

1	"The Night Riders of Western Kentucky" Sunday, July 28, 2019 5:00 p.m. – 6:00 p.m. Vol 1 Pg 2
2	"Easiest Catch: Don't Be Another Fish in the Dark 'Net'" Monday, July 29, 2019 10:30 a.m. – 3:00 p.m. Vol 1 Pg 19
3	"Ethical Considerations In Media Relations" Monday, July 29, 2019 3:00 p.m. – 4:30 p.m. Vol 1 Pg 35
4	Digital Evidence Tuesday, July 30, 2019 8:30 a.m. – 9:45 a.m. Vol 1 Pg 37
5	Developing an Electronic Records Preservation and Disposition Plan Tuesday, July 30, 2019 10:00 a.m. – 11:00 a.m. Vol 1 Pg 142
6	What's Bugging You? Tuesday, July 30, 2019 2:45 p.m. – 3:45 p.m.
7	"Grant-Funded Technology Innovations in California" Wednesday, July 31, 2019 8:30 a.m. – 10:30 a.m. Vol 2 Pg 2
8	Discussion on the Texas Judicial Commission on Mental Health Wednesday, July 31, 2019 10:45 a.m. – 11:30 a.m. Vol 2 Pg 15
9	Applying Education: What We've Learned (Members Only) Wednesday, July 31, 2019 11:30 a.m. – 12:30 p.m. Vol 2 Pg 16
10	"Can You Like the Court? Social Media Use by Courts and Court Officials" Wednesday, July 31, 2019 2:00 p.m. – 3:30 p.m. Vol 2 Pg 22
11	Joint Session with the Association of Reporters of Judicial Decisions "Public Requests to Remove Personal Information from Opinions" Thursday, August 1, 2019 8:30 a.m. – 9:30 a.m.



SUSAN STOKLEY CLARY
COURT ADMINISTRATOR
GENERAL COUNSEL

SUPREME COURT OF KENTUCKY

(502) 564-4176

ROOM 235, STATE CAPITOL, FRANKFORT 40601

NEWS RELEASE

CONTACT: Susan Stokley Clary
(502) 564-4176

Justice Bill Cunningham of the 1st Supreme Court District will be invested formally in ceremonies conducted in the Supreme Court Courtroom, at the Capitol building in Frankfort, at 2:00 p.m. on Tuesday, January 16, 2007.

Justice Cunningham was born in Eddyville, Kentucky in 1944 and raised in Lyon and Marshall counties. He received his B.S. degree from Murray State University in 1966 and his J.D. from the University of Kentucky Law School in 1969. He is an author of numerous publications in national, state and local periodicals as well as a veteran of the United States Army (Germany, Korea and Vietnam). He was City Attorney for Eddyville, Kentucky, 1974-1991; Public Defender for Kentucky State Penitentiary, 1974-1976; Commonwealth Attorney for the 56th Judicial District, 1976-1988; Hearing Officer for the Kentucky Board of Claims, 1981-1985; Trial Commissioner for Lyon District Court, 1988-1992; Circuit Judge, 1992-2006 and elected to the Kentucky Supreme Court November 7th, 2006. Justice Cunningham is married to Paula Trull, has five sons, four grandchildren and resides in Kuttawa, Kentucky.

END



About Bill Cunningham....

Circuit Judge of the 56th Judicial Circuit consisting
of Caldwell, Livingston, Lyon and Trigg Counties.

Personal History

Born October 15, 1944, Eddyville, Kentucky.
Raised in Lyon & Marshall counties.
Currently resides in Kuttawa, Kentucky
Graduated Benton High School, 1962
Graduated Murray State University, 1966
University of Kentucky Law School, 1969
Captain, United States Army--Germany, Korea and Vietnam

Professional Career:

City Attorney, Eddyville, Kentucky
Public Defender
Hearing Officer for Kentucky Board of Claims
Trial Commissioner
Commonwealth Attorney
Circuit Judge

Author:

Books
Flames in the Wind
On Bended Knees: The Night Rider Story
Castle, The Story of A Kentucky Prison
Kentucky's Thomas D. Clark
Children of Promise
A Distant Light

Numerous publications in national, state and local periodicals

Family:

Parents and grandparents from Calloway and Trigg counties
Married to Paula Trull, Charlotte, North Carolina
Five sons, four grandchildren

Judge Bill Cunningham
P.O. Box 790
Eddyville, KY 42038
Tel: 270 388 5182
Fax: 270 388 0869
www.judgecunningham.com

JUSTICE BILL CUNNINGHAM (1969)

Kentucky Supreme Court

As a small child, Bill Cunningham was a batboy in the Kentucky State Penitentiary in Eddyville, Kentucky. Opened in 1889 and still in use today as a maximum and supermax security prison, the "castle on the Cumberland" was just across the street from Cunningham's childhood home. His father worked on the river, and his family lived in the government reservation lock-house. For Cunningham, life within the walls of the prison took on a similar normalcy as life outside the prison, and these youthful interactions developed in him a profound compassion and respect for prison inmates that he carried with him throughout his career.

Raised in a typical small western Kentucky town with solid, strict southern Baptist sensibilities, the legal profession was appealing for its opportunity to touch the most lives and do the most good. Cunningham's brother-in-law was an attorney and a major career influence. But it was the example and expectation of his parents that Cunningham describes as key. Despite having completed the requirements, his father repeated the 8th grade three times because he couldn't afford to go to high school but had such a thirst for education. Today, his father's 8th grade diploma hangs in Cunningham's office in the Kentucky State Capitol.

"My parents lived a life that set themselves as an example," said Cunningham. "You see your dad working day and night on the river, sometimes in some pretty dangerous situations. You see your mom going to teach at a two-room schoolhouse where she collects the kindling on Sunday nights to start the fire in the potbelly stove the next morning in the country school. You grow up seeing these things and you know that if you go anywhere, you're going to have to work hard."

Cunningham took that work ethic with him to law school. During his 3L year, he worked three jobs including weekend

deliveries for Sir Pizza on Romany Road. Four years as an Army JAG officer serving in Germany, Vietnam and Korea followed law school.

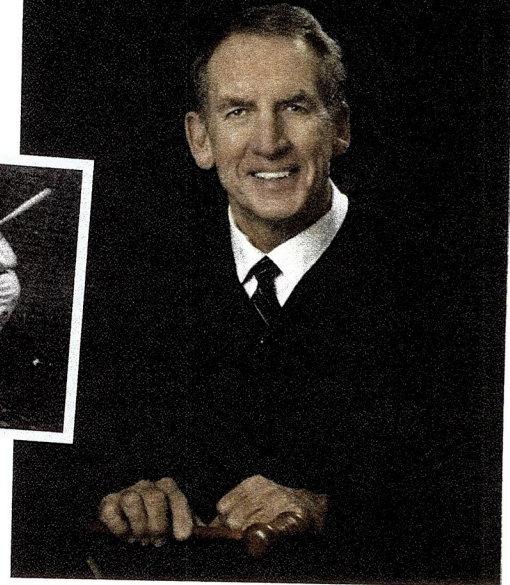
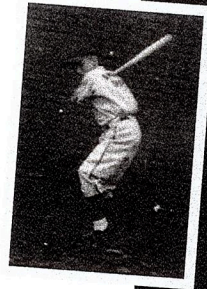
"The service was a huge part of my education," said Cunningham. "I tried cases all over the world. It was a tremendous experience. I hadn't seen the Atlantic Ocean or ridden in an airplane until I was 21 years old. I was pretty wet behind the ears. My life would have been really limited without this experience. I think I would have been diminished because of lack of broadening viewpoints. Mary Twain said 'travel is fatal to prejudice' and that was pretty much the situation with me."

After leaving the military, Cunningham took a job as a public defender at Kentucky State Penitentiary for two years before serving as Commonwealth's Attorney for over a decade. He was a circuit court judge for 15 years before being elected to the Kentucky Supreme Court in 2006.

Initially concerned by the lack of persons of color on his juries, over the years Cunningham has quietly worked to advance minority investment in the justice system, as well as encouraging Kentucky children of color to consider careers as lawyers, police officers and other law enforcement jobs.

"It's not only important that our justice system be fair, it also must appear fair. It must appear just," said Cunningham. "Several years ago on my birthday my oldest son asked me what was the greatest change I had seen in my lifetime, and I told him civil rights and the ending of the Cold War. Those were the biggest changes we've seen. Though sometimes today I wonder how far we've really come."

A great storyteller in the southern tradition, Cunningham has written a number of books on regional history,



including "A Distant Light," which relates to the history of western Kentucky's struggle for racial justice. He has also written "Castle," the history of the Kentucky State Penitentiary.

Whether defending, prosecuting or sitting as judge, Cunningham approaches defendants and inmates with a profound sense of compassion and respect. As you would with a childhood home, he still visits Kentucky State Penitentiary regularly.

"I am comfortable with inmates," said Cunningham. "I have friends in the penitentiary. A lot of guys I sent there have been there for several years and we have a certain amount of mutual respect, and we have become friends over the years. I'm not talking about a whole lot. Just a few guys I've gotten to know over time. Simply, it's part of my DNA. Part of the calling. You reach out, try to be an influence on them. I think if you are exposed to people like that, you realize that almost all of them are Jekyll and Hyde. But for good strong parents and that sort of thing, you could have been there. You get to know them as human beings, and know that they are capable of doing some very bad things, but at the same time they are capable of being very good people."

When asked if other attorneys are friends with some of the people they put away, Cunningham responds ruefully, "Probably not. In fact, my wife and my secretary all think I'm a little weird."

Bill Cunningham (judge)

Bill Cunningham (born October 15, 1944)^[1] was elected to the Kentucky Supreme Court in November 2006 to represent the 1st Appellate District.

Contents

Education

Early judicial career

Personal life

References

External links

Education

Cunningham earned his bachelor's degree from Murray State University in 1962 and his Juris Doctor in 1969 from the University of Kentucky College of Law.

Early judicial career

Cunningham served the court system in several capacities before entering his judicial career. He was the Eddyville city attorney from 1974 to 1991 and public defender for the Kentucky State Penitentiary from 1974 to 1976. He served as Commonwealth's Attorney for the 56th Judicial District from 1976 to 1988. During his tenure in that position, he was voted the Outstanding Commonwealth Attorney of Kentucky by his peers.

Cunningham also served as a hearing officer for the Kentucky Board of Claims from 1981 to 1985 and as a trial commissioner for the Lyon County District court from 1989 to 1992.

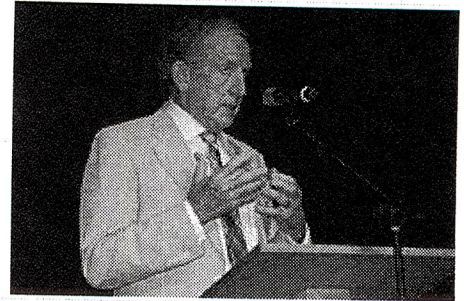
Cunningham served as a circuit court judge for 15 years. He was elected to the Circuit Court Bench in November 1991 to serve the 56th Judicial Circuit, which consists of Caldwell, Livingston, Lyon and Trigg counties. He was re-elected in 1999 and served as circuit judge until January 2007.

Personal life

Born in Eddyville,^[2] Cunningham is a native of Kuttawa, Kentucky in Lyon County and an author of five books about regional history, which chronicle the struggle for racial justice in western Kentucky since the American Civil War as well as a book about the history of the Kentucky State Penitentiary in Eddyville.

He is a veteran of the U.S. Army, having served in Korea, Germany, and Vietnam.

Bill Cunningham



Associate Justice of the Kentucky Supreme Court

Incumbent

Assumed office

2007

Personal details

Born October 15, 1944
Eddyville, Kentucky, U.S.

Political party Democratic

Children Joe Cunningham

Residence Kuttawa, Kentucky

Alma mater Murray State University
University of Kentucky

NEWS RELEASE

CONTACT: Susan Stokley Clary

(502) 564-4176

Justice Bill Cunningham of the 1st Supreme Court District will be invested formally in ceremonies conducted in the Supreme Court Courtroom, at the Capitol building in Frankfort, at 2:00 p.m. on Tuesday, January 16, 2007.

Justice Cunningham was born in Eddyville, Kentucky in 1944 and raised in Lyon and Marshall counties. He received his B.S. degree from Murray State University in 1966 and his J.D. from the University of Kentucky Law School in 1969. He is an author of numerous publications in national, state and local periodicals as well as a veteran of the United States Army (Germany, Korea and Vietnam). He was City Attorney for Eddyville, Kentucky, 1974-1991; Public Defender for Kentucky State Penitentiary, 1974-1976; Commonwealth Attorney for the 56th Judicial District, 1976-1988; Hearing Officer for the Kentucky Board of Claims, 1981-1985; Trial Commissioner for Lyon District Court, 1988-1992; Circuit Judge, 1992-2006 and elected to the Kentucky Supreme Court November 7th, 2006. Justice Cunningham is married to Paula Trull, has five sons, four grandchildren and resides in Kuttawa, Kentucky.

END

He and his wife, Paula, have five sons and eleven grandchildren. His son, Joe, is the U.S. Representative from South Carolina's 1st congressional district.^[3]

References

1. Trigg Co, Kentucky Veterans (https://books.google.com/books?id=Qzu82QxUn1AC&pg=PA242&dq=Bill+Cunningham+Kentucky+october+1944&hl=en&ei=R7pUTae3AoH88AbyoJ3pBg&sa=X&oi=book_result&ct=result&resnum=4&ved=0CDYQ6AEwAw#v=onepage&q&f=false) Turner Publishing Company; 2002
2. [1] (https://www.bgamplifier.com/arts/after-shock-on-bended-knees-with-bill-cunningham/article_57b96786-1ed3-53d1-a7e8-872c813983fc.html)
3. "Joe Cunningham For Congress | South Carolina | Meet Joe Cunningham" (<https://www.joecunninghamforcongress.com/meet-joe>). *Joe Cunningham For Congress | South Carolina*. Retrieved 2018-12-06.

External links

- Justice Bill Cunningham Official Court Biography (<http://courts.ky.gov/courts/supreme/Pages/cunningham.aspx>)

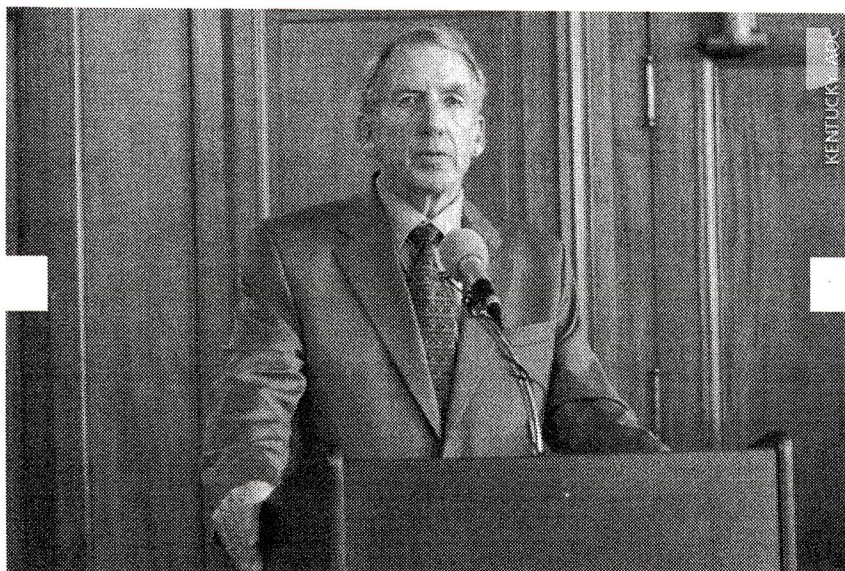
Retrieved from "[https://en.wikipedia.org/w/index.php?title=Bill_Cunningham_\(judge\)&oldid=884029992](https://en.wikipedia.org/w/index.php?title=Bill_Cunningham_(judge)&oldid=884029992)"

This page was last edited on 19 February 2019, at 02:36 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[Courts](#) [Administrative Office of the Courts](#) [Commissions & Committees](#) [Court Programs](#) [Resources](#)[Kentucky Court of Justice](#) [Courts](#) [Supreme Court](#) [Justice Bill Cunningham](#)

Justice Bill Cunningham

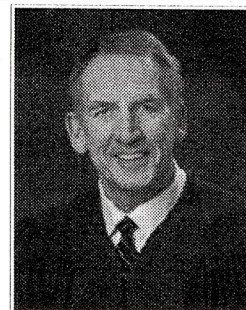


Justice Bill Cunningham was elected to the Supreme Court of Kentucky in November 2006 to serve the 1st Supreme Court District.

Before becoming a member of the state's highest court, Justice Cunningham served as a circuit court judge for 15 years. He was elected to the Circuit Court Bench in November 1991 to serve the 56th Judicial Circuit, which consists of Caldwell, Livingston, Lyon and Trigg counties. He was re-elected in 1999 and served as circuit judge until January 2007.

Justice Cunningham served the court system in several capacities before entering his judicial career. He was the Eddyville City Attorney from 1974 to 1991 and the Public Defender for the Kentucky State Penitentiary from 1974 to 1976. He served as Commonwealth's Attorney for the 56th Judicial District from 1976 to 1988. During his tenure in that position, he was voted the Outstanding Commonwealth Attorney of Kentucky by his peers. Justice Cunningham also served as a hearing officer for the Kentucky Board of Claims from 1981 to 1985 and as a trial commissioner for Lyon County District Court from 1989 to 1992.

Justice Cunningham earned his bachelor's degree from Murray State University in 1962 and his juris doctor in 1969 from the University Of Kentucky College Of Law. He is a veteran of the U.S. Army, having served in Vietnam, Korea and Germany.



CONTACT INFORMATION

1st Supreme Court District

State Capitol
700 Capitol Avenue, Room 216
Frankfort, KY 40601
Phone: 502-564-4163

103 West Court Square
P.O. Box 757
Princeton, KY 42445-0757
Phone: 270-365-3533

RESOURCES

News of Interest

[Supreme Court District Map](#)

Jail Mail

I came within 200 yards of being born in prison.

My mother gave birth to her fifth child in government housing just across the street from the Kentucky State Penitentiary in Eddyville, Kentucky. We youngsters grew up in the shadows of those brooding gray walls. The prison was a part of our lives. I first went to prison as a small boy, acting as a bat boy for a local baseball team. That's right. I was in and out of prison several times as a juvenile.

The prison shaped our early lives and we got to know many of the prisoners who served time there, especially the trustees who worked outside on the sprawling grounds of the Castle on the Cumberland. My third cousin, Hodge Cunningham, was the first guard killed there by inmates in October of 1923.

I went there as public defender for the inmates and then as Commonwealth's Attorney. As Circuit Judge, I presided over inmate cases in the little courtroom we have there. Even today, as Supreme Court Justice, I visit frequently. Some of the wardens and guards have become my good friends. So have many of the prisoners.

There is a saying, "If you have a thousand friends, you don't have a one to spare." I cherish my friendships with guards and prisoners alike.

Some of my inmate friends are actually people I have prosecuted or sentenced. I did my duty with respect for them as human beings. They took their medicine manfully. I never added one word of scorn or ridicule onto their sentences. Never humiliate anyone when they are helpless. Out of those unique encounters, guided with a proper respect, have come friendships. There are also others down through the years that I did not know prior to their incarceration, and met them for the first time at the prison. I also have friends who have stumbled badly, committed crimes, and are doing time in prison. I have searched in vain and have not found in our penal code the penalty of loss of friends as a required punishment. Nor the banishment of hope. For Shakespeare wrote, "The miserable have no other medicine but only hope."

So, I get mail on a weekly basis from inmates. Some of the mail comes from people that I do not know. People with whom I have had only a causal passing. Some may have passed through my court over the years. Some of the mail is from people that I have never encountered directly, but know who I am. Their letters are what we call *ex parte* attempts to reach directly into the Supreme Court of our state. These correspondents want their sentences reduced, a new trial, parole, or some other relief. They claim innocence, blame a prosecutor for being unfair, a defense lawyer for being inept, or a judge for being bias. Many blame girlfriends, wives, mothers, or anyone else but themselves. A letter lies on my desk, even as I write, asking me to intervene and grant probation.

These letters are easy to handle. I simply send them on to the appropriate person or agency—judge, defense lawyer, prosecutor, clerk, minister, Commissioner of Corrections, or whoever I might decide is

appropriate. Then I send the inmate a polite response, "Sorry son, I can't help you. I'm on the state Supreme Court." Or words to that effect.

Sometimes the letters are totally out of touch with reality. A few border on the humorous. I once received a letter from a female prisoner I had sentenced which read: "Judge, I really would like to serve the two years you gave me, but I really don't have the time. I've got other things I need to be doing."

The tough letters, the ones that lie around on my desk for days, sometimes weeks, awaiting a response are the letters I get from friends in prison. They are not asking me for anything. They are not asking for their sentences to be reduced, for me to send money to their accounts, or for me to talk to their lawyers or prosecutors. They are not even asking for my sympathy. They are asking for nothing except maybe a reply. Something from the outside world; from another human being; yes, from a friend. Words from someone outside of bondage who recognize they still exist. That they are still relevant to the world in some way. That they still merit some of our time and attention, meager as it may be.

I've been receiving these types of letters for years. I always respond, sometimes belatedly. But I have never fashioned what I consider an adequate reply. How do you tell a person in prison to "have a nice day"?

Have a nice day wearing the same khaki garb you wore yesterday and will wear tomorrow.

Have a nice day eating three meals of institutional food on stainless steel trays in a roomful of hundreds of sullen convicted felons.

Have a nice day hearing the continuous sound of metal doors clanging instead of the hum of a passing car or the shrieks of children down the street.

Have a nice day seeing your loved ones through Plexiglas only on certain days and times.

Have a nice day sauntering around the same sterile landscape of concrete and asphalt, paradoxically called "the yard."

Have a nice day living like this for the next five years, ten years, or the rest of your life.

I've never found the right words—ones that do not sound hollow or meaningless.

Neither does it seem humane to mention even the most mundane things in my life which we all take for granted. Things like mowing the grass, shopping at the mall, taking your kids or grandkids to ball practice, eating fresh vegetables, or simply sitting through the dawn of a summer day on your front porch with a porcelain cup of steaming coffee in your hand. All of these things would surely make the heart of the deprived reader ache at the thought of such blessings needlessly forfeited.

So, these letters lie on my desk for a while as I conjure the will to respond to them. To tackle the daunting task of writing something which is honest and yet hopeful. It doesn't take much. I have another letter on my desk from a friend in a Louisiana prison. He is 72 years old. He said that my last letter to him had "motivated him to go out on the yard" and do something about his poor physical shape by doing pushups and sit ups. I think that all I said in my letter was to merely inquire about his health.

We do not have to receive jail mail from friends in prison to be confronted with this somber challenge. The need to respond and offer hope to people confronts us all, almost on a daily basis. We are constantly encountering those friends who have fallen upon the thorns of life and bleed. The friend dying from cancer, the friend whose spouse is dying from cancer, the friend who has lost a child, the friend who has suffered a stroke and cannot move or speak. We all must answer "jail mail" from those dear people who have been imprisoned—perhaps for the rest of their lives—by a terminal disease, unbearable loss, or a life changing tragedy. It may even be a friend who has been the victim of crime and who is unalterably scarred by the experience. An injury inflicted by a person similarly situated with my friends who write me "jail mail" from prison.

We all struggle with the words to say. A good friend of mine was asking me for advice about visiting his nephew who was in prison on drug crimes. "What do I say to him, Bill, when I go visit?" I told him he didn't have to worry about what he said. Just being there would be enough.

Life is hard. Harder for some than for others. So we continue to meet those friends at the funeral home, in the hospital, casually on the street, in prison, who are suffering in seemingly hopeless situations. Muted and witless we stand with that friend who is bereft of hope. In that awful moment we share for a short distance their weary road, groping together in the desperate darkness for a hidden light.

That is the best we can do.

Law Day Speech to new Lawyers at the Capitol May 1, 2019
By Justice Cunningham(retired)

This is the 13th consecutive year that I have attended the May Day ceremony in this historic chamber. It's been my honor to hear outstanding speakers speak from this podium **the best of which some of my fellow brothers and sisters of the Supreme Court.**

I'm also mindful that perhaps the greatest orator in the history of the United States, the great **William Jennings Bryan** stood on this very spot and addressed the joint meeting of the Kentucky General Assembly on **January 19, 1922**—over 97 years ago.

So, to be very honest with you today...**I've always wanted to speak at this event.**

Wendell Ford story; the old prospector; I always wanted to.

So thank you Chief Justice and Associate members and **Ms. Clary**, for giving me the opportunity this morning to do something I've always wanted to do.

