WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 13, ISSUE 2 WINTER 2018

REPORT AND RECOMMENDATIONS OF THE ARIZONA TASK FORCE ON COURT MANAGEMENT OF DIGITAL EVIDENCE

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

Mike Baumstark
Deputy Administrative Director
Arizona 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 County 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
Superior Court in Mohave County

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

Honorable Michael Jeanes
Clerk of 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

Cite as: 13 Wash. J.L. Tech. & Arts 165 (2018)

http://digital.law.washington.edu/dspace-law/handle/1773.1/1788

ABSTRACT

The court record has three components, each historically paper-based and tangible: (1) filings; (2) transcripts; and (3) exhibits. Given technology changes, filings and transcripts now are often kept as digital files. Exhibits, however, continue to be received and held by the court in tangible form. Technology changes mean that will

soon change, and will change drastically.

The 2016 Joint Technology Committee Resource Bulletin: Managing Digital Evidence in Courts, warned that "[c]ourt 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." This article is the first published response to that urgent warning.

The article summarizes recommendations for court management of digital evidence. The article next discusses the evolving court record format and the truly digital evidence concept. Detailed workgroup reports follow, addressing: (1) digital formats; (2) storage and management; and (3) rules, including suggested rule changes. The article is designed to make sure this critical analysis is available now as well as to serve as a resource for courts, academics, technology experts, and others for years to come.

TABLE OF CONTENTS

INTRODUCTION

Arizona Supreme Court Chief Justice Scott Bales issued Administrative Order 2016-129, establishing the Arizona Task Force on Court Management of Digital Evidence (the "Task Force"), on December 6, 2016. The Task Force 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.[1] The Task Force was created 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

[1] *See*, *e.g.*, JOINT TECHNOLOGY COMMITTEE, JTC RESOURCE BULL.: MANAGING DIGITAL EVIDENCE IN COURTS, at ii (2016) [hereinafter JTC RESOURCE BULL.] (noting "exponential increase in the quantity of digital evidence"); *id.* at 3 (noting "explosion of digital video evidence. . . . The submission and use of digital evidence of all kinds in state and local courts has surged over the last few years."); Press Release, Mayor's Press Office, Chicago Continues Expansion of Policy Body Worn Cameras (June 12, 2017), https://www.cityofchicago.org/city/en/depts/mayor/press_room/press_releases/2017/june/BodyCameras.html; Ashley Southall, *Judge Clears Way for Police Body Cameras in New York*, N.Y. TIMES, Apr. 21, 2017, https://www.nytimes.com/2017/04/21/nyregion/judge-police-body-cameras-new-york.html; Chris Haire & Sean Emery, *Body cameras are becoming the norm in Southern California*, ORANGE COUNTY REG., Feb. 23, 2017, http://www.ocregister.com/2017/02/23/body-cameras-are-becoming-the-norm-in-southern-california; Allen Cone, *Taser-maker offers U.S. police free body camera for a year*, UPI, Apr. 6, 2017, https://www.upi.com/Top_News/US/2017/04/05/Taser-maker-offers-US-police-free-body-camera-for-a-year/5921491433254.

policy development."[2] 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.[3] The Task Force was charged with making recommendations on five policy questions posed in the bulletin:

- 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?[4]

The Task Force Process

Members of the Task Force were selected to represent a wide variety of perspectives in the Arizona judicial system. The Task Force undertook various outreach efforts and solicited and encouraged input from interested stakeholders and the general public.

The Task Force met approximately monthly, learning about and discussing various issues and technology related to digital evidence formats, storage, and management, and considered how best to approach the policy questions and what recommendations to make.

---

[2] Establishment of the Task Force on Court Management of Digital Evidence and Appointment of Members, Admin. Order No. 2016-129 (2016) at 1.

[3] *See* JTC RESOURCE BULL.

[4] Establishment of the Task Force on Court Management of Digital Evidence and Appointment of Members, Admin. Order No. 2016-129 (2016) at 1–2.

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. Between Task Force meetings, the workgroups met to investigate, develop, and refine recommendations addressing these key components of the Task Force's work. Task Force meetings included workgroup presentations, during which the members took questions and feedback from 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, and ensured the workgroups were not working in isolation.

