Report and Recommendations of the Arizona Task Force on Court Management of Digital Evidence

October 1, 2017

Table of Contents

Arizona Task Force on Court Management of Digital Evidence

MEMBERS

Honorable Samuel A. Thumma, Chair
Chief Judge, Arizona Court of Appeals, Division One

Mike Baumstark
Deputy Administrative Director
Administrative Office of the Courts

David Bodney
Partner, Ballard Spahr LLP

Honorable Kyle Bryson
Presiding Judge
Superior Court in Pima County

Colleen Clase
Senior Counsel
Arizona Voice for Crime Victims

Jessica Cortes
Court Administrator
City of Flagstaff Municipal Court

Honorable David Cunanan
Superior Court in Maricopa County

Karen Emerson
Deputy Public Defender
Maricopa Office of the Public Defender

Honorable Maria Felix
Justice of the Peace
Pima County Consolidated Court

Jeff Fine
Court Administrator
Maricopa County Justice Courts

Jennifer Garcia
Assistant Federal Defender
Federal Public Defender

Honorable Charles Gurtler
Presiding Judge
Mohave County Superior Court

Aaron Harder
Bureau Chief - Vehicular Crimes
Maricopa County Attorney's Office

Honorable Michael Jeanes
Clerk of the Court
Superior Court in Maricopa County

Laura Keller
Electronic Records Archivist
Arizona State Library, Archives, and Public Records

Michael Kurtenbach
Executive Assistant Chief
Community Services Division
City of Phoenix Police Department

William Long
Organized Crime/Intelligence Bureau
Commander
Arizona Department of Public Safety

Zora Manjencich
Assistant Division Chief, Criminal
Office of the Attorney General

James Melendres
Partner, Snell & Wilmer LLP

Michael Mitchell
Special Assistant to the Chief Deputy
Maricopa County Attorney's Office

Jamie Sheppard
Senior Project Manager
E-Discovery Services & Strategy
Perkins Coie LLP

Honorable Don Taylor
Chief Presiding Judge
City of Phoenix Municipal Court

AOC Staff

Theresa Barrett
Manager, Court Programs Unit
Court Services Division

Jennifer Albright
Senior Court Policy Analyst
Court Services Division

Kay Radwanski
Senior Court Policy Analyst
Court Services Division

Sabrina Nash
Court Programs Specialist
Court Services Division

Additional Resources

Jennifer Thorson
Law Clerk
Superior Court in Pima County

Report and Recommendations of the Arizona Task Force on Court Management of Digital Evidence

October 1, 2017

EXECUTIVE SUMMARY

Creation and Charge of the Task Force

Arizona Supreme Court Chief Justice Scott Bales issued Administrative Order No. 2016-129, establishing the Arizona Task Force on Court Management of Digital Evidence, on December 6, 2016. The administrative order is the result, in no small part, of the recent exponential growth of digital evidence used in court, from devices such as smart-device cameras, body-worn cameras, and other public and private surveillance equipment. The administrative order created the task force to address the unique challenges faced by courts in receiving, retrieving, accessing, formatting, converting, and retaining digital evidence.

The administrative order cites to the *Joint Technology Committee Resource Bulletin: Managing Digital Evidence in the Courts* as providing "a good framework for discussion and relevant policy development." The bulletin is a February 2016 publication of the Joint Technology Committee established by the Conference of State Court Administrators, the National Association for Court Management, and the National Center for State Courts. The administrative order established the task force to review and make recommendations on five policy questions posed in the bulletin:

> *"Court management systems are not currently designed to manage large quantities of digital evidence, which means that courts and industry must find creative ways to deal immediately with the dramatically increasing volume of digital evidence, while planning for and developing new capabilities."*
>
> Joint Technology Committee Resource Bulletin: Managing Digital Evidence in the Courts at 1.

- Should standardized acceptable formats, viewing, storage, preservation, and conversion formats or technical protocols for digital evidence be adopted for all courts?
- Should court digital evidence be stored locally, offsite, or using cloud services and how long and in what manner should such evidence be retained?
- Should management of court digital evidence be centralized or decentralized considering technology costs, expertise, and infrastructure necessary to manage it?
- Should court rules governing public records be revised to address access and privacy concerns, including for victims, non-victim witnesses, and other identifying information often included in video evidence?
- Should new or amended rules on chain of custody evidence be developed for handling court digital evidence?

The administrative order further directed the task force to review the Bulletin for additional information on these and other policy issues, as well as any other relevant journals, publications, and other research related to the topic, and make recommendations as deemed appropriate. The administrative order directed the task force to submit this report and recommendations to the Arizona Judicial Council (AJC) by October 1, 2017, and to file any rule change petition not later than January 10, 2018, with respect to any proposed rule changes.

Overview of this Report

This report begins with a summary of the membership of the task force, the processes used to develop the recommendations, and a summary of the recommendations themselves. The report then discusses court management of digital evidence, starting with a background discussion providing context for the issues explored. This background is followed by a discussion of the evolving court record format and the truly digital evidence concept. The report then provides a summary of each task force meeting, with additional detail available on the task force's website. Detailed workgroup reports providing the core foundation for the recommendations round out the body of the report. The report includes appendices containing reference documents and recommended rule changes.

The Task Force and the Task Force Process

Members of the task force were selected, quite intentionally, to represent a wide variety of different perspectives in dealing with court management of digital evidence. Members include rural and urban superior court and city court judges; a justice of the peace; lawyers in private practice; a county prosecutor; an assistant Arizona Attorney

General; state and federal criminal defense attorneys; a victims rights advocate; an electronic discovery expert; representatives of the Arizona Department of Public Safety and the City of Phoenix Police Department; the Maricopa County Clerk of Court; rural and urban justice and municipal court administrators; an electronic records archivist from the Arizona State Library, Archives and Public Records, as well as experts from the Arizona Administrative Office of the Courts (AOC). The intention was to make sure the task force included all perspectives in its work while keeping the number of members manageable. The task force also undertook various outreach efforts and solicited and encouraged input from the public in general and a variety of stakeholders interested in the effort.

Starting in January 2017, the task force met approximately monthly, learning about and discussing various issues and technology related to digital evidence formats, storage, and management, considering the approaches to use and recommendations to make, and then preparing and refining this report. The task force heard from speakers, both nationally and locally, in the private and public sectors, and within and outside of the courts, addressing various topics relevant to the effort. These discussions were interactive and included demonstrations of past, current, and emerging technology.

Early in the effort, the task force formed three workgroups: (1) digital formats, (2) storage and management, and (3) court rules. Each task force member was affiliated with one workgroup. In between task force meetings, task force members met with their workgroups to investigate, develop, and refine recommendations addressing these key components of the task force's work. Task force meetings included presentations by the workgroups, along with questions from and feedback by all task force members about the efforts of the individual workgroups. This facilitated input from different perspectives, avoided communication gaps, accounted for overlap among workgroups, ensured the workgroups were not working in isolation, and recognized that members of one workgroup may have substantial interest in and knowledge that would help the efforts of another workgroup.

Summary of Task Force Recommendations and Ongoing Efforts

Through the work of the members, including its workgroups, the task force developed a strong consensus on the following recommendations for court management of digital evidence, in response to the policy questions posed in the administrative order, addressing: (1) digital formats, (2) storage and management, and (3) court rules.

1. A standardized set of formats and technical protocols should be identified, adopted, and set forth in the relevant sections of the Arizona Code of Judicial Administration (ACJA) for all courts for the submission, viewing, storage, and archival preservation of digital evidence. Standardization requirements should account for five interdependent principles: (1) efficient handling of digital evidence at all phases—from submission of the evidence to the court through viewing, storage, and archival preservation; (2) rapidly changing technologies; (3) flexibility to account for technology in a specific case to ensure the just resolution of the case; (4) maintaining the integrity of the evidence; and (5) reasonable access to the parties and the public.

2. An amendment should be made to the ACJA requiring digital evidence to be submitted in a standard format, unless a court makes a specific finding that the admission of evidence in a non-standardized format is necessary in the interests of justice. The recommended exception should include a requirement that the party submitting digital evidence in a non-standardized format provide technology to allow the evidence to be played or otherwise used in court. Training for judicial officers is also recommended to assist the court in determining whether non-standardized formats are necessary.

3. Deciding whether digital evidence should be stored locally, off-site, using cloud services, or some combination or alternative, as well as whether storage and management should be centralized or decentralized, should be guided by a set of minimum technical requirements. Local courts should include specific considerations in their decision-making, including the capacity to afford and maintain the necessary technology, availability of adequate bandwidth, storage capacity expansion, and integration capabilities with other existing or future software applications.

4. Courts should take measures to enhance the use and presentation of digital evidence in the courtroom, including the use of technology to accept digital evidence in the courtroom, how parties can submit and present digital evidence from personal devices (including necessary conversion and redaction), and staff training for the acquisition, storage, and management of digital evidence. These measures should include guidance for self-represented litigants.

5. The Arizona Administrative Office of the Courts (AOC) should develop best practices as well as policies and procedures to increase the success of digital evidence management solutions adopted. The AOC should also work with local courts on developing a means to offset the costs associated with technology needs created by the increased receipt and storage of digital evidence.

6. Arizona Supreme Court Rules 122 and 123 govern public access to court records. The rights and privacy of victims and non-victim witnesses can be at opposition with the right of the public to access evidence admitted into the court record. Rule 123 should be amended to ensure that it addresses digital evidence, including exhibits, and that the portions of the rule that govern public access, particularly remote electronic access, be amended to ensure sufficient protection of victims' rights and privacy concerns. The Arizona Supreme Court should work with local courts, prosecuting and defending agencies, law enforcement groups, media organizations, and other interested individuals and organizations to develop consistent policies around the issue of non-victim witnesses. In addition, consideration should be given to management of digital evidence introduced by self-represented litigants that may not be redacted to protect victim and non-victim witness privacy rights upon submission to the court.

7. Amendments should be made to the Arizona Rules of Evidence to expressly address digital evidence, including adding a definition of "video" to Rule 1001 and adding references to "video" in Rules 1002, 1004, 1007, and 1008.

8. Amendments should be made to the Arizona Rules of Criminal Procedure, the Arizona Rules of Family Law Procedure, the Arizona Rules of Protective Order Procedure, the Arizona Juvenile Court Rules, and the Arizona Rules for Eviction Actions to modernize the rules to include references to digital evidence and electronically stored information, as has already occurred in other rule sets such as the Arizona Rules of Civil Procedure.

9. A standard definition of digital evidence should be added to the various procedural rule sets where not otherwise included. The recommended

definition is "Digital evidence, also known as electronic evidence, is any information created, stored, or transmitted in digital format."

10. Education and training, on both legal and technical competence, should be developed and implemented to facilitate and advance court management of digital evidence, for attorneys, parties (including self-represented persons), court staff, and judicial officers. The AOC should develop resource guides for self-represented litigants as well as templates for local court use that include information on requirements surrounding redaction, standardized formats, converting, submitting, and using digital evidence in the court.

A more detailed description of the background and reasoning supporting these recommendations follows in the section on Workgroup Reports.

Although this report is now finalized, the task force continues in other ongoing efforts. The task force continues to solicit input on proposed rule changes identified by the Rules Workgroup, endorsed by the task force and attached in current form as Appendices G – L to this report. The hope is to file a rule change petition with final versions of those proposed rule changes not later than January 10, 2018. In addition, on August 31, 2017, the Arizona Supreme Court referred Petition R-17-0027 (which seeks to provide an express procedure for the disclosure of video from officer body-worn cameras in the Arizona Rules of Criminal Procedure 15.1 and 15.4) to the task force for consideration. That consideration is a work in progress, with comments to be provided after the completion of this report. Task force members also are continuing their outreach efforts.

MANAGEMENT OF DIGITAL EVIDENCE

Background

For centuries, the court has been the keeper of the record for court cases. Until recently, this court record could be categorized as having three components, each consisting of paper documents or paper documents and things: (1) written filings made by the parties; (2) a written word-by-word transcript of what was said at hearings; and (3) exhibits used at hearings consisting of documents, pictures, and things, such as guns, drugs, etc. Although complicated and important, keeping this court record involved making sure paper filings were in the physical file, transcripts were included in or accounted for in that physical file, and exhibits received by the court (be they paper documents or things) were accounted for in the physical file, an exhibit locker, or a storage location.

These documents and things were expected to follow the case wherever it went and to be preserved for the applicable retention period for the case. In a case originating in the Arizona Superior Court, for example, the case might be resolved with no appeal; these documents and things in the court record would then be physically transferred to storage to be held for the appropriate retention period. On the other hand, if there was an appeal, these documents and things (or at least many of them) in the court record would be physically transferred to the Arizona Court of Appeals, then perhaps to the Arizona Supreme Court, and then perhaps to the United States Supreme Court. And in a criminal case, there could be a second round of litigation through post-conviction relief proceedings following a similar path, and a third round of litigation in habeas corpus proceedings in federal court. For each round, these paper documents and things in the court record would physically follow the case wherever it went.

A common characteristic of these written filings, written transcripts, and written or physical exhibits in the court record was that they could be touched, physically delivered, received and returned, accounted for by sight, found, stored, and, on occasion, lost. They were physical things that could be observed by a person with their senses.

The Evolving Court Record Format

Technology advancements outside of the court system have resulted in profound changes to the nature of the court record.

In summarizing court systems in a somewhat different context, "these paper-based institutions appear increasingly outmoded in a society in which so much daily activity is enabled by the internet and advanced technology." [1] Relatively recently,

[1] Ethan Katsch & Ornal Rabinovich-Einy, DIGITAL JUSTICE TECHNOLOGY AND THE INTERNET OF DISPUTES, Forward by Richard Susskind at xiii (2017).

the computer age has substantially changed filings and transcripts, two of the three key components of the court record. These changes, in turn, altered the very nature of the court record and how that court record is kept.

Filings by the parties are now, quite often, electronic filings, not in paper form, and may include materials that never existed in paper form. In many court systems, electronic filing of pleadings is required, absent leave of court to make such filings in paper form. For electronic filings, there is literally no physical thing provided to the court where the filing is made. Rather than a physical thing moving from a party to the court, a digital file crosses that threshold. The party making the filing submits to the court and the other parties in the case a digital file containing the filing. That filing is then kept by the court as a digital file in the court record that follows the case wherever it goes.

Similarly, today the transcript of court proceedings is frequently provided in a digital file or may, at times, be in the form of a digital audio or audio-video recording. The digital transcript then may become part of the court record to be kept by the court (or submitted to the court on appeal), with the digital file following the case wherever it goes. As with electronic filings, such a digital transcript is kept by the court in a digital file, not a physical paper-based file.

By contrast, how exhibits are handled in the court record has changed very little. Exhibits continue to be offered, received, handled, held, and transported by the court in physical form in much the same way they have been for decades. A party wishing to offer an exhibit has the clerk of court mark a physical exhibit (be it a document, a picture, a disc, a tape containing a video, a gun, etc.) for identification. For evidence stored digitally, this typically requires transferring that digital file to a physical thing like a disc so that the physical thing can be marked by the clerk of court as an exhibit for identification. Even if a digital file can be submitted to the court on a Universal Serial Bus (USB) drive, it is the USB as a thing that is received and used by the court (as opposed to the file on the USB being transferred to a court computer to be received and used by the court).