Another reason this is special for me personally is, that I celebrate 50 years as a lawyer this year. You are just beginning. ***I'm falling into the sere, the yellow leaf, you are just bursting into full bloom.***

I have no magical words of wisdom for you this morning...no profound insights, but only, to paraphrase the great **Patrick Henry**, **"I have but one lamp to guide you here today, and that is the lamp of my experience."**

First, the good news. If I had it all to do over.....I'd choose to be a lawyer everytime. There is no greater boast in the grand pantheon of callings, than to say, **"I am a lawyer. I work for justice."** You are only a few minutes away from joining that noble band.

My limited time this morning compels me to share with you only **two** of the most important things my experience of being a lawyer has taught me.

First, if you want to have a happy life as a lawyer be nice to everyone. ***If you want to have a disastrous life that will lead to alcohol and drug addictions, ruined marriages, and mental illness, then follow those miserable barristers who follow the deceptive sirens of greed, win at all cost—hard ball. They follow the failing banner that nice guys finish last. I present to you exhibit A to totally destroy that myth this morning. The seven justices sitting right here are all in first place. They are all some of the nicest people I have ever met. I rest my case.***

Be nice to everyone—opposing lawyers, their clients, jurors and witnesses, and secretaries and law clerks. *Be nicer to the judge's secretary than you are to the judge; nicer to the deputy clerks than you are to the clerks; nicer to the people who clean the building, than the person who owns the building.* Back on a rainy afternoon in the late 1890s, an elderly lady walked into a Philadelphia department store. Young clerk asked if he could help, and she responded that she was just getting out of the rain. He didn't try to sell her anything, but simply got her a chair to sit in. After the rain stopped, she asked for his card and left. It was Andrew Carnegie's mother. Andrew Carnegie was one of the wealthiest men in the history of the United States. Later the store received a letter from Andrew Carnegie requesting that the store furnish his entire castle in Scotland and that the young man who gave his mother a chair be sent to fulfill the order. Yes, always be nice to everyone.

Make small professional courtesies, steeped in the aged tradition of our profession a part of you being nice, a part of your practice.

****Marvin Prince.**

Secondly, do not let technology swallow up who you are. Do not lose your humanity to technology. The toughest thing about suffering through my speech right now is having your cell phone off. **Steve Jobs, the founder of Apple, refused to allow his children to have an iPad.** "We limit how much technology our kids use," he said, "We think it's too dangerous." **Senator Ben Sasse in his book "Them" says, "we are likelier to spend time seeking validation from our digital 'friends' than to spend time with flesh and blood friends."**

You would be offended if I told you that you were enslaved to your girl friend, or your husband, or to a senior lawyer in the firm. Yet, we become impervious to being enslaved to technology. The ones here today who will rise above all others will be the ones who know when to quit the texting and make the phone call; when to turn off the e-mail and communicate face to face. Construct an inner antenna to recognize that need. It's ironic that modern technology makes it easier for us to communicate, but we use it to communicate less successfully.

In November of 1972, I voted by absentee ballot from Vietnam in the presidential election between incumbent **Richard Nixon** and challenger **George McGovern**. President Nixon won that election 3 with 60.7 % of the vote, carrying every state but one. Years later I was sitting in a fancy restaurant with my friend David Whalin, congressional aide to Congressman Carl Perkins. A man walked in the restaurant and began greeting people at the next table. He looked vaguely familiar. "You know who that guy is?" David asked. "I don't know. He looks very familiar." I responded. "That's George McGovern" he replied. I was incredulous. It couldn't be George McGovern. This man was smiling, shaking hands, engaging people in conversation. He was warm and appealing. I liked him. The real George McGovern did not come through on the technology of television. Don't let that happen to you. God gave each and everyone of you a personality. Use it. Don't lose it to the cold screen and unfeeling touch of your cell phone or computer.

Technology is the great equalizer..making everyone bland and lifeless.

With all of that said I fully recognize that it is highly unlikely that any of you will remember anything I say here today. In fact, fifty years down the road, when you are where I am, I bet you the farm, you will not even remember who was the speaker here today. *If you do....call me. I'll give you the farm.*

But I promise that there are two things which you will remember about today.

1. **You will remember how you felt.** You will remember the joy of being here with your family and loved ones, who look on proudly. Picture taking. Snap, snap, snap. Seeing your friends who also made it to the top of the heap, great sense of accomplishment from all the hard work.
2. You will remember this moment just as you will remember the thrill of that moment you learned that you passed the bar exam. **Hold onto that feeling.** You are going to need it over the long, challenging journey ahead of you. Put it in a bottle, and put it on your shelf. And when those days come, as they do in any profession worthwhile, when you become stressed from the burden of other people's problems; when you are discouraged and depressed from a series of setbacks and losses; when you dread getting up to face a particular client, a particular hearing; a particular judge.....when you have second thoughts about being a lawyer..take a big swig of this feeling and be renewed with that energy and pride....knowing that any job that matters, any job dedicated to helping others, and problem solving, any job worthwhile...the job of being a lawyer, will have days and moments like that.
3. The second thing you will remember is that you took **an oath** here today. The oath that you will be giving shortly.....the magical oath.....the scant few words. One moment you are a lay person, and the next.....poof....you are a lawyer. **You ride up here with family members who you have been giving free legal advice to for the past three years, and now you can charge them for it on the way home.**

What is an oath? The dictionary defines a oath as ***“a solemn promise, often invoking a divine witness, regarding ones future action or behavior.” A promise. Giving your word.***

I have taken this same oath seven times in my life. When I became a lawyer, and six times being sworn in to public office. I’ve adminstered this oath to Governors, Lt Governors, other constiutinal officers, judges and lawyers, school board members and mayors. I’ve never let them get off with a yes or no answer. I make them repeat it. It’s not my oath; it is their oath. Ms. Clary will let you off with a yes or no answer here today. But.....it is still your oath. You are giving your word to us, to the people of Kentucky, and “so help you God.”, that you will **support the constituion of the United States and the Commonwealth of Kentucky.**

We live in the land of the free and the home of the brave. We remain free only if we remain brave. It is not large fleets of black bottomed ships, nor marching brigades of soldiers that keep us free. It is the constiution. **The executive branch doesn’t keep you free. Unfettered it will become tyranical; it is not the legislative branch which keeps you free, for unchecked it becomses an oligarchy. It is the judicial branch and lawyers which keeps us free, through the enforcement of our constitutions.** So, in effect, *you are freedom fighters.* Outside your wedding vows, it will be the most important promise you will ever make.

During my 12 years working in this beautiful temple of democracy, I kept on my wall in my office the old and tattered 8th Grade Diploma of my father framed and hanging on my wall. My father only had an eighth grade education but he had a juris doctorate in character. My character was molded out of watching the way he lived his life with honesty, self-discipline, integrity, charity, hard work, and total devotion to my mother and his children. **Character is caught more than it is taught.** But there was one verbal admonition he gave me,

not once, but many times as I was growing up. He gave it to me so many times that that I came to think that *even my Baptist conversion would not save me from eternal damnation if I violated it*. That admonition was simply this. **“Always keep your word....even when it takes the skin off your nose.”** That description quickly catches the attention of a small child. Every rambunctious child knows the pain of having the skin taken off your nose.

Please take heed that keeping your oath, keeping your word to support and uphold the constitution may sometimes take the skin off your nose.

For Example: *A prosecutor provides evidence to a criminal defendant who has committed a heinous crime knowing that such evidence is likely to cause that criminal to go free—because the constitution through the interpretation of the U.S. Supreme Court requires it. *It takes the skin off his nose.*

For example: a trial judge suppresses evidence in a serious criminal trial—because the constitution requires it. And pays a terrible political price. *It takes the skin off his nose.*

For example: *this Court right here late last year struck down two important laws enacted by the General Assembly, and both the executive and legislative branch announced war upon the court and the judiciary for their upholding their oath of office in supporting the constitution of the Commonwealth of Kentucky.

For example: *a legislator stands here in this chamber and votes no to proposed legislation because he knows or strongly suspects it is unconstitutional while a mob of voters scream out in the rotunda for him or her to vote yes. Knowing that his vote may well lose him the next election he remains true to his word in supporting the constitution. *It takes skin off his nose.*

I wish I could impress you with these remarks of the gathering storm clouds which threaten our republic. It's the growing disrespect for our constitution. Our country is imperiled. **More and more public officials, some of them lawyers, are treating the constitution like a**

side dish no one ordered. More and more are treating it like an impediment to power, rather than a birthright to democracy. We live in the most perilous times in our history, endangered not by foreign powers, but by our own neglect of our constitutions. The only thing which prevents us from being ruled by dictators or tyrants is our constitution. If the 34 lawyers at the 1787 U.S. Constitutional convention had not been lawyers first, and politicians second....we would not have a constitution. If you are not lawyers first and politicians second, we will not keep our constitution.

I'm not sure we're going to make it. And I'm not the only one. But there is hope. The hope is in our lawyers. **David Brooks, noted columnist who is not a lawyer, was referring to these perilous times when he wrote in the New York Times on Feb 22 of this year:**

In speaking of lawyers as the saviors of America he said, "The legal institutions instill codes of excellence that are strong enough to take the heat. Those people(lawyers) have enough character to live up to those codes. They are clinging tenaciously to old standards of right and wrong, to the Constitution, and the rule of law. And if we get through this, it will be because of people like them."

So, when you stand here in a few moments and Ms. Clary ask if you will support the constitution of the United States and the constitution of the Commonwealth of Kentucky.... In that fleeting moment please insert in your own passing thought, "even if it takes the skin off my nose." Then, and only then, will you have the right to call yourself a lawyer.

(pause)

In closing, this old warrior wishes you nothing but success and happiness in the exciting years ahead. We send you off with the words of Virgil, **"God's speed to your youthful valor, may you scale the stars."**

Easiest Catch: Don't Be Another Fish in the Dark 'Net

You've read the headlines. Unfortunately, the question now is not if your information is going to be accessed or stolen, but when. To inform the attendees of current developments in the digital underground as well as provide realistic advice for cyber protection, Mark Lanterman will be discussing recent high-profile cybercrime events, including website breaches impacting a variety of organizations and sectors. Mark will discuss particularly dangerous types of threats that might affect individuals involving the Dark Web, the Internet of Things, phishing, and Wi-Fi attacks; additionally, Mark will demonstrate the value of leveraging digital evidence and ESI in the courtroom.

Speaker Bio

Mark Lanterman is the Chief Technology Officer of Computer Forensic Services. Before entering the private sector, Mark was a member of the U.S. Secret Service Electronic Crimes Taskforce. Mark has 28 years of security and forensic experience and has testified in over 2000 cases.

Mark is faculty for the Federal Judicial Center in Washington, D.C., the National Judicial College in Reno, Nevada, the University of Minnesota and the Mitchell Hamline Law School. Mark is a professor in the cybersecurity program at the St. Thomas School of Law in Minneapolis, Minnesota.

Mark has provided training in digital evidence, computer forensics and cyber security to the United States Supreme Court. He has also presented to the 8th and 11th Circuit Federal Judicial Conferences as well as numerous State and Federal Judicial Conferences across the United States.

Mark completed his postgrad studies in cybersecurity at Harvard University and is certified as a Seized Computer Evidence Recovery Specialist (SCERS) by the Department of Homeland Security.

Mark is a member of the Minnesota Lawyers Professional Responsibility Board and serves on its Opinions Committee.

Bench & Bar

OF MINNESOTA



***More implications
of the new
Minnesota
LLC law***

***Trends in legal
office space***

***The creation
of the Client
Security Board***

***Preparing
the Witness
to Win the
Deposition
Battle***

Is the Internet of Things spying on you?



So is your phone spying on you? Yes, it's possible.

A few months ago, Computer Forensic Services analyst Sean Lanterman spoke to KARE 11 News about a topic that makes a lot of people nervous. "Is my phone spying on me?" may have seemed like a paranoid question at one point, but it now seems like a perfectly plausible notion. Given the vast amounts of data created, stored, and transmitted by the average person's phone, it's actually a question we should all be asking. Sean pointed out the very real fact that our phones are basically snitches in our

pockets, and it's not impossible that advertisers would take advantage of this fact. After all, what better source of information is there than our phones when it comes to gathering intel about our preferences, shopping trends, and habits?

So is your phone spying on you? Yes, it's possible. Your smartphone's capabilities allow for the kind of spying that many suspect;

your phone may communicate information about you to advertisers, and from there, personalize ads to match what has been gathered. This information can be gathered in pretty sneaky ways, too—for instance, by using your phone's microphone to capture your conversations without your awareness. The question can grow still more complicated when you apply it to your other internet-connected devices. Smartphones are probably the biggest storehouses of our personal information that we utilize on a daily basis, and for that reason, they are probably the devices that transmit the most data about us as well. But now, internet-connected devices can include everything from your thermostat to your car to your refrigerator.

These devices often feature a large range of multimedia capabilities that extend far beyond their technical use. Microphones and cameras are common elements of some of our internet-connected devices, not to mention other more advanced technologies such as GPS and voice recognition. To further confuse things, the average consumer may not know which devices have which features, especially since something as simple as a washing machine may now be equipped with exceedingly advanced technology. How do we manage all of these devices and ensure the best possible security practices?

Keeping a tally of all the internet-connected devices in your home may be more difficult than you think. Smartphones, watches, laptops, computers, entertainment systems, security cameras, TVs, cars, and the types of home appliances mentioned earlier may come to mind. But there are also trickier sources of internet-connection lurking in your home, like your kids' toys. And at the community level, everything from water plants to the power grid are connected by the internet. Can we effectively manage the risks to our privacy and security when so many of the devices we now rely on store and communicate our personal information? And what do we do when this information is compromised or our devices are taken over by cybercrime? Many of us are familiar with company and organizational policies relating to

cybersecurity best practices. But when it comes to our own homes, many are less equipped and less eager to train themselves and their families in cybersecurity.

First, taking stock of which devices could potentially be spying on you, besides your phone, is important. Understanding what you buy is critical to maximizing effective use of the product and minimizing the potential risks. This is especially important when privacy concerns come into play. Knowledge of your devices includes a basic understanding of what kinds of data they collect, how this data is stored, and why and how it is communicated. If a microphone is suspected of being the culprit in leaking information, navigate settings to figure out a way to turn it off. Ideally, this kind of research is done beforehand, but proper device setup and knowledge of an item's security features can be critical in mitigating risk. Ultimately, you may decide that an internet-connected thermostat or fire detector isn't worth the hassle.

Second, once you've decided which devices are worth keeping around, take stock of the potential threats against your privacy and security. You may not be completely aware of the devices that create, save, and communicate sensitive information about you. Even though many people click the "I agree" button, most are not fully aware of what their consent implies, or means for the companies that profit from this kind of mass data sharing. A compromised device can also be used to execute greater attacks. It should be noted that hackers don't discriminate. An internet-connected device is always a target, regardless of whether it's a toy, a phone, or a computer.

If one or more devices are spying on you, it's difficult to pinpoint who or what is doing it. As Sean explained on KARE 11, there are no individuals at the receiving end, but rather an automated process comprising advanced algorithms to decipher the data being sent. Knowing how best to configure the settings on your internet-connected devices, and being aware of how many devices may pose security and privacy risks, are two keys to a proactive approach to minimizing the potential of digital spying. ▲



MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

Bench & Bar

OF MINNESOTA


***Lessons
for lawyers
from the
post-Weinstein
reckoning***

***#MeToo as
a moment
opportunity***

***How to change
firm culture***

***Trump Year One:
A conversation
with immigration
lawyers***

***Beyond the
travel ban:
Headaches
for employers***

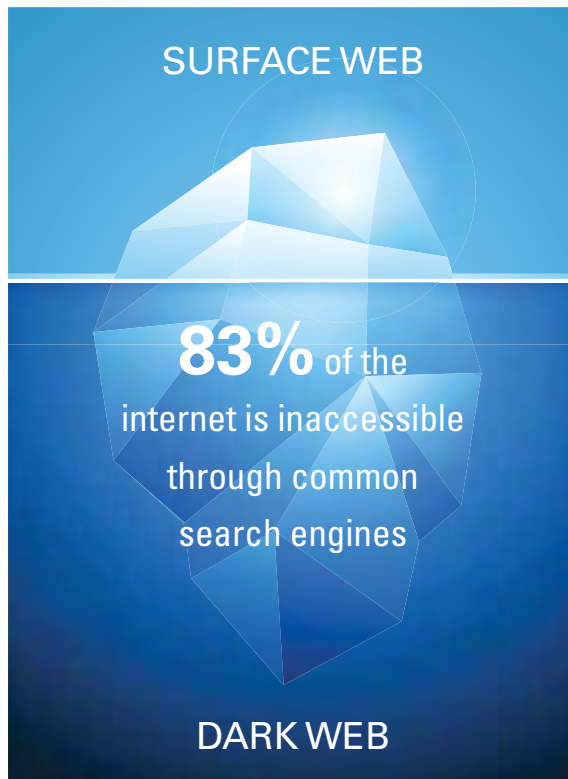


**#MeToo
IN THE
LAW FIRM**

Stephen Allwine: When crime tries to cover its digital tracks

In late 2016, I was approached by the Washington County (MN) Attorney's Office to conduct forensic analysis on a number of devices in a homicide investigation. It soon became clear that the case would be one of the most interesting of my career, involving murder-for-hire, religious convictions, insurance money, infidelity, and a distinctly modern element—the Dark Web—that combined to make for one of the most tragic and complex cases I've encountered.

The Dark Web, a broad term used to describe the 83 percent of the internet inaccessible through common search engines like Google or Bing, is where many people go to find illegal drugs, child pornography, stolen credit card numbers, and hacking services (though not every service and product available in this online marketplace is illegal). Enter defendant Stephen Allwine: After his attempts to



affairs through this site—many users who sign up for Ashley Madison and similar cheating sites don't actually end up having affairs—he still did not regard divorce as an option. Constrained by the marital requirements of his church, Allwine took a dive into the Dark Web to search for other solutions to his predicament. It wasn't long before Allwine discovered Besa Mafia, a Dark Web group claiming to provide anonymous hitman services.

Besa Mafia was a Dark Web vendor that advertised themselves with the slogan "Hire a killer or a hacker." The enterprise was later revealed to be a scam, but Allwine—using the pseudonym "dogdaygod"—communicated extensively with Besa Mafia, communications which were subsequently released to the internet. These communications included multiple references to Amy



MARK LANTERMAN is CTO of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security/forensic experience and has testified in over 2,000 trials. He is a member of the MN Lawyers Professional Responsibility Board.

hire a hitman on the Dark Web failed, Allwine murdered his wife in their Cottage Grove home and staged it as a suicide. In January 2018, Allwine was sentenced to life in prison; forensic analysis played a critical role in fleshing out the narrative details that helped the jury make their decision.

In 2015, Steve Allwine began exploring a website known for neither its upstanding moral

quality nor its cybersecurity strength—Ashley Madison. Through this cheating website, Steve began experimenting with extramarital affairs and the underbelly of the internet. Analysis of Allwine's devices revealed communications with at least two women through the site; their conversations illustrated Allwine's dissatisfaction with his marriage and his desire to become involved with other women, unhindered.

Exploring the Dark Web

While Ashley Madison itself is not part of the Dark Web, I would consider it to be a kind of gateway to the darker aspects of internet usage. It wasn't long after his first few Ashley Madison-initiated affairs that the Dark Web became a prominent part of Steve Allwine's browsing.

Jurors learned that Allwine first discovered Ashley Madison as a marriage counselor for couples in his church. Though Allwine ultimately initiated

Allwine and included her home address, phone number, physical description, and a photograph. One particularly thorough attempt to organize the hit once and for all involved Allwine providing particular location information, a current picture, and a description of her vehicle. Of particular note was the photo shared, which was subsequently discovered in a folder on one of Allwine's devices. But the hit he sought to arrange never occurred, and Allwine would later report his lost thousands of dollars to the police.

While Allwine clearly endeavored to remain invisible on the Internet, a key piece of evidence unequivocally tied him to a Bitcoin payment made to Besa Mafia for the murder of Amy Allwine: a unique, 34-digit alpha-numeric Bitcoin wallet address typed out in his iPhone's Notes app that had been deleted. This Bitcoin address matched the one used by "dogdaygod" to make a payment to Besa Mafia.

Though Bitcoin has become increasingly popular in recent months even among non-Dark Web users, it remains the preferred currency for Dark Web exchanges. The address found in Steve Allwine's deleted note proved to be critical to the case. As Washington County prosecutor Fred Fink explained later, "It was absolutely vital for the State to prove that 'dogdaygod' was, in fact, Stephen Allwine. With that connection made, we were able to show intent to kill and premeditation."

A pattern of deception

My analysis of Steve Allwine's devices also reveal a steady pattern of anonymizing service use, disposable account creation, and a desire to conceal his identity from law enforcement. My office was provided with a staggering 66 devices—a huge number in comparison to the typical homicide case. Allwine used multiple devices to further obscure his online activity. On his Reddit account, also using the pseudonym "dog-daygod," Allwine frequently researched

questions pertaining to safe use of the Dark Web, the likelihood of law enforcement presence on the Dark Web, how to use disposable computers, and how to remain anonymous on the Internet. To access the Dark Web, Allwine used virtual private network services and the TOR network. These services act as portals to the Dark Web and encrypt accessed information by relaying it through a series of other networks. Incredibly, Allwine also used disposable email accounts to report evidence of his stolen Bitcoin to police after the hit did not materialize. He even created a fictitious person to frame for the stolen Bitcoin.

Allwine's digital narrative also revealed a browsing history consistent with his intention to murder Amy and his desire to frame fictitious parties. On more than one occasion, Allwine reviewed his and Amy's insurance policies as well as real estate and future home construction possibilities. In an effort to blame an unidentified third party, Allwine sent his wife a threatening email using an anonymous email service—after he had used

doxxing (the process by which personal information is bought and sold on the Internet, often with malicious intent) to uncover information about Amy's family to personalize his email and make it appear as if it was sent by a business rival.

Ultimately, forensic analysis shed light on the actual truth of what occurred, which pointed solely to Stephen Allwine as the guilty party. This case incorporates some of the most complicated aspects of digital evidence. It was complex in part because Allwine had done everything in his power to conceal his activity, remain anonymous, and hide as much as possible about his intent. Digital forensic analysis revealed critical details that filled in gaps in the physical evidence—gaps that may have inspired doubt in the jury and led to a different verdict. As Washington County attorney Pete Orput described the role of digital evidence in this case, "Mark's forensic work and testimony about it to a jury made my murder case seem simple and overwhelming, and without this work the case would have been a horse race." ▲

Minnesota Legal Ethics

An ebook published by the MSBA – written by William J. Wernz

Free download available at: www.mnbar.org/ebooks

***This guide
belongs
at every
Minnesota
attorney's
fingertips!***



7TH EDITION

Bench & Bar

OF MINNESOTA

***How Law
Firms Can
Prepare
for Partner
Retirement***

***Succession
Planning for
Small Law
Firm Owners***

***Is your firm
complying
with the
Minnesota
Professional
Firms Act?***

***2017 CLIO
Legal Trends
Report***

GOODBYE TO ALL THAT

**Thoughts on turning 67
and knowing when to quit**



How digital evidence supported gerrymandering claims

Earlier this month, I had the once-in-a-lifetime opportunity to travel to the United States Supreme Court to witness the headline-making gerrymandering oral arguments out of Wisconsin. Some people are calling this case the most important of the year, with enormous potential consequences for political redistricting and any number of similar cases in which gerrymandering claims play a part.

During a five-month period in the Senate in 2012, the Democratic party made the most of its short-lived majority to gather digital evidence in support of their extreme gerrymandering claims against the Republicans. I was asked on behalf of the Campaign Legal Center in Washington, D.C. to provide digital forensic analysis of hard drives that had been gathered from Wisconsin lawmakers. These hard drives had been used by the mapping drafters and ultimately showed that one party had worked to gain a clear advantage, even in the event that they did not win a majority of votes. My analysis led to the discovery of several key deleted files, including deleted spreadsheets, that revealed a systematic pattern of intent: The metadata revealed that with each draft of the spreadsheets, the map-drawing lawmakers attempted to strengthen their party's majority and retain control.

Does delete mean deleted?

Upon my initial review of the hard drives provided, it became clear that a large number of files had been deleted immediately before the digital evidence had been delivered to my office. It is interesting to note that even at the state Senate level, key players in this case didn't understand that delete doesn't always mean deleted. I determined (and later testified) that hundreds of thousands of files had been deleted using a commercial wiping program in the week prior to the computers being turned over to Wisconsin Senator Mark Miller.

The Campaign Legal Center's request for an independent forensic investigation was instrumental in constructing this case. Seeing that fraud or some kind of misconduct had most likely taken place, the court granted the request, which ultimately led to my review of the hard drives in question. The pattern of purposeful wiping further confirmed suspicions.

A second review of the digital evidence

After the first case settled out of court in 2013, I was approached again to conduct another limited analysis of the hard drives to uncover more relevant digital evidence. As attorneys built their case for the United States Supreme Court, digital evidence continued to play a key role in unraveling



a narrative of purposeful, extreme gerrymandering on the part of one of the political parties.