Summary of Task Force Recommendations and Ongoing Efforts

In response to the policy questions listed above, the Task Force developed a strong consensus supporting the following recommendations for court management of digital evidence:

1. A standardized set of formats and technical protocols should be identified, adopted, and set forth in 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. The ACJA should be amended to require 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 stakeholders to develop consistent policies around the issue of non-victim witnesses. In addition, consideration should be given to the 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. The Arizona Rules of Evidence should be amended to expressly address digital evidence, including adding a definition of "video" to Rule 1001 and adding references to "video" in Rules 1002, 1004, 1006, 1007, and 1008.

8. Amendments should be made to various Arizona rule sets to modernize them 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 various Arizona rule sets where not otherwise included. The original recommendation was "Digital evidence, also known as electronic evidence, is any information created, stored, or transmitted in digital format." The recommendation was later changed to use the phrase "electronically stored evidence" in various Arizona rule sets where appropriate, as reflected in a rule change petition filed January 10, 2018.

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.[5]

---

[5] An unabridged version of this report with appendices, originally issued October 1, 2017, along with other Task Force information, can be found at http://www.azcourts.gov/cscommittees/Digital-Evidence-Task-Force.

I. MANAGEMENT OF DIGITAL EVIDENCE

A. Background

For centuries, the court has been the keeper of the record for court cases. This court record could be categorized as having three components that, until recently, consisted of paper documents or paper documents and other physical items: (1) written filings by the parties; (2) a written word-by-word transcript of hearings; and (3) exhibits used at hearings, consisting of documents, pictures, and items, such as guns, drugs, etc. Keeping this court record involved making sure paper filings were in the physical file, transcripts were in or accounted for in that physical file, and exhibits received by the court were accounted for in the physical file, an exhibit locker, or a storage location.

These documents and other items were expected to follow the case wherever it went. If a case resolved with no appeal, these documents and items in the court record would 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 items (or at least many of them) 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. 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, these paper documents and items in the court record would physically follow the case wherever it went.

A common characteristic of these three components of the court record was that they could be touched, physically delivered, received, returned, seen, found, stored, and, on occasion, lost. They were physical items that could be observed by a person with their senses without the aid of technology.

B. The Evolving Court Record Format

Technological advancements have resulted in profound changes to the nature of the court record. As noted 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."[6] The computer age has substantially changed filings and transcripts, two of the three key components of the court record, with a profound impact on how the court record is kept.

Filings by the parties are, quite often, electronic, not in paper form, and may include materials that never existed in paper form. Frequently, electronic filing (e-filing) of pleadings and motions is required, absent leave of court to make paper filings. For e-filing, 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. That filing is then kept by the court as a digital file in the court record that follows the case wherever it goes.

Similarly, the transcript of court proceedings frequently is provided in a digital file or recording. The digital transcript then becomes part of the court record kept by the court, or submitted to the court on appeal, with the digital file following the case wherever it goes. As with e-filings, such a digital transcript is kept by the court in a digital file, rather than a physical, paper-based file.

By contrast, the handling of exhibits 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, which is then marked by the clerk of court as an exhibit for identification. Even when 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.

If admitted into evidence, the physical exhibit is 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

---

[6] Richard Susskind, *Foreword* to DIGITAL JUSTICE TECHNOLOGY AND THE INTERNET OF DISPUTES, xiii (Ethan Katsch & Ornal Rabinovich-Einy eds.) (2017).

becomes a tangible part of what, until recently, was a paper court record, including the paper filings and paper transcripts. Except for exhibits, there is increasingly not a paper component of the court record. Thus, exhibits have become the 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 court record (the result of e-filing 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 e-filings and electronic transcripts.

The need to consider allowing digital evidence to cross the threshold from party to court in digital form was further enhanced by the increase in technology used in capturing and storing digital evidence for use at trial. Body-worn camera use has expanded at an almost algebraic rate, and its use promises to continue to expand.[7] Current technology allows body-worn camera images to be captured and stored in digital files. Those files are digital when created and remain digital until the eve of trial (from creation, to capture, to disclosure by law enforcement to a prosecutor, to disclosure by a prosecutor to a defense attorney). The issue, then, is whether there is a way for 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 digital images onto a physical disc or similar thing to be marked as a physical exhibit. If so, what additional issues would such a transfer

---

[7] *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 (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 (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"); *see also* Haire & Emery, *supra* note 1.

in digital form create?