If admitted into evidence, the physical exhibit is then received by the court, used by witnesses, counsel, parties, the court, and jurors and then safely held by the clerk of court. That physical exhibit then becomes a tangible part of what until recently was a paper court record, including the paper filings and paper transcript. More and more often, however, other than exhibits, there is no longer a paper component of the court record. Thus, exhibits have become outliers; often they are the only tangible, non-digital part of the court record.

Given the technology-driven changes to the first two key components of the record (resulting in electronic filings and electronic transcripts) but not the third (exhibits), and the increasing instances of exhibits originating in digital form, the task force looked to see how the process might change if exhibits were treated more like electronic filings and electronic transcripts.

The need to consider allowing digital evidence to cross the threshold from party to the court in digital form was further enhanced by the increase in technology used in capturing and storing digital evidence and the increase in the use of such digital evidence at trial.

Recently, body-worn camera use has expanded at an almost algebraic rate, and its use promises to continue to expand.[2] Current technology allows body-worn camera images to be captured and stored in digital files. Those files are digital when created and remain digital from the time of creation through the eve of trial (from creation, to capture, to disclosure by a law enforcement agency to a prosecutor, to disclosure by a prosecutor to a defense attorney, to use by all throughout) and can be only viewed electronically. The issue, then, is whether there is a way for these digital images to cross the threshold from a party to the court as an exhibit to be used in court without having to transfer the evidence—digital images—onto a physical disc or similar thing that is then marked as a physical exhibit.

Given the change to digital form for filings and transcripts (but not exhibits), coupled with the proliferation of evidence in digital form (including digital body-worn camera video), the task force addressed issues surrounding the submission and use of digital exhibits in purely digital form. For example, is there a way that an exhibit, such as an electronic recording that exists only in digital format, can be submitted to the court in that digital format, instead of having to be transferred to a physical format like a disc before being marked as an exhibit for use in court? If so, what additional issues would such a transfer in digital form create?

The Truly Digital Evidence Concept

One charge of the task force was to analyze the implications of allowing exhibits to cross the threshold from party to the court in digital form and then be used, going forward, in digital form. This truly digital concept would apply to exhibits that exist only in digital format and to those that can easily be converted into or scanned into digital format. The task force also considered the resulting impact on court operations, and on management and retention of that digital evidence over its life within the courts.

---

[2] *See, e.g.*, Kami N. Chavis, *Body-Worn Cameras: Exploring the Unintentional Consequences of Technological Advances and Ensuring a Role for Community Consultation*, 51 Wake Forest L. Rev. 985, 987 (Winter 2016) ("Currently, one-third of the nation's 18,000 local and state police departments use body-worn cameras, but these numbers are growing rapidly, with the federal government's support encouraging this effort.") (footnotes omitted); Kyle J. Maury, Note, *Police Body-Worn Camera Policy: Balancing the Tension Between Privacy and Public Access in State Laws*, 92 Notre Dame L. Rev. 479, 486 (2016) ("Body camera implementation is a tidal wave that cannot be stopped."); Kelly Freund, *When Cameras are Rolling: Privacy Implications of Body-Mounted Cameras on Police*, 49 Colum. J.L. & Soc. Probs. 91, 94 (Fall 2015) (citing October 2012 survey for the proposition that "[a]pproximately a quarter of the country's police departments use body-mounted cameras, and 80% are evaluating their possible use").

To build on this issue, the task force discussed technology that would facilitate a trial with truly digital evidence. Not a trial using technology to present evidence in the courtroom or what is needed in a "high tech" courtroom, but a truly digital trial.[3] Focusing on court management of digital evidence, the task force looked at functionality and related issues of an electronic portal to an electronic data repository that could be populated and used by all in final trial preparation, at trial, and beyond (with the same concept applying to non-trial evidentiary hearings).

The concept would be court-driven, confirming the critical aspect of the clerk of court in receiving, managing, and securing evidence for use before, during, and after trial. The concept could consist of an electronic portal where electronic exhibits could be submitted to the clerk of court, in digital form, in advance of or at a hearing or trial. This concept is akin, in the paper world, to having paper exhibits marked for identification by a clerk for use at a hearing or trial. The difference, however, is that the portal concept would (1) allow exhibits to cross the threshold from party to the court in digital form and (2) allow electronic submission and marking of potential exhibits by a party to the case outside of normal court business hours.

Looking to electronic filings as a guide, the task force discussed a possible user fee (perhaps per exhibit or per case) to help offset the cost of technology. In doing so, the task force recognized statutory restrictions on fees, fee waiver requirements, and other issues that govern the collection of fees in various case types and that allow for court access regardless of financial resources. Any user fee concept would need to account for those issues and restrictions.

By submitting such exhibits to the clerk in digital form, just as with a paper exhibit marked by a clerk but not yet received, the exhibits would be ready to use in court at the appropriate time. Instead of physical items being held by the clerk, however, digital exhibits would reside in digital form in an electronic repository managed by the clerk. At the appropriate time, the digital exhibits marked for identification in a case could be accessed in court by the parties, counsel, the court, witnesses, and the clerk using courtroom monitors or on a network allowing such access on monitors provided by the parties.

Many courts currently have monitors in at least some courtrooms. Others have "technology carts" that can be moved from courtroom to courtroom as needed. For courts that have some form of such technology in the courtroom, this electronic repository concept would facilitate the use of such technology; for those that do not, it would necessitate acquiring or accounting for such technology.

If a digital exhibit was admitted into evidence, this electronic portal concept would allow the clerk to mark the exhibit as having

[3] Perhaps the closest example of a paperless trial in the United States in the sense of what the task force considered is described in Leonard Polyakov, *Paperless Trials Are The New Litigation Reality*, 57 Orange County Lawyer 36 (Sept. 2015).

been admitted in the electronic repository. As in the paper world, this would allow the participants to use the exhibit for proper purposes, including viewing the exhibit on courtroom monitors. Similarly, a digital exhibit marked but not received in evidence would be treated in the same manner as such an exhibit is treated in the paper world. Applying the concept to deliberations, the jurors could access the admitted exhibits in digital form using technology in the deliberation room.

After the trial ended, the admitted exhibits would be preserved for future reference; exhibits not admitted would be deleted (or retained, if necessary for subsequent proceedings), akin to what happens with paper exhibits. Again, however, given that the exhibits are in digital format, and are not physical things, there would be no need to store them in a physical location. Adequate server space, however, would be required.

Admitted exhibits then would be included in the record on appeal and transmitted electronically. The courts on appeal (and, for subsequent or collateral proceedings, other state or federal courts) could then access the admitted exhibits as needed for years to come.

It is this electronic portal and electronic repository concept, and various related issues, that the task force contemplated in addressing court management of digital evidence.

In its work, the task force looked to see whether any other court system in the United States is using this electronic portal and electronic repository digital evidence concept for truly digital trials. For decades, there has been a good deal of helpful information about how to conduct a trial by using exhibits in electronic form in the courtroom *after* exhibits are submitted to the clerk in paper form or on disc.[4] But the focus of the task force was different: a truly digital trial where trial exhibits cross the threshold from party to court in digital form and remain in digital form thereafter.

The task force contacted many groups to see if such a concept is being used anywhere in the United States, including the Federal Judicial Center, the United States Administrative Office of the Courts, the National Center for State Courts (NCSC), The Sedona Conference, private sector entities, other state court systems, and many other entities and individuals. The task force found no court in the United States that currently uses this concept. As such, the hope that the task force could follow in the wake of work done by others or adapt in Arizona what was being done elsewhere in the United States did not prove to be fruitful. As a result, the task

[4] *See, e.g.*, David L. Masters, *How to Conduct a Paperless Trial*, Vol. 39, No. 3 Litigation 52 (Summer 2013); Thomas E. Littler, *Litigation Trends in 2013*, 49 Arizona Attorney 30 (June 2013); Thomas I. Vanaskie, *The United States Courts' Case Management/Electronic Case Filing System: Perspectives of a District Judge*, Vol. 8, No. 3 e-Filing Report 1 (April 2007) (predicting, in discussing "The Paperless Trial Court Record," that "[a]s use of evidence presentation technology expands, it may be that the actual exhibits introduced at trial will be the digital version that counsel utilize in their presentation."); Carl B. Rubin, *A Paperless Trial*, Vol. 19, No. 3 Litigation 5 (Spring 1993).

force contemplated the electronic portal and electronic repository concept in addressing court management of digital evidence without the benefit of best practices and lessons learned by other courts in the United States.[5]

Task Force Meetings

The task force as a whole met seven times. The initial meetings involved many educational presentations from a variety of different perspectives.

The first meeting in January 2017 began with introductions and an overview of the background and substance of the JTC Resource Bulletin by Paul S. Embley, Chief Information Officer, Technology, National Center for State Courts. That first meeting also included presentations on digital evidence from a variety of different perspectives, including prosecutors, defenders, victims' rights advocates, and law enforcement as well as information about the exhibit workflow process and procedure currently used in Arizona Superior Court.

The February 2017 task force meeting continued with this educational focus, starting with a presentation on court use of cloud technology from the perspective of the Arizona Administrative Office of the Courts. This meeting also included a presentation from the perspective of the Arizona State Library, Archives and Public Records on hurdles and challenges with permanent storage of digital records and a demonstration of body-worn camera data storage and use. At this meeting, the task force first began discussing the effort in three workgroups: (1) digital formats, (2) storage and management, and (3) court rules, discussed in more detail below.

The March 2017 task force meeting continued the educational approach of the prior meetings. Presentations included discussion and demonstration of the Integrated Court Information Systems Next Generation case management system used by the Arizona Superior Court in Maricopa County, and the amount of physical storage space needed for digital evidence in physical form as currently required. A Maricopa County justice court also provided insight into that court's creative solution for capturing digital evidence submitted by self-represented litigants in various types of cases, including order of protection hearings, injunctions against harassment, eviction actions, and small claims matters. Time was then provided for workgroups to break out to continue discussion on related topics and subsequently report back to the task force as a whole.

The April 2017 task force meeting primarily involved reports from the

[5] Very recently, the task force learned of a London-based entity that has launched a system in British courts that appears to have some similarities to the truly digital evidence concept the task force considered. *See* www.caselines.com. It does not appear that any court in the United States has adopted that technology as of the date of this report. *See* http://caselines.com/ caselines-uk-leader-digital-court-solutions-beacon-british-exports-usa (September 8, 2017, press release noting an intention to provide a preview of the technology in the United States at the CTC 2017 Court Technology Conference in Salt Lake City later that month).

workgroups, but it also included an overview of the Arizona Commission on Technology (COT) and the OnBase technology used for electronic storage of filings in Arizona courts.

By the June 2017 task force meeting, the workgroups had prepared their first draft written reports. The task force spent much of that meeting discussing those draft reports, asking questions, and providing feedback. The workgroups then met and prepared revised reports for consideration before and during the August and September 2017 task force meetings. Considerable time was spent discussing various aspects of the workgroup reports and making revisions based on the consensus of the task force members during those meetings. Similar feedback and revisions were made to each version of the draft report. Consistent with prior practice, the workgroups also met separately during each meeting and reported back to and took questions from the task force as a whole.

The ultimate product of those workgroups (and, more broadly, the task force as a whole) is set forth in the workgroup reports. The workgroup reports, in their entirety, including reasoning for the individual recommendations, follow.

WORKGROUP REPORTS

Digital Formats Workgroup Report

Policy Question

- Should standardized acceptable formats, viewing, storage, preservation, and conversion formats or technical protocols for digital evidence be adopted for all courts?

Summary

The Digital Formats Workgroup was tasked with addressing the following policy question: "Should standardized acceptable formats, viewing, storage, preservation, and conversion formats or technical protocols for digital evidence be adopted for all courts?" Guided by this question, the workgroup performed its investigation, analysis, and due diligence, which included discussions, debates, and research, before formulating a response.

Ultimately, the workgroup concluded that standardized formats and technical protocols for the viewing, storage, and preservation of digital evidence should be adopted for all courts. Further, the workgroup concluded that standardization requirements should reflect and account for five interdependent principles: (1) the requirements must promote the efficient handling of digital evidence at all phases—from submission of the evidence to the court through viewing, storage, and archival preservation; (2) the requirements must account for rapidly changing technologies; (3) the requirements must be flexible enough to account for technology in a specific case to ensure the just resolution of the case; (4) the requirements must maintain the integrity of the evidence; and (5) the requirements must permit reasonable access by the parties and the public. Consistent with these general principles, the Arizona Supreme Court has already promulgated rules that provide a useful framework for standardization of digital evidence. These rules can be found in the Arizona Code of Judicial Administration (ACJA), particularly Chapters 5 (Automation) and 6 (Records).

The ACJA, however, expressly applies to the court and to court records, and thus, it applies only to digital evidence that qualifies as a court record and ultimately places the burden for compliance on the court. Section 1-507 of the ACJA includes administrative, case, electronic, and online records within the definition of court records. It broadly defines each type of record to encompass a wide range of content. The definitions do not require the material to be admitted in evidence as a court record and do not require the material to be created by the court. The definitions contemplate and include material created outside the court and offered to the court in an official manner, such as a filing or a marked exhibit.

Application of the current ACJA to digital evidence and ideas for amendments to the current ACJA to encompass digital evidence format requirements are discussed below. It is important, however, to recognize that because of the rapidly changing pace of technology, the ACJA's technical regulations should be reviewed and updated at least every other year to ensure consistency with current technology.

Conversion

By adopting a policy that requires court records to comply with standard formats, the ACJA implies that a record that does not comply with the standard formats must be converted to one that is compliant.

Section 1-507(D)(1)(a) of the ACJA provides: "Courts shall not create or store electronic records using systems that employ proprietary designs, formats, software, or media or that require use of non-standard devices to access records, in accordance with ACJA § 1-504(C)(1)." Thus, this provision sets forth the requirement that court records must comply with standard formats and be accessible with standard devices.

Similarly, ACJA § 1-507(D)(1)(b) specifically addresses conversion and preservation by requiring courts to "preserve all electronic documents so that the content of the original document is not altered in any way and the appearance of the document when displayed or printed closely resembles the original paper without any material alteration, in accordance with ACJA § 1-506(D)(1)." This requirement applies only to electronic documents, and is easily met via conversion to a portable document format (PDF) or other comparable standardized file format for electronic documents.

At the same time, § 1-507(D)(1)(c) states: "Courts shall preserve evidence and fingerprints in their submitted format—hardcopy items shall not be converted to electronic records for the purpose of storage and electronically submitted items shall not be converted to hardcopy for the purpose of storage." This section contemplates that a court may receive evidence electronically or physically and specifically prohibits the court from altering the evidence from its submitted format. In other words, it prohibits conversion of hardcopy or electronically submitted items for storage. This provision also may conflict with the § 1-507(D)(1) prohibition on using proprietary designs, formats, devices, etc., when creating or storing electronic records.