This subsequent analysis of the provided hard drives led to the uncovering of several deleted spreadsheets, and detailed the redistricting map drafters' plans to gain a 54-45 projected majority over the other political party, regardless of whether or not they actually won the majority of votes. One particularly damning spreadsheet, labeled "Tale of the Tape," demonstrated that the minority political party in Wisconsin would need at least 54 percent of the vote to gain an Assembly majority. Clearly, the map drafters had been attempting to manipulate the mapping as much as possible to put the minority at an extreme, and perhaps unconstitutional, disadvantage.

My subsequent examination of the digital evidence also revealed some critical metadata, data which may have been overlooked had the plaintiffs opted for a simple e-discovery procedure over digital forensics. Metadata is a term used to describe "data about data," and in this instance, the critical metadata consisted of timestamps. The creation dates of the maps located on the hard drives, and their associated revisions, allowed for the reconstruction of a timeline revealing that with each round of revisions, the maps' drafters were purposefully solidifying their majority. It should be noted that these maps would determine which political party would be in control for a span of over 10 years. The stakes were high, and as with many forensic analyses, the devil was in the details.

Conclusions

The opportunity to play a role in a Supreme Court case was an amazing experience, and it served to underscore some of the things I know to be true about digital evidence. The faster you can gather it and preserve it, the better. The plaintiffs made the absolute most of their temporary majority in the Senate. Prioritizing the collection and preservation of digital evidence was a strategic move that showcased the profound impact of digital evidence in shaping the course of a case. In this instance, it could have nationwide consequences for gerrymandering and political mapping. Apart from the political consequences, I think this is a clear-cut example of how digital evidence can make a case by serving as an impartial witness in court. As if that weren't enough, I also sat directly behind Arnold Schwarzenegger during the arguments. ▲



MARK LANTERMAN is the chief technology officer of Computer Forensic Services. A former member of the U. S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security and forensic experience and has testified in over 2,000 cases.

Bench & Bar

OF MINNESOTA

GRAVE MATTERS

The law and practice of disinterment,
reinterment, and exhumation in Minnesota



WE'RE
MOVING!

Why You May Need
an LLC Update

Your Personal Data
– Or Is It?

An Out of Court
Article on Hearsay

RENEW YOUR MSBA DUES AT:
MNBAR.ORG/RENEW

Your Personal Data – Or Is It?

Doxxing and online information resellers pose threats to the legal community

By MARK LANTERMAN

Photo © iStockphoto



Given the sensitive nature of the courtroom and of the emotions that may arise there, attorneys, judges, and others in the legal community are at particular risk of becoming victims of doxxing-related crime. *Doxxing* is a term used to describe the buying, selling, gathering, posting, or distributing of private information online. Importantly, doxxing is typically carried out with malicious intent and is often aimed at damaging someone's reputation. As opposed to the mere gathering of information from someone's Facebook or LinkedIn profile, doxxing is often abetted by targeted data breaches. The distinction here is that anyone who posts on social media is essentially allowing the public at large to view, and use, that information. The kinds of private information spread through doxxing are not typically shared by the subjects themselves.

Everything from health to legal information is valuable to cybercriminals and hackers, and it is therefore exactly the kind of information that is commonly put on online. Apart from financial data, information related to health and legal circumstances can be of particular interest to an individual interested in harming another's reputation or career. Unfortunately, many doxxing victims don't realize that they have become victims until

something serious has occurred or they realize that the information has already been widely distributed.

Though the personal information-gathering associated with doxxing can often be assisted by cyberattacks, doxxing itself is not necessarily illegal. Many people are not aware that their private information is widely available on personal information reseller websites. These websites are easily accessible by the average user, no Dark Web required. The information contained on these sites can divulge where you live, who your past employers were, and can even connect you to the last person living in your home or apartment. Fortunately, these websites give people the ability to opt out and remove their information. The problem is that the actual time it takes to remove the info, or the processes required to achieve this, can be confusing or cumbersome depending on the website.

Furthermore, some of the websites do not directly store your private information, but rather give users a list of other websites that do. For this reason, the individual is left to chase down their information on a number of websites instead of just one. And the fact is, even if someone takes the time to opt out of each one of these websites, it is very possible that they will repopulate their sites within a matter of months with the same informa-

tion you requested be taken down. With this in mind, I would say that the majority of people are not aware of exactly how much private information is available about them online at any given time.

Private information can be used to physically stalk, harass, or threaten individuals. But it can also be used to harm a person's reputation or disrupt the victim's personal life. Recent headlines have focused on judges that have been targeted; however, everyone in the legal community is at an increasing risk of having their private information accessed without consent or knowledge. Given the rise of the Internet of Things (IoT), more and more data from our daily lives is being collected, stored, and distributed. Though this may be convenient, more data makes for a greater risk that it will be compromised. The number of devices comprising the IoT also makes for a wider array of potential access points for the cybercriminal. Since the process of doxxing often relies on the successful execution of data breaches, the Internet of Things presents the perfect blend of vulnerabilities and useful data.

The legal community is not immune to the changes brought about by the IoT. Living in a world of interconnected devices makes for easier communication, more efficient workflows, simpler data collection and storage, and a generally

OPT-OUT FORMS FOR MAJOR PERSONAL INFO RESELLERS

LINKS	VERIFICATION NEEDED	TURN-AROUND TIME
pipl.com/help/remove	Pipl is a search engine that does not host personal information, but it is a good starting point for identifying personal information from other sources.	Depends on other sources from which Pipl populates its search results.
www.beenverified.com/optout	Email address	24 hours in most cases
www.checkpeople.com/optout	None	7-14 days
www.intelius.com/optout.php	Government-issued ID	7-14 days
www.peoplesmart.com/optout-go	Email address	Up to 72 hours
www.publicrecords360.com/optout.html	State-issued ID	This site does not disclose turn-around time.
www.spokeo.com/opt_out/new	Email address	30 minutes
support.whitepages.com	Email address and phone number	Immediate
www.zabasearch.com/block_records	Redacted state-issued ID card or driver's license	4-6 weeks
www.zoominfo.com/lookupEmail	Email address	"Within a few days"
www.familytreenow.com/optout	Email address	Unknown

more productive way of managing things. Smartphones and Wi-Fi-connected devices mean greater accessibility and use of our personal information; for many IT departments, this convenience is the most important consideration when developing new technology policies. But the IoT is as risky as it is convenient. Many people don't understand the sheer amount of data that is being produced and stored about them. And each connected device is essentially another access point for a cybercriminal to compromise this data. For the same reasons that connectivity is great for communication, it is detrimental for security and keeping vulnerabilities contained.

In addition to providing opt-out information in this article, I will also provide some realistic risk-management advice. While it often feels as if the expansion of our digital lives is necessary, taking stock of the risks is important in managing security. For those in the legal community, developing a sound cybersecurity protocol is not only a responsibility to clients. It is also an important step in protecting your own privacy and keeping your personal information safe.

When assessing your current cybersecurity strategies, try to look from the outside in. Identify what data is most important and valuable. Also try to figure out where this data is currently being

kept and what measures are in place to safeguard it against cyberattacks. Issues of employee compliance or outdated policies may arise during this examination, but making this kind of assessment is a very important step toward improvement.

To help those who are interested, I'm listing the names of several major personal information resellers and corresponding information about how to remove your personal data from their websites.

Opting out of personal information reseller websites is a solid step toward bettering your online behaviors. Keeping private information secure is not automatically guaranteed, especially when there are websites that profit from selling your info to anyone who might be interested. And like other cybersecurity protocols, checking these kinds of websites should be done fairly regularly. Opting out only removes the information that is currently posted; it doesn't neces-

sarily prevent one of these websites from re-populating with your personal information in the future. Also, bear in mind that it is important to be proactive when it comes to removing your information the first time. Be mindful of the websites' turn-around times and don't let your opt-out request fall of your radar, or theirs, in the meantime. Though it may seem like an annoying chore, for those that are worried about becoming victims of doxxing, it is well worth the effort.

Like many changes that have arisen with the Internet of Things, doxxing is yet another issue that may affect you. Being mindful of what data you are sharing through your digital devices and doing your best to monitor your online presence are important elements of your personal cybersecurity strategy. Protecting your personal information is ultimately just as important as protecting your clients' data. ▲



MARK LANTERMAN is the chief technology officer of Computer Forensic Services. Before entering the private sector, Mark was a member of the U. S. Secret Service Electronic Crimes Taskforce. Mark has 28 years of security and forensic experience and has testified in over 2000 cases. He is an adjunct instructor for the University of Minnesota M.Sci. Security and Technology program, Mitchell Hamline Law School, and the National Judicial College in Reno, Nevada. Mark also conducts training for the Federal Judicial Center in Washington, D.C.

✉ MLANTERMAN@COMPFORSENSICS.COM

Bench & Bar

OF MINNESOTA

LITIGATING SPORTS CONCUSSIONS

**WHAT YOU NEED
TO KNOW ABOUT
THE SCIENCE
AND THE LAW**

*Ethical Considerations
in Working with
Aging Clients*

*Happy Birthday,
Whistleblowers:
Minnesota law turns 30*

Plus
***Are Title Company
Kickbacks Harming
Your Clients?***



Digital evidence: New authentication standards coming

As it is now written, Federal Rule of Evidence 902 pertains to self-authenticating records such as newspapers and public records that require no external evidence to be made admissible at trial. Soon, the rule will encompass digital records generated by electronic processes in addition to records preserved directly from electronic devices or files, such as emails. This December, new amendments to Rule 902 will affect the standards for the admissibility of digital evidence. Newly proposed paragraphs 13 and 14 of Rule 902 will remove authentication hurdles for electronic evidence, whether it consists of an electronic document, file, or raw data. The proposed text of rule is as follows (emphasis added):

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces *an accurate result*, as shown by a certification of a *qualified person* that

complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.

Data copied from an electronic device, storage medium, or file, if *authenticated by a process of digital identification*, as shown by a certification of a *qualified person* that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

With this change, digital evidence, and the story it tells, have many foundational questions out of the way. Without knowing how courts will apply the rule, however, I think that there is one caveat that will impact litigants—chain-of-custody/acceptable collection practices. With these upcoming changes in mind, it is clear that proper evidence collection and acknowledgment of best practices are critical. In this article, I will describe issues pertaining to proper digital evidence handling and the increased need for digital forensic professionals in light of these upcoming amendments.

A focus on best practices

The rules being implemented this December will greatly ease the burden of authenticating digital evidence and allow for a more cohesive system of evidence collection. These amendments largely serve to replace live testimony from any number of witnesses for the purpose of authentication with an affidavit from a certified person who can reliably attest to the evidence's authenticity. These new amendments underscore the court's increasing reliance on expert witnesses in preserving and bringing forth digital evidence.

Digital evidence is undeniably a prominent feature in the courtroom. In a growing number of situations, pieces of electronically stored information are the basis of investigations within organizations, for law enforcement, and in litigation. This degree of importance requires an equally high degree of care. Issues of authentication and proper evidence handling are particularly pertinent, since digital evidence is extremely susceptible to alteration and mishandling if not done properly by a qualified individual.

To illustrate, I will describe a typical, though always frustrating, situation that I encounter when assisting an organization or company responding to an incident involving digital evidence. Let's start here: Your company has a summer internship program. Each summer, one or two interns join your team and are assigned a number of different tasks that require varying degrees of access to your company's data. At some point during the internship period, it is discovered that one of these interns has been attempting to send confidential client data to a personal email address without prior authorization. IT is subsequently alerted and they are asked to handle the situation. Their first step is to retrieve the systems issued by the company to the offending party.

In an effort to deduce what exactly has occurred (i.e. what kinds of information were shared, with whom, and how many times), the IT person logs into the system with the intern's user credentials one day after the incident has been reported. The IT person clicks around on the intern's issued computer, trying to figure out what has transpired. This is not best practice. Although it is well-meaning, simply turning on a computer or electronic device permanently alters the state of the data. Think of it like a crime scene. Just as law enforcement wouldn't want to go snooping through a scene without taking proper precautions to ensure evidence will not be contaminated, digital evidence requires the same degree of care.

In reality, the IT person has unknowingly altered date and time stamps, overwritten useful deleted data, and skewed the original digital narrative of the intern's activity. In this instance, the intern's computer has been mishandled, making authentication an even greater hurdle down the road. While this evidence potentially held information that would have made the details of this event crystal clear, the IT person's involvement has made things murkier, and possibly not self-authenticating under the proposed additions to Rule 902.

So what should the IT person have done instead? Turn off the system as



MARK LANTERMAN is the chief technology officer of Computer Forensic Services. A former member of the U. S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security and forensic experience and has testified in over 2,000 cases.

quickly as possible and find a digital forensic expert for forensic preservation. While IT departments promote cybersecurity and technology policies, it is important to differentiate between IT services and digital forensics. The former is proactive or precautionary, and the latter is reactive (e.g. used in litigation).

Therefore, using forensic methodologies that leave the “crime scene” unaltered, so to speak, is key for ensuring compliance with Rule 902. Adhering to best practices in the collection of digital evidence is emphasized in the upcoming additions to Federal Rule 902. Relying on digital forensic professionals is necessary in ensuring the usability of digital evidence, as well as taking advantage of the lower burdens for authentication for it under Rule 902.

Digital evidence is an unbiased witness

Standardizing methods for the collection of electronically stored information is a big step toward recognizing the value of digital evidence as an unbiased witness. As society begins to move further away from “hard copies,” this addition demonstrates the law’s flexibility in accommodating our digital age. Unlike other types of information that may be collected for a trial, digital evidence is capable of presenting an unbiased record of activity. Admittedly, electronic evidence is not necessarily a complete repository of critical data, but think of the one device that most likely goes everywhere with you—your smart phone. I would argue that, for most of us, smartphones hold the most information about our day-to-day lives and much can be gleaned about our plans, intentions, and daily lives by reviewing their contents. The recent controversy over whether or not people should be forced to unlock their phones using a finger-

print illustrates exactly how protective people are of what is stored on their phones. With good reason, I often refer to phones as being like “snitches in our pockets.” It doesn’t matter how someone appears, how someone acts, or how convincing someone’s story may be—digital evidence doesn’t lie. Geolocation, text messages, emails, fitness applications, web browsing history, phone call logs, social media apps, and photos are only some of the ways that our phones offer glimpses into our lives. All of this information would be self-authenticating under the proposed 902(13), so long as it is certified by a qualified person.

Furthermore, the sheer volume of electronically stored information is constantly growing—creating an ocean of potentially useful data. As more and more is always being created, gathered, and stored on the vast number of diverse devices, litigants are presented with a huge amount and variety of potential evidence to use in court. Law enforcement is also faced with the problems posed by an influx of new technology, as data must be extracted from a variety of devices utilizing a number of different methods and tools. It would seem that as more emphasis is placed on digital evidence, it has become correspondingly difficult to gather, authenticate, and present in court. The revised Rule 902 responds to these issues for litigants by lowering the authentication hurdles.

Digital evidence can be open to interpretation

As an expert witness, I am frequently called upon to validate and explain digital forensic findings and their significance given the particulars of a case. Revealing hidden artifacts of long-forgotten digital activity is one thing—but constructing reliable narratives based on these facts and explaining their

significance? Quite another. Questions of admissibility are only the beginning in establishing the value of electronic evidence. Making testimony understandable can be very difficult when computer lingo is a factor. And let’s face it—computer people don’t always have reputations for being effective communicators. And this is especially problematic, since oftentimes one piece of digital evidence can be the key that unlocks an entire case.

If it can be uncovered and related in an understandable way to a judge or jury, digital evidence is absolutely critical. Apart from the processes of uncovering data and ensuring its admissibility, the purpose of a digital forensic examination is to uncover a usable and understandable timeline, or narrative of digital activity. Ideally, forensic evidence is presented in such a way that it makes sense to everyone, not just the IT people in the room. Digital forensic experts are ultimately tasked with effectively explaining why a piece of evidence is significant, or possibly critical, in a case.

The expansion to include digital evidence in Federal Rule of Evidence 902 marks a definitive movement toward the standardization of data collection and authentication. No doubt, this will impact practitioners in federal court immediately, but also state court practitioners, as states commonly adopt rules that substantially track the federal rules. As such, this change underscores the need for digital forensic expert witnesses who can attest to both the authentication and significance of electronically stored information in both state and federal courts. While these changes go into effect on December 1 of this year, in reality, they are in place now. Following best practices for digital collection is now pertinent for any case going to trial after this date. ▲


SDK
Schechter, Dokken, Kanter
CPAs • Business Advisors

612.332.5500
www.sdkcpa.com

Forensic Accounting and Valuation Services Team

Bench & Bar

OF MINNESOTA



How "trial lawyer" became an oxymoron

No time? No problem! Two great online pro bono outlets

Facial recognition technology brings security & privacy concerns

Inspired to Serve

In-house pro bono is on the rise

Facial recognition technology brings security & privacy concerns

In recent years, facial recognition technology has had some great successes. They include recognizing the faces involved in terroristic attacks, scanning faces at the airport for identification instead of using a passport, and—now—becoming a feature of our digital devices. It's clear that new applications of this technology are being utilized to streamline and simplify.

Facial recognition is a biometric identifier, but it has very different implications from using our fingerprints, or more traditionally, our passcodes. While some point to their similarities, it is very important to recognize that biometrical markers are not necessarily interchangeable, depending on their application.

FRT as biometrical authentication

Not all human characteristics are created equal when it comes to being used as biometrical markers. Eye scans, fingerprints, and facial recognition are probably the most prevalent, though all have weaknesses, strengths, and associated risks. Even among this group, each has different applications that vary widely depending on the environment in which they are being used. Some are more expensive than others, more difficult to use, or come with varying degrees of accuracy.

While eye scans are typically very expensive and require a lengthy enrollment process, and fingerprints cannot be used for surveillance purposes, facial recognition technology theoretically enables identification from a distance and doesn't require as much work getting individuals enrolled.

Some key variables sur-

rounding biometrical markers involve the kind and degree of protection these identifiers are afforded in court. Recent cases include a verdict allowing an individual to be forced to give her fingerprint to unlock a phone. This situation sparked a debate over what an individual "has" (their fingerprint) vs. what he or she "knows" (their passcode) and whether there's a difference when both serve the same purpose. Since smartphones are essentially snitches we carry around in our pockets and typically contain huge amounts of information, it is not surprising that "what" is being unlocked with a biometrical marker is a very important consideration.

It was ultimately determined that a fingerprint is different in kind from a passcode, because it's classified as something that someone has. But what will the ruling be when it's someone's face and they may or may not be aware that it's being used to unlock a device or to surveil them without their knowledge? Clearly, issues of privacy and security will be at the forefront, as people attempt to determine a balance between convenience, privacy, and security.

Surveillance, privacy, and security

Facial recognition technology poses a number of interesting problems because it implies a degree of surveillance of which the average person may not be aware. Should people have to consent? How will this information be stored once collected? Will the uses of this information be transparent? When using a biometrical marker that is—unlike a fingerprint—readily perceptible, it is important to consider how people will be informed of how this identifier is to be used, and what the benefits are on a wider scale.

Clearly, privacy is also at stake when using facial recognition technology. Compared to using a fingerprint as the go-to method of opening your phone, using your face may be even more problematic. The September 12 Apple Keynote described the newest iPhone, iPhone X, and one of its most amazing features: Face ID. By using the improved camera, Face ID serves

as the new authentication for opening an iPhone. While the security aspects seem strong—there is a purported 1 in 1,000,000 chance that a stranger will be able to open your phone with his or her face—it's important to remember the implications of biometrical authentication for law enforcement. Since your face is something you have, not something you know, it's also important to recognize that this biometric marker is most likely not going to have the same protections as a passcode in court. Given that this feature is always "on" and can be used in almost any condition, night or day, it's clear that it would be fairly easy for law enforcement to obtain access to someone's phone.

Using your face as your digital identifier also comes with security risks. If someone gets your biometric information, there is seemingly little that can be done, especially since facial information is more or less unchangeable. And unfortunately, many experts agree that facial recognition technology is currently not as accurate as fingerprint technology, meaning it may be easier to access a phone with a faulty scan. Or a photo stolen from a social media account. Keeping a passcode safe is one thing, but especially today, many people post a number of photos of themselves that may be the key to anything using facial recognition technology. While Apple assured its customers that Face ID is secure, it should be acknowledged that what may be secure today will not necessarily be secure tomorrow.

In sum, facial recognition technology poses the same kind of problem as many other technologies that make our lives easier. Where convenience is gained, privacy and security are often diminished. While we may be assured today by security efforts, that may change: Cybercriminals tend to adapt quickly to new technologies and new vulnerabilities. And while facial recognition technology may be easier to use than a passcode, it comes with the same privacy caveats as any other biometrical identifier in court. ▲



MARK LANTERMAN is the chief technology officer of Computer Forensic Services. A former member of the U. S. Secret Service Electronic Crimes Taskforce, Mark has 28 years of security and forensic experience and has testified in over 2,000 cases.

Thomas D. Hall

Thomas D. Hall is a former Clerk of the Court for the Supreme Court of Florida. Prior to that Mr. Hall was the Chief Staff Attorney at the Florida First District Court of Appeal in Tallahassee for approximately 10 years. He was also a judicial law clerk for Judge Daniel S. Pearson at the Florida Third District Court of Appeal in Miami. Mr. Hall is Of Counsel with Bishop & Mills practicing exclusively appellate law in all six of Florida appellate courts. He is based in the Tallahassee office of Bishop & Mills. Mr. Hall also has a consulting company, TLH Consulting Group LLC, which provides advice to those doing business with Florida (and other) courts.

He practiced law in Miami for approximately ten years before moving to Tallahassee. He is a member of the Appellate Practice, Government Lawyer and Real Property, Probate and Trust Law sections of The Florida Bar. He is Chair of the Appellate Court Rules Committee of The Florida Bar. He is also on the Rules of Judicial Administration Committee of The Florida Bar.

He has taught at the University of Miami and St. Thomas University law schools. He has presented at numerous national conferences such as the National Center for State Court's E-Court Conference, the National Conference of Appellate Court Clerks and Council of Appellate Staff Attorneys. He has taught in Florida's New Appellate Judge School, the Advanced Judicial Studies program, plus the Appellate, Circuit and County Judicial Conferences. Mr. Hall received the James C. Adkins Award from the Appellate Practice Section of The Florida Bar given to a member of the Bar who has made a significant contribution to appellate practice in Florida. He received NCACC's J.O Sentell Award. He has been teaching ethics for clerks at the Florida Court Clerks and Comptrollers' summer conference for the last four years.

Lisa Hall

Lisa Hall draws from nearly three decades of media experience - on both the receiving and sending ends. After nearly 17 years as a broadcast news producer, she launched her originally intended career in public relations in 2000. She led the public affairs practice as Senior Vice President of Salter>Mitchell until July of

2013. At that time, Lisa formed her own firm - Hall+Media Strategies. She remains a Senior Consultant with Salter>Mitchell.

Lisa has led statewide campaigns that have resulted in major client victories. She mounted a campaign to save the State Library of Florida when a Governor proposed to do away with it. She has established a reputation as a leading advocate for Fair and Impartial Courts through her repeated success in defending Florida's judiciary from political attacks. In 2011, she helped concerned members of the legal community come together as "Floridians for Fair and Impartial Courts" to beat back a political power grab led by the House Speaker. The following year, as the media relations director for "Democracy at Stake", she engaged Florida newspapers as reliable and outspoken allies for three Florida Supreme Court Justices facing organized efforts to remove them from the bench in the 2012 merit retention races. The more than 272 articles covering the unprecedented attempt to politicize the court included 120 editorials and opinion columns published during a 10 month period. In 2014, the National Association of Women Judges relied on Lisa to develop and launch "Informed Voters, Fair Judges" campaign to build public understanding of courts and the need for fair and impartial judges. A rapid round of editorial board meetings in the fall of that year secured strong editorial opposition that helped defeat Amendment 7, a legislatively-proposed constitutional amendment that would have allowed an out-going governor to appoint Justices to vacancies occurring after the end of his term. In addition to her other clients, for the past 15 years Lisa has been the principle media strategist for the town of Babcock Ranch in southwest Florida. Babcock Ranch is the first solar powered town in the U.S.

A graduate of the University of Oklahoma, Hall moved to Florida in 1987 to accept a position as news producer for WSVN in Miami. In 1990 she migrated north to Tallahassee, where she continued her journalism career as capital bureau chief and regional manager for a television news cooperative serving 10 stations across Florida. She went on to serve as News Director for WTWC and then as Managing Editor for Florida's News Channel before making the move to public relations. Lisa is Accredited in Public Relations (APR) and is also credentialed as a Certified Public Relations Counselor (CPRC) by the Florida Public Relations Association. She is the 2011 recipient of NCACC's Morgan Thomas Award.