C. The Truly Digital Evidence Concept

One charge of the Task Force was to analyze the implications of allowing exhibits to cross the threshold from parties to court in digital form and then, going forward, using them 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 by the parties.

Building 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, but a truly digital trial.[8] 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 also 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 digital evidence could be submitted to the clerk of court in digital form, in advance of or at a hearing or trial. The portal concept would (1) allow exhibits to cross the threshold from parties to 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 e-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 governing the collection of fees in various case types and allowing for court access regardless of financial resources. Any user fee concept would need to account for those issues and restrictions.

By submitting exhibits to the clerk in digital form, the exhibits would be ready to use in court at the appropriate time. Digital

---

[8] Perhaps the closest example of a truly digital trial in the United States in the sense the Task Force considered is described in Leonard Polyakov, *Paperless Trials Are The New Litigation Reality*, 57 ORANGE COUNTY LAW. 36 (2015).

exhibits would reside in digital form in an electronic repository managed by the clerk. At the appropriate time, digital exhibits marked for identification could be accessed in court by the parties, counsel, the court, witnesses, and the clerk, using courtroom monitors or on a network allowing access on monitors provided by the parties.

If a digital exhibit was admitted into evidence, this electronic portal concept would allow the clerk to mark the exhibit in the electronic repository as having been admitted in evidence. As with physical exhibits currently, this would allow the participants to use the exhibit for proper purposes, including viewing it 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 currently. Applying the concept to deliberations, the jurors could access admitted exhibits in digital form using technology in the deliberation room.

At trial's end, the admitted exhibits would be preserved for future reference; exhibits not admitted would be deleted (or retained, if necessary for subsequent proceedings). Again, however, given that the exhibits would be in digital format, and not physical objects, there would be no need to store them in a physical location. Adequate server space, however, would be required.

Admitted exhibits would be included in the record on appeal and transmitted electronically. The courts on appeal (and for subsequent or collateral proceedings) 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.

For decades, there has been a good deal of helpful information about how to conduct a trial using exhibits in electronic form in the courtroom *after* exhibits are submitted to the clerk in paper form or on disc.[9] But the focus of the Task Force was different: a truly digital

---

[9] *See, e.g.*, David L. Masters, *How to Conduct a Paperless Trial*, 39, No. 3 LITIGATION 52 (2013); Thomas E. Littler, *Litigation Trends in 2013*, 49 ARIZ. ATT'Y 30 (2013); Thomas I. Vanaskie, *The United States Courts' Case Management/Electronic Case Filing System: Perspectives of a District Judge*, 8, No. 3 E-FILING REPORT 1 (2007) (predicting, in discussing "The Paperless Trial Court Record," that "[a]s use of evidence presentation technology expands, it may

trial where exhibits cross the threshold from parties 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, 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. Therefore, the Task 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.[10]

D. Task Force Meetings

The Task Force met in person seven times. Meetings included an overview of the background and substance of the Joint Technology Committee Resource Bulletin by Paul S. Embley, Chief Information Officer, Technology, National Center for State Courts; presentations and discussions on digital evidence from various perspectives; the exhibit workflow process; case management systems; OnBase technology; and court use of cloud technology, as well as presentations by the Arizona State Library, Archives and Public Records, and the Arizona Commission on Technology.

During these meetings, and at separate workgroup meetings, the Task Force discussed draft workgroup reports as well as drafts of

---

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*, 19, No. 3 LITIGATION 5 (1993).