Lastly, the ACJA contemplates the handling of digital files beyond just documents. Section § 1-506(D)(5)(b) states: "Graphics, multimedia and other non-text documents may be permitted as follows: Other multimedia files (for example, video or audio files) shall adhere to established industry standards and shall be in a non-proprietary format (for example, MPEG, AVI, and WAV)."

The desirability of standard or non-proprietary file formats for court records applies equally to digital evidence received by the court and may necessitate conversion (by a party before offering the evidence) from an original, proprietary or non-standard format to a standardized or non-proprietary format. Additionally, changes to software and digital devices may necessitate conversion by the

courts during viewing, storage, or preservation.

Standardization requirements favoring conversion of digital evidence from non-standard or proprietary formats must, however, allow for exceptions when the interests of justice cannot be met through strict compliance with the requirement. First, standardization requirements must provide for exceptions when conversion will compromise the integrity of the evidence as determined by the purpose for which the evidence is submitted. For example, a video introduced at trial to prove the exact moment a gun was fired may lose its evidentiary value if converted to a standardized format that alters the frame rate such that the exact moment of firing is no longer discernable. On the other hand, if that same video was introduced to prove only that a person was at a specific location when the gun was fired, minor alterations that result from conversion would not appear to impact its evidentiary value.

Standardization requirements must also provide for an exception to accommodate the resource limitations of the parties when necessary to effectuate the just resolution of a case. Litigants, particularly self-represented litigants, may lack the technological tools necessary to convert digital evidence and may be unable to acquire such tools without undue hardship. For example, if critical evidence of an event was captured on a surveillance camera that used a proprietary video format, and this video could not be converted to a standardized format without significant costs to the party, a court may determine that admission of the non-standard digital format is necessary to ensure justice.

For the reasons stated above, there was a consensus that the ACJA and any rules of procedure dictating standardized digital evidence formats must allow for reasonable exceptions when required to serve the interests of justice. As such, the workgroup recommends an amendment to the ACJA defining the criteria a court must use in deciding when an exception to the standardized format requirement is warranted and the conditions that the party must meet in order to submit the evidence in question in non-standard or proprietary format.

Additionally, judges should make specific findings and create a record to document why a non-standard or proprietary format is necessary. Judges should also ensure the clerk of court is notified that additional measures may be needed for proper use, retention and preservation of evidence admitted in a non-standard or proprietary format. Finally, training for judges to aid them in recognizing, evaluating, and analyzing whether an exception to the rule requiring digital evidence to be submitted in a standard format is necessary. When non-standard or proprietary formats must be used, it should generally be the party offering the non-conforming digital evidence that has the responsibility to ensure the court is provided with the necessary technology ("native player") to allow viewing of the evidence both during the proceedings and after the matter has concluded.

Viewing and Presentation

The viewing and presentation of court records typically contemplates two scenarios. One scenario is the litigation of a case or controversy in a court. In this scenario, digital evidence is likely offered by a party to or participant in the litigation, and it becomes a court record when it is filed, marked as an exhibit, or otherwise offered to or received by the court. The primary concern in this scenario is the ability of the court and the parties to view and present the digital evidence at court proceedings.

The second scenario is public access to court records, which can include media requests. In this scenario, a person who is interested in the litigation, but not involved in it, seeks to access the digital evidence in a case or controversy. The primary concern in this scenario is the ability of persons unrelated to cases to view the digital evidence.

Adopting standard formats for digital evidence will likely maximize the ability of litigants and the public to access court records whether it is before, during, or after litigation is resolved. The ACJA accomplishes this by addressing these scenarios in separate sections as discussed above. In addition, the rules of court for the various types of cases (civil, criminal, family, juvenile, etc.) are consistent with the ACJA in that they govern the nature of the material that might become a court record at the request of a party to the case. When a litigant complies with both the rules and the ACJA, it maximizes the probability that the record will be accessible in the present and the future.

Storage

The ACJA also contains requirements for the storage of court records in § 1-507(D)(3). This section addresses primary and secondary electronic storage and sets forth specific hardware, power supply, and redundancy requirements for court records. "Storage" is specifically defined in § 1-507(D)(3) as "a permanent repository for holding digital data that retains its content until purposely erased, even when electrical power is removed" and applies "to electronic case records, administrative records and regulatory case records in the custody of judicial entities in Arizona, as defined by Supreme Court Rule 123." Section 1-507(H) also contains a section that addresses the electronic archives of closed cases in limited jurisdiction courts in recognition of the challenges unique to those courts, given the types of records and the more limited resources of those courts.

The workgroup concluded that the current language of the ACJA as to storage requirements sufficiently addresses the policy questions it was charged with answering. The ACJA sections reviewed here are flexible enough to account for new and existing technologies and the ever-increasing volume of digital evidence that will need to be stored. There is nothing in the storage-related provision of the ACJA, or any other provision of the sections cited herein, that would prevent a court from accepting evidence electronically submitted, regardless of whether it was submitted on a compact disc, by email, or through information sharing on the cloud. The workgroup recommends however, that once received by the court, digital evidence should be stored in the format

in which it was received, unless it is an electronic document. *See* ACJA § 1-507(D)(1).

Preservation

The ACJA does not clearly distinguish between storage and preservation, and while it defines the former, it does not define the latter. Storage requirements are set forth in ACJA § 1-507(D)(3), which does not discuss preservation. Preservation is directly addressed in ACJA § 1-507(D)(5)(c) and (f). Subsection (c) addresses preservation of records primarily by referencing the state retention schedules, specifically stating:

"Records generated by or received by courts shall be preserved in accordance with the applicable records retention schedule. Case records required to be submitted to Arizona State Library, Archives, and Public Records (ASLAPR) shall meet the submittal requirements specified by ASLAPR at the time of submittal, regardless of storage medium. Records destruction is subject to the notification requirements of ASLAPR."

Collectively, subsections (d), (e), and (f) require the courts to employ various procedures, including refreshing electronic records, replacing or upgrading systems to ensure records do not become "obsolete," and using backward-compatible software to address the challenge of providing access to electronic records over a long period of time.

Thus, it is likely that the distinction between storage and preservation in the ACJA is that the term "storage" suggests a shorter and more immediate time frame, while the term "preservation" suggests a longer and more enduring time frame.

Regardless of the time frame involved, the storage and preservation processes are compatible. The main challenge of preservation is maintaining the accessibility of records, including digital evidence, with minimal alteration, over a long period of time. The workgroup determined these challenges were more closely aligned with the policy questions addressed by the Storage and Management Workgroup. Through workgroup meetings and full task force meetings, this overlap was discussed broadly with the task force and with the Storage and Management Workgroup. The Formats Workgroup supports the recommendations of the Storage and Management Workgroup as to the setting of minimum requirements for any digital evidence storage and management solution adopted by the AOC or a local court.

Storage and Management Workgroup Report

Policy Questions

- Should digital evidence be stored locally, offsite, or using cloud services and how long and in what manner should such evidence be retained?
- Should management of digital evidence possessed by courts be centralized or decentralized considering technology costs, expertise, and infrastructure necessary to manage it?

Summary

The Storage and Management Workgroup was tasked with addressing the following policy questions:

- "Should digital evidence be stored locally, offsite, or using cloud services and how long and in what manner should such evidence be retained?"
- "Should management of digital evidence possessed by courts be centralized or decentralized considering technology costs, expertise, and infrastructure necessary to manage it?"

The digital world is not new to courts. For nearly a generation, courts have used and managed digital documents, digital recordings, e-filing, and, to a much lesser degree, digital evidence. Currently in Arizona, digital evidence is offered into evidence in a physical form, such as a photo, a smart phone screen shot transferred to paper, or a document or video captured on a compact disc or other electronic media storage device. In Arizona, judges, clerks of court, and court administrators apply existing rules addressing technology to constantly evolving technology. For the most part, it works. However, the rapid increase in offering digital evidence in court is very real, particularly given the exponential growth in law enforcement body-worn cameras, digital video captured by cell phones, security cameras, and other digital media generated from Amazon Echo, Google Home, traffic control systems, and other devices that make up the Internet of Things.

The workgroup recognizes most courts are just beginning to experience the increase in the volume and types of digital evidence they are required to manage. Fortunately, for planning purposes, courts are at the bottom of the evidence screening funnel. For example, in criminal cases, law enforcement, prosecutors, and defense attorneys must review and manage many times the volume of digital evidence than ultimately is deemed to be

relevant and admissible in a case, or even that is marked as an exhibit in a case. There is, however, a rapid increase in the submission of digital evidence in court, requiring courts to implement policy and technical standards that are flexible enough to accommodate storage needs tomorrow that are not measurable or predictable today.

The workgroup concluded that the policy decisions regarding whether management of digital evidence should be centralized or decentralized and whether storage should be local, off-site, or in the cloud should be guided by a set of technical requirements and policy considerations discussed in this workgroup report.

Arizona establishes technical requirements and policy through the Arizona Code of Judicial Administration (ACJA). For example, the ACJA establishes minimum technical requirements for Electronic Reproduction and Imaging of Court Records (Section 1-504); Enterprise Architectural Standards (Section 1-505); Filing and Management of Electronic Court Documents (Section 1-506); and Protection of Electronic Case Records in Paperless Court Operations (Section 1-507). The workgroup was not tasked with establishing and did not establish, technical requirements, per se, for the storage and management of digital evidence; however, below is a list of suggested minimum requirements to consider in addressing those issues.

Suggested Requirements

The workgroup recommends the following set of minimum technology requirements for any digital evidence storage and management solution used by Arizona courts—centralized or decentralized.

1. Single Solution. Whenever possible, a single-source solution for the storage and management of all digital material acquired by, generated by, and stored with the judiciary should be acquired.

2. Solution Integration. Whenever a single solution is not available or cannot be feasibly acquired, the solutions adopted must have the ability to integrate with other software solutions to reduce the need for numerous applications to store and manage not just digital evidence, but all digital material.

3. Media Type. Any storage and management solution adopted must be able to accept all types of digital media and files. The portion of this report that details the input of the Digital Formats Workgroup thoroughly discusses the current ACJA requirements related to standardized formats for all digital evidence submitted to a court. This workgroup supports the recommendation of the Digital Formats Workgroup regarding standardized formats as a default requirement, with courts having discretion to allow submissions of digital evidence in a non-standard, propriety form when the interest of justice requires,

as long as a native player is provided with the submission of the digital evidence.

The adoption of new digital evidence storage and management solutions will likely require changes to the rules surrounding what types of content a court is required to store as well as how that content is to be received by a court (e.g., admitted versus tendered evidence or redacted versus un-redacted versions of digital evidence). Such issues must be considered and resolved parallel to the decision-making process for adopting a new solution.

4. Sealing, Restricting, and Redacting. Any software solution for the storage and management of digital evidence must be able to mark digital evidence as sealed or restricted from general access to account for redaction or other protection of confidential or sensitive information. Further, any solution must have capabilities for redaction in the rare circumstances a court orders the clerk of court to redact a copy of digital evidence before making a copy of the evidence available for general viewing. These capabilities are imperative to meeting the requirements of protecting evidence not available for general viewing in accordance with law.

5. Security. Any hardware and software solutions adopted to store and manage digital evidence must meet the most current cyber security requirements as set forth in the ACJA for all types of digital evidence. Those solutions must also be capable of meeting ever-evolving cyber security standards.

6. Data Backup and Recovery. All hardware and software solutions must meet the data backup and recovery requirements set forth in the ACJA.

7. Authentication and Audit Trails. Software solutions must be able to provide the necessary metadata to authenticate the digital media and establish an audit trial for purposes of authenticating and establishing the reliability of the evidence. In considering whether a software solution meets this requirement, the deciding authority must take into consideration the requirements of rules of procedure and rules of evidence to ensure the software does not alter the digital evidence in the mechanics of uploading, retrieving, viewing, or retaining the material.

8. Retention. All hardware and software solutions must be capable of storing and preserving digital evidence in the format submitted for the applicable retention periods as established by ACJA §§ 2-101, 2-201, 3-402, 4-301, and 6-115, and any other retention schedules applicable to court records.

9. **"Physical Digital" Security**. Currently, digital evidence submitted to a court via a physical format, such as a CD, cannot be connected to network computers (e.g., Arizona Justice Information Network

(AJIN) or Criminal Justice Information Systems (CJIS) computers). This currently prevents such evidence from being uploaded to case management systems for storage and for use in court hearings and trials. Any digital evidence storage and management solution should include a safe pathway to eliminate the need to store digital evidence in physical formats instead of electronically.

10. Public Access. All software solutions must meet the requirements for user access as set forth in Rule 123, Arizona Rules of Supreme Court, and ACJA § 1-604, if the application will be accessible via remote electronic access. This includes protections afforded to media designated as confidential, sealed, or otherwise restricted from public access.

11. Viewing. Any software solution adopted for the storage and management of digital evidence must allow a user to preview the content of the evidence in the application while searching or indexing. As an alternative, the software solution must allow for some type of description of the evidence beyond what a file name provides. Such functionality is for the purposes of ease of searching for and indexing digital evidence.

Additional Considerations

The workgroup is aware that economies of scale and the limited capacity of many courts to store and manage digital evidence locally may necessitate that digital evidence storage and management solutions be centralized versus decentralized. However, who should store and manage digital evidence—local courts or more globally as part of a centralized solution—is not the whole of the question. There is not a one-size-fits-all solution to the question of digital evidence storage and management. Any court that can meet the minimum technical requirements set forth in the ACJA should be able to store and manage its digital evidence locally if it wishes to do so.

The workgroup further recommends that the following additional considerations be a part of a local court's analysis of whether to be a part of a centralized solution or to adopt a decentralized storage and management solution:

- **Capacity to Manage Locally (Cost and Technology)**. The fiscal challenges and technical abilities of local courts must be considered. Even with a centralized system, local courts will be required to have the operating power and equipment to connect with the centralized system. Such needs ultimately will require budget increases that often are difficult to acquire from local funding sources. Moreover, local court staff will need to quickly acquire and constantly update the skills to enter and retrieve digital material from the centralized system throughout the time a legal matter is pending and retained with the court.
- **Bandwidth**. Changes and improvements to digital evidence storage and management solutions likely will come

with a greater need for bandwidth, particularly when the storage and management system is centralized at an off-site location or in the cloud. Bandwidth issues continue to be a hurdle for local courts, even in the most urban areas. In making decisions about storage and management solutions, it is imperative that the solution adopted will be functional in each court. Limited or insufficient bandwidth that impedes the ability to upload and retrieve digital evidence so that it can be used quickly and effectively will be a detriment to day-to-day court proceedings as well as public access.