Samuel Anderson Thumma
Chief Judge
Arizona Court of Appeals, Division One
State Courts Building
1501 West Washington
Phoenix, Arizona 85007

SAMUEL ANDERSON THUMMA. Chief Judge (2017-present), Vice Chief Judge (2015-2017) and Judge (2012-present), Arizona Court of Appeals, Division One. Judge, Arizona Superior Court, Maricopa County (Criminal and Juvenile rotations) (2007-2012).

Nationally, Sam is a Uniform Law Commissioner, where he chairs the Study Committee on Jury Selection and Service; is a member of the Committee to Monitor Developments in Civil Litigation and Dispute Resolution and chaired the Uniform Employee and Student Online Protection and Privacy Drafting Committee. Sam is an Advisor to the American Law Institute's RESTATEMENT OF THE LAW (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM; is secretary of the American Bar Association's Judicial Division Appellate Judges Conference and of the Appellate Judges Education Institute, Inc., (AJEI) Board of Directors and is co-chair of the *Judges' Journal* Editorial Board. He chairs the Education Committee for the 2019 AJEI Summit to be held November 2019 in Washington, D.C. In 2019, he served as a law school site visit team member for the ABA's Section of Legal Education and Admissions to the Bar. He also is a National Center of State Courts appointee to the Joint Technology Committee.

In Arizona, Sam is a member of the Arizona Judicial Council; co-chair of the Arizona Supreme Court's Committee on the Rules of Evidence; chairs the Judicial Ethics Advisory Committee; chairs the Task Force to Supplement Keeping of the Record by Electronic Means; chaired the Digital Evidence Task Force; is a member of the Arizona Supreme Court's Committee on Juvenile Courts and is co-editor of the ARIZONA APPELLATE HANDBOOK. Previously, Sam chaired the State Bar of Arizona's Civil Practice and Procedure and Fee Arbitration Committees and served as a member of the State Bar's Civil Recommended Arizona Jury Instructions and Rules of Professional Conduct Committees.

Sam has presented at more than 340 seminars and published 12 law review, and 50 other law-related, articles. Previously, Sam was a partner at Perkins Coie Brown & Bain, P.A., in Phoenix, and an associate at Arnold & Porter in Washington, D.C. He served as a law clerk for Arizona Supreme Court Chief Justice Stanley G. Feldman and Judge David R. Hansen, United States District Court for the Northern District of Iowa. Sam graduated Order of the Coif from the University of Iowa College of Law in 1988, where he was a Note & Comment Editor on the IOWA LAW REVIEW, and from Iowa State University in 1984, where he was a Harry S. Truman Memorial Scholar.



Arizona's Look at Court Management of Truly Digital Evidence

NCACC 46th Annual Meeting

Lexington, Kentucky July 30, 2019



Presenter

Samuel A. Thumma

Chair, Arizona Task Force on Court
Management of Digital Evidence

Judge, Arizona Court of Appeals,
Division One

Thanks to Task Force Members and
Staff, including Jennifer Albright and
Kay Radwanski

Thanks, also, to Paul Embley,
National Center for State Courts

Discussion Overview

The Evolving Court Record Format

The Truly Digital Evidence Concept

Body-worn cameras

The creation and mission of the
Task Force

Task Force function and
Recommendations

Next steps

Questions and discussion
throughout

The Evolving Court Record Format



Filings: Then = paper
 Now = digital file or by scanning
 paper

Transcripts: Then = paper
 Now = digital file or audio recording

Exhibits: Then and now = digital content
 transferred to paper (photos, stills
 of video) or to physical item
 (CD or USB)

Body Worn Camera video as
example of policy issues addressed
by the Task Force

<https://www.youtube.com/watch?v=lx3--h8PmgQ>

What is Digital Evidence?

“Any information stored or transmitted in digital form that a participant in a court case may seek to use in a proceeding.”

Not new evidence, but types and formats are changing rapidly and the amount of this kind of evidence is increasing exponentially.

Think: Film -> DHS/Betamax
-> laser disc -> DVDs ->
electronic files.



Challenges

Spike in amount of digital evidence

Rapidly changing formats

Need for technology, training,
equipment

No proportional increase to funding

Integrity of evidence, preservation

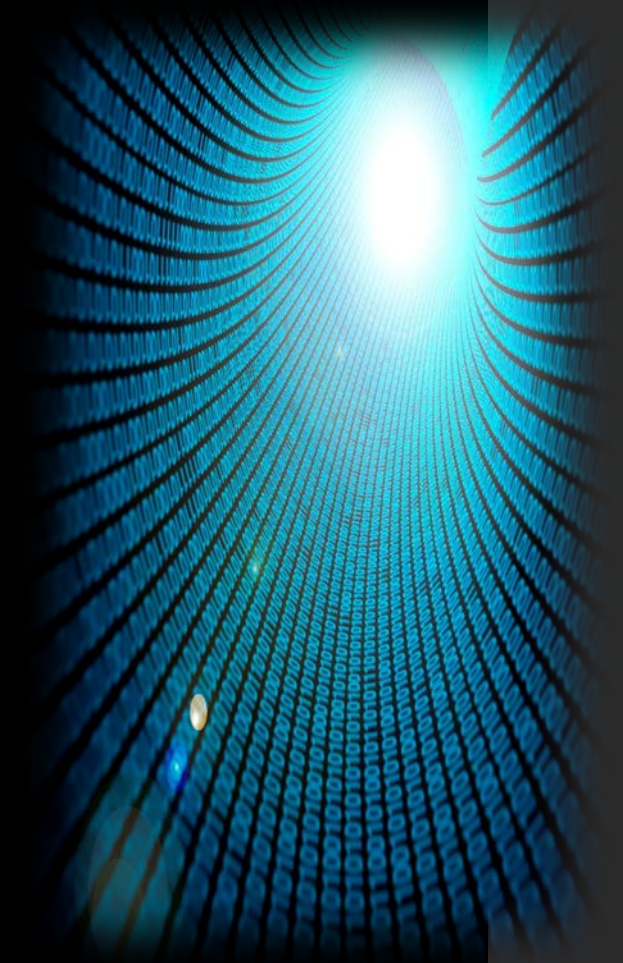
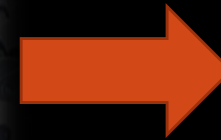
Access and Security

Privacy (victim, witness, other)

Current Laws



Challenges From the Court's Perspective



What is
vs.
What is yet to come



Digital-Ally Solutions

Call to Action

Managing Digital Evidence in Courts, Joint Technology Committee (JTC) Resource Bulletin Version 1.0 (2/2016)

- JTC is a cooperative effort of the Conference of State Court Administrators; National Association for Court Management; National Center for State Courts and Court Information Technology Officers Consortium.
- JTC produces white papers on various technical topics that are posted on NCSC website.
 - *Social Media Marketing for Courts* (12/2018)
 - *General Data Protection Regulation for US Courts* (9/2018)
 - *Marketing a Court Website* (7/2018)
 - *Online Dispute Resolution for Courts* (11/2017)

The Truly Digital Evidence Concept

- An electronic portal and electronic repository concept that goes beyond electronic records (formerly paper records) and includes exhibits that are purely electronic.
- Exhibits cross the threshold from party to court in digital form.
- Currently, no court in the nation uses this concept, but pre-court discovery and disclosure use the digital concept.



Arizona's Digital Evidence Task Force

- Court Management of Digital Evidence
- Arizona Administrative Order 2016-129
- 22 members encompassing every stage of digital evidence creation, submission, admission, storage, and preservation.
- Met a bunch of times in 2017 and divided into 3 workgroups: formats; storage and management and rules
- 5 policy questions addressed
- 10 recommendations



DETF Final Report

Report and Recommendations of the Arizona Task Force on Court Management of Digital Evidence (Oct. 1, 2017)

- Posted at <http://www.azcourts.gov/Portals/74/DETF/Report/DETF%20Final%20Report.pdf>.
- Published, in an abbreviated form, “Report and Recommendations of the Arizona Task Force on Court Management of Digital Evidence,” 13 *Wash. J.L. Tech. & Arts* 165 (2018).
- Wanted to make it available to provide a starting point for efforts in other states.

Should standardized acceptable formats and viewing, storage, preservation & conversion formats be adopted?

Recommendation 1:

A standardized set of formats and technical protocols should be identified, adopted, and set forth in the Arizona Code of Judicial Administration (ACJA).

Recommendation 2:

ACJA language requiring digital evidence to be submitted in a standard format, unless interests of justice warrants otherwise.



Should digital evidence be stored locally, offsite, or using cloud services?

Should management of digital evidence be centralized or decentralized?



Recommendations 3-5:

- Decision-making should be guided by a set of minimum technical requirements.
- Should take measures to enhance the use and presentation of digital evidence in the courtroom.
- Arizona Administrative Office of the Courts should develop best practices and other measures to increase success of solutions adopted.

Minimum technical requirements and other considerations on page 21-26 of the Final Report.

Recommendations 3-5 (Continued):

- Education and training on legal and technical competence to facilitate and advance court management of digital evidence.
- Arizona AOC should work with local courts on developing a means to offset costs associated with technology needs created by the increased receipt and storage of digital evidence.



Should new or amended rules be developed for handling court digital evidence?

Recommendations 7 and 9:

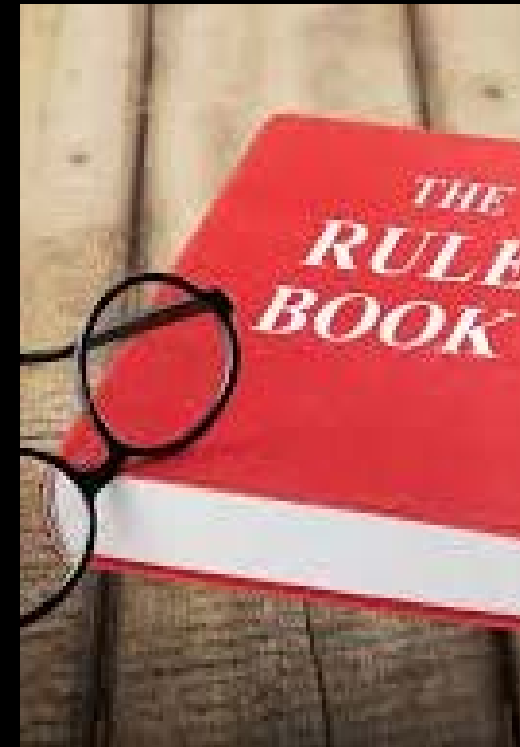
- Amendments to the Arizona Rules of Evidence to expressly address digital evidence, including adding a definition of “video.”
- “Video is an electronic visual medium for the recording, copying, playback, broadcasting, or displaying of moving images, which may or may not contain an audio recording.”
- Define digital evidence in other rule sets (although ultimately it was determined to use the phrase “*electronically stored information*” instead of “*digital evidence*”).



Should court rules governing public records be revised to address privacy concerns for victims, non-victim witnesses?

Recommendations 6 and 8:

- Amendments to various procedural rule sets to modernize language to include digital evidence.
- Amendments to rule governing access to judicial records to ensure protection of victims' rights and privacy concerns.
- Cooperative efforts with various stakeholders to ensure policies and procedures related to victims and non-victim witnesses are consistent.



Education, Training and Self-Represented Litigants

Recommendations:

- Develop resource guides for self-represented litigants. R4
- Develop templates for local court use on redaction, formats, converting, submitting, and using digital evidence in court. R10
- Amendments to Arizona Rule of Supreme Court 123 (access to judicial records) to manage digital evidence introduced by self-represented litigants that may not meet redaction requirements. R6
- Education and training generally. R10



Corresponding Rule Change Petition R-18-0008



Rule change petition filed January 10, 2018
recommending rule changes:

- Ariz. R. Evid. 1001, 1002, 1004, 1006, 1007 & 1008
- Ariz. R. Crim. P. 15.1, 15.2, 15.3
- Rules of Procedure for Juvenile Court 16, 44, 73
- Rules of Procedure for Eviction Actions 10

Arizona Supreme Court granted petition, on August 28, 2018, adopting proposed changes effective January 1, 2019.

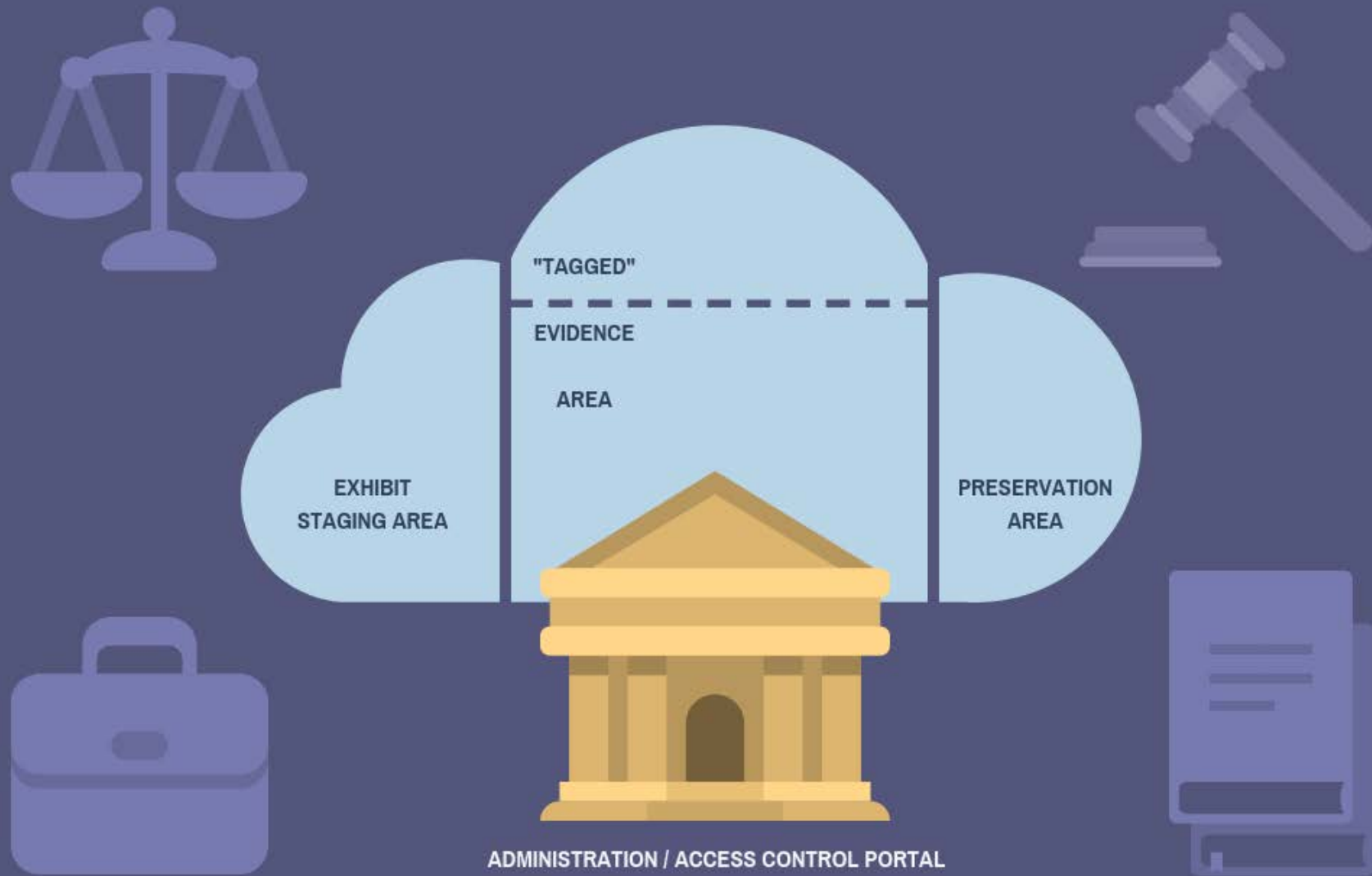
Petition (including suggested specific changes) and Arizona Supreme Court Order are available at <http://www.azcourts.gov/Rules-Forum/aft/825>.

The rest of the story is a work in progress

- Outreach Efforts
 - Archives
 - Court Clerks
 - Presiding Judges
 - Technology/ESI folks
- Chronology
 - JTC -> DETF
 - DETF -> Arizona Commission on Technology (COT)
 - COT -> Technical Advisory Council (TAC)
 - TAC work and report back to COT
 - Ongoing effort