[10] A London-based entity has launched a system in British courts that appears to have some similarities to the truly digital evidence concept the Task Force considered. *See* CASELINES THE DIGITAL COURT PLATFORM, www.caselines.com (last visited Feb. 6, 2018). At present, it does not appear that any court in the United States has adopted that technology.

the final Task Force report. The product of that discussion and supporting rationale are set forth here, as supplemented in a rule change petition filed January 10, 2018.[11]

II. WORKGROUP REPORTS

A. Digital Formats Workgroup Report

1. Summary

The Digital Formats Workgroup ("DFW") addressed 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?"[12] Ultimately, the DFW concluded that standardized formats and technical protocols for the viewing, storage, and preservation of digital evidence should be adopted for all courts. Further, it 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

---

[11] Along with preparing this report, Administrative Order 2016-129 directed the Task Force to "file a rule change petition not later than January 10, 2018, with respect to any proposed rule changes." That petition, designated R-18-0008 and pending as of the date of this article, and related comments, can be found on the Arizona Supreme Court's Court Rules Forum. *See* http://www.azcourts.gov/Rules-Forum.

[12] *See supra* note 4.

be found in the ACJA, particularly Chapters 5 (Automation)[13] and 6 (Records).[14]

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.[15] The ACJA includes administrative, case, electronic, and online records within the definition of court records.[16] It broadly defines each type of record to encompass a wide range of content.[17] 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.[18] 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.[19] Although these references are helpful, 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.

2. 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. "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)."[20] Thus, this provision sets forth the requirement that court records must comply with standard formats and be accessible with standard devices.

Similarly, the ACJA specifically addresses conversion and

---

[13] Ariz. Code Jud. Admin. §§ 1-501–507.

[14] Ariz. Code Jud. Admin. §§ 1-601–606.

[15] *See*, *e.g.*, Ariz. Code Jud. Admin. §§ 1-504, 1-602(C), (D).

[16] Ariz. Code Jud. Admin. § 1-507.

[17] *Id.*

[18] *See id.*

[19] *See, e.g.*, Ariz. Code Jud. Admin. §§ 1-504(A), 1-506(A), 1-507(A), 1-602(A).

[20] Ariz. Code Jud. Admin. § 1-507(D)(1)(a).

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)."[21] 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.[22]

At the same time, "[c]ourts 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."[23] This provision contemplates that a court may receive evidence electronically or physically and 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 ACJA § 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. "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)."[24]

The desirability of standard, 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, 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,

---

[21] Ariz. Code Jud. Admin. § 1-507(D)(1)(b).
[22] *Id.*
[23] Ariz. Code Jud. Admin. § 1-507(D)(1)(c).
[24] Ariz. Code Jud. Admin. § 1-506(D)(5)(b).

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. 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. But if that same video was introduced to prove that a person was at a specific location when the gun was fired, not the exact moment of firing, 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 format is necessary to ensure justice.

For these reasons, there was a consensus among the DFW 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. The DFW 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 the party must meet in order to submit evidence 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 is necessary for judges to recognize, evaluate, and analyze whether an exception to standardization is necessary. When non-standard or proprietary

formats must be used, the party offering the non-conforming digital evidence should generally have 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.

3. Viewing and Presentation

Viewing and presentation of court records typically contemplates two scenarios. One scenario is litigation of a case or controversy in a court. In this scenario, digital evidence is likely offered by a party to or a participant in the litigation. The digital evidence 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 before, during, and after litigation is resolved. The ACJA accomplishes this by addressing these scenarios in separate sections as discussed above. In addition, the court rules for the various types of cases 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 now and in the future.

4. Storage

The ACJA also contains requirements for storage of court records, addressing primary and secondary electronic storage and specifying hardware, power support and redundancy requirements

for court records.[25] "Storage" is specifically defined 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."[26] Another provision 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.[27]

The DFW concluded the current language of the ACJA sufficiently addresses the policy questions on storage requirements. 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 here, that would prevent a court from accepting evidence electronically submitted, regardless of whether on a compact disc, by email, or through information sharing on the cloud. Once received by the court, however, digital evidence should be stored in the format in which it was received.[28]

5. Preservation

The ACJA does not clearly distinguish between storage and preservation, and while it defines the former, it does not define the latter.[29] The provision setting forth storage requirements does not discuss preservation.[30] The provision addressing preservation does so primarily by referencing retention schedules:

> Records generated by or received by courts shall be preserved in accordance with the applicable records retention schedule. Case records required to be

---

[25] *See* Ariz. Code Jud. Admin. § 1-507(D)(3).
[26] Ariz. Code Jud. Admin. § 1-507(D)(3).
[27] *See* Ariz. Code Jud. Admin. § 1-507(H).
[28] *See* Ariz. Code Jud. Admin. § 1-507(D)(1).
[29] *See id.* at § 1-507(A).
[30] *See id.* at § 1-507(D)(3).