- **Resource Capabilities**. Assessment of the magnitude of the impact of electronically storing digital evidence is imperative. Moreover, adoption of a storage and management solution that is capable of expansion, can remain integrated with new versions of other software, and that will integrate with later-acquired software is necessary for local courts to effectively serve the parties and the public.
- **Self-Represented Litigants.** For some time, courts, counsel, and prosecution and defense agencies have dealt with redaction of confidential or otherwise restricted information in evidence offered in court of all types. This may not be not true, however, for self-represented litigants, who may lack the knowledge of the legal requirements or lack the tools and abilities to comply with redaction requirements. Courts are increasingly facing issues related to the submission of digital media-based evidence by self-represented litigants who lack the knowledge, tools or ability to comply with redaction requirements. It may be that future technology advances will help resolve these important issues. For now, however, the AOC should look to determine what efforts for self-represented litigants may be appropriate to ensure that they do not submit digital evidence containing confidential or otherwise restricted information, recognizing such efforts should not place court personnel in a position of providing legal advice or improperly assisting a specific party. At a minimum, the workgroup recommends the AOC develop resource guides for self-represented litigants or templates for local court use that include information on requirements surrounding redaction, standardized formats, converting, submitting, and using digital evidence in the court.

Other Issues

The workgroup was charged with policy questions that focus on what to do once digital evidence is received by the court—what could be referred to as the "back end" of the process of digital evidence after it crosses the threshold from party to the court. Limited jurisdiction courts are seeing self-represented litigants in small claims, eviction, debt collection, or other cases where the amount in controversy may be modest (although critically important to the parties) who wish to

offer in evidence smart phone photos, recordings, or other digital evidence from portable or home devices that are not reformatted and submitted via a CD. It was noted that the Superior Court also faces the same challenges in certain case types. Guidance should be developed for litigants presenting and courts managing this type of evidence.

The workgroup recommends that the AOC work with local courts in developing policies and procedures and, where feasible, implementing technological solutions, for cases in limited jurisdiction courts to account for the specific needs in such cases. In particular, the following areas were identified for consideration:

- **Courtroom recordings.** Many courtrooms are equipped with digital recording devices used to record audio, video, or both. Ideally, digital evidence played in limited jurisdiction courts would be captured and preserved by the court's digital recording device. Rule changes allowing this in certain cases may be needed.
- **Courtroom presentation.** There needs to be a manner of connecting litigant technology to courtroom technology or otherwise using courtroom technology to capture presentation of digital evidence presented in court by litigants, particularly self-represented litigants, for admission into the record and meeting evidence retention requirements.
- **Transition to a new digital solution.** The implementation of storage and management solutions for digital evidence will require time for acquisition, implementation, and training on its use. The difficulty will be compounded by the need to timely tackle a fast-approaching problem using new, emerging, and constantly-evolving technology and training court staff and judges on how to use that technology. Information on submitting and presenting digital evidence for litigants, particularly self-represented litigants, is also necessary.
- **Cost recovery.** The cost of new technology is always present in this discussion. The workgroup recommends establishing a fee, where appropriate and permissible, for submission of digital exhibits. Such a fee could offset the financial impact associated with digital evidence storage and management solutions.

Rules Workgroup Report

Policy Questions

- Should court rules governing public records be revised to address access and privacy concerns, including for victims, non-victim witnesses, and other identifying information often included in video evidence?
- Should new or amended rules on chain of custody evidence be developed for handling court digital evidence?

Discussion

The Rules Workgroup was tasked with addressing the following policy questions:

- "Should court rules governing public records be revised to address access and privacy concerns, including for victims, non-victim witnesses, and other identifying information often included in video evidence?"
- "Should new or amended rules on chain of custody evidence be developed for handling court digital evidence?"

The Rules Workgroup was guided by these questions and, by definition, built on the work of the Formats and Storage and Management Workgroups.

In substance, digital evidence is not new or different evidence. Digital evidence involves the same types of evidence courts, attorneys, and parties have always handled. It is the form of the evidence and media the evidence is produced on that has changed; for instance, reports are no longer printed on paper, photos are no longer chronicled on film, videos are no longer recorded on a Video Home System (VHS) tape or digital video disc (DVD), and audio recordings are no longer captured on an audio tape or compact disc (CD). Instead, this evidence is saved and stored in some type of digital format, often a format that is stored on a portable device or on a server, either locally or in the cloud.

The most significant issue regarding digital evidence that may necessitate rule changes is volume. The volume of digital evidence will create the need for a significant increase in digital storage capacity and require additional time for redactions, such as that created by body-worn cameras and other footage captured on digital recording devices to protect victims' rights and privacy interests of citizens.

Among others, the Rules Workgroup reviewed the Arizona Rules of Evidence, Arizona Rules of Civil Procedure, Arizona Rules of Criminal Procedure, Arizona Rules of Family Law Procedure, Arizona Rules of Protective Order Procedure, Arizona Juvenile Court Rules, Arizona Rules for Eviction Actions, Arizona Rules of Probate Procedure,

Arizona Justice Court Rules of Civil Procedure, Arizona Supreme Court Rule 123, and rules, statutes, and constitutional provisions involving victims' rights. The workgroup also reviewed relevant portions of the Arizona Code of Judicial Administration (ACJA).

The workgroup's review of the various rules of procedure revealed that current rules overall appear to be working when it comes to disclosure and submission of digital evidence for use at a hearing or trial. As such, the procedural rules do not need wholesale substantive revision to address the increasing use of digital evidence, although a few areas where revisions are necessary were identified and are discussed below. In addition, although the current rules are working, the workgroup believes that the rules need modernization to use language that includes digital media types of today and the future.

The following is a summary of the rule changes recommended by the workgroup:

1. Defining "Digital Evidence." The workgroup first proposes that there be a definition for the phrase *digital evidence*. The following definition of *digital evidence* is proposed: "Digital evidence, also known as electronic evidence, is any information created, stored, or transmitted in digital format." The workgroup recommends that this definition be added to the appropriate definition sections of the procedural rule sets.

2. Arizona Rules of Evidence. The workgroup focused its review of the Arizona Rules of Evidence on the rules on authentication and identification (Article IX) and the rules on the contents of writings, recordings, and photographs (Article X). The workgroup concluded that the Arizona Rules of Evidence do not require any amendments, changes or additions to authenticate or identify digital evidence for use in court proceedings.

Conversely, the language and concepts in Rules 1001 through 1008 do need modernization. In particular, Rule 1001(b) limits the definition of the term "recording" to "letters, words, numbers, or their equivalent recorded in any manner." Although the workgroup recognized that the phrase "their equivalent" currently is applied to digital images and video that involve non-verbal action not involving any "letters, words, [or] numbers," it recommends the rules be updated to include the term *video* and that a definition of the term *video* be added to the rule. The workgroup considered various definitions of the term and considered the variety of digital evidence that is not a still image as contemplated by the term *photograph* defined in Rule 1001(c) and suggests as a definition: "*Video is an electronic visual medium for the recording, copying, playback, broadcasting, or displaying of audio or moving images.*" The workgroup further recommends that Rules 1002, 1004, 1007, and 1008 be amended to insert the newly defined term *video*. (See Appendix G.)

3. Arizona Rules of Civil Procedure. The workgroup notes that the Arizona Rules of Civil Procedure underwent a comprehensive

restyling in 2016, with the restyled rules taking effect January 1, 2017. *See* September 2, 2016 Order adopting Petition R-16-0010. Moreover, during the workgroup's consideration, a rule petition was pending before the Supreme Court that would significantly change many of the civil rules surrounding discovery and disclosure. After review of the rules in place and the pending rule petition, other than perhaps to expressly use the phrase "digital evidence" and the corresponding definition, the workgroup determined that the Arizona Rules of Civil Procedure thoroughly address digital evidence head on, particularly the disclosure rules in Article V (Rules 26 through 37). Moreover, unlike the Arizona Rules of Evidence, the Arizona Rules of Civil Procedure do not address the admission of digital evidence into evidence in court.

4. Arizona Rules of Criminal Procedure. The workgroup closely reviewed the Arizona Rules of Criminal Procedure, including Rules 15.1, 15.2, 15.4, 15.5 (the disclosure rules), and Rule 22.2 (materials used during jury deliberation) to determine if any changes were needed to address the handling of digital evidence. Currently, the disclosure rules do not appear to be causing any challenges in relation to the disclosure of digital evidence, despite there not being language that specifically includes disclosure of materials or information that exists in a purely digital format. Despite the lack of current issues, as digital evidence increases, its disclosure via electronic means is increasing versus disclosure after transfer to a tangible item such as a disc or onto a physical format like paper. The workgroup notes that Rules 15.1 and 15.2 do not contain language that includes video, digital evidence, or other electronically stored information. As such the workgroup recommends that Rules 15.1 and 15.2 be amended to include language specifically identifying disclosure of digital evidence.

In particular, the workgroup reviewed language that requires disclosure of "a list of all papers, documents, photographs and other tangible objects." [6] The increase in digital evidence, such as body-worn camera video and digital video, images, or other content from smart phones or other personal recording devices, are not accounted for in the specific language of the rules. The workgroup notes that, particularly as disclosure of the evidence moves more and more toward a cloud-based model, there is a need for modernization of the rules. (See Appendix H.)

Rule 22.2 addresses materials that may be used during jury deliberations. The rule refers to "tangible evidence as the court directs," with no mention of evidence that is in a purely digital form, such as admitted evidence that has not been transferred to a tangible physical thing like a disc. Currently, in Arizona, digital

[6] Rules 15.1(b)(5), (i)(3)(c) and 15.2(c)(3), (h)(1)(d) of the Arizona Rules of Criminal Procedure in place as of the date of this report, before the January 1, 2018 effective date of amendments to these rules. *See* http://www.azcourts.gov/rules/Rule-Amendments-from-Recent-Rules-Agenda-s (August 31, 2017 Order adopting Petition R-17-0002).

evidence is submitted and admitted for trial after being transferred to tangible item. However, digital evidence is increasingly cloud-based, and disclosure of that evidence is increasingly becoming possible via cloud-based file sharing.

For example, prosecutors and law enforcement officers in some locations use a digital drop-box to transfer or disclose digital evidence to the defense. Another example is body-worn camera manufacturer Axon's (formerly Taser International) deployment of a cloud-based portal (evidence.com) to allow cloud sharing between law enforcement agencies and prosecutors and its ongoing development of cloud-based disclosure between prosecutors and defense counsel. This expansion of cloud-based sharing of digital evidence is quickly coming to courts. If Arizona were to adopt rules and procedures for allowing cloud-based submission and admission of digital evidence, then Rule 22.2(d)[7] would require amendment to account for both tangible and cloud-based evidence.

The workgroup finally concluded that the above-referenced definition of digital evidence would be a benefit to the Arizona Rules of Criminal Procedure and recommends addition of that definition in Rule 1.4.

5. Arizona Rules of Family Law Procedure. The workgroup reviewed the disclosure and discovery rules of family law procedure. The workgroup recommends that a change be made to Rule 49 to include a subsection on electronically stored information. Several subsections of Rule 49 refer to disclosure and discovery of such information, but the rule does not currently provide guidance for parties in relation to a duty to confer regarding the form in which the information will be produced or resolution of disputes related to electronically stored information. As property records and financial records are increasingly available via the Internet and as more and more people manage finances electronically, having guidelines and procedures for managing this type of discovery will be increasingly beneficial to parties and the courts. (See Appendix I.)

The workgroup also understands that, pursuant to Administrative Order No. 2016-131, the Arizona Supreme Court established a task force to "review the Arizona Rules of Family Law Procedure to identify possible changes to conform to modern usage and to clarify and simplify language . . . with the goal of submitting a rule petition by January 10, 2018, with respect to any proposed rule changes." The Arizona Rules of Family Law Procedure are based on the Arizona Rules of Civil Procedure, but "as they existed before the 2016 amendments" effective January 1, 2017. Ariz. R. Fam. L.P. 2(A). Accordingly, the workgroup would encourage the task force

[7] Amendments to the Arizona Rules of Criminal Procedure were adopted, effective January 1, 2018, which change Rule 22 to Rule 22.2, specifically Rule 22.2(a)(4). *See* http://www.azcourts.gov/rules/Rule-Amendments-from-Recent-Rules-Agenda-s (August 31, 2017 Order adopting Petition R-17-0002).

addressing the Arizona Rules of Family Law Procedure to, in its work, not only consider the amendments to the updated Arizona Rules of Civil Procedure but also ensure digital evidence is expressly addressed.

6. Arizona Rules of Protective Order Procedure. Increasingly, persons seeking orders of protection and injunctions against harassment come to court with some form of digital evidence to demonstrate to the court the need for the protective order. The workgroup recommends that Rule 36 of the Arizona Rules of Protective Order Procedure, addressing admissible evidence in contested protective order hearings, be modernized to include digital and electronic evidence specifically. (See Appendix J.)

7. Arizona Rules of Probate Procedure. The workgroup noted that the Arizona Rules of Probate Procedure incorporate by reference Rules 26-37 of the Arizona Rules of Civil Procedure. As such, the rules address electronically stored information; therefore, no amendments are recommended. The Arizona Rules of Probate Procedure are heavily driven by statutory requirements. The workgroup notes that, if statutory changes occur in the future, then rule changes would need to follow. Future rule changes should keep in mind the changing landscape of digital evidence and its role in legal proceedings.

8. Arizona Rules of Juvenile Court. The current disclosure and discovery rules, Rule 16 (for delinquency and incorrigibility proceedings); Rule 44 (for dependency, guardianship and termination of parental right proceedings); and Rule 73 (for adoption proceedings), do not include any reference to digital or electronic evidence. The workgroup acknowledges that, despite the lack of such specificity, the rules currently appear to work. However, considering the increasing volume of digital evidence, including in delinquency matters like adult criminal matters, a technical amendment that would modernize the language of the rule is recommended.

For these reasons, the workgroup recommends that a technical change be made to Rule 16(B)(1)(d) and 16(C)(3)(c) of the Rules of Juvenile Court to include reference to digital and electronic evidence. (See Appendix K.) For similar reasons, the workgroup also recommends similar technical changes to include digital evidence and electronically stored information be made to Rules 44 and 73. (See Appendix K.)

9. Arizona Justice Court Rules of Civil Procedure. The workgroup's review of the Arizona Justice Court Rules of Civil Procedure, particularly Rules 121-127, demonstrated that electronically stored information and digital evidence are adequately addressed. This rule set both directly addresses electronically stored information and incorporates some of the Arizona Rules of Civil Procedure that similarly address disclosure and discovery of such information. Moreover, Rule 125(a) contains language that includes digital evidence. The workgroup has no

recommendation for amendments or a new rule in this rule set.

10. Arizona Rules on Eviction Actions. Like the Arizona Rules of Protective Order Procedure, the Arizona Rules on Eviction Actions do not need substantive changes to address digital evidence. However, the workgroup recommends a technical amendment to include digital evidence or electronically stored information in Rule 10, which addresses the types of content that must be disclosed. (*See* Appendix L.)

The ACJA.

The workgroup reviewed several sections of the ACJA and concluded the code currently is an excellent framework for requirements pertaining to digital evidence. The Digital Formats and Storage and Management Workgroups were tasked with policy questions more directly aligned with the ACJA provisions that address digital evidence. Throughout its review, the Rules Workgroup provided input and feedback to those workgroups as they reviewed ACJA sections. The Rules Workgroup has no recommendations beyond those made by the Digital Formats and Storage and Management Workgroups. The following describes the thought processes regarding relevant ACJA sections and any overlap with procedural rules discussed above.