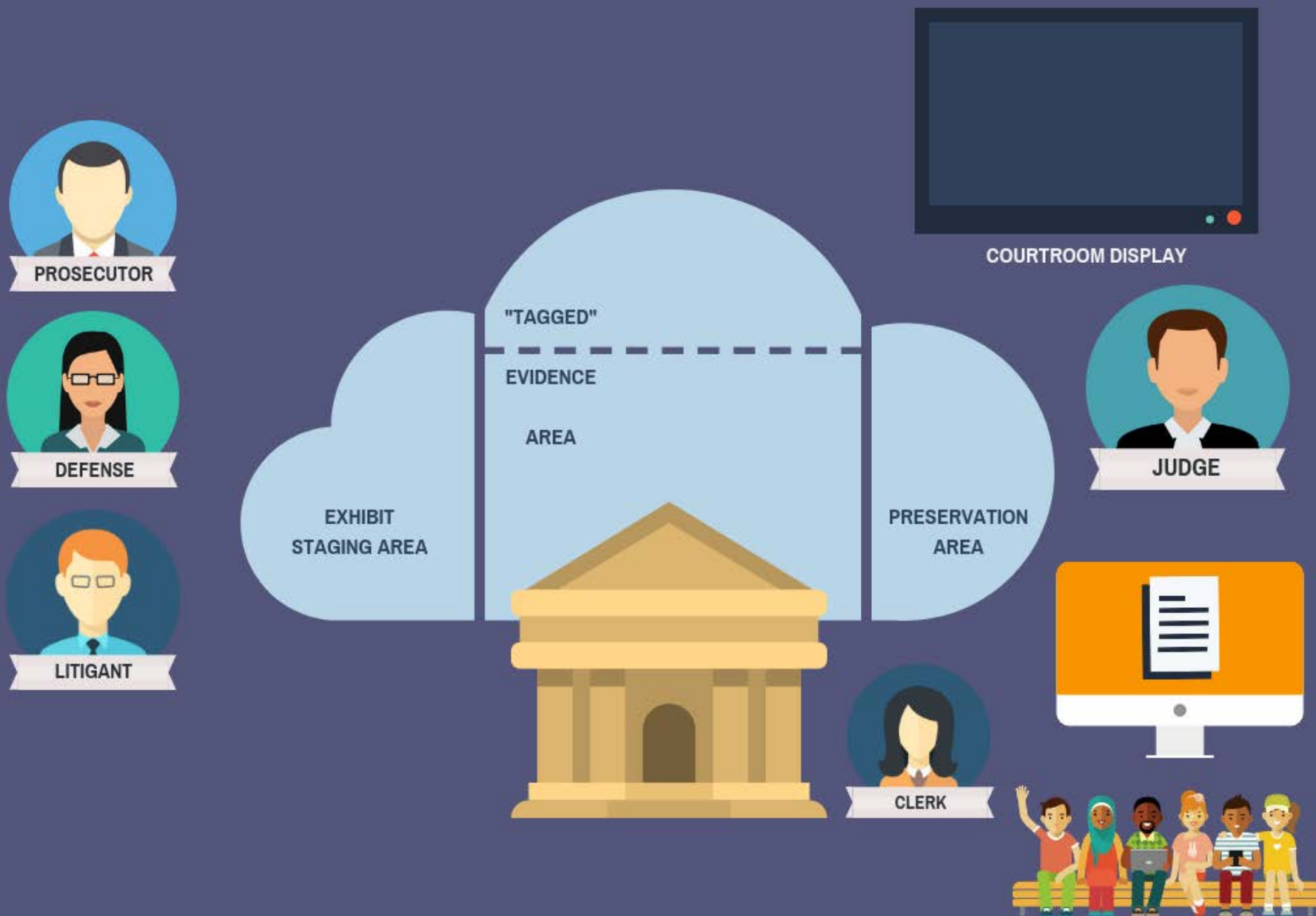
TAC's Digital Evidence Foundation

VENDOR DIGITAL EVIDENCE CLOUD ARCHITECTURE



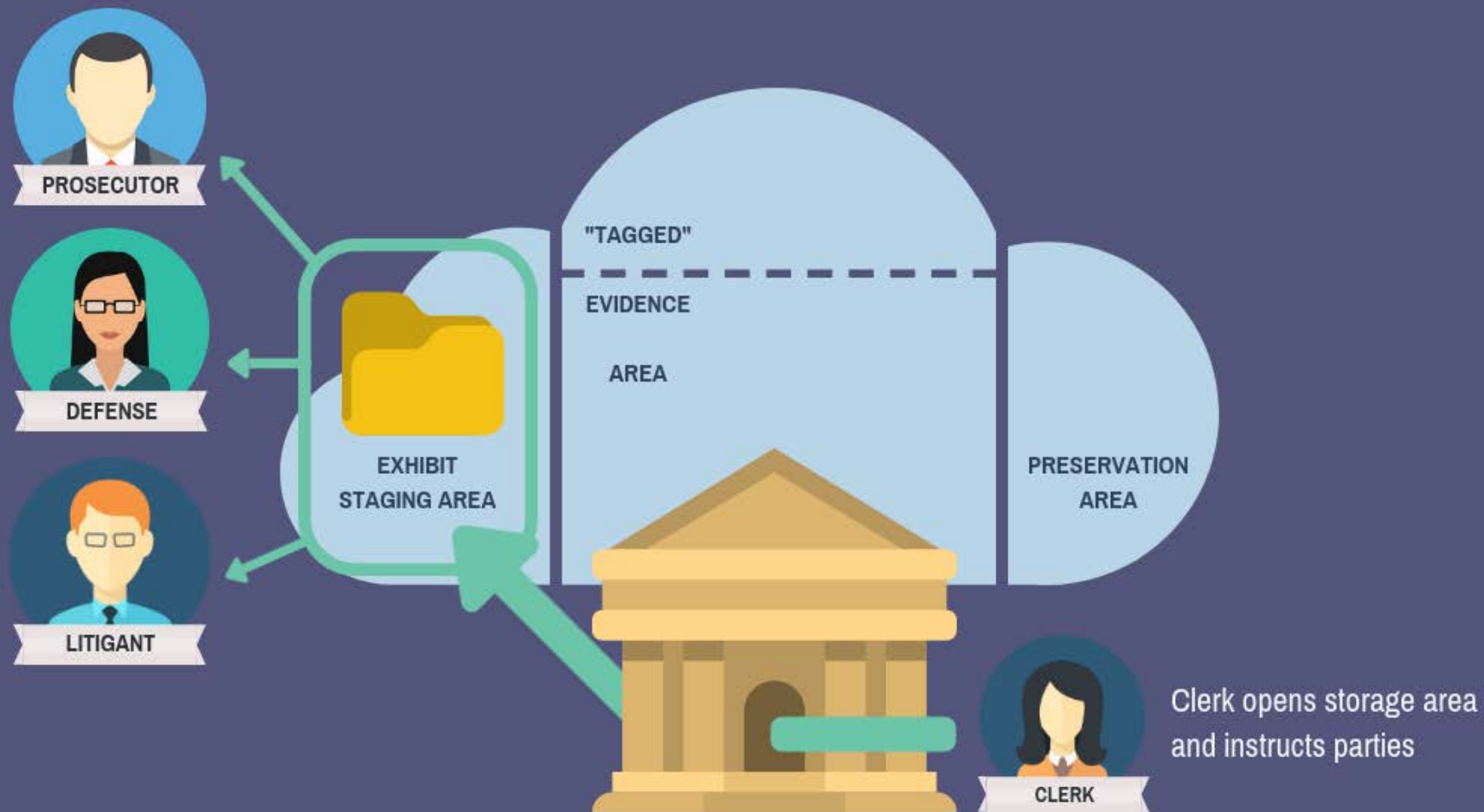
TAC's Digital Evidence Foundation

USERS, FILE SOURCES, AND OUTPUT



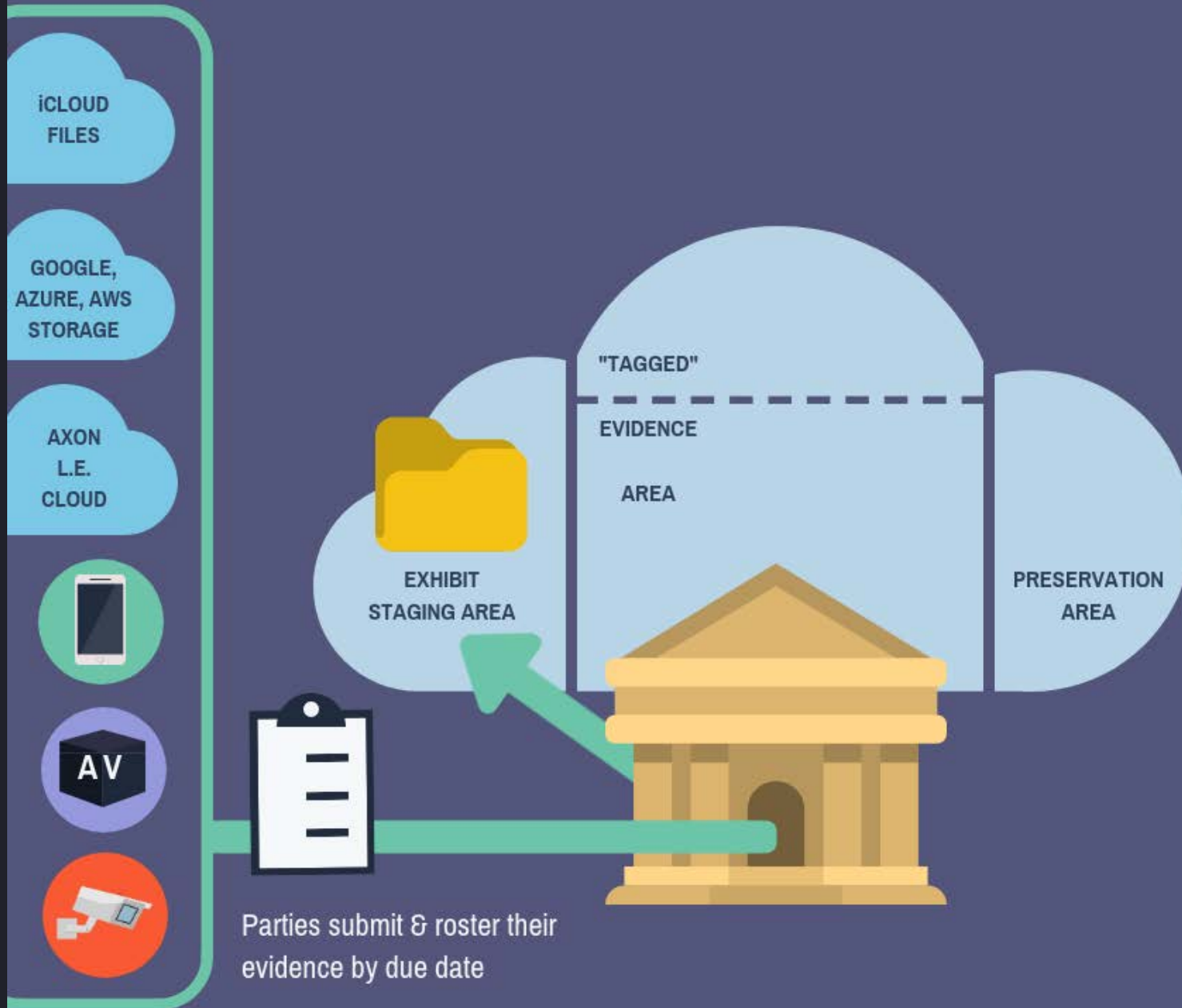
TAC's Digital Evidence Foundation

PROCESS STEP 1: CASE INITIATED



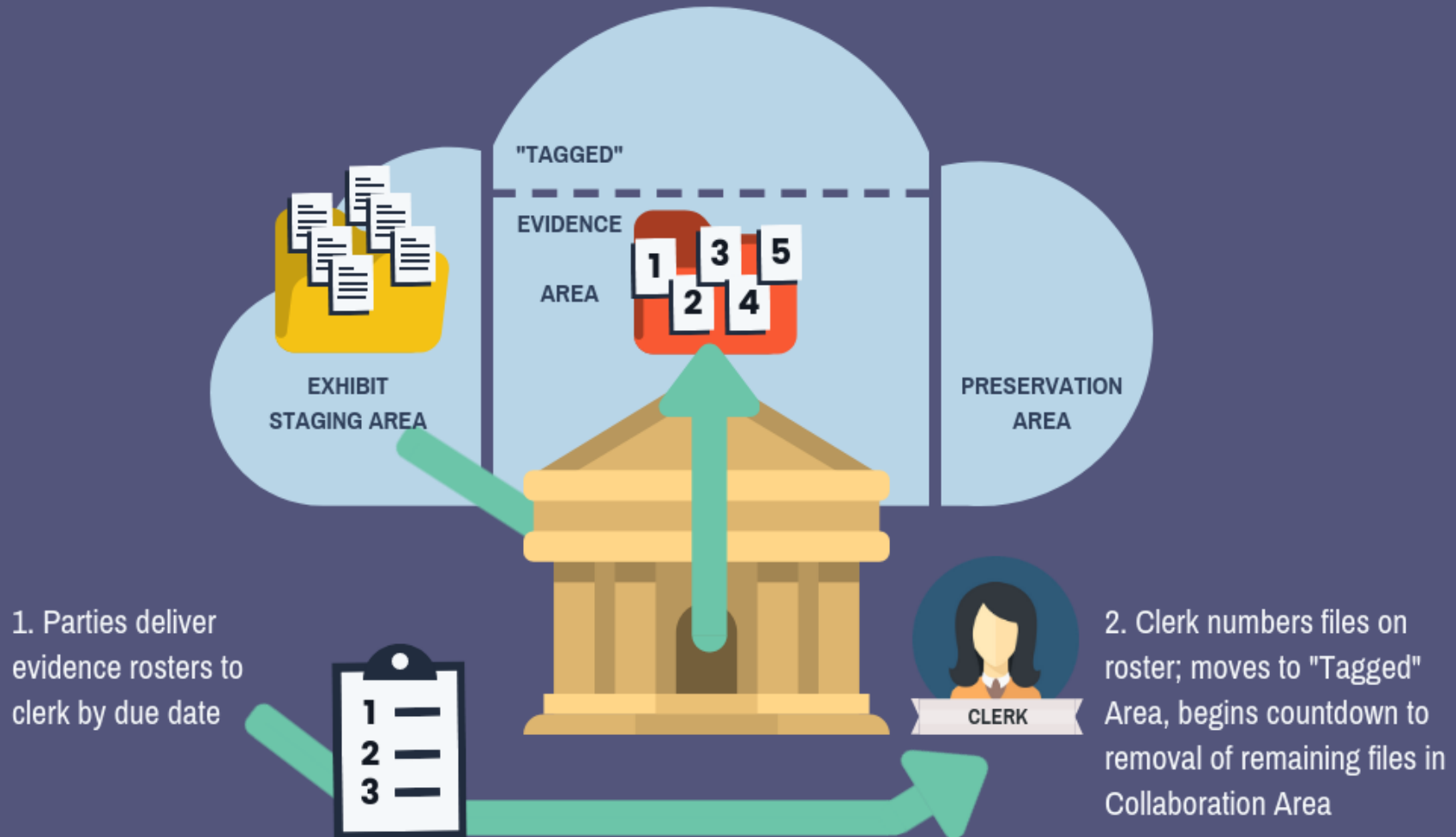
TAC's Digital Evidence Foundation

PROCESS STEP 2: EVIDENCE SUBMITTED



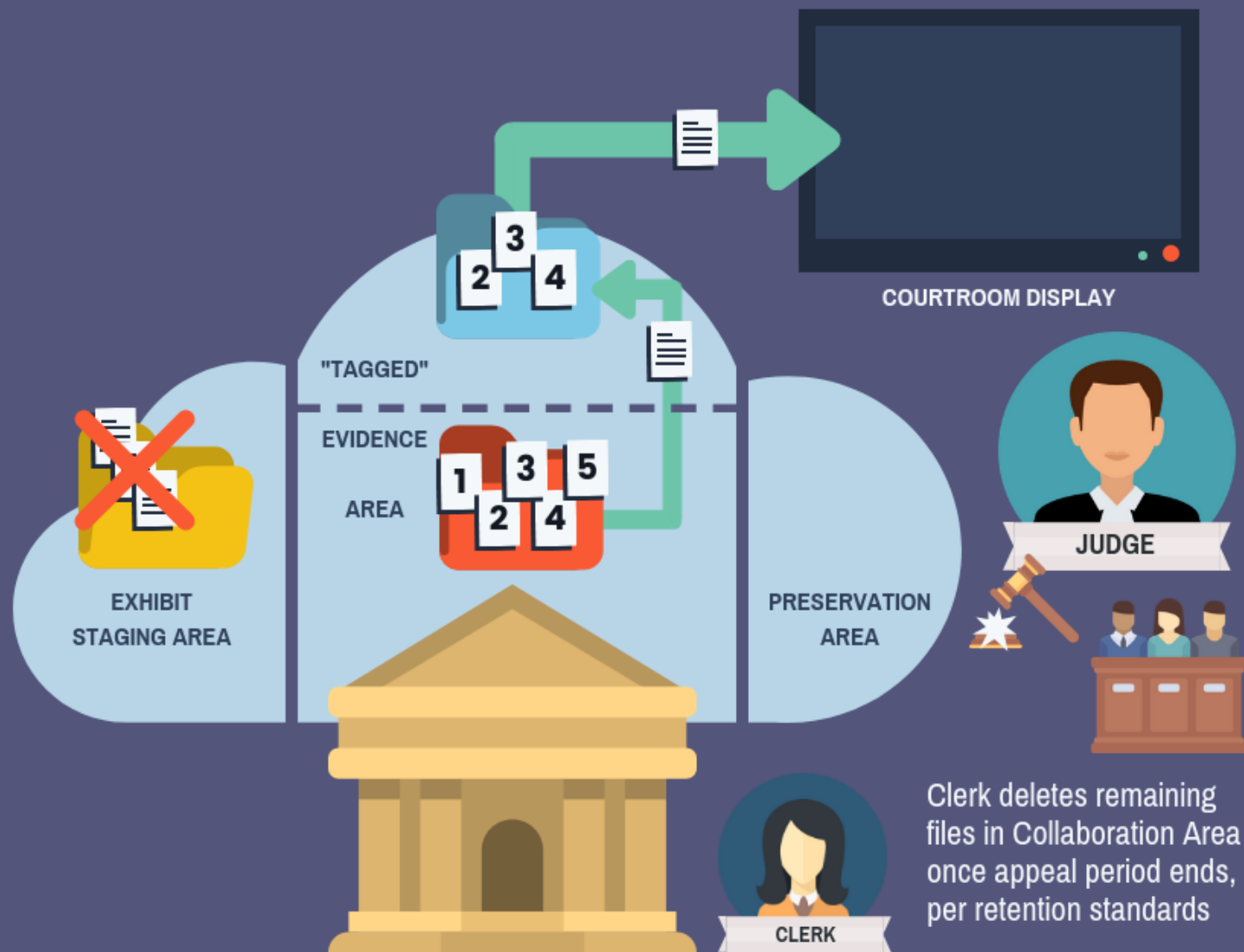
TAC's Digital Evidence Foundation

PROCESS STEP 3: EVIDENCE "TAGGED"



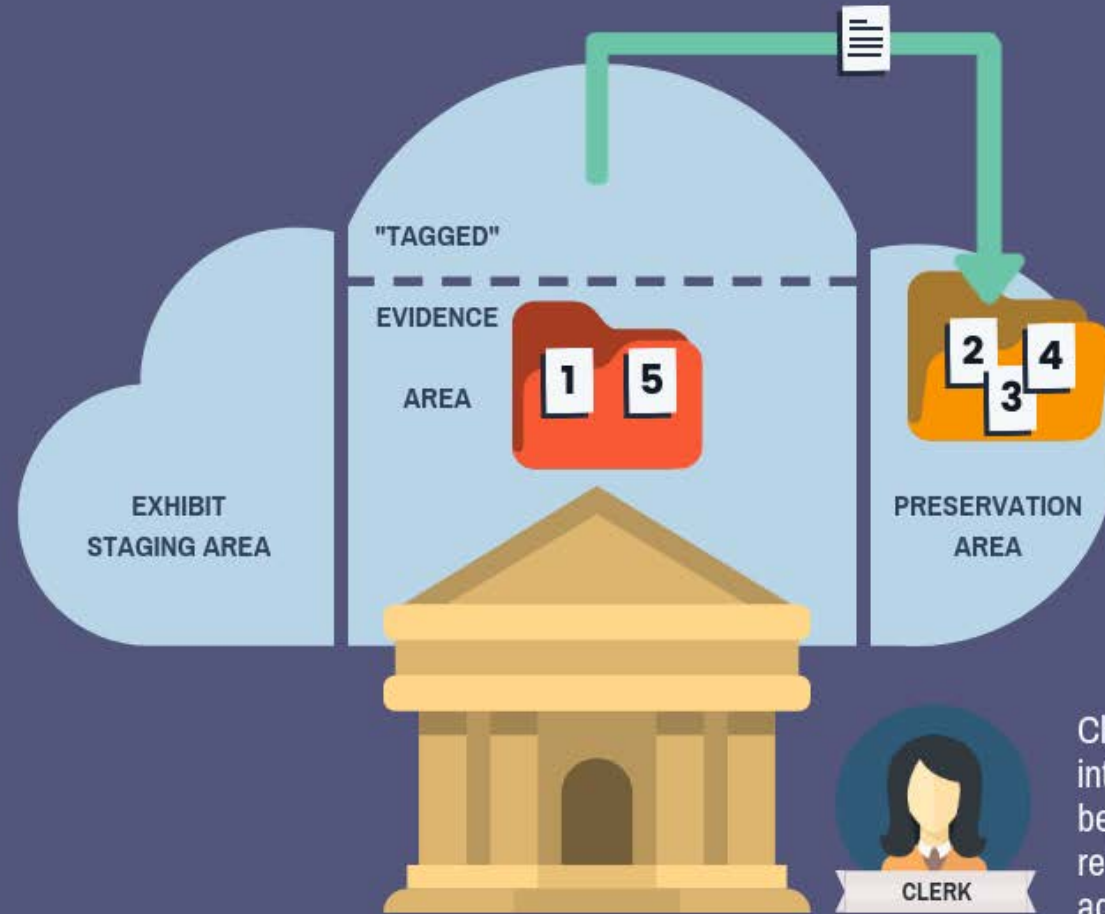
TAC's Digital Evidence Foundation

PROCESS STEP 4: TRIAL HELD



TAC's Digital Evidence Foundation

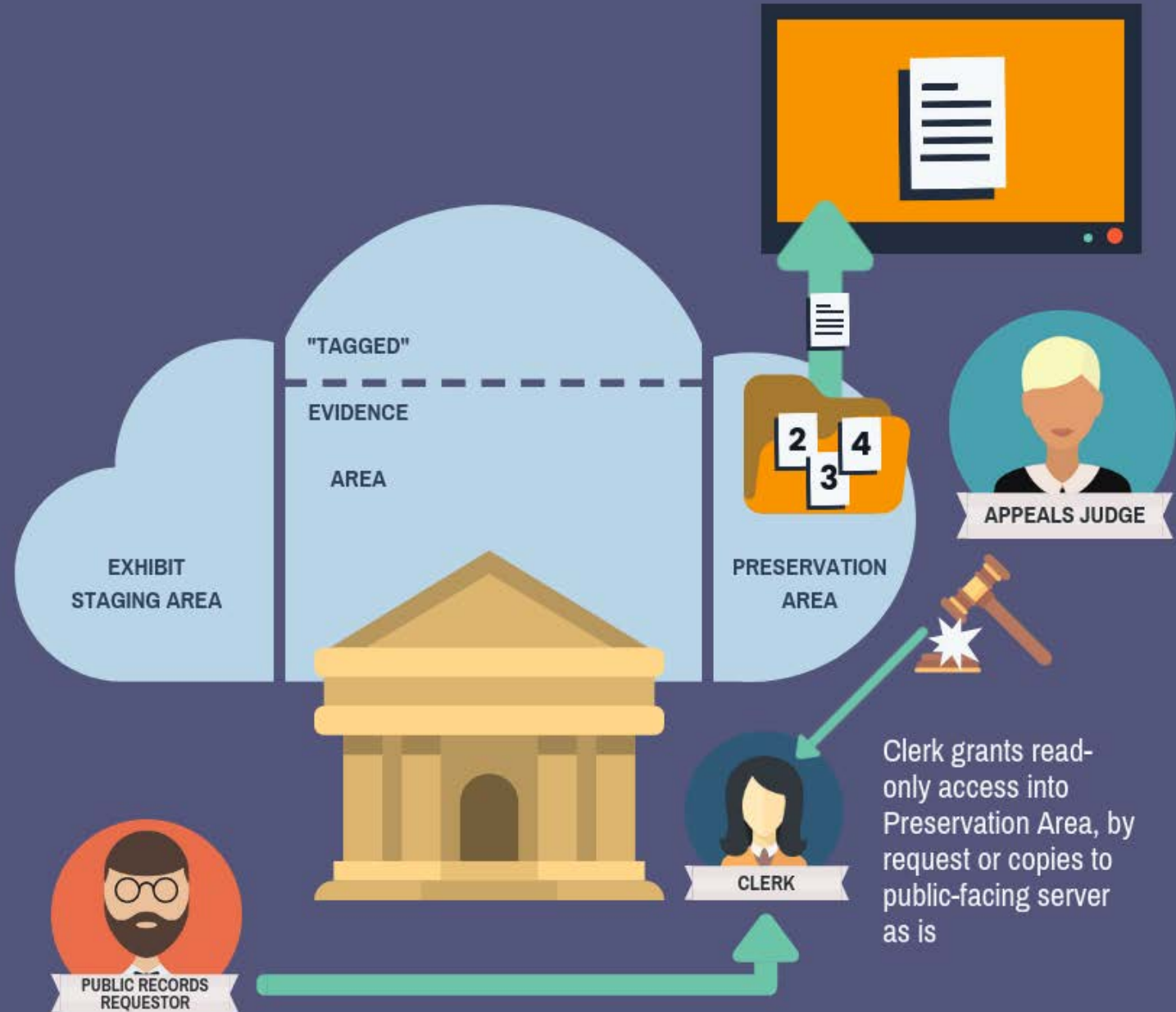
PROCESS STEP 5: FINAL MOVE & APPEAL PERIOD



Clerk moves all used files into Preservation Area, begins countdown to removal of any remaining admitted evidence in "Tagged" Area

TAC's Digital Evidence Foundation

PROCESS STEP 6: PUBLIC ACCESS/APPEALS ACCESS



PROCESS STEP 7: DELETION PER RETENTION



Arizona Digital Evidence – Circa June 2019

- Automate the flow from inception to appeal and archive/destruction
- Establish a unified portal for filer submissions
- Establish an affordable, flexible cloud-based system
- Status: Vendor Analysis/Design Stage



Final Questions/Concluding Remarks



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

October 1, 2017

Table of Contents

MEMBERS	1
EXECUTIVE SUMMARY	3
Creation and Charge of the Task Force	3
Overview of this Report	4
The Task Force and the Task Force Process	4
Summary of Task Force Recommendations and Ongoing Efforts	5
MANAGEMENT OF DIGITAL EVIDENCE	9
Background	9
The Evolving Court Record Format	9
The Truly Digital Evidence Concept	11
Task Force Meetings	14
WORKGROUP REPORTS	16
Digital Formats Workgroup Report	16
Storage and Management Workgroup Report	21
Rules Workgroup Report	27
APPENDIX A— Administrative Orders	35
APPENDIX B-Arizona Code of Judicial Administration § 1-504	40
APPENDIX C-Arizona Code of Judicial Administration § 1-506	44
APPENDIX D-Arizona Code of Judicial Administration § 1-507	48
APPENDIX E-Arizona Code of Judicial Administration § 1-604	54
APPENDIX F-Arizona Code of Judicial Administration § 1-606	57
APPENDIX G— Proposed Amendments to the Arizona Rules of Evidence	59
APPENDIX H— Proposed Amendments to the Arizona Rules of Criminal Procedure	61
APPENDIX I—Proposed Amendments to the Arizona Rules of Family Law Procedure	65
APPENDIX J—Proposed Amendments to the Arizona Rules of Protective Order Procedure	66
APPENDIX K—Proposed Amendments to the Arizona Juvenile Court Rules	67
APPENDIX L—Proposed Amendments to the Arizona Rules for Eviction Actions	70



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

Jeff Fine

Court Administrator
Maricopa County Justice Courts

David Bodney

Partner, Ballard Spahr LLP

Jennifer Garcia

Assistant Federal Defender
Federal Public Defender

Honorable Kyle Bryson

Presiding Judge
Superior Court in Pima County

Honorable Charles Gurtler

Presiding Judge
Mohave County Superior Court

Colleen Clase

Senior Counsel
Arizona Voice for Crime Victims

Aaron Harder

Bureau Chief - Vehicular Crimes
Maricopa County Attorney's Office

Jessica Cortes

Court Administrator
City of Flagstaff Municipal Court

Honorable Michael Jeanes

Clerk of the Court
Superior Court in Maricopa County

Honorable David Cunanan

Superior Court in Maricopa County

Laura Keller

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

Karen Emerson

Deputy Public Defender
Maricopa Office of the Public Defender

Michael Kurtenbach

Executive Assistant Chief
Community Services Division
City of Phoenix Police Department

Honorable Maria Felix

Justice of the Peace
Pima County Consolidated Court



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, proprietary 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 trail 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)	Administrative Order
FORCE ON COURT MANAGEMENT)	No. 2016 - <u>129</u>
OF DIGITAL EVIDENCE AND)	
APPOINTMENT OF MEMBERS)	
)	

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)	Administrative Order
THE TASK FORCE ON COURT)	No. 2017 - <u>27</u>
MANAGEMENT OF DIGITAL)	(Affecting Administrative
EVIDENCE)	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.

concerns the same individual or organization.

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
 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.

I.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]



NIAL RAAEN

PRINCIPAL COURT MANAGEMENT CONSULTANT

Mr. Nial Raaen is a Principal Court Management Consultant at the NCSC with over forty years expertise in court operations and management, specializing in court governance, caseload management, court performance, collections and records management. In addition to serving as a consultant on numerous projects in the United States, his international experience includes rule of law and judicial reform projects in the Balkans, Asia, Africa, the Caribbean, and the Middle East.

After beginning his career as a probation officer in the Michigan court system, Mr. Raaen served as a district court magistrate before being appointed court administrator and clerk of court for the Washtenaw County District Court. Mr. Raaen later joined the staff of the Michigan Supreme Court as Director of Trial Court Services. Before joining NCSC Mr. Raaen served as Chief of Court Management for the International Criminal Tribunal for the former Yugoslavia in The Hague.

Mr. Raaen is a cum laude graduate of Vanderbilt University, a graduate fellow of the Institute for Court Management, and holds master's degrees in public administration and social work from the University of Michigan. He is a Certified Records Manager.

Electronic Records Preservation & Disposition Planning



Nial Raaen, CRM
NCSC Principal Consultant

Planning for “Digital Continuity”

**Keeping and managing digital information to ensure
it can be used
in the way that is required,
for as long as required,
and no longer.**

The Challenges...



- Increasing reliance on digital systems as e-filing and EDMs are adopted, records are “born digital”
- Rapid technological change and evolving technical skills
- Complexity of ER retention and disposition
- Planning and collaboration are more critical

No universal solution exists today for permanent or long-term digital preservation

Four Ways of Losing Digital Information:

- ⊗ Can not find it
- ⊗ Can not read it
- ⊗ Can not interpret it correctly
- ⊗ Can not validate its authenticity





A “Digital Dark Age?”

“Old formats of documents that we've created or presentations may not be readable by the latest version of the software because backwards compatibility is not always guaranteed.

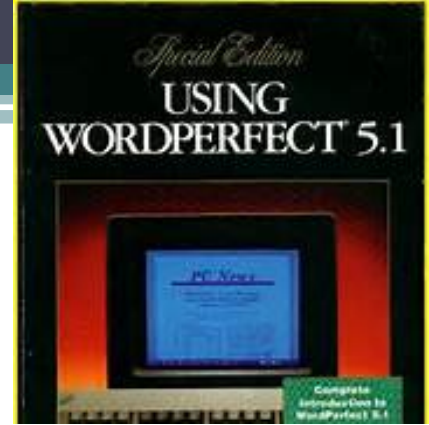
Even if we accumulate vast archives of digital content, we may not actually know what it is.”

Vint Cerf, VP Google

The Technical Issues

- ▣ **Media longevity**
- ▣ **Media obsolescence**
- ▣ **Hardware lifespan**
- ▣ **Software obsolescence**
- ▣ **File format obsolescence**





Software and Formats

- A file format may be superseded by new versions, no longer be supported by the current vendor
- Software may be superseded by newer versions or newer generations with more features
- Characteristics as hidden text and change history, macros, and animations may be difficult to archive
- Vendors compete, merge, or go out of business leaving application software unsupported

Hardware & Media



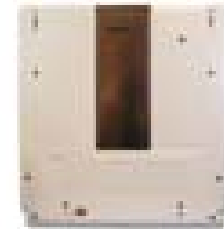
- Storage medium may be superseded by newer versions or by new types of media—smaller, denser, faster, and easier to read.
- Computers are continually superseded by faster and more powerful machines.
- Computer components and media physically fail due to human error, natural events, and age.