> 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.[31]

Collectively, these provisions require 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 access to electronic records over a long period of time. Thus, the distinction between storage and preservation in the ACJA suggests that "storage" refers to 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. These challenges are more closely aligned with the policy questions addressed by the Storage and Management Workgroup. The DFW 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.

B. Storage and Management Workgroup Report

1. Summary

The Storage and Management Workgroup ("SMW") addressed 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?"[32]

---

[31] *Id.* at § 1-507(D)(5)(c); *see also id.* §1-507(D)(5)(f) (also addressing preservation).

[32] *See supra* note 4.

- "Should management of digital evidence possessed by courts be centralized or decentralized considering technology costs, expertise, and infrastructure necessary to manage it?"[33]

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 another electronic media storage device. Judges, clerks of court, and court administrators apply existing rules 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 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.[34]

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 that is marked as an exhibit. However, the rapid increase in digital evidence requires courts to implement policies and technical standards that are flexible enough to accommodate tomorrow's storage needs.

Policy decisions require consideration of whether management of digital evidence should be centralized or decentralized and whether storage should be local, off-site, or in the cloud. These decisions should be guided by a set of technical requirements and policy considerations discussed below.

Arizona establishes technical requirements and policy through

---

[33] *See supra* note 4.

[34] *See, e.g.*, *supra* note 1.

the ACJA. The ACJA establishes minimum technical requirements for Electronic Reproduction and Imaging of Court Records;[35] Enterprise Architectural Standards;[36] Filing and Management of Electronic Court Documents; [37] and Protection of Electronic Case Records in Paperless Court Operations.[38] While not establishing technical requirements per se, for storage and management of digital evidence, what follows is a list of suggested minimum requirements to consider in addressing those issues.

2. Suggested Requirements

The following minimum technology requirements should apply to any digital evidence storage and management solution used by Arizona courts—centralized or decentralized.

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

2. Solution Integration. Whenever a single solution is not available or feasible, 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 DFW Report thoroughly discusses the current ACJA requirements related to standardized formats for digital evidence submitted to a court. The SMW supports those recommendations, including both for standardized formats as well as discretion to allow submissions of digital evidence in a non-standard or propriety form.

The adoption of 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

---

[35] *See* Ariz. Code Jud. Admin. § 1-504.
[36] *See id.* at § 1-505.
[37] *See id.* at § 1-506.
[38] *See id.* at § 1-507.

content will 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. This is imperative to protecting evidence not available for general viewing in accordance with law.

5. Security. Any solution 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, as well as 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 an audit trial for purposes of authenticating and establishing the reliability of the evidence. This consideration must take into account the requirements of evidentiary and procedural rules to ensure the software does not alter digital evidence in 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 and any other retention schedules applicable to court records.[39]

9. **"Physical Digital" Security**. Currently, digital evidence submitted to a court via a physical format, such as a disc, cannot be

[39] *See* Ariz. Code Jud. Admin. §§ 2-101, 2-201, 3-402, 4-301, 6-115.

connected to network computers (e.g., Arizona Justice Information Network ("AJIN") or Criminal Justice Information Systems ("CJIS") computers). This prevents such evidence from being uploaded to case management systems for storage and use in court hearings and trials. Any digital evidence storage and management solutions 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 by rule and the ACJA if the application will be accessible via remote electronic access.[40] 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.

3. Additional Considerations

The SMW 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. 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 for digital evidence storage and management. Any court that can meet the minimum technical requirements in the ACJA should be able to store and manage digital evidence locally if it wishes to do so.

The following additional considerations should be a part of a local court's analysis of whether to be a part of a centralized solution

[40] *See* ARIZ. R. SUP. CT. 123; Ariz. Code Jud. Admin. § 1-604.

or to adopt a decentralized 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 solutions 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 and can remain integrated with new software (both updated versions and later acquired) is necessary for local courts to effectively serve the parties and the public.