Section 1-504 provides standards that apply to all records imaged by courts, including the methods used to create or reproduce records electronically. In particular, § 1-504 designates the methods and formats that must be used to maintain and preserve electronically stored and archived records and the reproduction of such records. This section also covers general requirements for security to ensure evidence is not destroyed or altered. In addition, § 1-504 addresses accessibility. Courts must ensure that the public is afforded reasonable access to records, consistent with Arizona Supreme Court Rule 123, via the public access portal managed by the Arizona Administrative Office of the Courts, at a minimum. Further, courts are required to ensure records sealed or designated confidential by rule, law, or court order contain appropriate metadata to enable any electronic document management system (EDMS) in which they reside to protect them from inappropriate access.

Section 1-506 provides standards for the filing and management of electronic court documents. Subsection B provides the purpose as follows: "This section provides administrative requirements, standards and guidelines to enable Arizona courts to implement a uniform, statewide, electronic filing system and to achieve the reliable, electronic exchange of documents within the court system as well as between the court and court users." In addition, ACJA § 1-507 provides standards for the protection of electronic case records. These provisions address most types of digital evidence, including the formatting and authentication of such evidence.

Sections 1-604 and 1-606 provide standards addressing the accessibility to digital court records, which would include digital

evidence. Both code sections address the ability to access court records remotely.

In summary, the Rules Workgroup does not have recommendations, independent from those of the other workgroups, regarding changes to the ACJA.

Privacy and Digital Evidence.

Victims have concerns regarding their privacy in the digital age that differ significantly from the issues faced by courts and attorneys. Crime victims are pulled into the inner workings of the criminal justice system by the unlawful acts, often physically and emotionally harmful, of others. In addition, understandably, victims' knowledge of the criminal justice system and the courts may be limited. It is not uncommon for victims to become increasingly concerned with privacy, especially as it related to images and information captured via digital devices like body-worn cameras, cell phone video, digital photographs of their injuries, crime scenes, and autopsies. Particular sensitivity surrounds the ability of the public to obtain this digital evidence through court filings, evidence received in court, and the record of court proceedings more generally.

Arizona's Victims' Bill of Rights guarantees crime victims a right to justice, due process, and to be treated with fairness, respect, dignity, as well as to be free from intimidation, harassment, and abuse. Ariz. Const. art. II § 2.1(A)(1). The workgroup also recognizes that the open records policies applicable in Arizona's courts may cause victims concerns.

The Arizona Supreme Court has enacted rules related to victims' rights. For example, Rule 39 of the Arizona Rules of Criminal Procedure provides an avenue for victims to seek protection of their identity and location. Rule 39 is cross-referenced in several rules related to discovery and disclosure. Arizona Supreme Court Rule 122 includes consideration of victim's rights in relation to broadcasting of trials. And Arizona Supreme Court Rule 123 limits public access to court records when confidential or sensitive information is involved and where access is otherwise restricted by statute.

It may be that an increased use of digital evidence may result in an increase in public requests, including media requests, for access to such digital evidence which, in turn, may implicated victims' rights and privacy concerns. In addition, the workgroup recognizes that although the various rules mentioned above currently work to protect victims' rights, victims continue to advocate for additional protections.

The workgroup was charged in part with reviewing rules governing public records to determine if changes were warranted to address access and privacy concerns. Based on its work, the workgroup determined generally that Arizona courts treat digital evidence like traditional evidence and that current policies and procedures applicable to all types of evidence (including digital evidence) are working. However, the workgroup notes that Arizona Supreme Court Rule 123 does not consistently address digital evidence,

including exhibits, received by a court. The workgroup recommends that Rule 123 be amended to ensure that it addresses digital evidence, including exhibits, and that the portions of the rule that govern public access, particularly remote electronic access, be amended to ensure sufficient protection of victims' rights and privacy concerns.

A related issue is that digital evidence regularly (but incidentally) captures images of individuals and their property, including personal identifying information. Often this information and these images are captured in public places where individuals do not have privacy rights as parties or as victims. The ease of using facial recognition software or access to databases that may lead to identification of these individuals may create concerns regarding expectations of reasonable anonymity. Moreover, often this information and these images are not relevant to why the digital evidence is being offered in a specific matter and may be concerning to bystanders, given issues of safety, identity, contact information, etc. Therefore, the workgroup also recommends that the AOC (a) work with local courts, prosecuting and defending agencies, law enforcement groups, media organizations, and other interested individuals and organizations to develop consistent policies and approaches addressing these issues, and (b) consider how to handle digital evidence being introduced in evidence by self-represented litigants that may not be redacted.

APPENDIX A—Administrative Orders

IN THE SUPREME COURT OF THE STATE OF ARIZONA

In the Matter of:	)	
	)	
ESTABLISHMENT OF THE TASK FORCE ON COURT MANAGEMENT OF DIGITAL EVIDENCE AND APPOINTMENT OF MEMBERS	)	Administrative Order No. 2016 - 129

Litigation increasingly involves digital evidence, particularly from audio and video recording devices. Technology used to create, store, and display information has changed dramatically over the years and will continue to do so in the future. More recently, the creation of digital video evidence through the use of smart-device cameras, body-worn cameras, and other public and private surveillance equipment has grown exponentially. Courts responsible for managing digital evidence face unique challenges related to receiving, retrieving, accessing, formatting, converting, and retaining digital evidence as well as protection and disposition issues.

Earlier this year, the Joint Technology Committee (JTC) of the Conference of State Court Administrators, the National Center for State Courts, and the National Association for Court Management published the "JTC Resource Bulletin: Managing Digital Evidence in the Courts." The JTC Resource Bulletin recommends that state court leadership develop policies for court management of digital evidence. This Bulletin provides a good framework for discussion and relevant policy development.

Policy questions described in and suggested by the Bulletin include:

1. Should court digital evidence be stored locally, offsite, or using cloud services and how long and in what manner should such evidence be retained?
2. Should management of court digital evidence be centralized or decentralized considering technology costs, expertise, and infrastructure necessary to manage it?
3. Should court rules governing public records be revised to address access and privacy concerns, including for victims, non-victim witnesses, and other identifying information often included in video evidence?
4. Should new or amended rules on chain of custody evidence be developed for handling court digital evidence?
5. Should standardized acceptable formats, viewing, storage, preservation, and conversion formats or technical protocols for digital evidence be adopted for all courts?

Therefore, pursuant to Article VI, Section 3, of the Arizona Constitution,

IT IS ORDERED that:

ESTABLISHMENT: The Task Force on Court Management of Digital Evidence is established.

1. PURPOSE: The Task Force shall review the questions presented above and make recommendations on each. The Task Force shall review the JTC Resource Bulletin for additional information on these and other policy issues, as well as any other relevant journals, publications, or other research related to this topic and make recommendations as it deems appropriate.

The Task Force shall submit its report and recommendations to the Arizona Judicial Council not later than October 1, 2017, and file a rule change petition not later than January 10, 2018, with respect to any proposed rule changes.

2. MEMBERSHIP: The individuals listed in Appendix A are appointed as members of the Task Force effective immediately, and ending July 31, 2018. The Chief Justice may appoint additional members as may be necessary.

3. MEETINGS: Task Force meetings shall be scheduled at the discretion of the Chair. All meetings shall comply with the Arizona Code of Judicial Administration § 1-202: Public Meetings.

4. STAFF: The Administrative Office of the Courts shall provide staff for the Task Force and shall assist the Task Force in developing recommendations and preparing any necessary reports and petitions.

Dated this 6th day of December, 2016.

_____

SCOTT BALES
Chief Justice

Attachment: Appendix A

Appendix A

Membership List
Task Force on Court Management of Digital Evidence

Chair

Vice Chief Judge Samuel A. Thumma
Arizona Court of Appeals, Division One

Members

Mike Baumstark
Deputy Administrative Director
Arizona Supreme Court
Administrative Office of the Courts

David Bodney, Partner
Ballard Spahr

Judge Kyle Bryson
Presiding Judge
Superior Court in Pima County

Colleen Clase
Senior Counsel
Arizona Voice for Crime Victims

Jessica Cortes
Court Administrator
City of Flagstaff Municipal Court

Judge David Cunanan
Superior Court in Maricopa County

Karen Emmerson
Deputy Public Defender
Maricopa County

Judge Maria Felix
Justice of the Peace
Pima County Consolidated Court

Jeff Fine
Justice Court Administrator
Maricopa County Justice Courts

Jennifer Garcia
Assistant Federal Defender
Federal Public Defender
District of Arizona

Judge Charles Gurtler
Presiding Judge
Mohave County Superior Court

Aaron Harder
Bureau Chief - Vehicular Crimes
Maricopa County Attorney's Office

Hon. Michael Jeanes
Clerk of Court
Superior Court in Maricopa County

Michael Kurtenbach
Executive Assistant Chief
Community Services Division
City of Phoenix Police Department

Zora Manjencich
Assistant Attorney General
Office of the Attorney General

James Melendres, Partner
Snell &Wilmer

Michael Mitchell
Special Assistant to the Chief Deputy
Maricopa County Attorney's Office

Jamie Sheppard
Senior Project Manager
E-Discovery Services & Strategy
Perkins Coie

Lt. Col. Heston Silbert
Deputy Director
Department of Public Safety

Judge Don Taylor
Chief Presiding Judge
City of Phoenix Municipal Court

IN THE SUPREME COURT OF THE STATE OF ARIZONA

In the Matter of:	)	
	)	
APPOINTMENT OF MEMBERS TO THE TASK FORCE ON COURT MANAGEMENT OF DIGITAL EVIDENCE	)	Administrative Order No. 2017 - 27 (Affecting Administrative Order No. 2016-129)

Administrative Order No. 2016-129 established the Task Force on Court Management of Digital Evidence. The Order provides that the Chief Justice may appoint additional members as may be necessary. Therefore, after due consideration,

IT IS ORDERED that Inspector William Long, Department of Public Safety, and Laura Keller, Arizona State Library, Archives and Public Records, be appointed as members of the Task Force on Court Management of Digital Evidence for a term beginning upon signature of this Order, and ending July 31, 2018.

Dated this 9th day of March, 2017.

SCOTT BALES
Chief Justice

APPENDIX B-Arizona Code of Judicial Administration § 1-504

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-504: Electronic Reproduction and Imaging of Court Records

A. Definitions. In this section, the following definitions apply:

"ANSI/AIIM" means the American National Standards Institute and the Association for Information and Image Management. These two organizations are responsible for promoting and facilitating voluntary consensus standards and conformity assessment systems and promoting their integrity.

"Archival" means that point in the electronic document management process when the subject matter (for example, a case) associated with a document is no longer subject to modification, related documents are purged and the long-term or permanent copy of the document is created and maintained so as to reasonably ensure its preservation according to approved records retention schedules.

"Backward compatible" means that a document storage system is compatible with earlier models or versions of the same product. Software is backward compatible if it can use files and data created with an older version of the same software program. Hardware is backward compatible if it can run the same software as the previous model.

"Consultative Committee on International Telegraphy and Telephony" (CCITT) means an organization that sets international communications standards.

"Electronic Document Management System" (EDMS) means a collection of computer software application programs and hardware devices that provide a means of organizing and controlling the creation, management and retrieval of documents through their life cycle. It may include workflow software which enables organizations to define routing and processing schemes to automate the business processes for document handling. It may also include imaging and optical character recognition (OCR) software and devices to support the capture, storage, and retrieval of document images from paper ("imaging").

"Electronic record" means any record that requires the aid of a computer to read the record.

"Imaging" means the process of creating electronic copies by electronically photographing a document, photograph, color slide or other material using a scanner. Scanners record images digitally rather than on paper or film.

"Imaging system" means the collection of computer software application programs and hardware devices that provides a means to capture, store, and retrieve document images from paper. An imaging system is often a part of an EDMS.

"Index" means descriptive locator information about a digital document that allows the user to accurately identify it on electronic storage media. An index in an EDMS is an electronic file distinct from

the collection of documents it catalogues. The act of providing the descriptive locator information is referred to as "indexing." For example, a document might be "indexed" by its case number, party names, document type and date filed.

"Media" means physical devices for storing data and images. It includes write once/read many (WORM) compact discs, compact disc-read only memory (CD-ROM), and digital video disc (DVD).

"Metadata" means descriptive information about a document that is not displayed within the viewable content of the document but is an inherent part of the document. Document management systems rely on metadata for search indexes.

"Migration" means the process of upgrading to new technologies while preserving accessibility to existing records. It includes translating one electronic data format to another when a new computer or data management system is incompatible with the existing system. It also means the process of moving electronic data from one storage device or media to another.

"Non-proprietary" means material (particularly software) that is not subject to ownership and control by a third party. "Proprietary," on the other hand, generally refers to vendor-owned material whose specifications are not public.

"Open system standard" means a published and commonly available interface specification that describes services provided by a software product. As a result, the specification is available to anyone and evolves through a consensus process that is open to the entire industry.

"Pixel" means picture element and is the smallest element of a display surface that can be independently assigned color or intensity. The number of pixels determines the sharpness or clarity of an image and in imaging is often expressed in dots per inch (dpi).

"Records" means the electronic or imaged documents and files in an EDMS.

"Refresh" means the copying of an image or a whole storage medium for the purpose of preserving or enhancing the quality of the images.

"Reproduction" means the process of making an identical copy from an existing document on the same or different media.

"Structured query language" (SQL) means a standardized query language for requesting information from a database.

"Tagged image file format" (TIFF) means a format for storing images on computers. It includes a standardized header or tag that defines the exact data structure of the associated image.

B. Applicability. These standards shall apply to all records imaged by courts, including the methods used to electronically reproduce or create records and also the methods and formats used to electronically store, archive and reproduce records for the purpose of maintenance and preservation.

C. General Requirements

1 Courts shall use the Commission on Technology-approved EDMS or one approved by COT as an exception. Exception EDMSs shall not employ proprietary designs, formats, software or media or require use of non–standard devices to access records.

2. Courts shall employ indexing procedures and security procedures that prevent unauthorized modification or deletion of records.

3. Courts shall establish written procedures to ensure imaged records accurately replicate the source document.

D. Imaging and Indexing Requirements

1. The imaging system shall output Portable Document Format (PDF) or TIFF.

2. The imaging system shall support scanning densities of 200 to 600 pixels (dots) per inch or higher.

3. Scanning quality must adhere to the standards presented in *Recommended Practices for Quality Control of Image Scanners* (ANSI/AIIM MS44-1988 (R1993)).

4. The imaging system must support the current CCITT image compression/decompression Group 3 or Group 4 techniques without proprietary alterations to the algorithm. If the use of a proprietary compression algorithm is unavoidable, the system must provide a gateway to either Group 3 or Group 4 standards (or to a compression standard subsequently adopted by ANSI/AIIM).

5. The imaging system shall use standard relational database technology to store the index and provide access using ANSI SQL.

6. Image processing procedures shall include population of an index as well as an index entry verification step, to ensure that each image is easily and accurately retrievable.

7. Image processing procedures shall include a quality assurance step to ensure each scanned image contains high fidelity to the paper original. Documents that become unreadable as a result of the scanning process shall be re-scanned immediately.