Rest in Peace!

8 inch floppy: 1971-81*



5.25 inch floppy: 1972 – mid 1980s



12 inch optical: 1985 – 1992

Jazz disk: 1996 – 2002



****You would need more than 130,000 8-inch floppy disks to store 32GB of memory
- the size of an average memory stick***

source: Cornell University *Chamber of Horrors*

“Unstructured” Records

- Email
- Office automation work products
 - Documents
 - Spreadsheets
 - Presentations
- Social media
- Web content
- Evidence

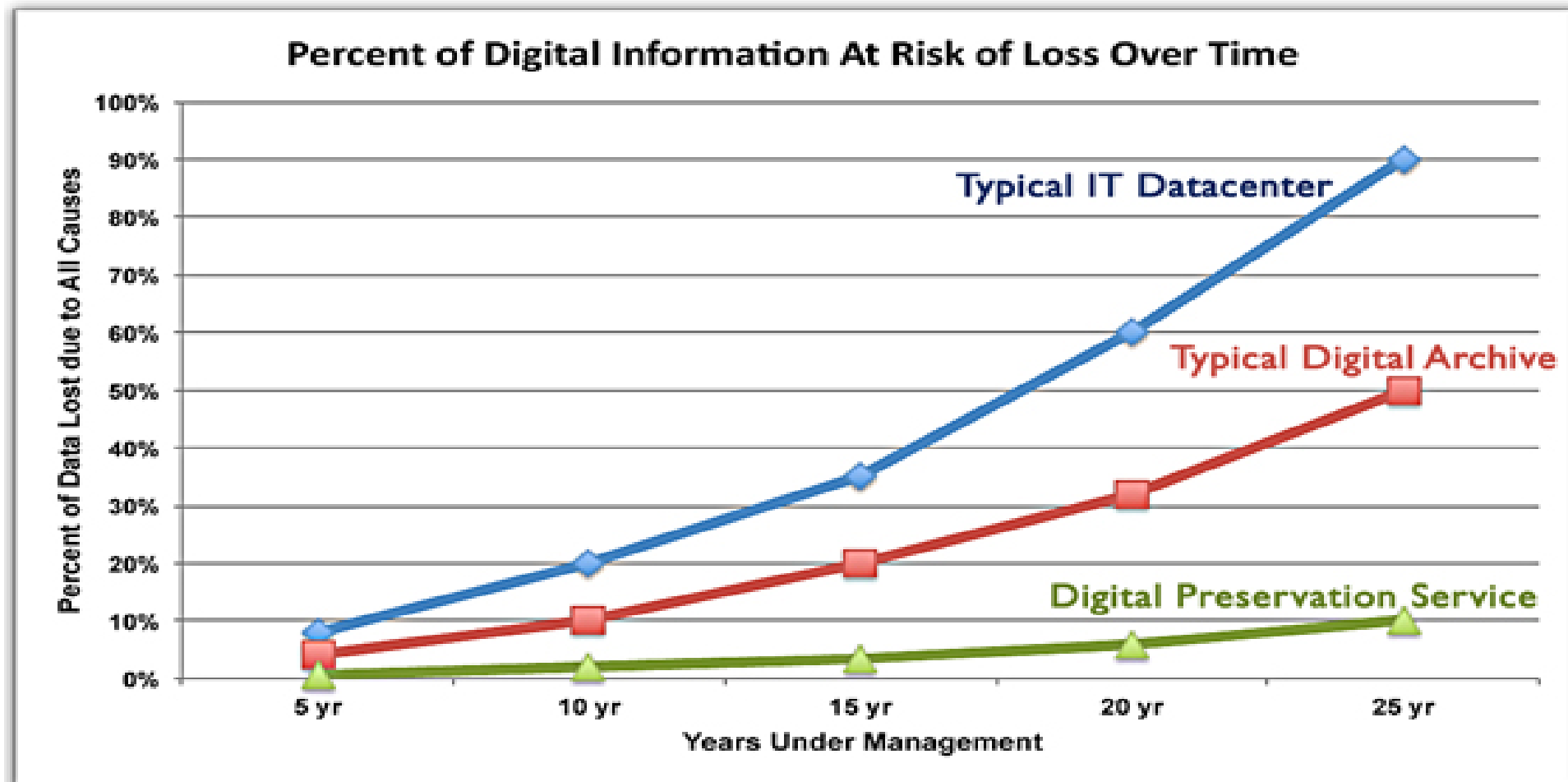


How Long is Long-Term?

ISO 14721 –

“Long enough to be concerned with the impacts of changing technologies, including support for new media and data formats, or with a changing user community.”

Ready....or Not?



Methods of E-Preservation

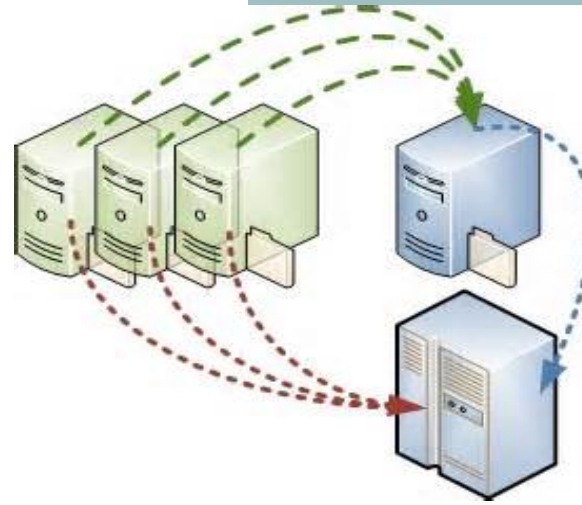
PASSIVE

- Ensures the **integrity** of, and access to, digital objects and their associated metadata.
- Attempts to keep the original object intact without changing the storage or access technologies.

ACTIVE

- Ensures continued accessibility by active intervention to move the digital object from legacy to current storage environments.
- May involve technologies not in existence when the record was created.

Migration



A strategy for avoiding obsolescence

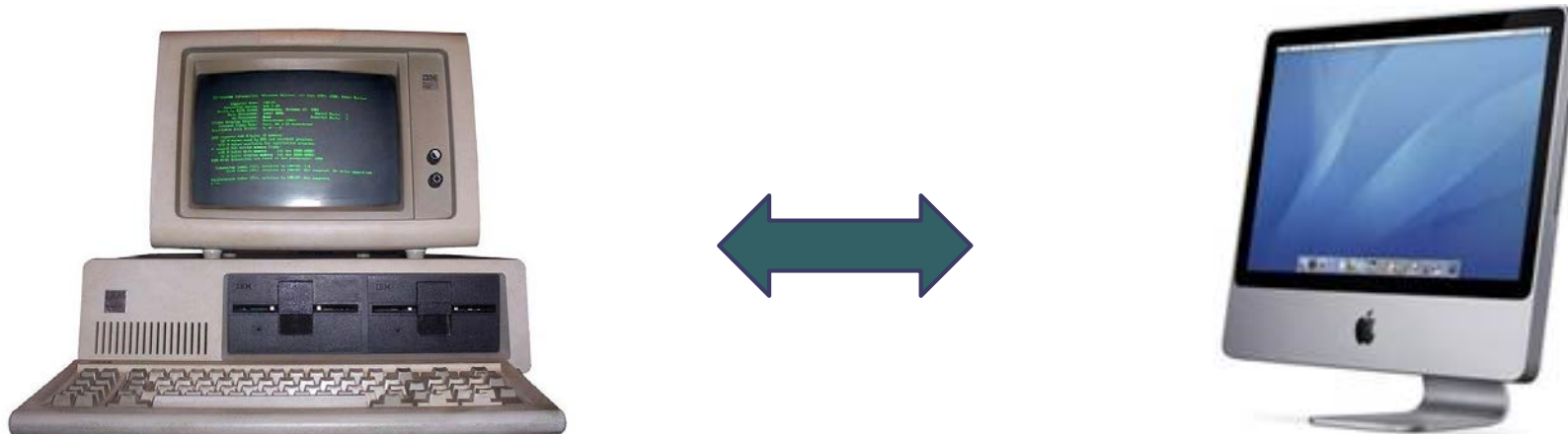
- Cycle is approximately every 10-15 years
- Media and file types must provide a stable repository for preservation and access
- A migration strategy and schedule should be established for specific media and file types

Other Preservation Methods

Emulation - recreating the legacy technical environment

Refreshing – moving records from one medium to another, primarily as a preventive measure

Preservation – maintaining the original technical environment





Storage is Cheap, but...

- Data is already growing at 40% per year.
- Data must be periodically migrated to another medium.
- Migrations are far from perfect - some data is invariably lost or corrupted.
- Migrations represent 60% of some large companies' IT budgets.

(source: Harvard Business Review
When Old Technologies Create New Industries)

Preservation Ready Formats

- **TIFF**
- **XML**
- **JPEG**
- **PDF/A**



About PDF/A



- Archival file format and standard (ISO 19005-1)
- One component of a digital preservation strategy
- Preserves the static visual appearance over time
- A framework for recording metadata
- Continues to evolve

Metadata Matters!

Metadata is data that describes or characterizes a digital object, whether internal or external to the object itself.

Metadata provides meaning, access, context and chain of custody verification for e-records.

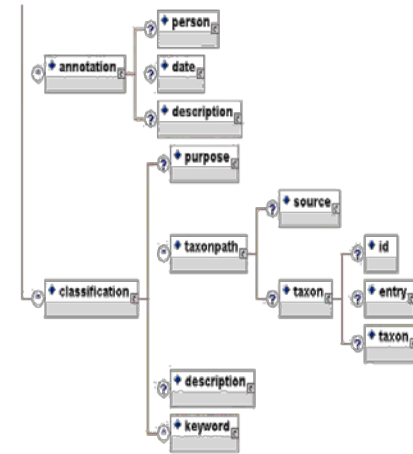
It is essential to record retrieval and integrity.

Types of metadata include *descriptive, administrative, structural, and preservation.*

Preservation Metadata

Preservation metadata includes:

- Identifying record “owner” or custodian
- Confirming the authenticity of the record
- Describing the technical environment of origin
- Tracking changes to original content
- Identifying changes related to preservation



Check Sums

Validate changes in record content or characteristics



RECORD CONTENT

Put the money in the bag,
I have a gum!

Put the money in the bag,
I have a gun!

HASH CALCULATION

9874 4646 8765

1288 0987 3601

Preserving Record Integrity



- Control of physical security and user access
- Training and documentation
- Integrity and validation checking for corruption, deterioration and accessibility
- Internal compliance audits
- Hazard mitigation and disaster planning
- Selection of appropriate storage systems

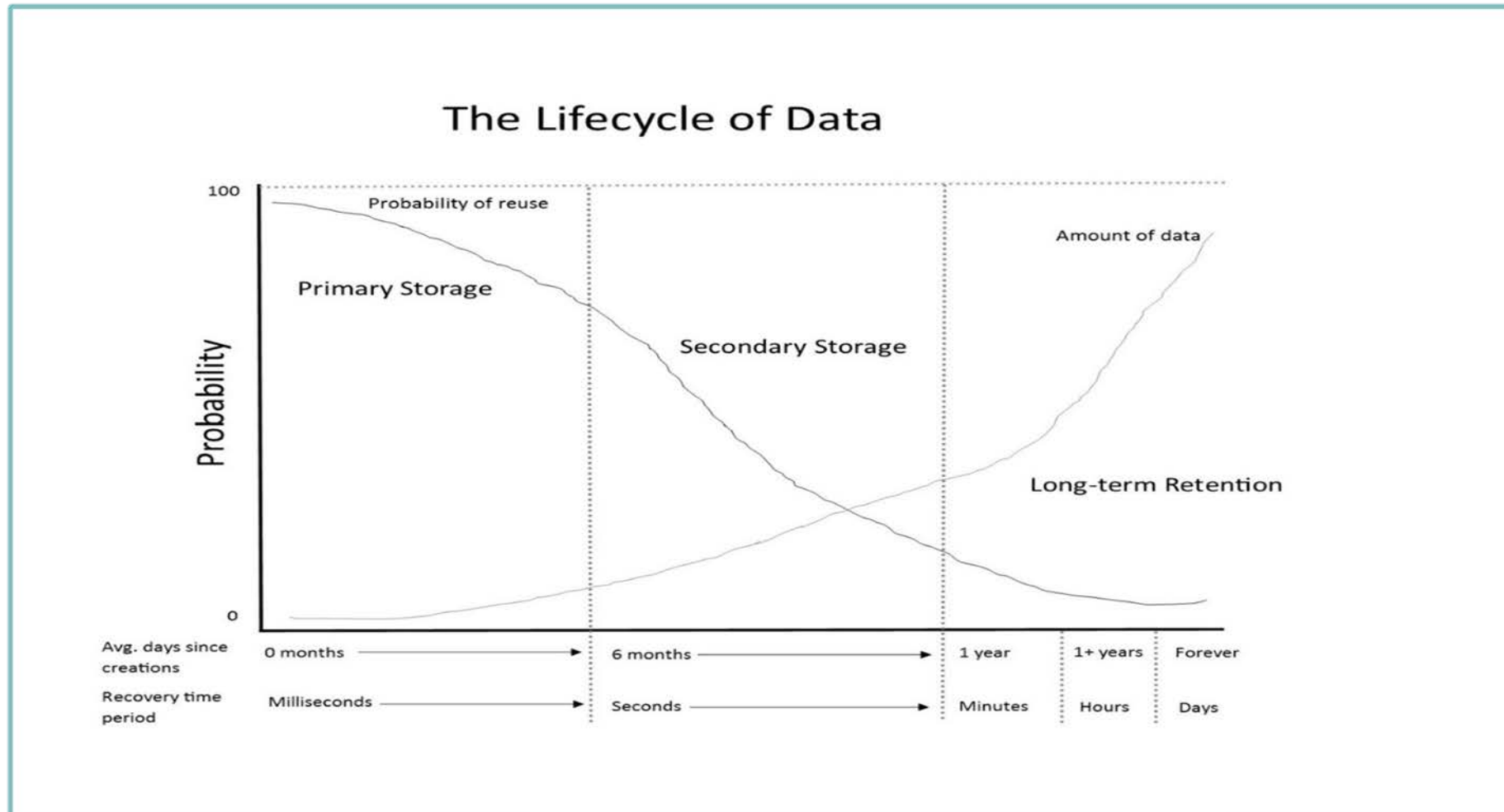
Selection of Storage Technology

- Access requirements (speed and frequency)
- Media lifespan
- Hardware compatibility over lifespan
- Technical capacity and capabilities of staff
- Cost of acquisition and maintenance

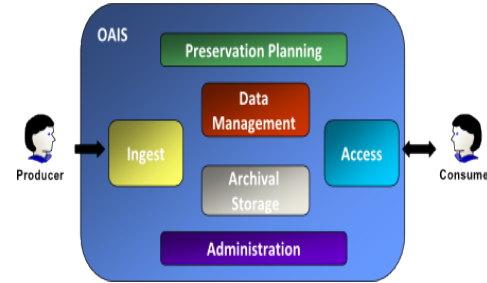
=> **Consider total record lifecycle needs**



Information Storage Lifecycle



Trusted Digital Repository



- Scheme supported by the National Archives and Records Administration
- Audit mechanism for assessing repositories for secure and reliable long-term preservation
- Includes technical requirements as well as organizational infrastructure and policies
- Provides a set of assessment criteria
- ISO standard 14721/Open Archives Information System

Preservation Strategy

- 1) Finalize retention periods
- 2) Identify and map current holdings
- 3) Eliminate Redundant, Obssolete & Transitory records (ROT)
- 4) Assess existing capabilities, capacity and risks
- 5) Select storage systems and architecture
- 6) Continually verify security and authenticity
- 7) Apply disposition and preservation standards and methodologies

Retention & Disposition Issues

Rethinking retention schedules:

- Permanent & long term retention rationale
- Media-dependent v. non-dependent
- Provision for legal/research/historical holds

Electronic record disposition considerations:

- Purging non-critical records/documents
- Automated disposition
- Disposition methods
- Accession (to other agencies)

Retention and Record Access

E-records Access and Publication

- How long and for who
- Controls/limitations (redaction)
- Maintaining a “non-public” archive
- Digital rights management



ER Disposition Issues

- Disparate Digital Systems / Interrelated Information
 - Case management
 - Document management
 - Office automation
 - Court recording
- Adequacy of Metadata
- Automated v. Manual Disposition



How long is too long?



- Consider total costs of retention – search, storage, back-ups, migration.
- Coordinate paper and electronic retention schedules
- Inconsistent practices diminish trust and confidence
- Impact on access to public information



Utah's Document Retention Strategy

In 2014, Utah's Technology Committee reviewed the court's document retention policies

Objectives:

- *Establish a document retention schedule that ensures the availability of documents that are critical to the process of the court.*
- *Create an automated document management system that permanently retains critical documents and deletes non-critical documents after a specified period of time.*

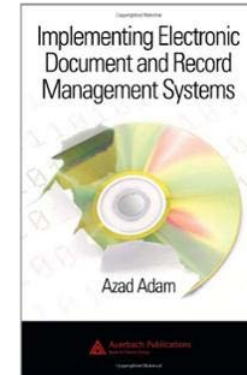
Keys attributes of the Utah retention policy:

- *Case history is retained as a permanent record*
- *Permanency can be maintained over time through refreshes in technology*
- *Document access and retention policies are based on court needs, not the needs of third parties*
- *Critical documents are permanent records*
- *Document retention is no longer a clerk duty*

Disposition Strategy

- Take an “enterprise” and “life cycle” approach
 - Case data and documents
 - Office automation products
 - Email, social media and web content
- Apply appropriate methods of disposition
 - Destruction
 - Archiving
 - Accession/transfer
- Conduct disposition actions regularly and consistently
- Verify and document disposition actions
- Adopt industry standards

Resources



ARMA International – www.arma.org

National Archives and Records Administration – www.archives.gov

Association for Information and Image Management – www.aiim.org

Council of State Archivists - www.statearchivists.org

National Association of Government Archivists and Records Administrators – www.nagara.org

Self-Assessment Tools



- ❖ Digital Preservation Capability Maturity Model
- ❖ Digital Continuity Checklist
- ❖ NDSA Levels of Digital Preservation Framework
- ❖ NCSC Judicial Records Maturity Matrix

Core Preservation Standards

ISO Standards

- OAIS (Open archival information system) Reference Model - ISO 14721:2012
- Trustworthy Digital Repository Audit and Certification – ISO 16363:2012
- Producer-Archive Interface Specification – ISO 20652:2015
- Other Useful Resources

PREMIS – Library of Congress Data Dictionary for Preservation Metadata

- <http://www.loc.gov/standards/premis/>

PRONOM – Online Technical Registry

- <http://www.nationalarchives.gov.uk/PRONOM/Default.aspx>

JHOVE – Object Validation API

- <http://jhove.sourceforge.net/>

COSCA Principles of Judicial Records Management

<http://cosca.ncsc.org/Policy-Papers.aspx>

ACCESS

GOVERNANCE

COMPLIANCE

INTEGRITY

PRESERVATION

DISPOSITION

Where Do You Go From Here?

- Resources
- Training
- Technical infrastructure
- Collaboration within and outside the organization
- Learn about prevailing standards and models
- Identify significant digital collections
- Create communities of interest with internal and external colleagues
- Benchmark your organization's digital repositories using available audit and certification criteria





JTC Resource Bulletin

Developing an Electronic Records Preservation and Disposition Plan

Version 1.0

Adopted December 5, 2014

Executive Summary

Courts have long had records retention and destruction schedules for paper case records. However, courts often lack the staffing resources needed to actually go through old files, sort and then destroy records. Thus, many such standing court record retention and destruction policies are generally permissive in nature, not closely followed and out-of-date in this new era of digital records.

Now that more jurisdictions are digitizing court records (data and documents), it is possible to systematically purge electronic records on an automated basis. However, before a court does so, a number of questions must be addressed in order to develop a sound electronic records policy.

This technology resource bulletin addresses the following policy areas and provides recommendations surrounding best practices in electronic records retention and destruction:

1. Should the electronic records destruction be automatic and, if so, what kinds of safeguards should be in place to ensure that the automated system is operating pursuant to court policy?
2. Should the electronic records destruction include both data and electronic documents?
3. What is the best way to delete court case data?
4. How long should a court system publish court records on-line, via the internet?
5. How long do records need to be maintained for research purposes and are records maintained beyond the standard retention periods subject to public disclosure?
6. How do courts designate historically significant cases for preservation? Should such designated case records be maintained by the court, the state office of record archives, or both?

After reviewing and consider the concepts in this bulletin, Court leaders will be able to develop a robust electronic court records retention and destruction policy for their courts.

Acknowledgments

This document is a product of the Joint Technology Committee (JTC) established by the Conference of State Court Administrators (COSCA), the National Association for Court Management (NACM) and the National Center for State Courts (NCSC).



JTC Mission:

To improve the administration of justice through technology

JTC Electronic Records Preservation and Destruction Work Group

David Slayton (Chair)
Texas Office of Court Administration

David K. Byers
Supreme Court of Arizona

The Honorable O. John Kuenhold
State of Colorado

Marcus Reinkensmeyer
Supreme Court of Arizona

Nial Raaen
National Center for State Courts

Joint Technology Committee:

COSCA Appointments

David Slayton (Co-Chair)
Texas Office of Court Administration

David K. Byers
Arizona Supreme Court

Laurie Dudgeon
Kentucky Administrative Office of the Courts

Gerald A. Marroney
Colorado Administrative Office of the Courts

Robin Sweet
Nevada Administrative Office of the Courts

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

Ex-officio Appointments

John Greacen
Forum on the Advancement of Court Technology

NACM Appointments

Kevin Bowling (Co-Chair)
Michigan 20th Judicial Circuit Court

Paul DeLosh
Supreme Court of Virginia

Yolanda Lewis
Superior Court of Fulton County, Georgia

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Craig Burlingame
Massachusetts Trial Court

NCSC Staff

Paul Embley
Jim Harris
Ilonka Dazevedo

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	12/5/2014	JTC	Release document

Contents

Executive Summary	ii
Acknowledgments	iii
Document History and Version Control	iv
Contents	v
Background	1
Questions in Development of an Electronic Records Policy	2
Should the electronic records destruction be automatic?	3
Should the electronic records destruction include both data and electronic documents?	3
How best to delete court case data?	3
How long should a court system publish court records on-line?	4
How long do records need to be maintained for research purposes and are records maintained beyond the standard retention periods subject to public disclosure?	4
How do courts designate historically significant cases for preservation?	4
Records Preservation	5
Preservation Policy Recommendations	10
Preservation Planning	10
Storage Management	11
Security Access and Control	12
Disaster Mitigation and Preparedness	13
Auditing and Quality Control	13
Adoption of Open Standards	14
Classification, Indexing and Metadata	14
Archival Storage	15
Adoption of Standards and Performance Measures	15
Multi-media records	16
Historical / research value holds	16
Records Disposition	16
Retention Schedules	17

Records Appraisal	18
Deletion/Destruction of Data.....	19
Disposition by Transfer (Archiving).....	21
Disposition by Accession	21
Disposition Policy Recommendations	22
Criteria for disposition	22
Approval Mechanism	22
Documentation	23
Metadata.....	23
Related Records	24
Selection of Disposition Methods	24
Alignment with Paper Destruction	24
Holds and exceptions	25
Duplicates and non-records.....	25
Jointly held records.....	26
“Unstructured” records.....	26
Email Management.....	26
Social networking records	27
Exhibits and other submissions by parties	27
Purging documents.....	27
Conclusion	28
Reference.....	28
Emerging Models.....	28
Open Archival Information System Reference Model.....	29
Digital Preservation Capability Preservation Model.....	30
Levels of Digital Preservation Framework	31
Applicable Standards.....	31
Digital Document Management	31
Indexing and Metadata	32
Facilities and Storage.....	33
Vital Records and Risk Mitigation.....	33

Background

Most state and local courts probably have a records retention and destruction schedule for paper case records. However, courts often lack the staffing resources needed to actually go through old files, sort and then destroy records. Thus, many existing policies are generally permissive in nature, not closely followed and do not address the retention and destruction of digital records.

Now that more jurisdictions are digitizing court records (data and documents), it is increasingly important that courts have a sound electronic records policy. While it is possible to systematically purge electronic records on an automated basis, the policies and processes that drive that automation must address a number of new and complex issues. Because paper records have historically not been destroyed on a consistent basis - at least not without microfilming - the standing destruction policies must be revisited, bearing in mind that the purged records will no longer exist.