- **Self-Represented Litigants.** Self-represented litigants may lack the knowledge of the legal requirements or lack the tools and abilities to comply with redaction requirements. It may be that future technological 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 AOC should develop resource guides for self-represented litigants or templates for local courts use that include information on requirements surrounding redaction, standardized formats, converting, submitting, and using digital evidence in the court.

4. Other Issues

The SMW was charged with policy questions that focus on what to do once digital evidence is received by the court—the "back end" of the process of digital evidence after it crosses the threshold from parties to the court. Many courts are experiencing self-represented litigants, in cases like small claims or protective order matters, 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 disc. Guidance should be developed for litigants presenting and courts managing this type of evidence.

The SMW recommends that the AOC work with local courts in developing policies and procedures and implementing technological solutions (where feasible) for cases in limited jurisdiction courts to account for the specific needs in such cases. 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 relevant in this discussion. The SMW recommends establishing a fee, where appropriate and permissible, for submission of digital exhibits. Such a fee could help offset the costs associated with digital evidence storage and management solutions.

C. Rules Workgroup Report

1. Discussion

The Rules Workgroup ("RW") addressed 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?"[41]

- "Should new or amended rules on chain of custody evidence be developed for handling court digital evidence?"[42]

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

---

[41] *Supra* note 4.
[42] *Supra* note 4.

evidence and media the evidence is produced on that have 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 disc. Instead, this evidence is saved and stored in some type of digital format, often one 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 citizens' privacy interests.[43]

The RW reviewed various Arizona rule sets, including evidence, civil criminal, family and juvenile, probate, protective orders, eviction actions, Arizona Supreme Court Rule 123, as well as rules, statutes, and constitutional provisions involving victims' rights. The RW also reviewed relevant portions of the ACJA.

This review 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 for revision were identified and are discussed below. And although current rules are working, the RW believes 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 RW:

1. Defining "Digital Evidence." The phrase *digital evidence* should be defined. The following definition was proposed: "Digital evidence, also known as electronic evidence, is any information created, stored, or transmitted in digital format." This recommendation was later changed to use the phrase "electronically stored evidence," as used in the Arizona Rules of Civil Procedure

[43] *See* Maury, *supra* note 7.

for nearly a decade, in various other Arizona rules sets where appropriate, as reflected in a rule change petition filed January 10, 2018.

2. Arizona Rules of Evidence. In addressing the Arizona Rules of Evidence,[44] the focus was on the rules on authentication and identification (Article IX)[45] and the contents of writings, recordings, and photographs (Article X).[46] 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, the definition of "recording" is limited to "letters, words, numbers, or their equivalent recorded in any manner."[47] Although recognizing 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,"[48] the rules should be updated to include *video* as a defined term. After considering various definitions of the term and the variety of digital evidence that is not a still image as contemplated by the current definition of the term "photograph,"[49] the following definition was suggested: "Video is an electronic visual medium for the recording, copying, playback, broadcasting, or displaying of audio or moving images," later refined to "Video is an electronic visual medium for the recording, copying, playback, broadcasting, or displaying of moving images, which may or may not contain an audio recording." Rules 1002, 1004, 1006, 1007, and 1008 should be amended to insert the newly defined term *video*.

3. Arizona Rules of Civil Procedure. The Arizona Rules of Civil Procedure underwent a comprehensive restyling, effective

---

[44] Given amendments effective January 1, 2012, as applicable here, the Arizona Rules of Evidence "correspond to the Federal Rules of Evidence as restyled." ARIZ. R. EVID. Prefatory Comment to 2012 Amendments.

[45] ARIZ. R. EVID. 901–903.

[46] *Id*. 1001–1008.

[47] *Id.* 1001(b).

[48] *See id.*

[49] ARIZ. R. EVID. 1001(c).

