'm not sure what a JPEG 2000 is.
16. I never knew what JPEG stood for! Curious!!
17. bmp
18. BTIF, as aforementioned, this is a format that is more flexible than any of the above. It is based on TIFF.
19. Depends on application.
20. Canon Mark II camera now uses RAW images called .CRT files. (3)
21. File format depends on the client's demands.
22. I use PSD files for many of my pre-output images because they are smaller than TIFF files, and I can keep my layers separate.
23. The majority of our imagery is displayed as JPEG's within a HTML context, or is converted to a PDF format for printing purposes.
24. I use TIFFs for my professional use and JPEGs for e-mail purposes.
25. Also use TGA.
26. NEF and CRW
27. JPEG is the most commonly accepted file format for digital photos for both Mac and PC environments.
28. My use of digital is minimal; and I hope to keep it so until 'they' pry my film camera from my cold blue hands.
29. Whatever the client asks for....
30. We have been receiving everything from GIF, DCR, NEFs, PSDs, JPEGs and TIFFs. We convert to either TIFFs for our files and JPEGs for our customers in most cases.

Question 8:

1. This answer is the "theoretically true one"- in practice, since I have such limited appreciation of the in-camera image, I find the first opening of the image on a computer or laptop for preliminary (non-invasive) editing, functionally "my" original.
2. I still consider it to be the "original" after it is downloaded onto a computer.
3. I typically copy my images from the card to the computer and would consider those files to be the originals.
4. I would like to amend that the RAW file is the original regardless of storage media.
5. My answer to this question depends on my method of production, which varies. When shooting with a digital camera, I consider the original file to be the file saved to the camera. When scanning an image, I consider the original to be the first scan I save using Photoshop, after having made any adjustments to the scan immediately necessary.
6. While the camera image file on the memory card is the first instance an original image is saved, it is our practice to download the image in it's native (RAW/ TIFF depending upon the purpose of the image) format save it to the hard drive and burn a CD-R for permanent storage.
7. Or RAW file downloaded from card to computer.
8. I would consider the RAW file the "digital original."
9. There are not enough options for this question, I would classify the original file as the RAW file first saved to the hard drive, as in most cases we are shooting tethered.
10. This question is confusing as you are combining analog and digital formats. If I'm scanning, the original is the piece of film, and the "original" or RAW scan always requires manipulation, and doesn't require storage, as you can always rescan the film. With a digital camera file this is more critical, as there is no film to go back to.
11. I'm answering as if you are talking about "digital capture" only.
12. Question is not clear, as this file is unchanged when it is first saved on the computer from the card. This is the original, also.
13. A digital file straight from the lens to the recording device is just like a negative in my mind.
14. No difference between the file on memory card and once it is downloaded onto the computer.

15. As with analog (film) formats, most believe that the negative/positive is the original work.
16. Always use SAVE AS and leave the original untouched.
17. If the image was captured on film, the digital original is the scan file.
18. But only if true RAW unprocessed data.
19. The original RAW image made and transferred to the PC is our 'original' file and the one we refer to for all uses. You have not allowed for this option so I have checked the above.
20. SWGIT guidelines call for the "original" to be the unaltered image as saved onto digital recordable only media (CD-R for example) directly from the memory card. The image on the memory card is the "primary" if I recall. It also depends on the capture device, but it is always the first created/captured image that is the original. We name this as the Primary Image and it is never worked on. Only a copy of the Primary is worked on.
21. As I am a studio-based photographer, and the image as it is taken on the digital camera in its own software is the original on the hard disc, in the studio I shoot straight to desktop machine.
22. I download RAW files and save them unchanged.
23. Actually, I consider the file original even if I copy it from the memory card to the main picture server, as long as it has not been opened, saved, or worked on.
24. The RAW file and I would include a file converted with the new Adobe DNG file format.
25. I maintain the out of camera files as original to protect my works credibility, and legal status, and as a method of tracing what others do to my work.
26. Post-digitization/pre-manipulation, generally speaking.
27. The originals are: 1) from the digital camera, 2) Or from the film scanner (old analog production) or from the first scan of a print out of the flatbed scanner.
28. We also shoot direct to our file server using fire wire when in the studio. Cards are used on location.
29. There are laws in some parts of North America that state that anything that can be viewed is the original. Therefore, the image on the Compact Flash card, viewed on the camera is the original. Copy it to a computer and email it across the continent and the recipient has the original. If he prints it, that is the original.
30. Or the RAW format file moved from Camera to computer