Courts may address that concern by instituting a policy requiring no destruction of electronic records. However, that will lead to rapid growth in required storage space. Not only is the maintenance of this storage costly, but an automated records management system will quickly reach the point that backup and restore features can become unworkable due to the volume of records. Ultimately, large data stores will also result in inordinately long search and retrieval times, reducing efficiency of court operations. Life cycle costs associated with data and document storage are delineated in Figure 1.

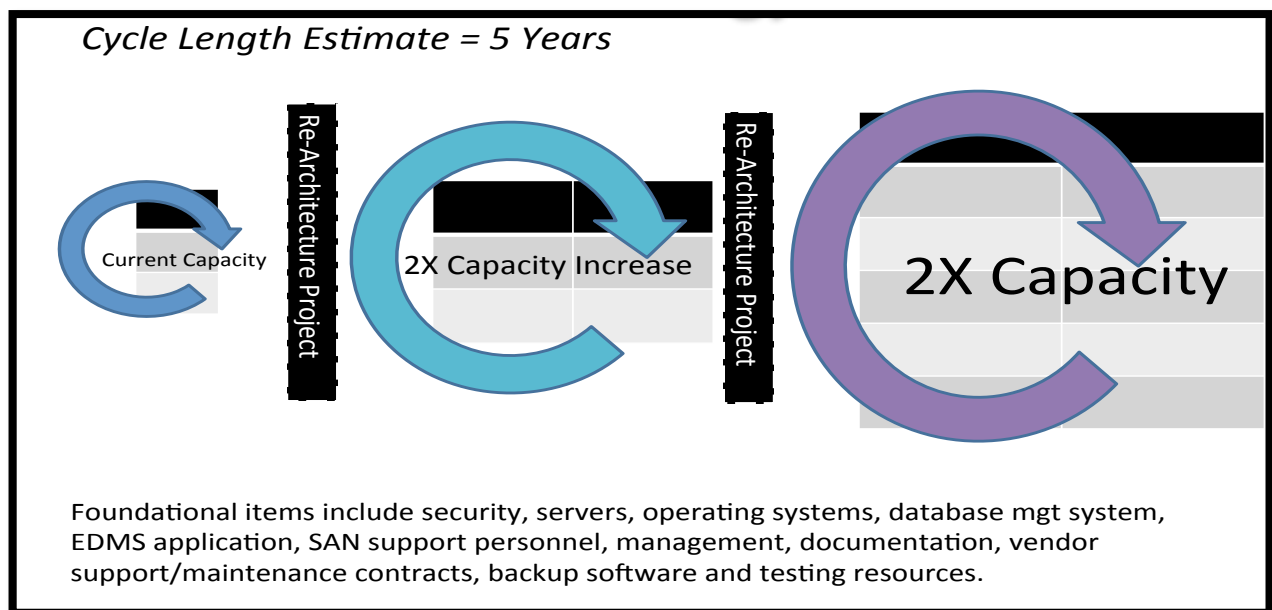


Figure 1: Future Cycles of Storage Technology

Questions in Development of an Electronic Records Policy

In developing comprehensive electronic records retention and destruction policies, courts must consider records access, operations and technical issues. Once the retention period for a particular category of case has been reached, will the destruction of records be mandatory or permissive?¹

Whether a centralized or decentralized court system, there are good arguments that records management policies be consistent throughout the statewide judicial system. Litigants can be harmed or helped by the status and availability of their records.² Other justice entities also regularly access court records and expect consistency in the availability of records. Thus, as a general guiding principle, electronic records management policy and practices should not be a local option.

Other electronic records policy issues include the scope of records under consideration, methods of records destruction, the length of time records are available to the public online and the historical value of certain court records. These issues fall in three interrelated areas of policy, which are best considered collectively in record policy formation: retention, destruction and public access.

¹ Addressing best practices under the principle of disposition, the COSCA 2012-2013 Policy Paper, "[To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records](#)," states that courts should, "Remove non-essential, obsolete or duplicate records routinely."

² "State court systems must ensure that records disposition policies are implemented in a consistent manner statewide, particularly considering the fact that individuals rights can be adversely affected by such records and manage them consistently from jurisdiction to jurisdiction." COSCA 2012-2013 Policy Paper.

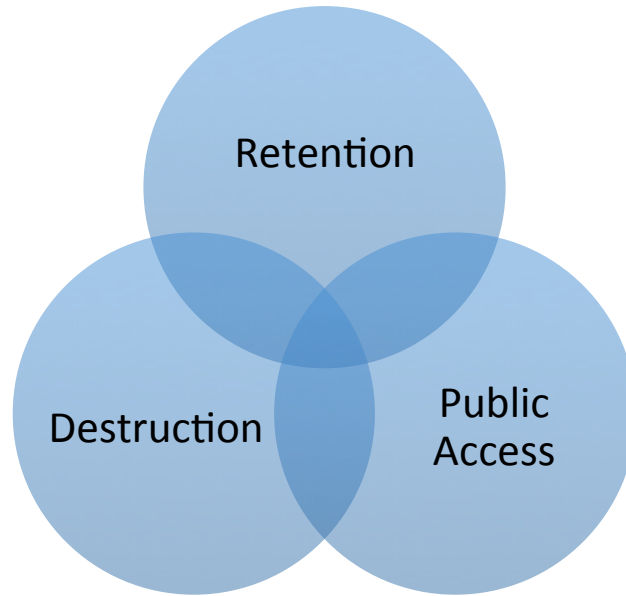


Figure 2: Electronic Court Records Policy

Specifically, a comprehensive electronic court records policy should address the following questions and clearly delineate supporting procedures:

Should the electronic records destruction be automatic?

If so, what kinds of safeguards should be in place to ensure that the automated system is operating pursuant to court policy?

Should the electronic records destruction include both data and electronic documents?

It is unlikely that a policy should allow for maintenance of case management data, while at the same time mandating destruction of supporting court documents. This situation would be problematical when a litigant returns to court for some action, following the destruction of the records, e.g., a motion to set aside a conviction.

How best to delete court case data?

Deleting case data is not easy. Case management systems will place data about a case in a variety of locations. Actual deletion of a case may have to be mapped. Local courts using the same CMS may not use it consistently. An alternative is “soft deletion,” wherein the data remains, but the searchable link is broken. This approach would prevent a case lookup. While this method is easier than that of physical data destruction from a technical standpoint, it does not reduce data storage space needs. Thus there are pros and cons of each method. Compounding the problem is the issue of financial records associated with a

case. Deleting records that have data linked to the general ledger system will cause technical and operational issues.

How long should a court system publish court records on-line?

Many court systems have a case look-up system on-line. One approach is to make the time period consistent with the records destruction time period. Another approach is to make the on-line access time period subject to any “look back” requirements, e.g., reference to criminal convictions for prior offenses as provided by statute or court rule. The Arizona state courts found that even after expiration of this time period, there was still a need for the courts to maintain records to allow involved litigants to return to court to request a “set aside” of conviction or records expungement.³ Litigants may need this extended records availability “service” in order to qualify for a job related licensing requirement, housing, passport and visa requirements or other reasons. This is true both for misdemeanor and local ordinance violations, as well as criminal felony convictions.

How long do records need to be maintained for research purposes and are records maintained beyond the standard retention periods subject to public disclosure?

In considering the optimal scope of records required for research purposes, it is advisable for courts to fully consider data/document requirements for legislative inquiries, program evaluation and longitudinal studies.

How do courts designate historically significant cases for preservation?

Should such designated case records be maintained by the court, the state office of record archives, or both?

In addressing the foregoing policy questions, courts are challenged to balance the public’s need for long-term access to court records with the high cost of digital records storage. Potential harm to litigants due to longstanding convictions in limited jurisdiction courts (e.g., convictions for misdemeanor and local ordinances offenses) should also be considered in this context. The analysis should take into account the frequency of reference to disposed records for each specific case type (e.g., civil, criminal, probate, family, juvenile) for each jurisdictional level of court (limited, general and appellate jurisdiction courts).

³ *Report of the Advisory Committee to Develop Policies for Retention, Destruction, and Access to Electronic Court Records*. Rep. Supreme Court - State of Arizona, Dec. 2013. Web. 6 Nov. 2014.

Figure 3 depicts a framework for defining an optimal retention period (“sweet spot”), predicated upon the likelihood that records will be needed, versus long-term storage costs. This analysis is best informed with input from court record users, including litigants, the media, data aggregators, investigators, etc. Input can readily be gathered through surveys, focus groups and on-line public comments regarding proposed electronic records policies.

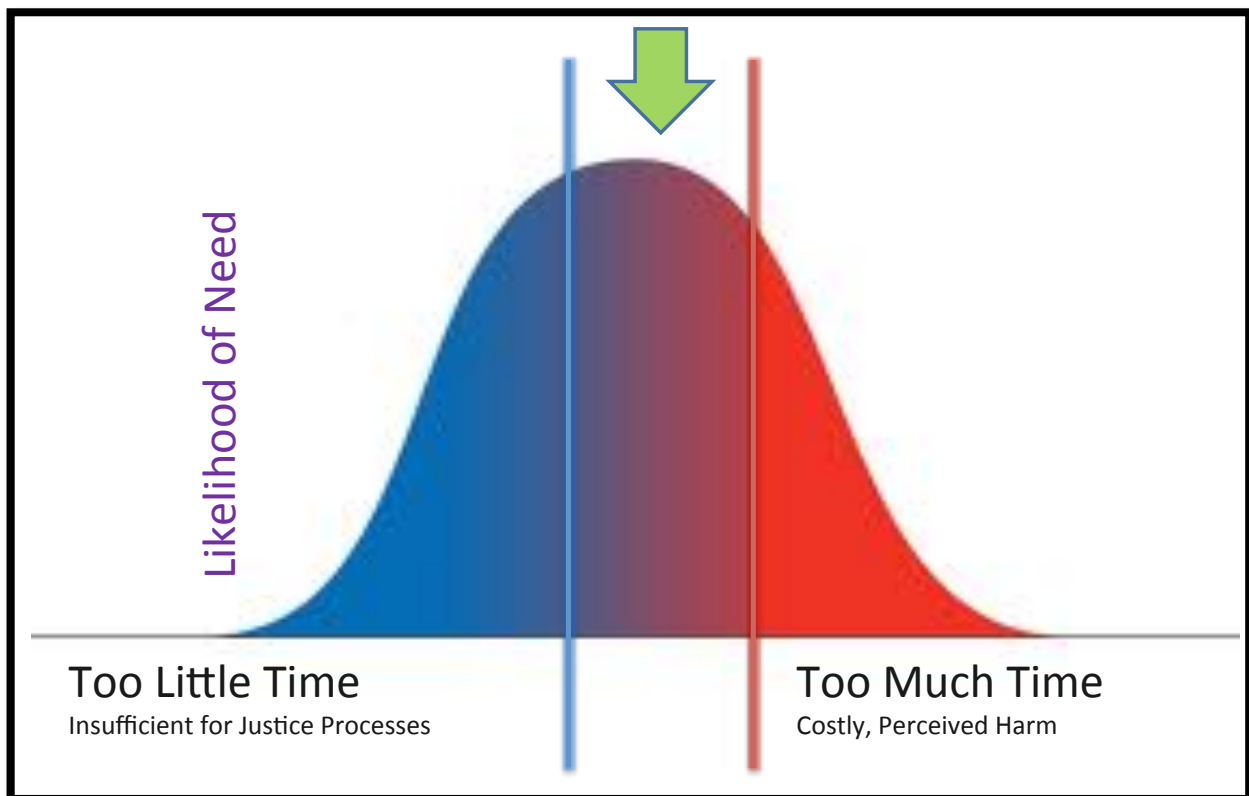


Figure 3: Locating the "Sweet Spot" for Records Retention

Records Preservation

Records preservation is one of six key principles identified by the 2012-2013 COSCA white paper, *To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records*.⁴ The paper sets forth a set of principles as a framework for assessing and implementing effective judicial records management practices based on the Generally Accepted Recordkeeping Principles© developed by ARMA

⁴ Linhares, Gregory J., and Nial Raaen. *To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records*. Conference of State Court Administrators, 2012-2013 Web. 10 Nov. 2014.

International⁵. This paper explores the issues, key elements, and emerging solutions for preserving electronic records.

The increasing adoption of e-filing and digital imaging systems is bringing the courts closer to the promise of truly paper-on-demand record systems. Rules in many states now authorize courts to destroy paper records upon digitization and authorize the digital version as the official record. However, record retention requirements for long-term preservation of some record types will require preserving digital records over periods of time exceeding ten years. The readiness of many courts to maintain digital records in the face of continuing hardware, software, and storage media obsolescence and evolution is a matter of concern. Further, many courts have not applied retention schedule requirements to the destruction of digital records that have exceeded their required retention period or engaged in adequate preservation planning.

Responses to a 2011 survey distributed on the COSCA list serve illustrated the variety of policies concerning approved media for long-term preservation of court records. Most survey respondents indicated that their state has adopted standards for short-term retention of records in both paper and digital form, however, only a few had adopted standards for long-term digital preservation. The respondents were about equally divided on the continued reliance on microfilm as the primary media for long-term records preservation.

The lack of readiness of governmental agencies to ensure the long-term preservation of digital records has been an issue of increasing concern outside the courts as well. A 2011 survey of state archives in fifty states and four territories conducted by the Council of State Archivists (CoSA) confirmed the inadequacy of electronic records programs across the country:⁶

- 35 states reported they do not have an electronic records program;
- 34% do not accession electronic records;

⁵ **About ARMA International and the Generally Accepted Recordkeeping Principles®**

ARMA International (www.arma.org) is a not-for-profit professional association and the authority on information governance. Formed in 1955, ARMA International is the oldest and largest association for the information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes Information Management magazine, and the Generally Accepted Recordkeeping Principles®. More information about the Principles can be found at www.arma.org/principles.

⁶ *State Electronic Records Initiative - Phase I Report*. Council of State Archivists', State Electronic Records Initiative (SERI) Committee, June 2012. Web. 6 Nov. 2014.

- Few state archives have the resources and support necessary to integrate special project results into long-term electronic records management strategies;
- Few state archives have a working relationship with their state IT departments, and most are not integrated into the system decision making processes;
- One-quarter of the state archives and all four territorial archives indicated that they had done nothing to manage and preserve electronic records;
- Only five state archives indicated that they have a planned system for developing electronic records management and preservation.

The CoSA report concludes that it is “likely [that] no state has a system which would pass the test audit for the ISO standards for a Trusted Digital Repository.” The apparent lack of capability of state archival agencies to maintain electronic records raises concerns that other state and local government agencies, including the judiciary, are similarly unprepared.

The CoSA findings are supported by many experts who maintain that few organizations currently have the technical capacity for long-term preservation, and that a substantial proportion of digital information is therefore at risk for loss. The following graph from savingthedigitalworld.com, an organization dedicated to raising awareness of digital preservation issues, predicts substantial loss of information over time in traditional data centers:

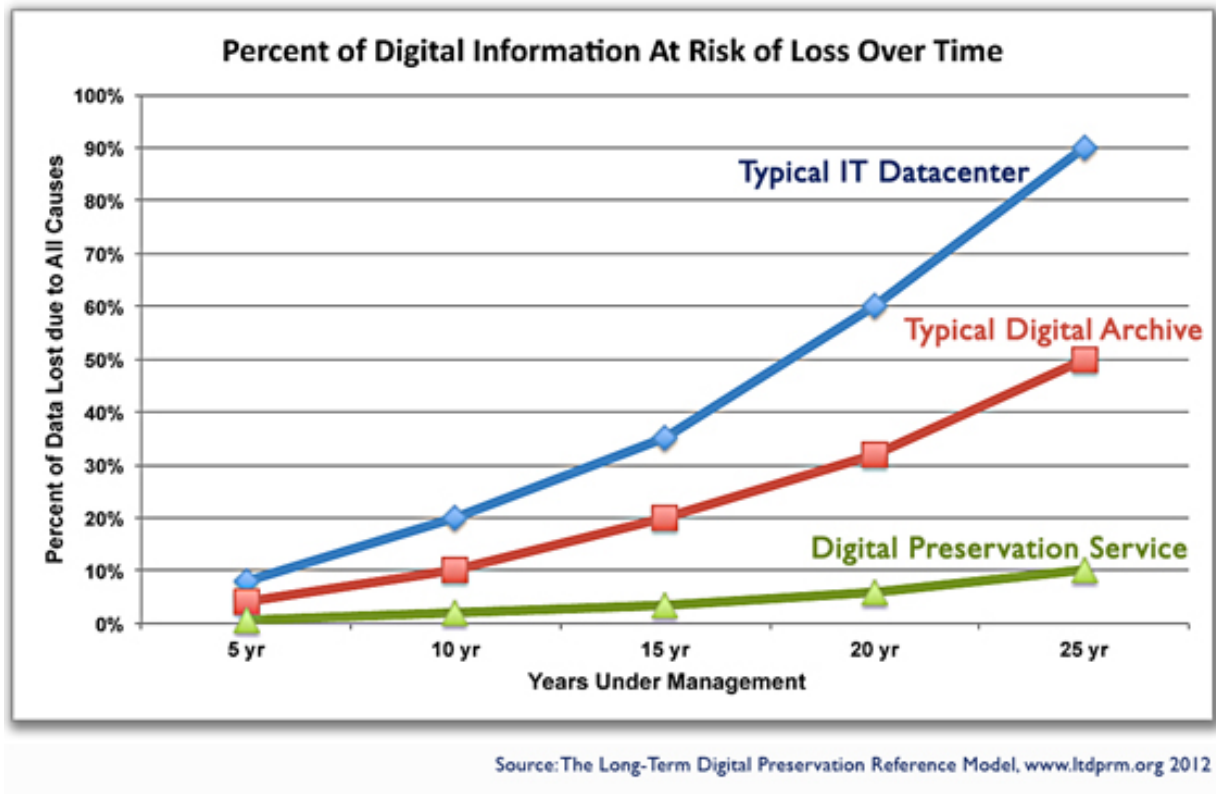


Figure 4: Percent of Digital Information at Risk of Loss Over Time

Compared to their paper and microfilm counterparts, electronic recordkeeping systems are generally more vulnerable to undetected alteration or loss. This vulnerability means that there is the need for more comprehensive and detailed planning to preserve digital records over time.⁷ The preservation of digital records also requires more intervention and expertise than is the case with paper records. Stored under the proper conditions, paper records have survived for centuries. Long-term digital preservation, on the other hand, involves regular monitoring, frequent intervention, and specialized technical capabilities. Finally, the longevity (market life) of digital records technology products and the vendor community providing systems and support services is volatile. Maintaining this long-term commitment to use digitally stored information requires a series of activities that maintain its retrievability, readability, and intelligibility.

Perhaps the greatest challenge to long-term usability of digital information are the rapid improvements in software applications and computer hardware that have led to what is

⁷ "Electronic Records Management Handbook." (n.d.): n. pag. *DGS Digital Services, Office of State Publishing*. State of California, Department of General Services, Feb. 2002. Web. 7 Nov. 2014.

known as technological obsolescence. Technological obsolescence is attributable to a number of factors unique to the digital world. These include:⁸

Media obsolescence. The options for storage and presentation of digital data continue to evolve. New technologies and higher density storage materials are regularly replacing older products and techniques.

Media failure. Various media have estimated life spans which represent their useful life cycle under ideal conditions. All media are susceptible to various levels of failure, with removable media being more vulnerable. Manufacturing defects, poor storage conditions, frequent handling, physical damage and deterioration of media surfaces are factors that can reduce the useful life span.

Hardware and software obsolescence. The continuing development and increasing sophistication of hardware and application software results in rapid obsolescence of software used to create and process electronic information.

File format obsolescence. The increasing range and complexity of formats in which data is maintained creates another challenge. Features such as hidden text and change history make digital documents more useful, but also create challenges with long term storage and retrieval.

Forward/Backward Compatibility. The need for wholesale conversion or migration of records can be deferred when newer systems are able to read data and files from older versions. However, older files may lose their formatting or other characteristics that have been improved or no longer exist in newer versions.

The term “readiness” as defined by the National Archives and Records Administration implies the need for a proactive approach to electronic records management. The following are some of the activities that are part of a planned response to preservation:⁹

1. Continually identifying records that are endangered by technology obsolescence, media fragility and other threats;
2. Developing preservation rules and methodologies for the entire lifecycle of electronic records;
3. Addressing security, privacy and custodial issues to ensure authorized and authenticated access to digital materials;

⁸ Tilbury, Jonathan. *The Active Preservation of Digital Information* (July 2013). Web. 8 Nov. 2014.

⁹ "Fast Track Guidance." *National Archives and Records Administration*. National Archives and Records Administration, n.d. Web. 11 Nov. 2014.

4. Planning for obsolescence of formats, software and hardware by adopting preservation methods to ensure that electronic records will remain accessible;
5. Developing appropriate storage architecture and infrastructure for electronic records and related preservation metadata.

Clearly, effective preservation is not an afterthought but requires attention to long-term needs throughout the records lifecycle.

Preservation Policy Recommendations

While there is no single comprehensive solution to this challenge, there are a number of steps that judicial organizations can take to address digital preservation, including policies, planning, and technical conditions that collectively contribute to a higher probability that today's records will still be usable tomorrow. These are described and summarized in a series of policy recommendations that courts should consider adopting as part of an overall records management plan. The elements described below should be incorporated into a *digital preservation strategy* to ensure that digital records remain accessible and usable over time.

Preservation Planning

Plan and implement processes and procedures for the conversion and migration of digital records and the systems that support them to new formats, storage media, and technologies.

A preservation strategy may involve planning for one or more of the following methods of preserving digital information:¹⁰

Migration – Migration transfers data or objects from one format to another in order to ensure continued access using new technologies. There are a number of strategies that can be employed, including normalization, migration at obsolescence, and migration on demand. It is possible that bits of data may be modified during migration, which can compromise data integrity.

A sound migration strategy requires technical support and supervision to ensure the preservation of the original characteristics of the record upon migration. The long-term usability of digitally stored information, including scanned document

¹⁰ Brown, Adrian, Shadrack Katuu, Peter Sebina, Anthea Seles, and International Records Management Trust. "Training in Electronic Records Management, Module 4: Preserving Electronic Records." 2009. Web. 7 Nov. 2014.

images, digital data, and descriptive index data, will best be achieved by implementing a sound policy for migrating data to future technology generations, adhering to well-documented image file-header formats, and monitoring media degradation.

Preserving Legacy Systems - Many courts are now using second or third generation electronic case management systems. Older data may still reside on legacy hardware accessed by software that is no longer supported by the vendor. In many instances data residing on these systems will be used for information purposes only. However, information retained under these circumstances will remain viable only as long as replacement hardware and qualified programmers are available to keep these systems running. As a strategy, maintaining outdated systems can be risky but may be the only viable option in some instances.

Emulation – Emulation involves using a computer or software program to imitate the functionality of an older system and offer the best possible rendition of the original document or data. Emulation may include application software, hardware, and operating systems. However, this strategy may only prolong technical dependence on the emulator itself.

Transfer to Other Media - At some point the original software may no longer be available to access or read information. Digital records which are at the point in their life cycle where case processing functionality is not needed but the content of those records must be maintained for reference or archival purposes can be migrated to other less volatile media, including laser disk, microforms, and even paper.¹¹

The best preservation option will depend on a number of factors, including the record lifespan, format, frequency of and need for access, cost, and support capabilities.

Storage Management

Digital records must be maintained under physical storage conditions appropriate to the type of media and in compliance with manufacturer and industry standards.

The longevity of all records, regardless of the type of media, is determined in part by the conditions under which they are stored. In addition to maintaining

¹¹ Stephens, David, and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles." *Information Management Journal* Oct. 2000: 38-52. .

environmental stability (temperature and humidity) and protection from contaminants and sunlight, digital media require other specialized storage conditions. Redundant and separate logical or physical storage mitigates the risk of losing records from device failure, unintended deletion, and natural disaster, among other factors. The selection of storage systems should consider acquisition and maintenance costs, as well as the projected system life cycle.

The selection of storage methodologies should be based on the preservation requirements specific to the record series and media, along with the need for access by information users.

Various media and storage systems offer different options for maintaining digital records. For Instance, hierarchical storage systems can organize data storage between higher-cost, more accessible storage media and lower cost off-line storage according to the need to access or update a record series. Specialized software is available to monitor data utilization and can automatically move information from higher cost disk storage to tapes or other storage devices which more economically storage large volumes of data.

One approach is to implement an “active archive” solution combining disk and tape storage for storage of archival data while allowing more active data or documents to reside on more readily accessible disk storage. Before adopting a storage architecture approach the court must be able to clearly define the conditions or circumstances under which documents or information are most economically and efficiently maintained between various storage levels.¹²

Security Access and Control

All digital records under the judiciary’s control should be protected from inadvertent or intentional alteration, destruction, or disposal through the maintenance of security access controls appropriate to the record and corresponding users’ rights.