8. The indexing process shall also identify documents which are subject to approved criteria for purging in ACJA § 3-402 prior to performing any conversion to a permanent archival format.

9. Courts shall meet the requirements of ACJA § 1-507 prior to destroying any paper document associated with an image.

E. Accessibility. Courts shall ensure that the public is afforded reasonable access to records, consistent with Supreme Court Rule 123 via the public access portal managed by the Administrative Office of the Courts, at a minimum. Courts shall ensure that records that are sealed or confidential by rule or law contain appropriate metadata to enable any EDMS in which they reside to protect them from inappropriate access.

F. Migration Requirements for Courts Having Standalone or Exception EDMSs

1. Courts shall ensure accessibility with a planned migration path so devices, media and technologies used to store and retrieve records are not allowed to become obsolete and are promptly replaced or upgraded.

2. Courts shall ensure that any new equipment or software for an existing imaging system is backward compatible and shall obtain a vendor certification that the system will

convert 100% of the image and index data to the new system so access to existing records is never impeded.

3. Courts shall periodically refresh electronic images in order to ensure their accessibility for as long as the applicable record retention schedules require. These procedures may require recopying of images to new media.

G. Retention and Storage Requirements

1. All media used for storing records must comply with accepted computer industry standards.

2. The manufacturer's recommendation for storage and use of storage media shall dictate the criteria for storing and using such media.

3. Courts shall annually inspect and test a random sampling of media used for storing records to verify its good condition.

4. Courts shall use only non-reusable media for storing records for archival purposes.

5. Courts shall ensure that records generated by or received for the courts are preserved in accordance with the applicable records retention schedules and security requirements.

H. Disconnected Scanning Requirements for Limited Jurisdiction Courts

1. Courts shall complete the necessary index and quality assurance steps, including verification of each document's legibility and appropriateness of metadata, required to commit the scanned document to the central EDMS maintained by the AOC.

2. Courts shall change the case status code for each active case that becomes subject to no further action to "Completed" within any case management system that is integrated with the central EDMS maintained by the AOC.

3. Courts shall use the AOC's designated event code when scanning closed records for archival purposes on the central EDMS maintained by the AOC. All documents associated with a closed case in a limited jurisdiction court shall be scanned as a single, multi-image file.

Adopted by Administrative Order 2001-11 effective January 11, 2001. Amended by Administrative Order 2012-05, effective January 11, 2012.

APPENDIX C-Arizona Code of Judicial Administration § 1-506

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-506: Filing and Management of Electronic Court Documents

A. Definitions. In this section the following definitions apply:

"Browser" means a computer application that interprets hypertext markup language (HTML), the programming language of the Internet, into the words and graphics that are viewed on a web page.

"Electronic document management system (EDMS)" means a collection of computer software application programs and hardware devices that provides a means of organizing and controlling the creation, management and retrieval of documents through their life cycle. It may include workflow software which enables organizations to define routing and processing schemes to automate the business processes for document handling. It may also include imaging and optical character recognition (OCR) software and devices to support the capture, storage, and retrieval of document images from paper ("imaging").

"Electronic filing (e-Filing) system" means a collection of software application programs used to transmit documents and other court information to the court through an electronic medium, rather than on paper, most notably AZTurboCourt, but including local pilot systems being superseded by AZTurboCourt. An electronic filing system includes functions to send and review filings, pay filing fees, and receive court notices and information.

"Graphics document" means a picture or image (even of text) processed by a computer only as a single entity. Graphics files are not searchable by computers.

"IEC" means the International Electrotechnical Commission, an international organization that sets standards for electronics, headquartered in Geneva, Switzerland.

"ISO" means the International Organization for Standardization, a network of the national standards institutes of more than 150 countries coordinated by a central secretariat.

"Non-proprietary" means material (particularly software) that is not subject to ownership and control by a third party. "Proprietary" generally refers to vendor-owned material whose specifications are not public.

"Render" means to convert digital data from an image or text file to the required format for display or printing.

"Text-based document" means a collection of characters or symbols that can be individually manipulated but are processed collectively to comprise a document. Text-based documents are searchable by computers.

B. Purpose. This section provides administrative requirements, standards and guidelines to enable Arizona courts to implement a uniform, statewide, electronic filing system and to achieve the

reliable, electronic exchange of documents within the court system as well as between the court and court users.

C. Authority. Consistent with Rule 124, Rules of the Supreme Court of Arizona and related administrative orders, electronic filing is authorized as part of a uniform, statewide approach. All pre-existing, local electronic filing systems shall be transitioned into the statewide system, AZTurboCourt, using a timetable ordered by the supreme court in specific administrative orders.

D. Document Specifications. Documents filed or delivered electronically shall comply with the following:

1. All documents shall be preserved so that the content of the original document is rendered without any material alteration.

2. Text-based documents shall be in a format that provides for browser accessibility and high fidelity to the original and should be searchable. Documents shall be formatted in either:

   a. PDF (Portable Document Format) version 2.x or higher;

   b. Open Document Format for Office Applications, ISO/IEC 26300:2006 or subsequent; or

   c. Open Office XML (OOXML), ISO/IEC 29500-1, -2, -3, -4:2008, or subsequent.

3. Hyperlinks to static, textual information or documents may be included within a document solely for the convenience of judicial officers, attorneys, and pro se litigants. Materials accessed via hyperlinks are not part of the original record since they could become unavailable during the retention period of the document.

4. Bookmarks are allowed in documents. A bookmark shall only be used to direct the reader to another page within the same document. When multiple documents are contained within a single submittal, a separate bookmarked entry for each appended document shall be included in a table of contents.

5. Graphics, multimedia and other non-text documents may be permitted as follows:

   a. Documents in imaged or graphic formats (for example, pictures or maps) shall be in a non-proprietary file format (for example, TIFF, GIF, or JPEG) and shall comply with ACJA § 1-504.

   b. Other multimedia files (for example, video or audio files) shall adhere to established industry standards and shall be in a non-proprietary format (for example, MPEG, AVI, and WAV).

6. E-mail communications may be used for receipt, confirmation, and notification correspondence.

7. An electronic filing system, such as AZTurboCourt, may provide fill-in forms for routine matters. Courts may accept electronically-filed Arizona traffic ticket and complaint forms from law enforcement agencies or affidavit of service forms from process servers. The forms-based electronic filing system shall be capable of reproducing or printing the form with the data supplied by the filer, however, courts are not required

to preserve the form's text and data together in PDF. The forms-based electronic filing system shall comply with all other requirements of this section.

8. In accordance with Supreme Court Rule 124 and related administrative orders, electronic, case-related documents shall be submitted exclusively through the statewide electronic filing portal, AZTurboCourt.gov.

E. Authentication.

1. Authentication of document source. AZTurboCourt shall contain a registration system having sufficient security to verify and authenticate the source of electronically filed documents and maintain current contact information for filers.

2. Authentication of documents. AZTurboCourt shall indicate the date and time when submittal of each electronic filing occurred.

3. Maintenance of electronic documents. Any individual court maintaining electronic records shall employ local security procedures that prevent unauthorized access to, modification of, or deletion of the records. These procedures shall include all of the following:

   a. Establishing written procedures to ensure the integrity of electronic documents, so that any copies produced may be regarded as true and correct copies of the original document;

   b. Performing virus checking to ensure documents are free from viruses prior to storage on any device attached to the court's data network;

   c. Employing procedures that insure the availability of at least one other copy of the electronically filed document at all times;

   d. Performing system backups at least daily;

   e. Using recording media for storing electronic records that comply with industry standards; and

   f. Using non-reusable media for archiving court records electronically.

   Courts placing case documents in an EDMS controlled by the AOC meet the above maintenance requirements.

4. Filing of confidential and sealed documents. Courts shall employ standard keywords or metadata, as determined by the Commission on Technology's Technical Advisory Council, with associated security procedures to protect electronically filed or scanned confidential and sealed documents from unauthorized access.

F. Communications. The statewide electronic filing system shall:

1. Provide for electronic filing via the Internet and

2. Provide for appropriate party, attorney, arbitrator, public, and governmental entity access, in accordance with Supreme Court Rule 123, using standard browser technology.

G. Processing.

1. The statewide electronic filing system shall generate an acknowledgment receipt for electronically filed documents.

2. All case management and document management systems used by courts shall have automated interfaces with the statewide electronic filing system that will:

    a. Provide and validate case management data;

    b. Automatically docket e-filed documents; and

    c. Automatically index documents as required for locating the document and facilitating integration with the case and document management systems. Indexing elements shall include, at a minimum:

        (1) Full case number;

        (2) Document storage identifier;

        (3) Restricted security indicator; and

        (4) Sealed security indicator.

3. The official court record shall be the one stored by the clerk's or court's EDMS, whether in native electronic format or scanned into the system from paper. Unless otherwise directed by the Supreme Court, each standalone EDMS shall communicate case-related documents stored locally to the AOC's central document repository and receive documents from the statewide electronic filing system, prior to implementing electronic filing in the court.

    a. Each court imaging paper documents shall comply with ACJA § 1-504 (C) and (D) to ensure usefulness of those documents for public access.

    b. Each court having or implementing an EDMS shall coordinate the transfer of case-related electronic documents to and from the AOC's central document repository and electronic filing portal, respectively.

H. Periodic Review. These requirements are designed to be flexible to allow for technical innovations and shall be reviewed biennially by the Commission on Technology and updated to adapt to technological changes or changes in e-filing strategy.

Adopted by Administrative Order 2001-116 effective December 7, 2001. Amended by Administrative Order 2012-06, effective January 11, 2012.

APPENDIX D-Arizona Code of Judicial Administration § 1-507

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 5: Automation
Section 1-507: Protection of Electronic Records in Paperless Court Operations

A. Definitions. In this section, the definitions set out in section 1-504 apply. In addition:

"Administrative record" means any record created or received by a court that does not pertain to a particular case or controversy filed with a court. Administrative records include any record maintained by any board, committee, commission, council, or regulatory body, including records of the regulation and discipline of attorneys.

"Case management system" (CMS) means the information system that captures, maintains and provides access to data related to court cases over time, enabling systematic control of records through their lifecycle. It is often connected to a document management system that stores case-related documents electronically.

"Case record" means any record pertaining to a particular case or controversy.

"Closed case" means any case file record that is no longer subject to modification.

"Courts" means courts or clerks of court.

"Electronic record" means any record that requires the aid of a computer to be read, including imaged documents and files, whether stored in an EDMS or a CMS.

"Electronic Archive" means an electronic document repository consisting of imaged or e-filed documents associated only with closed cases.

"Offsite" means a temperature-controlled storage location physically located sufficient distance away from the main storage environment that an adverse event that affects the one does not affect the other.

"Online" means the storage of digital data on magnetic disks (such as hard drives) to make it directly and quickly accessible on the network using the application associated with the data.

"RAID" means Redundant Array of Independent Disks, a data storage system made of two or more ordinary hard disks and a special disk controller. Various RAID levels exist including RAID 1 which mirrors disks for fault tolerance and RAID 5 which stripes a set of disks for increased performance with fault tolerance.

"Regulatory case record" means any record that pertains to the regulation of a particular professional or business registered, licensed or certified pursuant to rules adopted by the supreme court.

"Storage" means a permanent repository for holding digital data that retains its content until purposely erased, even when electrical power is removed.

B. Applicability. This section is applicable

to electronic case records, administrative records and regulatory case records in the custody of judicial entities in Arizona, as defined by Supreme Court Rule 123.

C. Purpose. This section provides minimum technical and document management prerequisites for destruction of paper records for which equivalent electronic records exist.

D. Requirements Applicable to Case Records.

1. General Requirements.

    a. Courts shall not create or store electronic records using systems that employ proprietary designs, formats, software, or media or that require use of non-standard devices to access records, in accordance with ACJA § 1-504(C)(1).

    b. Courts shall preserve all electronic documents so that the content of the original document is not altered in any way and the appearance of the document when displayed or printed closely resembles the original paper without any material alteration, in accordance with ACJA § 1-506(D)(1).

    c. Courts shall preserve evidence and fingerprints in their submitted format – hardcopy items shall not be converted to electronic records for the purpose of storage and electronically submitted items shall not be converted to hardcopy for the purpose of storage.

    d. Printouts of electronic records shall be provided to other courts, as needed, unless arrangements have been made for those courts to receive electronic documents in lieu of paper.

2. Document Management Requirements.

    a. Courts shall use an electronic document management system (EDMS) that complies with ACJA § 1-505, or be granted an exception by Commission on Technology to use a non-conforming system.

    b. The EDMS application shall reside on two physically separate servers each using separate internal storage, structured query language (SQL) databases, and backup software. Log shipping shall be employed not less than daily to maintain synchronization of the two EDMSs for disaster recovery.

    c. At least six months of full-time production use of an EDMS is required before a court may request authorization to begin destroying the paper records corresponding to electronic records stored on the system, as required by subsection (F) of this section.

3. Storage Requirements.

    a. Courts shall maintain primary and secondary copies of records online at all times using at least two physically separate storage arrays configured to assure the failure of a single component of the array will not impact the integrity of the

data. New records shall be written simultaneously to all disk arrays.

b. Primary and secondary storage shall be attached only to servers having redundant power supplies, network interface cards, and controller cards or to virtual servers having automatic failover hosts. Use of personal computers containing extra hard drives or attached storage devices is prohibited.

c. Courts shall use redundant network paths to connect workstations and imaging devices to EDMS application servers.

d. Courts shall employ uninterruptable power supplies and software that ensure a controlled shutdown of servers after batteries have been in use for at least five minutes.

e. Courts shall store a tertiary copy of records on highly-secured backup media. The tertiary copy shall only be accessed through a gateway technology that prevents direct access to the storage media from the system(s) being backed up. Manufacturer's usage specifications and backup system media replacement guidelines shall be followed at all times, in accordance with ACJA § 1-504(G)(2).

f. Backup media shall be stored in a secure, environmentally controlled, offsite location and retained a minimum of 28 days offsite before reuse. Full backups shall be made not less than weekly and retained a minimum of 28 days offsite before reuse.

g. Backup and restoration procedures shall be documented and tested for effectiveness.

h. Scanned records shall appear on the backup media as well as primary and secondary storage before corresponding paper is destroyed.

4. Imaging and Indexing Requirements.

   a. Scanning quality must comply with *Recommended Practices for Quality Control of Image Scanners* (ANSI/AIIM MS44-1988 (R1993)), in accordance with ACJA § 1-504(D)(3).

   b. The EDMS shall be integrated with the CMS or the following categories of metadata (as a minimum) shall be recorded in the EDMS:

      - Case number (including type code),
      - Party names,
      - Standard document type identifier,
      - Date of filing, and,
      - Citing agency number,

      where applicable.

   c. Index entries shall be verified to ensure records are accurately retrieved prior to destruction of any corresponding paper originals. Un-retrievable records shall be rescanned and re-indexed until they prove to be accurately

retrieved from the EDMS.