31. Load RAWs to personal computer, burn 2 disks, and these are originals.
32. As a prior professional photographer, I consider that the Camera file on my PCMCIA Card as the original. Now, I have learnt that imported images that could be manipulated should be considered "originals".
33. In practice, we can only keep the RAW file as the nearest to the in-camera original. This file is the original for me, but if possible, I keep the manipulations reversible by using adjustments and layers in PSD format.
34. Again, this is not something we have as a firm "policy" yet. For a long while, a version that had been manipulated in the software was considered the "master." We have now moved towards keeping an un-manipulated version (after importing into Photoshop though...) as the master, but it's not a written policy yet and there are issues still to explore.
35. The primary image-on the memory card. (2)
36. Re: The first file saved by the software program.
37. This is saving without doing ANY manipulation/touchups/cropping, right?
38. The uncorrected downloaded file corresponds to film negatives following development.
39. The file saved on the software program is identical to the original on the memory card. No alterations are made.
40. Also applied to the original camera file after downloading, but untouched by a software program.
41. I think that the RAW file just after download and before any manipulation is the original.
42. As with so many other analog & film-era absolutes, the lines have become blurred...
43. Always Shoot Tethered and the original is the RAW capture, I also archive the final, which is the finished file.
44. Primary file scanned from negative.
45. The file saved to a WORM disc directly from the camera's memory card before any work is carried out on the image
46. I'm not sure that the question of originality is important in the digital arena, given the nature of the technology. The image is infinitely manipulatible - are all possible states to be considered "originals"?
47. The mini-DV source tape.

48. None of the above - The RAW file (and any Finder copies made of it), when it is first transferred to the computer.
49. The first file copied across from the memory card to the PC before manipulation is the original file.
50. None of your answers. I consider the original as the camera image file or any unprocessed copy of this file, regardless of where it is transferred.
51. The original is the file before any manipulation has been applied. It doesn't matter if it resides on a memory card or in a computer. If nothing has been done to the file, it is the original. I always save all image capture files.

Question 13:

1. CD and DVD. (7)
2. But I am concerned about long-term storage. Will it be like film, were you could go back 20 - 30 years and still pullout a negative? Not likely because the programs that created/saved that image will probably not be around 30 years later.
3. About once every other month.
4. At the end of each week, all original images, as well as, final photos are backed up on to CD and stored.
5. We conserve digital images on Mitsui Gold CDs in 2 copies for the moment. We plan to conserve our digital images on servers in the future.
6. I always store all my digital files [not only image files], to CD and to an external hard drive, as backup. (3)
7. The RAW file is like a digital negative and a backup copy of everything you shoot is important.
8. Original digital images that are received are numbered and filed, once we transfer the TIFF file over to a Gold CD. They are also numbered and remain as the working copy while the original is kept in a temperature/humidity controlled room.
9. Burned to DVD, added to a disk jukebox for archiving.
10. The use of the words "move" and definition of "long-term" are not clear. Long term for us is 25 to 75 years depending on the case.

11. Working photographs and potential file photographs (basically the choice pictures of any shoot) are archived and saved onto servers where a program called MediaGrid is used to search, sort, etc. Then the entire shoot (as well as what is on the servers) is burned to CD.
12. Images are kept on a hospital server. IT department back-up files on a nightly basis.
13. External hard drive and DVD. (2)
14. I archive the edits from each day onto a hard-drive as TIFF's then to an external hard-drive after a few months, when the server clogs up.
15. Originals are all kept in a climate-controlled room.
16. I would like to say always, but we do the best we can with the very large number of images we deal with.
17. Only images that I feel are of value or may be used for stock.
18. I plan to. I have an off-site storage space.
19. A work in progress with technology changing.
20. Good ones that I may want for possible contests, etc.
21. About once every other month.
22. I don't know what is meant by "long term storage".
23. Not yet. Only been 100% digital 2 years, it will take a LONG time to have so many disks they'd need to go to storage!