January 1, 2017.[50] During the workgroup's consideration, a rule petition was pending before the Arizona Supreme Court that would significantly change many of the civil rules surrounding discovery and disclosure.[51] After review of the rules in place and the pending rule petition, and given the change in recommendation from defining "digital evidence" to using the phrase "electronically stored information," the RW determined that the Arizona Rules of Civil Procedure thoroughly address digital evidence, particularly the disclosure and discovery rules (Article V).[52]

4. Arizona Rules of Criminal Procedure. The Arizona Rules of Criminal Procedure, including Rules 15.1, 15.2, 15.4, 15.5 (disclosure rules), and Rule 22.2 (materials used during jury deliberation), were considered 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. As the use of digital evidence increases, its disclosure via electronic means will increase and, correspondingly, its disclosure on a tangible item (like a disc or in a physical format like paper) will decrease. The RW notes that Rules 15.1 and 15.2 do not contain language that includes video, digital evidence, or other electronically stored information. Accordingly, the RW recommends that Rules 15.1 and 15.2 be amended to include language specifically identifying disclosure of digital evidence, later refined to electronically stored information. A similar amendment was later recommended for Rule 15.3.

The RW reviewed language that, in 2017, required disclosure of "a list of all papers, documents, photographs and other tangible objects."[53] The increase in digital evidence, such as body-worn

---

[50] ARIZ. R. CIV. P. Prefatory Comment to the 2017 Amendments.

[51] That petition, designated R-17-0010, was adopted effective July 1, 2018; the petition, related comments and the order adopting the changes can be found on the Arizona Supreme Court's Court Rules Forum. *See* http://www.azcourts.gov/Rules-Forum.

[52] ARIZ. R. CIV. P. 26–37.

[53] ARIZ. R. CRIM. P. 15.1(b)(5), (i)(3)(c) and 15.2(c)(3), (h)(1)(d) in place

camera video and digital video, images, or other content from smart phones or other personal recording devices, is not accounted for in the specific language of the rules.[54] The RW notes that, particularly as disclosure of the evidence moves toward a cloud-based model, the rules need modernization.

Rule 22.2 addresses materials that may be used during jury deliberations.[55] 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.[56] Currently, in Arizona, digital evidence is submitted and admitted for trial after being transferred to a 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.[57] 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) would require amendment to account for both tangible and cloud-based evidence.

5. Arizona Rules of Family Law Procedure. The RW recommends that Rule 49 be changed to include a subsection on

---

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). The corresponding Arizona Rules of Criminal Procedure in effect as of January 1, 2018 are used in petition R-18-0008, filed January 10, 2018. *See* http://www.azcourts.gov/Rules-Forum.

[54] *See id.*

[55] ARIZ. R. CRIM. P. 22.2(d).

[56] *Id.*

[57] *See*, *e.g.*, https://www.axon.com/company (last visited Mar. 20, 2018).

electronically stored information. Several subsections of Rule 49 refer to disclosure and discovery of such information.[58] As currently written, Rule 49 does not, however, provide guidance for parties regarding their duty to confer about the form in which the information will be produced or resolution of disputes related to disclosure or discovery of electronically stored information.[59] 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 in place for managing this type of discovery will be increasingly beneficial to parties and the courts.

The RW also recommends that a task force currently addressing the Arizona Rules of Family Law Procedure consider the amendments to the updated Arizona Rules of Civil Procedure to ensure digital evidence is expressly addressed in that rule set.

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. Rule 36, addressing admissible evidence in contested protective order hearings, should be modernized to include digital and electronic evidence specifically, when the truly digital evidence concept is adopted in Arizona.

7. Arizona Rules of Probate Procedure. The Arizona Rules of Probate Procedure incorporate by reference Rules 26-37 of the Arizona Rules of Civil Procedure.[60] As such, the Arizona Rules of Probate Procedure address electronically stored information; therefore, no amendments are recommended. The Arizona Rules of Probate Procedure are heavily driven by statutory requirements. 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

---

[58] ARIZ. R. FAM. L.P. 49(E)(2), (E)(5), (E)(6), (F)(1).
[59] *See id.*
[60] ARIZ. R. PROB. P. 28(B).

discovery rules do not include any reference to digital or electronic evidence. Despite the lack of such specificity, the rules currently appear to work. However, considering the increasing volume of digital evidence, including in delinquency matters, as with adult criminal matters, an amendment that would modernize the language of the rule is recommended.

For these reasons, changes should be made to Rules 16(B)(1)(d), 16(C)(3)(c), 44 and 73 of the Rules of Juvenile Court to include reference to digital and electronic evidence, later refined to electronically stored information.