5. Support and Maintenance Requirements.

   a. Court personnel or contractors must be certified in the following areas required to proficiently operate and maintain the records management system:

      (1) Microsoft Certified Systems Administrator
      (2) Microsoft Certified Database Administrator
      (3) OnBase Certified Advanced System Administrator or equivalent for any approved, non-conforming EDMS.

   b. When any system outage occurs, all records must be available not later than the end of the following business day. If lost, redundancy must be re-established as quickly as is practicable, even if records remain fully available in the non-redundant state.

   c. Records generated by or received by courts shall be preserved in accordance with the applicable records retention schedule. Case records required to be submitted to Arizona State Library, Archives, and Public Records (ASLAPR) shall meet the submittal requirements specified by ASLAPR at the time of submittal, regardless of storage medium. Records destruction is subject to the notification requirements of ASLAPR.

   d. In accordance with ACJA § 1-504(F)(3), courts shall periodically refresh electronic records in order to ensure their accessibility for as long as the applicable records retention schedule requires. Refresh procedures may require recopying of files to new media or storage arrays over time.

   e. Courts shall ensure continued accessibility via a planned migration path so devices, media, and technologies used to store and retrieve records are not allowed to become obsolete and are promptly replaced or upgraded, in accordance with ACJA § 1-504(F)(1).

   f. Courts shall ensure that any new equipment or software replacing that used in an existing system is backward compatible and shall obtain a vendor certification that the system will convert 100 percent of the images and index data to the new system so access to existing electronic records is never impeded, in accordance with ACJA § 1-504(F)(2).

E. Requirements Applicable to Administrative and Regulatory Case Records. Requirements applicable to case records apply to administrative and regulatory case records with the following modifications.

1. The EDMS application may reside on one server, rather than two separate servers.

2. Copies of the records may be limited to one primary copy and one backup copy. The primary copy of all electronic records shall be maintained

online at all times using at least one RAID Level 5 disk or storage array.

3. The server on which the EDMS application and records reside shall, at a minimum, be attached to or contain magnetic storage in a RAID Level 1 configuration.

4. Servers used for an electronic archive shall be installed in a rack or other fixture located in a secure, environmentally controlled area.

5. The backup copy of the records shall be stored on highly-secured backup media. The tertiary copy shall only be accessed through a gateway technology that prevents direct access to the storage media from the system(s) being backed up. Manufacturer's usage specifications and backup system media replacement guidelines shall be followed at all times, in accordance with ACJA § 1-504(G)(2).

6. A daily, incremental backup of the primary copy of records added to the archive shall be made using automated backup software.

7. When any system outage occurs, all records must be available not later than the end of the tenth business day.

F. Authorization to Destroy Paper Case Records. Any court desiring to implement a paperless case record operation shall obtain advance written approval of its operational policies and EDMS infrastructure as described herein from the Administrative Office of the Courts (AOC). The AOC shall provide a form for courts to use to request approval. The form shall include a checklist of audit criteria for electronic records management practices and infrastructure.

1. Courts not using an EDMS on the effective date of this section shall complete and submit a written notice of intent to comply with the requirements of this section prior to purchasing an electronic records management system. The court shall submit the AOC request form after not less than six months of full-time production use of an EDMS.

2. Courts already using an EDMS on the effective date of this section shall submit the AOC request form and indicate the date on which full-scale production use of the installed EDMS commenced.

3. The presiding judge of the county, presiding judge of the court, and, elected clerk of court, if any, shall sign the AOC request form prior to submittal to the AOC.

4. The AOC shall formally review each request, working with court representatives to ensure that all requirements of this section are satisfied and electronic records are adequately safeguarded.

5. The AOC shall notify the court in writing of the authorization to destroy paper records. The authorization shall contain an effective date and a reminder of the audit criteria.

6. Court operational review evaluations shall include management of electronic records at courts granted authority to

destroy paper records.

7. Authorization is not needed to destroy paper case records maintained in the central document repository supported by the AOC or other document repository approved by the Arizona Judicial Council or the Commission on Technology, provided the court complies with subsections (D)(1)(c)&(d), (D)(4)(b)&(c), and (D)(5)(c) of this section and all related operational requirements of ACJA §§ 1-504 and 1-506.

G. Authorization to Destroy Paper Administrative and Regulatory Case Records. The presiding judge of the county is authorized to approve destruction of paper administrative and regulatory case records maintained by the courts under the presiding judge's supervision. The administrative director is authorized to approve destruction of paper administrative and regulatory case records maintained by the AOC. They shall ensure that the applicable standards and protocols established by subsection (E) have been met before approving destruction of paper records. Superior court clerks who meet the requirements of subsection (E) are authorized to destroy the paper administrative and regulatory records they maintain without prior approval of the presiding judge.

H. Electronic Archives of Closed Cases in Limited Jurisdiction Courts. Justice and municipal courts that wish to create an electronic archive of closed case files and destroy the corresponding paper records prior to the applicable retention and destruction date shall meet all standards and protocols established by this section, with the following modifications:

1. Copies of the archived records can be limited to one primary copy and one backup copy. The primary copy of all electronic records in the archive shall be maintained online at all times using at least one RAID Level 5 disk or storage array.

2. The EDMS application, SQL database, and backup software for the archive may reside on internal magnetic storage in a RAID Level 1 configuration, if these applications are not stored on the RAID Level 5 disk or storage array.

3. Servers used for an electronic archive shall be installed in a rack or other fixture located in a secure, environmentally controlled area.

4. The backup copy of the archive shall meet the requirements of subsection (D)(3)(e).

5. A daily, incremental backup of the primary copy of records added to the archive shall be made using automated backup software.

6. Courts are not required to comply with subsection (D)(3)(c).

7. When any system outage occurs, all archived records must be available not later than the end of the fifth business day.

Adopted by Administrative Order 2008-99, effective December 10, 2008. Amended by Administrative Order 2012-07, effective January 11, 2012. Amended by Administrative Order 2016-113, effective November 2, 2016.

APPENDIX E-Arizona Code of Judicial Administration § 1-604

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 6: Records
Section 1-604: Remote Electronic Access to Case Records

A. Purpose. Rule 123, Rules of the Supreme Court of Arizona ("Rule 123") authorizes courts to provide remote electronic access to case records. This code section sets forth the procedure for providing that access. The public's right of access to all non-sealed, non-confidential case records at a court facility, whether in paper or electronic format, shall not be limited by this section.

B. Definitions. In addition to the definitions found in Rule 123, the following definitions apply to this section.

"Authentication" means the security measures designed to verify a person's identity or authority to receive a specific category of remote electronic access to case records pursuant to Rule 123, Rules of the Supreme Court of Arizona.

"Registration" means the act of enrolling to receive remote electronic access to case records.

C. Remote Electronic Access to Case Records.

1. Access. Remote electronic access to case records in the judiciary is governed by Rule 123, this section, and all other applicable rules and laws.
2. Registration and Authentication.

   a. Registration is required for remote electronic access to case records other than the records identified in Rule 123(g)(1)(D)(ii). The following information must be provided by the potential registrant:

   (1) Attorneys, including attorney arbitrators, must provide their name; address; e-mail address; telephone number; date of birth; bar number or pro hoc vice number; bar number state; firm or agency name; credit card type, number, security code, and expiration date; username and password; and any additional information as determined by the supreme court.
   (2) Parties, non-attorney arbitrators, and general public users must provide their name; address; e-mail address; telephone number; date of birth; either Arizona driver license number or nonoperating identification license number; credit card type, number, security code, and expiration date; username and password; and any additional information as determined by the supreme court.

   b. Authentication of a potential registrant for remote electronic access to case records is required.

Authentication shall be carried out by the court submitting the potential registrant's name and Arizona driver license number or nonoperating identification license number to the Arizona Motor Vehicle Division (MVD), or by providing another acceptable form of identification, as determined by the supreme court, when both an Arizona driver license and nonoperating identification license are unavailable.

c. All information provided by a potential user for authentication and registration shall be closed to the public.

d. Remote access by government entities or public purpose organizations shall be governed by Rule 123(g)(1)(B).

3. User Agreement. All users shall accept a User Agreement in a form determined by the supreme court before remote electronic access to case records is granted.

4. Fees and Revenue for Remote Electronic Access.

a. The fee to print case records from a public terminal at a court facility shall be the same as for a copy of a paper record as provided in A.R.S. §§ 12-119.01, 12-120.31, 12-284, 22-281, and 22-404.

b. In accordance with Rule 123(g), the Arizona Judicial Council ("Council") shall periodically make recommendations to the supreme court with regard to the establishment of fees and disbursement of revenue generated for remote electronic access to case records.

(1) The Commission on Technology shall make recommendations to the Council on all matters pertaining to the establishment of fees and disbursement of revenue.
(2) Recommended fees for remote electronic access to case records shall be in an amount that allows development, implementation, maintenance, and enhancement of the remote electronic access to case records system.
(3) To assist the Council in recommending fees and disbursing revenue, upon request, a court shall submit the percentage of cost and comparable dollar amount incurred by the court associated with the supreme court's remote electronic access to case records system.

c. Any revenue generated by the fees for remote electronic access to case records shall be disbursed to each court that incurs the cost of operating a system for remote electronic access to case records based on the volume of requests for records of those courts. Monies received under this paragraph shall be deposited as described below:

(1) A division of the court of appeals shall deposit all monies received under this paragraph pursuant to A.R.S. §

12-120.31.

(2) A superior court shall send all monies received under this paragraph to the county treasurer for deposit in the clerk's document storage and retrieval conversion fund established by A.R.S. § 12-284.01.

(3) A justice court shall send all monies received under this paragraph to the county treasurer for deposit in an account designated for improving access to justice court records, as provided in A.R.S. § 22-284.

(4) A municipal court shall send all monies received under this paragraph to the city treasurer for deposit in an account designated for improving access to municipal court records, as provided in A.R.S. § 22-408.

Adopted by Administrative Order 2009-132, effective January 1, 2010.

APPENDIX F-Arizona Code of Judicial Administration § 1-606

ARIZONA CODE OF JUDICIAL ADMINISTRATION
Part 1: Judicial Branch Administration
Chapter 6: Records
Section 1-606: Providing Case Record Access to Public Agencies or to Serve a Public Purpose

A. Purpose. This section establishes minimum standards for a custodian or the administrative director to follow in providing case records or data to federal, state, tribal, and local government agencies and private organizations, the objective of which is to serve a public purpose, such as criminal justice, child welfare, licensing, mental health treatment, or research for scholarly or governmental purposes.

In accordance with this section, the local court's custodian of case records or the administrative director may provide specialized access to case records or data that may exceed the access available to the general public provided by Rule 123. Access to case records or data provided under this section shall be limited to those records necessary for the recipient's intended purpose.

B. Applicability. This section applies to requests from public agencies and private organizations identified in subsection (A) for one-time, periodic, or on-going access to electronic or paper case records in bulk, which may include requests for access by remote electronic means or by an application-to-application transmission of records. This section does not apply to requests from persons or entities governed by ACJA § 1-605, nor does it apply to any requests for one-time access to case records on a case-by-case basis.

C. Record Access Agreement. Before providing access to case records or data under this section, the custodian shall execute a record access agreement with the recipient that identifies the records or data to be provided and permissible uses. The local court's records custodian shall execute a record access agreement for any access to the local court's case management system data. The administrative director shall execute a record access agreement for any access to the statewide repository of aggregated case management system data maintained by the Administrative Office of the Courts. No record access agreement is needed for sharing or exchange of case records with other courts established pursuant to Article VI, Section 1 of the Arizona Constitution or with the Administrative Office of the Courts.

The record access agreement shall include the following terms and conditions:

1. Recipient shall protect the records and data from unauthorized access and misuse.

2. Recipient shall ensure the security and confidentiality of any records or data provided by the custodian that are sealed or closed by Rule 123 or any other rule or law.

3. Recipient will not copy or re-disseminate any records or data closed

by Rule 123 other than for the stated purposes.

4. Recipient will not use the records or data to sell a product or service to an individual or the general public.

5. Recipient will inform its employees of the requirements imposed by applicable federal and state laws, rules, and terms of the record access agreement.

6. If requested by the individual who is the subject of a record, recipient will cooperate in correcting any inaccurate or incomplete records provided by the custodian.

7. A recipient will consult with the custodian prior to releasing any records or data provided under the record access agreement in response to a public records request.

8. Prior to merging any records or data obtained from the custodian with other records or data concerning an individual or organization, recipient will ensure there is sufficient identifying information to reasonably conclude that the record or data concerns the same individual or organization.

9. Recipient will notify the custodian of any record or data inaccuracies discovered by the recipient.

10. Recipient will permit the custodian to audit recipient's use of and access to the records or data provided.

11. The parties shall agree on how the records or data will be exchanged, and if done so electronically, the format, timing, and frequency of exchanges.

12. The parties shall agree on a change management process and allocation of responsibilities for ensuring any unilateral software modifications do not disrupt the on-going exchange of electronic case record information.

13. All applicable rules and laws pertaining to the release of the records and data have been disclosed by the parties.

D. Court Order. The custodian or administrative director shall not release confidential records unless ordered by a court.

Adopted by Administrative Order 2009-130, effective January 1, 2010. Amended by Administrative Order 2011-92, effective August 31, 2011.

APPENDIX G— Proposed Amendments to the Arizona Rules of Evidence

Rule 1001. Definitions That Apply to This Article
In this article:
(a) A "writing" consists of letters, words, numbers, or their equivalent set down in any form.
(b) A "recording" consists of letters, words, numbers, or their equivalent recorded in any manner.
(c) A "photograph" means a photographic image or its equivalent stored in any form.
(d) A "video" is an electronic visual medium for the recording, copying, playback, broadcasting, or displaying of audio or moving images.
~~(d)~~(e) An "original" of a writing, ~~or~~ recording, or video means the writing, ~~or~~ recording, or video itself or any counterpart intended to have the same effect by the person who executed, ~~or~~ issued, or created it. For electronically stored information, "original" means any printout--or other output ~~readable~~ perceived by sight--if it accurately reflects the information. An "original" of a photograph includes the negative or a print from it.
~~(e)~~(f) A "duplicate" means a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original.

Rule 1002. Requirement of the Original
An original writing, recording, or photograph, or video is required in order to prove its content unless these rules or an applicable statute provides otherwise.

Rule 1004. Admissibility of Other Evidence of Contents
An original is not required and other evidence of the content of a writing, recording, ~~or~~ photograph, or video is admissible if:
(a) all the originals are lost or destroyed, and not by the proponent acting in bad faith;
(b) an original cannot be obtained by any available judicial process;
(c) the party against whom the original would be offered had control of the original; was at that time put on notice, by pleadings or otherwise, that the original would be a subject of proof at the trial or hearing; and fails to produce it at the trial or hearing; or
(d) the writing, recording, ~~or~~ photograph, or video is not closely related to a controlling issue.

Rule 1006. Summaries to Prove Content
The proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, ~~or~~ photographs, or video that cannot be conveniently examined in court. The proponent must make the originals or duplicates available for examination or copying, or

both, by other parties at a reasonable time and place. And the court may order the proponent to produce them in court.