Question 21:

1. Removable hard drives.
2. I try to save a jpg version of the image if the capture/acquire software changes.
3. Ensure the PSD saved file is saved with all compatibility turned to max.
4. I sometimes create analog versions of a digital file, such as printing to chromogenic photographic paper, but these are not 'archiving' practices: rather, they are in the production of exhibition quality visual art.
5. I try to keep duplicate copies onto CD.
6. Since I use a hybrid model, I consider my original film as my archival file.

7. As I shoot on film, I've always got negative or transparency to fall back on. This has saved my bacon several times this year.
8. I keep an old computer with all the relevant software running. (2)
9. I use one CD for items that need to be retrieved and another I don't use. Eventually, I will make copies of those.
10. We will update as software evolves.
11. Our major digital images are also archived to film.
12. We have used JPEG as a standard since 1993. There have been no damaging changes.
13. I need to do more, and I am looking into all alternatives.
14. To the point of keeping old computers with old programs and all the programs. Such as Windows 95 because some old file formats and programs only run on specific operating systems.
15. By staying aware of changes in software and file formats, I make sure that current technology will always be able to read my old data and file formats. Fortunately, it's all still current technology.
16. I burn a CD.
17. I store images in a dedicated archive.

Question 28:

1. Copyright symbol.
2. Color space/conversion information.
3. client, date, product
4. Information relative to the application.
5. Filename only
6. This information is found in the naming convention for each photo file.
7. Name of the distributor.
8. Any enhancement is described in the note taking with sufficient detail to allow another competently trained individual to carry out the same process.
9. All digital files for clients are backed up on CD. All pictures taken for license as stock are backed up on CD and kept on hard drive for easy access. I create contact

sheets of all the stock files to aid me in finding the images. A number on the contact sheet identifies each picture.

10. Filed using Job numbers/dates and diary entries.
11. Exif is important as well.
12. Not necessarily all of the above or all of the time.
13. My name and contact details (as copyright and personal advertising).
14. Information about what is captured by the image.
15. Caption info, where applicable.
16. At this point I don't use a sophisticated system, but will need to as I increase the percentage of digital work vs. traditional film.
17. Don't know if this applies to me. My images are on other people's (i.e., museum) websites.
18. Date and location. (3)
19. All images recorded in Nikon .NEF format will carry detailed date/exposure information.
20. Level of consent given by the patient is also recorded to prevent misuse of clinical images.
21. All images are stored on CDs and DVDs under client name in Storex plastic A4 sheets containing 4 CDs in ring binder folders. No information, apart from automatic information, is applied to my shot work. I'm hoping to be able to teach myself how to insert meta-data soon.
22. Notes describing processes applied (i.e.: values used when adjusting levels).
23. I do not require these things- any info I may want is embedded in the RAW image and can be accessed with various software.
24. I label the disk or client envelope with date etc.
25. Because of limited office software, images carry very little information.
26. Name of photographer, a one-word description and the last time the image was saved.
27. Technical relationships... is a good idea. But don't do it.
28. You've missed something out here - information about ownership. I leave no doubt that I am the owner of the intellectual property in my pictures.