9. Arizona Justice Court Rules of Civil Procedure. Arizona Justice Court Rules of Civil Procedure, particularly Rules 121-127, appear to adequately address electronically stored information and digital evidence. 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.[61] Moreover, although not using the phrase "digital evidence," Rule 125(a) references "electronically stored information."[62] No changes are recommended to this rule set.

10. Arizona Rules on Eviction Actions. The Arizona Rules on Eviction Actions do not need substantive changes to address digital evidence. However, an amendment should be made to include digital evidence or electronically stored information in Rule 10, which addresses the types of content that must be disclosed.

2. The ACJA.

The ACJA 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 RW provided input and feedback to those workgroups as they reviewed ACJA sections. The RW has no recommendations beyond those made by the Digital

---

[61] *E.g.*, ARIZ. JUSTICE CT. R CIV. P. 121(a)(3)(A), (a)(5), 122(f)(1), 125.
[62] *E.g.*, ARIZ. JUSTICE CT. R CIV. P. 125(a).

Formats and Storage and Management Workgroups. The following describes the thought processes regarding relevant ACJA sections and any overlap with procedural rules discussed above.

The ACJA provides standards that apply to all records imaged by courts, including methods used to create or reproduce records electronically.[63] The ACJA designates the methods and formats that must be used to maintain and preserve electronically stored and archived records and the reproduction of such records.[64] The ACJA also covers general requirements for security to ensure evidence is not destroyed or altered and addresses accessibility.[65] Courts must ensure that the public is afforded reasonable access to records via the public access portal managed by the AOC, at a minimum.[66] 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 in which they reside to protect them from inappropriate access.[67]

The ACJA provides standards for filing and management of electronic court documents,[68] expressly stating it "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."[69] The ACJA also provides standards for the protection of electronic case records.[70] These provisions address most types of digital evidence, including formatting and authentication of such evidence. Two ACJA sections provide standards addressing accessibility to digital court records, which would include digital evidence, both of which address the ability to access court records remotely.[71]

In summary, the RW does not have recommendations, independent from those of the other workgroups, regarding changes

---

[63] *See* Ariz. Code Jud. Admin. § 1-504.
[64] *Id*.
[65] *Id*.
[66] *See* ARIZ. SUP. CT. R. 123.
[67] *Id.*
[68] *See* Ariz. Code Jud. Admin. § 1-506.
[69] *Id.* at § 1-506(B).
[70] *See id*. at § 1-507.
[71] *See* Ariz. Code Jud. Admin. §§ 1-604, 1-606.

to the ACJA.

3. Privacy and Digital Evidence.

Victims have concerns regarding 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, victims' knowledge of the criminal justice system and the courts, understandably, may be limited. It is not uncommon for victims to become increasingly concerned with privacy, especially as it relates to images and information captured via digital devices like body-worn cameras, cell phone video, digital photographs of injuries, crime scenes, and autopsies. Particular sensitivity surrounds the public's ability 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.[72] The open records policies applicable in Arizona's courts may cause victims concern.

The Arizona Supreme Court has enacted rules related to victims' rights. For example, the Arizona Rules of Criminal Procedure provide an avenue for victims to seek protection of their identity and location.[73] This provision is cross-referenced in several rules related to discovery and disclosure, including consideration of victims' rights in broadcasting trials and limiting public access to court records when confidential or sensitive information is involved and where access is otherwise restricted by statute.[74]

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 implicate victims' rights and privacy concerns. In addition, although the various rules mentioned above currently work to protect victims' rights, victims continue to

---

[72] *See* ARIZ. CONST. Art. II § 2.1(A)(1); *see also* ARIZ. REV. STAT. ANN. §§ 13-4401, et seq.

[73] *See* ARIZ. R. CRIM. P. 39.

[74] *See* ARIZ. SUP. CT. R. 122, 123.

advocate for additional protections.

For rules governing public records, which implicate access and privacy concerns, Arizona appears to treat digital evidence like traditional evidence, and current policies and procedures applicable to all types of evidence, including digital evidence, are working. However, the rule does not consistently address digital evidence, including exhibits, received by a court.[75] The RW recommends that this rule 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 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, such information is 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, it is recommended 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 un-redacted digital evidence being introduced in evidence by self-represented litigants.

---

[75] *See* ARIZ. SUP. CT. R. 123.