Rule 1008. Functions of the Court and Jury

Ordinarily, the court determines whether the proponent has fulfilled the factual conditions for admitting other evidence of the content of a writing, recording, or photograph under Rule 1004 or 1005. But in a jury trial, the jury determines--in accordance with Rule 104(b)--any issue about whether:

(a) an asserted writing, recording, ~~or~~ photograph, or video ever existed;

(b) another one produced at the trial or hearing is the original; or

(c) other evidence of content accurately reflects the content.

APPENDIX H— Proposed Amendments to the Arizona Rules of Criminal Procedure

Pre-rule changes enacted through Arizona Supreme Court Order R-17-0002, filed August 31, 2017

Rule 15.1. Disclosure by State

. . .

b. Supplemental Disclosure; Scope. Except as provided by Rule 39(b), the prosecutor shall make available to the defendant the following material and information within the prosecutor's possession or control:
(1) The names and addresses of all persons whom the prosecutor intends to call as witnesses in the case-in-chief together with their relevant written or recorded statements,
(2) All statements of the defendant and of any person who will be tried with the defendant,
(3) All then existing original and supplemental reports prepared by a law enforcement agency in connection with the particular crime with which the defendant is charged,
(4) The names and addresses of experts who have personally examined a defendant or any evidence in the particular case, together with the results of physical examinations and of scientific tests, experiments or comparisons that have been completed,
(5) A list of all papers, documents, photographs, ~~or~~ tangible objects, and digital or electronic evidence that the prosecutor intends to use at trial or which were obtained from or purportedly belong to the defendant,
(6) A list of all prior felony convictions of the defendant which the prosecutor intends to use at trial,
(7) A list of all prior acts of the defendant which the prosecutor intends to use to prove motive, intent, or knowledge or otherwise use at trial
(8) All then existing material or information which tends to mitigate or negate the defendant's guilt as to the offense charged, or which would tend to reduce the defendant's punishment therefor.
(9) Whether there has been any electronic surveillance of any conversations to which the defendant was a party, or of the defendant's business or residence;
(10) Whether a search warrant has been executed in connection with the case;
(11) Whether the case has involved an informant, and, if so, the informant's identity, if the defendant is entitled to know either or both of these facts under Rule 15.4(b) (2).

. . .

i. Additional Disclosure in a Capital Case.

(1) The prosecutor, no later than 60 days after the arraignment in superior court, shall provide to the defendant notice of whether the prosecutor intends to seek the death penalty. This period may be extended up to 60 days upon written stipulation of counsel filed with the court. Once the stipulation is approved by the court, the case shall be considered a capital case for all administrative purposes including, but not limited to, scheduling, appointment of counsel under Rule 6.8, and assignment of a mitigation specialist. Additional extensions may be granted upon stipulation of the parties and approval of the court. The prosecutor shall confer with the victim prior to agreeing to an extension of the 60 day deadline or any additional extensions, if the victim has requested notice pursuant to A.R.S. Section 13-4405.

(2) If the prosecutor files notice of intent to seek the death penalty, the prosecutor shall at the same time provide the defendant with a list of aggravating circumstances the state will rely on at the aggravation hearing in seeking the death penalty.

(3) The prosecutor, no later than 30 days after filing a notice to seek the death penalty, shall provide to the defendant the following:

(a) The names and addresses of all persons whom the prosecutor intends to call as witnesses to support each identified aggravating circumstance at the aggravation hearing together with any written or recorded statements of the witness.

(b) The names and addresses of experts whom the prosecutor intends to call to support each identified aggravating circumstance at the aggravation hearing together with any written or recorded statements of the expert.

(c) A list of any and all papers, documents, photographs, ~~or~~ tangible objects, and digital or electronic evidence that the prosecutor intends to use to support each identified aggravating circumstance at the aggravation hearing.

(d) All material or information that might mitigate or negate the finding of an aggravating circumstance or mitigate the defendant's culpability.

(4) The trial court may enlarge the time or allow the notice required in Rule 15.1(i)(3) to be amended only upon a showing of good cause by the prosecution, or upon stipulation of counsel and approval of the court.

(5) Within 60 days of receipt of the disclosure required under Rule 15.2(h)(1), the prosecutor shall disclose to the defendant the following:

(a) The names and addresses of all persons whom the prosecutor intends to call as rebuttal witnesses on each identified aggravating circumstance together with any written or recorded statements of the witness.

(b) The names and addresses of all persons the state intends to call as witnesses at the penalty hearing together with any written or recorded statements of the witness.

(c) The names and addresses of experts who may be called at the penalty hearing together with any reports prepared by the expert.

(d) A list of any and all papers, documents, photographs ~~or~~ tangible objects, and digital or electronic evidence that the prosecutor intends to use during the aggravation and penalty hearings.

. . .
[remainder of rule remains unchanged]

Rule 15.2 Disclosure by Defendant

. . .

c. Disclosure by Defendant; Scope. Simultaneously with the notice of defenses submitted under Rule 15.2(b), the defendant shall make available to the prosecutor for examination and reproduction the following material and information known to the defendant to be in the possession or control of the defendant:

(1) The names and addresses of all persons, other than that of the defendant, whom the defendant intends to call as witnesses at trial, together with their relevant written or recorded statements;

(2) The names and addresses of experts whom the defendant intends to call at trial, together with the results of the defendant's physical examinations and of scientific tests, experiments or comparisons that have been completed; and

(3) A list of all papers, documents, photographs, ~~and~~ other tangible objects, and digital or electronic evidence that the defendant intends to use at trial.

. . .

h. Additional Disclosure in a Capital Case.

(1) Within 180 days after receiving the state's disclosure pursuant to Rule 15.1(i)(3), the defendant shall provide to the prosecutor:

(a) A list of all mitigating circumstances intended to be proved.

(b) The names and addresses of all persons, other than the defendant, whom the defendant intends to call as witnesses during the aggravation and penalty hearings, together with all written or recorded statements of the witnesses.

(c) The names and addresses of any experts whom the defendant intends to call during the aggravation and penalty hearings together with any reports prepared excluding the defendant's statements.

(d) A list of any and all papers, documents, photographs, ~~or~~ tangible objects, and digital or electronic evidence that the defendant intends to use during the aggravation and penalty hearings.

(2) The trial court may enlarge the time or allow the notice required in Rule 15.2(h)(1) to be amended only upon a showing of good cause by the defendant or upon stipulation of counsel and approval of the court.

(3) Within 60 days of receiving the state's supplemental disclosure pursuant to rule 15.1(i)(3), the defense shall disclose the names and addresses of any rebuttal witnesses, together with their written or recorded statements, and the names and addresses of any experts who may be called at the penalty hearing, together with any reports prepared by the experts.

APPENDIX I—Proposed Amendments to Arizona Rules of Family Law Procedure

Rule 49. Disclosure

. . .

I. Electronically Stored Information.
(1) Duty to Confer. When the existence of electronically stored information is disclosed or discovered, the parties must promptly confer and attempt to agree on matters relating to its disclosure and production, including:
a. requirements and limits on the disclosure and production of electronically stored information;
b. the form in which the information will be produced; and
c. if appropriate, sharing or shifting of costs incurred by the parties for disclosing and producing the information.
(2) Resolution of Disputes. If the parties are unable to satisfactorily resolve any dispute regarding electronically stored information and seek resolution from the court, they must present the dispute in a single joint motion. The joint motion must include the parties' positions and the separate certification of all counsel required under Rule 51(F). In resolving any dispute regarding electronically stored information, the court may shift costs if appropriate.
(3) Presumptive Form of Production. Unless the parties agree or the court orders otherwise, a party must produce electronically stored information in the form requested by the receiving party. If the receiving party does not specify a form, the producing party may produce the electronically stored information in native form or in another reasonably usable form that will enable the receiving party to have the same ability to access, search, and display the information as the producing party.

~~I.~~J. **Continuing Duty to Disclose.** The duty described in this rule shall be a continuing duty, and each party shall make additional or amended disclosures whenever new or different information is discovered or revealed. Such additional or amended disclosures shall be made not more than thirty (30) days after the information is revealed to or discovered by the disclosing party.

~~J.~~K. **Additional Discovery.** Nothing in the minimum requirements of this rule shall preclude relevant additional discovery on request by a party in a family law case, in which case further discovery may proceed as set forth in Rule 51.

APPENDIX J—Proposed Amendments to Arizona Rules of Protective Order Procedure

Rule 36. Admissible Evidence

…

(b) Reports, Documents, or Forms as Evidence. Any report, document, ~~or~~ standardized form, electronically stored information, or digital evidence required to be submitted to a court may be considered as evidence if either filed with the court or admitted into evidence by the court.

(c) Any digital evidence or electronically stored information may be considered as evidence if either filed with the court or admitted into evidence by the court.

APPENDIX K—Proposed Amendments to the Arizona Juvenile Court Rules

Rule 16. Discovery

. . .

B. Disclosure by the State.

1. Time Limits. Within ten (10) days of the advisory hearing, the prosecutor shall make available to the juvenile for examination and reproduction the following material and information within the prosecutor's possession or control:

a. The names and addresses of all persons whom the prosecutor will call as witnesses at the adjudication hearing together with their relevant written or recorded statements;

b. All statements of the juvenile and of any other juvenile for whom there is a companion adjudication hearing scheduled for the same time;

c. The names and addresses of experts who have personally examined the juvenile or any evidence in the particular case, together with the results of physical examinations and scientific tests, experiments or comparisons, including all written reports or statements made by an expert in connection with the particular case;

d. A list of all papers, documents, photographs, ~~or~~ tangible objects, and digital or electronic evidence which the prosecutor will use at the adjudication hearing, and upon further written request shall make available to the juvenile for examination, testing and reproduction any specified items contained in the list. The prosecutor may impose reasonable conditions, including an appropriate stipulation concerning chain of custody, to protect physical evidence produced under this section; and

e. All material or information which tends to mitigate or negate the juvenile's alleged delinquent conduct.

2. Prosecutor's Duty to Obtain Information. The prosecutor's obligation under this rule extends to material and information in the possession or control of members of the prosecutor's staff and of any other persons who have participated in the investigation or evaluation of the case and who are under the prosecutor's control.

3. Disclosure by Order of Court. Upon motion of the juvenile and a showing that the juvenile has substantial need for additional material or information not otherwise covered in these rules, the court may order any person to make the material or information available to the juvenile if the juvenile is unable, without undue hardship, to obtain the material or information or substantial equivalent by other means. The court may, upon the request of any person affected by the order, vacate or modify the order if compliance would be unreasonable or oppressive.

C. Disclosure by Juvenile.

1. Physical Evidence. The juvenile shall be entitled to the presence of counsel at the taking of evidence in connection with the allegations contained in the petition, as requested in writing by

the prosecutor, at any time after the filing of the petition. This rule shall supplement and not limit any other procedures established by law. The juvenile shall:

a. Appear in a line-up;
b. Speak for identification by witnesses;
c. Be fingerprinted, palmprinted, footprinted or voiceprinted;
d. Pose for photographs not involving re-enactment of an event;
e. Try on clothing;
f. Permit the taking of samples of hair, blood, saliva, urine or other specified materials which involve no unreasonable intrusions of the juvenile's body;
g. Provide handwriting samples; or
h. Submit to a reasonable physical or medical examination, provided such examination does not include a psychiatric or psychological examination.

2. Notice of Defenses/Witnesses. Within fifteen (15) days of the advisory hearing, the juvenile shall provide the prosecutor with written notice specifying all defenses which the juvenile will introduce at the hearing, including, but not limited to alibi, insanity, self-defense, entrapment, impotency, marriage, mistaken identity and good character. The notice shall specify for each defense the persons, including the juvenile, who will be called as witnesses at trial in support thereof. It may be signed by either the juvenile or the juvenile's counsel and shall be filed with the court.

3. Disclosures by Juvenile. Simultaneously with the filing of the notice of defenses/witnesses as required by this rule, the juvenile shall make available to the prosecutor for examination and reproduction:

a. The names and addresses of all persons, other than the juvenile, who will be called as witnesses at the adjudication hearing, together with all statements made by them in connection with the particular case;
b. The names and addresses of experts who will be called at the adjudication hearing, together with the results of physical examinations, scientific tests, experiments or comparisons, including all written reports and statements made by the expert in connection with the particular case; and
c. A list of all papers, documents, photographs, ~~and~~ other tangible objects, and digital or electronic evidence which the juvenile will use at the adjudication hearing.

4. Additional Disclosure upon Request. The juvenile, upon written request, shall make available to the prosecutor for examination, testing, and reproduction any item listed pursuant to this rule.

5. Extent of Juvenile's Duty to Obtain Information. The juvenile's obligation under this rule extends to material and information within the possession or control of the juvenile, the juvenile's attorneys and agents.

6. Disclosure by Order of the Court. Upon motion of the prosecutor, and a showing that the prosecutor has substantial need for additional material or information not otherwise covered in these rules, the court may order any person to make the material or information available to the prosecutor if the prosecutor is unable, without undue hardship, to obtain the material or information or substantial equivalent by other means and that disclosure thereof will not violate

the juvenile's constitutional rights. The court may, upon the request of any person affected by the order, vacate or modify the order if compliance would be unreasonable or oppressive.

. . .

Rule 44. Disclosure and Discovery

A. Scope of Disclosure. All information which is not privileged shall be disclosed. Disclosure shall be made in the least burdensome and most cost effective manner which shall include the inspection of materials, with or without copying. Disclosure shall include, but is not limited to the following:
1. Reports prepared by or at the request of any party;
2. Reports of any social service provider;
3. Foster Care Review Board and Court Appointed Special Advocate reports;
4. Transcripts of interviews and prior testimony;
5. Probation reports;
6. Photographs;
7. Physical evidence;
8. Digital evidence or electronically stored information;
9. ~~8.~~ Records of prior criminal convictions;
10. ~~9.~~ Medical and psychological records and reports;
11. ~~10.~~ Results of medical or other diagnostic tests; and
12. ~~11.~~ Any other information relevant to the proceedings.

. . . [remainder of Rule is unchanged]

Rule 73. Disclosure and Discovery

A. Scope of Disclosure. Disclosure shall include, but is not limited to the following:
1. Reports prepared by or at the request of any party;
2. Reports of any social service provider;
3. Foster Care Review Board and Court Appointed Special Advocate reports;
4. Transcripts of interviews and prior testimony;
5. Probation reports;
6. Photographs;
7. Physical evidence;
8. Digital evidence or electronically stored information;
9. ~~8.~~ Records of prior criminal convictions;
10. ~~9.~~ Medical and psychological records and reports;
11. ~~10.~~ Results of medical or other diagnostic tests; and
12. ~~11.~~ Any other information relevant to the proceedings.

. . . [remainder of Rule is unchanged]

APPENDIX L—Proposed Amendments to the Arizona Rules for Eviction Actions

Rule 10. Disclosure

a. Upon request, a party shall provide to the other party: 1) a copy of any lease agreement; 2) a list of witnesses and exhibits; 3) if nonpayment of rent is an issue, an accounting of charges and payments for the preceding six months; and 4) copies of any documents, digital evidence, or electronically stored information the party intends to introduce as an exhibit at trial.

[remainder of rule is unchanged]