29. The Five Ws in the caption, the name of the photographer, File number, image number and on which CD it is being kept!
30. I don't keep records about my digital images. (2)

Question 32:

1. Our current data should be able to port to any future standard.
2. I create my own standards and they are usually higher than others.
3. Probably not
4. Please see the DOG standard.
5. Only if it fitted in with my present practices.
6. Its reliability will have to be scientifically proven.
7. Probably. (2)
8. If it worked with my present workflow. (3)
9. As long as it's written in plain, simple English and does not occupy more than 1 A4 side of 12 point type!! There are not enough hours in the day already!
10. Freely and easily.
11. We have recommended guidelines from the Scientific Working Group for Imaging Technologies (SWGIT), which are most applicable to our profession.
12. ASCLD/LAB has recently recognized digital evidence as a credible discipline. It has looked to SWGIT and SWGDE (Scientific Working Group for Digital Evidence), for direction as not all issues in the sub-disciplines has been completely resolved to the community's satisfaction.
13. I would consider it, depending on the price and other measures. (3)
14. I would like to receive any information you have on this subject.
15. Only if it were made universally written and encoded/adaptable on every major computer platform, and had been examined for two years at least by leading industry developers.
16. PLEASE! Let me know what is the best scientific method to archive my digital images. (2)
17. YES, but only as one of several methods, and it would have to be affordable.

18. If this standard will not change the original format and if the PRESS around the world will accept it.
19. It would be against my will to use a format that was impractical or not easily integrated with older forms of archived storage.
20. I think new types of files will be created by Canon, Nikon etc. in the future and I assume that you mean not setting a standard file type for a camera to capture, but for saving after editing.
21. It would depend on cost and file compatibility and ease of use and so on. (3)

Table 1. Exif Schema - Attribute Information [212]

TAG NAME	FIELD NAME	SUPPORT
A. Tags Relating to Version	Exif Version	Mandatory
	Supporting FlashPix Version	Mandatory
B. Tag Relating to Image Data Characteristic	Color Space	Mandatory
C. Tag Relating to Image Configuration	Meaning of Each Component	Mandatory
	Image Compression Mode	Mandatory
	Valid Image Width	Mandatory
	Valid Image Height	Mandatory
D. Tags Relating to User Information	Manufacturer Notes	Recommend
	User Comments	Recommend
E. Tags Relating to Date and Time	Date & Time of Original Data Generation	Optional
	Date & Time of Digital Data Generation	Optional
	Date & Time Subseconds	Optional
	Date & Time Subseconds Original Data	Optional
	Date & Time Subseconds Digitized Data	Optional
F. Tags Relating to Picture Taking Condition	Exposure Program	Recommend
	Exposure Time	Recommend
	Flash	Recommend
	White Balance	Recommend
	Scene Capture Type	Recommend
	ISO Speed Ratings	Optional
	Shutter Speed Value	Optional
	Aperture Value	Optional
	Brightness Value	Optional
	Subject Distance	Optional
	Subject Location	Optional
	Metering Mode	Optional
	Lightsource	Optional
	Subject Area	Optional
	Focal Length	Optional
	Color Filter Array Pattern	Optional
	Spectral Sensitivity	Optional
	Digital Zoom Ratio	Optional
	Contrast	Optional
	Saturation	Optional
	Sharpness	Optional
G. Other Tags	Unique Image ID	Optional
	Copyright Information	Optional
H. GPS Tags		Optional

212. See Japan Electronics and Information Technology Industries Association, "Exchangeable Image File Format for Digital Still Cameras: Exif Version 2.2," JEITA (2002) http://www.exif.org (accessed June 3, 2005).30,31, 60-63.

Table 2. IPTC Core XMP Schema[213]

IPTC Custom Panel Name	Property Name
Contact Panel	Creator/ Author Creator Job Title Creator Contact Address Creator Contact City Creator Contact State-Province Creator Contact Postal Code Creator Contact Country Creator Contact Phone Creator Contact Email Creator Contact Website
Content Panel	Headline Caption/ Description Keywords IPTC Subject Code Caption/ Description Writer
Image Panel	Date Created Intellectual Genre IPTC Scene Location City State-Province Country ISO Country Code
Status Panel	Title Job Identifier Instructions Provider/ Credit Source Copyright Notice Rights Usage

213. See IPTC, "'IPTC Core' Schema for XMP, V1.0: Specification," *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005); David Riecks, "IPTC Core Schema for XMP, V1.0: Custom Panels User Guide," *IPTC Standards* (2005), http://www.iptc.org (accessed April 28, 2005).