All digital information should be subject to user controls and physical protection. This includes protection of the physical infrastructure from accidental or deliberate damage, protection from external intrusion or unauthorized users, and maintaining clearly defined access and permission controls so that the ability to alter or delete objects in a digital repository is limited to those responsible for

¹² Moore, Fred. *The Data Archive Challenge - What’s Your Game Plan?* Horizon Information Strategies, n.d. Web. 7 Nov. 2014.

preservation tasks. Access or duplicate versions of records should be created for public access.

Disaster Mitigation and Preparedness

A written disaster plan and recovery protocol should be in place and periodically updated to identify roles and responsibilities in the event of a natural or man-made disaster.

Judicial organizations must include the protection and preservation of mission-critical records and information in an overall continuity of operations and risk management planning. *Risk mitigation* includes conducting a regular assessment of records systems and storage conditions to identify potential risks or hazards before they compromise record integrity and access. A *risk assessment* is a systematic process that helps identify the chances of a damaging event, estimate the costs of remediation, and set priorities for corrective action. A *hazard audit* focuses on the identification of immediate and potential risks that exist in the workplace. *Continuity planning* includes planning and preparation for the most likely disaster scenarios to enable the organization to identify its most critical records and take immediate steps to minimize further loss and damage.

Auditing and Quality Control

Digital records and storage systems should be audited for integrity on a routine basis, as well as during migration, transfer, or system change events to test for data corruption and media failure.

A program of audits and reviews of records media and systems is a good strategy for all types of records. This includes monitoring media for deterioration, checking the accuracy of metadata entry and indexing by staff, comparing original documents with the captured electronic images and index data, and ensuring overall compliance with records policies. The integrity of digital objects should be validated through the use of check sums and other tools. Checks should occur upon creation, before and after migration, and at other points where digital objects are at risk of alteration. Media should be sampled at time of acquisition to check for manufacturing defects. Maintenance and review of system logs provide a record of who has accessed or modified digital records. When corruption or deterioration of any record or its associated metadata is found, steps should be taken to recover the record if possible, and documentation of the result maintained for the planned lifecycle of the record.



Adoption of Open Standards

Open standards and formats should be adopted to facilitate access, exchange, and transferability of digital records over time.

The use of archival, open formats for electronic record preservation is a recommended best practice in the records management field. Approaches include saving records to an archival format upon record creation, or moving records from proprietary systems and formats at a later stage in the lifecycle, such as at point of transfer to a digital archive. Open system computing promotes interoperability between differing systems, flexibility in upgrading and migration, and sustained access to content. While open formats do not solve the problem of hardware obsolescence, they do improve the chances that documents will remain readable and accessible over time provided the integrity of storage media is maintained.¹³

Classification, Indexing and Metadata

All records should be subject to an organizationally-defined indexing or classification scheme to promote efficient access and management.

Many records under care and control of the judiciary are maintained in structured databases and indexes. However, there are increasing amounts of “unstructured records” being created in all organizations that may be maintained on shared drives, tablets and personal computers that are created by employees as part of their daily work. The most common examples are office automation work products, email, and social media exchanges. It is often difficult to determine the extent and value of this information. A records inventory or information “map” can assist in determining the location and nature of unstructured information. The results of an inventory can be used to identify records and information that are transitory or duplicative from more critical information that supports on-going organizational functions. This information can be used to develop appropriate policies and procedures for naming, indexing, and preserving records.

Create and maintain appropriate metadata to ensure that digital information can be accessed and authenticated over time.

Metadata plays an important role in long term digital storage and preservation by recording the information necessary for accessing records, ensuring record integrity, and facilitating conversion and migration activities. Metadata serves

¹³ Hoke, Gordon E.J., CRM. "[Future Watch: Strategies for Long-Term Preservation of Electronic Records.](#)" *Information Management*. ARMA International, May-June 2012. Web. 7 Nov. 2014.

multiple purposes in the records lifecycle, and models which are designed to address preservation are available for adoption. The use of metadata to define changes in the logical and physical structure of records, define changes in technical attributes, and document changing relationships with other records is critical to maintaining record integrity and documenting chain of custody.

Archival Storage

Archival storage should be planned for retaining digital information over longer periods of time or for records which are considered “permanent.”

Digital archiving is a set of processes, activities, and technical conditions for managing digital information over time to prolong its accessibility and security. Dedicated archival storage, whether in-house or provided by a third party, is often required for records which are no longer in active use but which require preservation for historical or legal purposes. A number of standards and conditions for digital archives have been developed and continue to be refined. These are described in more detail in the Emerging Models section of this report.

Adoption of Standards and Performance Measures

Appropriate industry standards for digital preservation should be adopted along with performance measures to determine the effectiveness of preservation efforts.

There is also a growing body of records management standards available for reference and use, covering paper, microfilm and electronic records. Recognized standards have been developed by the [International Organization for Standardization \(ISO\)](#),¹⁴ [U.S. Department of Defense \(DoD\)](#),¹⁵ [ARMA International](#),¹⁶ the [Association for Information and Image Management \(AIIM\)](#),¹⁷ and the American National Standards Institute (ANSI). Court leadership and their

¹⁴ "[ISO/TC 46/SC 11 - Archives/records Management](#)." ISO. International Organization for Standardization, Web. 13 Dec. 2014.

¹⁵ Office of the Deputy Assistant Secretary of Defense/ Deputy Chief Information Officer, Information Policy Directorate. [Electronic Records Management Software Applications Design Criteria Standard](#). 25 Apr. 2007. DoD 5015.02-STD. Arlington, Virginia.

¹⁶ "[Records Management Is The Foundation Of Compliance](#)." *Electronic Records Management*. ARMA International, n.d. Web. 12 Dec. 2014.

¹⁷ "[Analysis, Selection, and Implementation of Electronic Document Management Systems \(EDMS\)](#)." *aiim: The Global Community of Information Professionals*. Association for Information and Image Management International, 5 June 2009. Web. 13 Dec. 2014.

technical partners should refer to these standards and adopt those that are relevant to the types of record systems under their control and care.

Multi-media records

Special provisions for the disposition of records containing multi-media content may need to be made for those records being preserved over longer periods of time.

The increasing sophistication of office automation products allows the embedding of files and materials created with un-related software programs. An example includes a Word or .pdf document with an embedded video or audio file. This may be problematic if the document is subject to long-term preservation in an archive, as it may be difficult to ensure that the supporting software for an embedded file will still be available at a later date.

Historical / research value holds

Records should be periodically assessed for their historical and research value in consultation with interested agencies and institutions.

Many state retention schedules require that courts notify the state archives of pending destruction of court files to provide an opportunity for action to be taken to preserve items of historical interest. Certain individual cases and related records may have historical value by virtue of their notoriety or precedential value. The research value of court information is more difficult to estimate, however, judicial leadership may wish to consult with other agencies or educational institutions regarding information that would most likely be used for research purposes.

Records Disposition

The foundation of this principle of disposition is the recognition that all records reach a point in their lifecycle where they are committed to archival storage and preservation, or scheduled for destruction. This section addressed the transfer and accession of digital information to archives, as well as the destruction or deletion of electronic information as activities that fall under the principle of disposition.

Storing terabytes or even petabytes of information is no longer unusual. The decreasing cost and increasing capacity of storage technologies for electronic records has had the unfortunate consequence of making it easy for many organizations, including courts, to retain digital information well beyond its useful life. However, it has also become evident that the retention of ever-increasing amounts of information that has passed its useful

lifecycle is costly. In addition to the costs for physical storage, electronic records must be periodically migrated to stay ahead of hardware and software obsolescence. Large volumes of data complicate search and retrieval. The indirect costs of managing data cannot be ignored. Further, the longer electronic records are retained the greater the risk to their integrity and accessibility.

All records have a life cycle which begins with their creation or acceptance through their final disposition. A comprehensive records management program ensures that attention is given to records over the entire life cycle from creation to disposition, regardless of format. As courts increasingly rely on electronic case management systems, office automation products, and document management systems, giving attention to the disposition of electronic records at the end of the life cycle is of critical importance.

Retention Schedules

A record retention schedule is the source of authority for records disposition and should address all records under the organization's care and control, including administrative records. The schedule should provide for the systematic destruction of electronic records which no longer serve business or legal needs, while ensuring the continued retention of those records that have an ongoing value. Disposition therefore includes both records destruction and long-term preservation.

Case files and related documents in the state courts are typically covered by general records retention schedules created by statute, court rule or policy directives. These schedules are unique to each jurisdiction, but in many cases have not kept up with the rapid change in record-keeping technologies. Further, many records created and maintained by the courts may not be specifically covered under general schedules. Courts therefore may need to develop internal retention schedules for records not covered by a general state schedule.

Although many schedules do address both paper and electronic records, there are different approaches to the format of retention schedules in a hybrid (multimedia) environment:¹⁸

Media specific – provides separate schedules for electronic and human-readable records

¹⁸ Stephens, David and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles". *Information Management*, October 2000, Vol. 34, No. 4; ARMA International.

Media independent – specifies the retention period for each record series without reference to the storage media, even though records may reside on several media simultaneously or during various stages of the lifecycle.

Multimedia – one that contains all media within a single schedule, but with separate retention periods for the records contained on each type of media

An informal NCSC review of state retention schedules found that most feature a media independent approach to retention and disposition. Typically, media issues are addressed in terms of approved formats and standards for preservation of digital records.

Records Appraisal

The process of determining the retention value of a record is often referred to as a *records appraisal*. The value of records can be evaluated on the basis of their *primary* and *secondary* value. Primary values are those which meet the basic business purpose of the record, such as maintaining a verbatim record of court proceedings for review and possible appeal. Secondary values are other uses for the information, which frequently follow the expiration of the period of primary value retention. Examples include retaining information for historical or research purposes.

There are four values that are generally used as guidelines in assessing records for retention:

Operational value – This is the period of time during which the court requires the record to perform its primary function. This may reflect only the time that records are required to meet user needs; they are not necessarily legal requirements.

Legal value – This refers to those records whose retention is defined by statute or court rule, or those that may be needed in case of further litigation or investigation. Legal value is determined by factors such as:

1. Statutes, court rules, or judicial orders requiring records to be kept for specific periods;
2. Statutes or regulations requiring records to be kept, but not specifying retention time periods;
3. Records which set legal precedent.

Fiscal value – This refers to records that are created for administrative purposes as well as case-related transactions. These include payment transactions, budget documents, purchasing records, and payable records. In addition to the

need to preserve fiscal records to meet business or operational requirements, fiscal value is generally determined by the time that these records must be retained for audit purposes under state or local statutes.

Historical value – This is the long-term value of records which may, by virtue of their exceptional age and/or connection with some significant historical event or precedent, have long-term value. In some situations, individual cases or records will be identified for historical preservation, or an entire series, by virtue of its age, may be retained for its historical value. There are requirements in many states that local or state archive agencies be consulted prior to the destruction of certain judicial records, or that records be moved to the custody of the archive.

A record series or individual records within a series can possess more than one value at the same time, or sequentially, over the record's life cycle.

A useful metric for determining operational value is the *reference rate*. This simply refers to the frequency with which a record in a given series is accessed by court staff, litigants, or the public. Determining the reference rate for a record series is useful in deciding when records should be moved from active to inactive or archival storage, as well as determining the appropriate retention and destruction period.

The increasing reliance on email communications and the emergence of business applications for social media contributes to the complexity of managing organizational records. Electronic record keeping in particular has resulted in widespread information redundancy due to the ease in which records can be duplicated, distributed, and modified. Part of the task of developing a retention schedule is determining what should not be considered a record for business purposes.

Deletion/Destruction of Data

There are currently a number of techniques which are available for the permanent disposal of electronic records. The choice of method depends on a variety of factors, most significantly the type of media on which the records are retained, the cost, and the need to protect confidentiality. Some of the most common techniques currently in use include:¹⁹

¹⁹ Stephens, David and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles". *Information Management*, October 2000, Vol. 34, No. 4; ARMA International.

Removable Media Destruction (Shredding). Various types of removable electronic media, including CDs, DVDs, diskettes, magnetic tapes, and cartridges can be shredded into particles. Shredding standards have been established that meet the needs for destruction of classified information.

Degaussing. Degaussing is a process that renders data stored on magnetic media unreadable by changing the magnetic properties of the media surface. The application of a strong alternating magnetic field results in the loss of exposed data and renders the media in a magnetically neutral state. Degaussing is appropriate for hard drives and certain types of removable electronic media, such as backup and digital tapes.

Hard Drive Destruction (Punching/Crushing). Hard drives can be destroyed by machines that hydraulically crush machines. The crusher utilizes a punch that causes irreparable damage to the hard drive chassis, while also destroying the internal platter. This force is sufficient to alter the drive so that it cannot be reconnected or inserted into a functioning computer.

Encryption and Media Overwrites. Digital information may also be rendered inaccessible through encryption and overwriting of the media with new information. These techniques may not be suited to records which are confidential, but are adequate for situations in which the physical media is still in good, reusable condition.

“Soft” Deletion. Information which is no longer required to be retained for public access or business purposes can be rendered inaccessible through the deletion of links or flagging the record to be deleted. The action will render the information temporarily inaccessible. A full or hard deletion of a record may be scheduled for a set period of time following the soft delete, after which the record is permanently deleted. The advantage of a soft delete is that it provides some protection in case records need to be accessed to correct errors in publication of court records which have passed their normal retention period.

The widespread use and dissemination of court records by private companies and the publication of court information to the internet increases the potential harm from incorrect or outdated information. Despite limitations on the use of public records for commercial purposes under the Fair Reporting Credit Act, information may remain published for periods of time that exceed the normal retention period for the particular record series. For this reason many courts have continued to retain case information, which would normally have been destroyed, well beyond the retention period as insurance against later disputes over information accuracy.



Disposition by Transfer (Archiving)

Electronic records which are no longer of business value but are required to be retained for longer (over ten years) periods of time may be disposed through transfer to an internal digital archives. Archiving is often a way of migrating documents and data from more costly, online media to secondary and less expensive storage based on the declining need to access the record series. Archiving is often confused with backups. Backups are copies of data which may be used to restore the original after a data loss event. Archives are not synonymous with storage of low-value data. Archives are an important method of disposition for records whose preservation is required for legal or historical purposes. New standards and approaches are being developed to address the need for longer term digital archiving. Another archiving option is to dispose electronic records by transfer to non-electronic or analog media for long-term preservation.

Disposition by Accession

Accession is defined as the transfer of a record to a third party or external agency for preservation. For court records, accession usually involves transfer of records to a state or local archives, which assumes responsibility for the records' further preservation. This procedure is used to preserve historical records by moving them to a facility where conditions and oversight are more conducive to long-term preservation. Several state archives have now begun to accept digital court records for long-term preservation. Successful accession requires attention to these additional tasks²⁰:

- Ensuring that each digital object is properly labeled with a unique identifier and associated metadata or finding aids
- Conversion of records, if necessary, to open standards formats (i.e., PDF/A, XML) as part of the transfer process
- Scanning of digital objects and hardware used in the process for viruses or malicious code
- Documentation of the transfer process in detail and verification of receipt for audit purposes
- Testing of transferred records before and after the process using checksums or other validation processes to verify integrity

Whether records are archived internally or to another agency, the judiciary must be certain that all operational and administrative needs have been satisfied prior

²⁰ International Records Management Trust. "[Training in Electronic Records Management, Module 4: Preserving Electronic Records](#)." 2009. Web. 7 Nov. 2014.

to transfer or accession, as well as maintain backup copies of transferred records until the transfer process has been completed and verified.

Disposition Policy Recommendations

The following are some of the policy considerations that should be taken into account when developing policies and procedures for the disposition of electronic records:

Criteria for disposition

The criteria for disposition of all records must be clearly specified in the records retention schedule.

When disposition is contingent upon a triggering date, the events associated with a records series must be clear and actionable. Triggering events typically will have associated dates such as a final verdict or disposition in a case file, or “employee termination” event date for employee personnel files. The meaning of “disposition” or “termination” must be clear and generally understood, particularly if the court relies on an automated process to delete or transfer the record or file. Exceptions must be clearly defined in the system, for instance, whether a re-open event resets the timer for disposition. The information must be properly and accurately captured in an information system. This is generally straight-forward in most case management systems, but may be more problematic with unstructured records such as office documents.

Robust records management software for removal of records should be in place with retention rules applied to effectively obliterate the data once all conditions for disposition are met. The system should further provide monitoring and oversight to ensure that only eligible records (i.e., those meeting retention requirements with no legal preservation holds) are destroyed.

When records are being held by an outside agency or vendor at the time of disposition, the court must ensure that the organization has the requisite capabilities to properly destroy the materials and require that verification of the destruction be provided.

Approval Mechanism

Policies for disposition of records should clearly identify the approval process for disposition, including whether disposition occurs automatically or requires human intervention for the disposition event.

Ensuring the proper disposition of electronic records requires a determination of the most appropriate manner for approval of destruction or transfer. This includes whether the migration of records and data from the primary storage system to secondary storage occurs automatically through system software controls, and whether any human intervention is required before this occurs. Some experts²¹ suggest that this depends on the type of storage management software that exists in the computing environment, if any. For instance, hierarchical storage management software may support the automatic migration of records from primary to secondary storage media without intervention.

Documentation

The disposition of all records, whether through destruction, transfer, or accession, must be accompanied by a record of that action.

Just as with paper records disposition, documentation must be retained that adequately describes the records series, the date and method of disposition, the authority for disposition, etc. An audit trail should exist and disposition metadata maintained for information such as disposition date and type, retention trigger and date, original creation date, closure date, etc. As with all records there must be documentation of the destruction process. For physical records this is often accomplished through a certificate of destruction. For electronic records it may be done using the audit trail from the destruction process and preserving related metadata.

Metadata

All records subject to disposition should have been assigned sufficient metadata to ensure proper identification of those records, including preservation metadata for records which are archived and a metadata “footprint” of records destroyed in accordance with the retention schedule.

Depending on the operating definition of public records, dispositional metadata may be considered to be a public record. As proof of proper disposition metadata may be the most reliable method of ensuring transparency and accountability. Steps will need to be taken to determine how the dispositional metadata itself is stored and made available.

²¹ Stephens, David, and Roderick Wallace. "Electronic Records Retention: Fourteen Basic Principles." *Information Management Journal* Oct. 2000: 38-52. .



Related Records

Related or integrated records with differing retention requirements must be identified and steps taken to ensure that disposition of one record does not compromise or cause a related record to be disposed of prematurely.

Court records are increasingly interrelated. Case management information residing in databases may be linked to court records on dedicated servers and documents in document management systems through hyperlinks. In addition, documents may be generated from data fields in the case management system. Staggered disposition of inter-dependent systems may disable certain features. In some cases, inter-related records may be subject to differing retention periods. This needs to be taken into account prior to disposition.

Selection of Disposition Methods

Retention schedules should specify the allowable methods of destroying digital records in accordance with record content and type of media.

The appropriate methods for disposing of records will need to be determined based on the type of media, relative confidentiality of the record, local technical capability, and availability of third party resources for archiving or destruction. As noted in the foregoing discussion, there are a number of commercial processes for properly destroying digital records, as well as archival systems for longer-term preservation that may be employed.

Alignment with Paper Destruction

Retention schedules should identify records preserved on more than one form of media (paper, microform, digital) and should clearly specify if there are different disposition timelines and types for each record/media type.

Many courts will continue to operate in a hybrid environment for the foreseeable future, maintaining hard-copy versions of records which also exist in digital form. If the current records retention schedule only addresses hard copy records, the court is left with a choice of either applying the same standard or adopting a separate period for electronic records. There may also be good reasons for separate retention periods, as electronic records may be more readily accessible to the public and court users.

The destruction of source (paper) documents within a short time following their conversion to a digital format is an important policy consideration. One of the great advantages of imaging systems is the savings in the access, storage and maintenance costs of paper records. The answer to this depends on the legal

authority to maintain the digital version as the official copy, as well as the retention requirement for the record, and agency capacity to maintain a digital version that is reliable and accessible for the full term of the document lifecycle.

Holds and exceptions

Disposition policies should include protocols and procedures for deferring the disposition of individual records or groups of records which may be subject to legal discovery or other circumstances that warrant their deferred disposition.

Accommodation should be made for individual records which are exempted from disposition for specific reasons. These would include records which are related to pending or expected litigation, have historical value, or for other reasons should be retained for a longer period of time than that specified for the records series.

Widespread access to court records for commercial purposes such as background checks has created a particular challenge for the courts. Without control over how long and in what format court information is made commercially available by a third party, a court may be destroying a record in compliance with the retention schedule but long before the same record disappears from the public domain. This potentially creates problems when an individual seeks to correct or update the information, for instance in the case where a criminal record is later expunged or information has been recorded in error by a third party. Many courts have continued to maintain case files or records of judgments well past their retention period for this reason.

Duplicates and non-records

Policies and procedures should be implemented to identify and eliminate duplicate and non-record material as soon as its usefulness has expired.

During the normal course of business multiple versions and copies of certain records may be created. Policies should define what records constitute the original version and identify the record owner. In addition, some of the material held by a court is not directly related to business needs. Examples of items which are typically considered non-records and therefore not included on a record retention and disposition schedule include:

- Identical copies of documents created for convenience or reference.
- Records created by staff for personal convenience.
- Blank forms and publications.



Jointly held records

The primary record-holder for records which are held jointly by the judiciary and other agencies should be identified for purpose of determining responsibility for disposition.

Certain records, such as personnel and finance records, may be maintained jointly by the judiciary and outside agencies. It will be necessary for the court to determine, in consultation with the other record holder, whether two versions should be maintained and for how long. If one copy is maintained as a reference for convenience, the reference copy should only be retained as long as needed for business purposes.

“Unstructured” records

All records created, accepted and managed by the judiciary that have business value should be adequately indexed and associated with sufficient metadata for assignment to the retention schedule.

Much of the information created and maintained by courts outside case files and records is “unstructured”. Unstructured records are not maintained in a database and may have little or no metadata or labels to identify their contents. Some of these records may be created and organized by individuals with little or no guidance. Examples include documents, spreadsheets, images, and recordings which residing on network servers, PC hard drives and removable media. The value and lifecycle of these records depends to a great extent on their content and it is therefore critical that these records not be overlooked in disposition planning.

Email Management

Email classification systems should be designed to identify those items which contain business content and to assign them to the corresponding record series category in the retention schedule.

One of the significant sources of unstructured records is email. Email itself is not considered a records series or category, but rather a means of communication and transfer of information. However, email messages containing content that is related to the work of the court may be considered records.

Email management has created a new set of problems for organizations, such as determining who maintains the record copy of a message, classifying the information contained in an email, determining the appropriate retention period, and managing the sheer size and volume of email and related attachments.



Before considering how to deal with email-related information in the retention schedule, it may be necessary to develop an email classification system and accompanying policies to ensure that the disposition of email content is compliant with applicable laws and regulations.

Social networking records

The value and relevancy of social networking communications should be assessed and steps taken to classify and include those that are deemed to be official records on the retention schedule.

A relatively new demand on electronic records management and disposition is the emergence of social networking exchanges. This shift in human communication patterns, while not fully tapped in the judiciary, will no doubt contribute to the increasing volume and complexity of electronic record management in the future. Judicial record managers should be assessing the business value of social networking communication for preservation needs. As with email, the relevancy of content is key to determining the retention and disposition requirements of these records.

Exhibits and other submissions by parties

The retention and disposition of exhibits and other records submitted by litigants and other third parties should be specified in the retention schedule.

Exhibits and other documents or information submitted by parties that are not entered into the court record but are in the court's custody may need to be addressed. Common practices provide for the return of exhibits and similar records to the submitting party shortly after the conclusion of the case. Unclaimed records will generally be destroyed after a period of time and notice is given to the submitting party. Similar procedures should be taken to document the disposition of electronic evidence as is the case for other court records.

Purging documents

Retention schedules should include any approved policies or procedures for removal of documents from case files or other collections at the time of transfer to other media or record holders.

The conversion of paper records to other storage media can be a time-consuming and costly process. Generally this process occurs at one of the following points in the case file life cycle:

- final disposition or closure
- transfer to archives or inactive storage
- conclusion of a specified minimum retention period

Purging is often justified by the time saved by users in not having to search and view non-essential documents and the additional cost of scanning and storing non-critical records on digital or microfilm medium, including staff time, equipment and consumable costs. The benefits are weighed against the potential consequences and likelihood of errors of omission of important documents, how readily documents can be identified and separated from each other during the purge process, and the cost in terms of staff time to separate documents before scanning.

Generally speaking, separating critical from non-critical documents is easier when documents are scanned upon intake, eliminating the need to go back through court files and review each document for scanning. If purging can be performed at the time the file is disassembled for scanning it should take less time than having a separate step that requires court staff to purge files prior to sending them out for scanning. This requires personnel who are performing the scanning function to have the training and knowledge to make accurate decisions regarding which documents should be purged.

Conclusion

Courts have long struggled with records retention and destruction. This problem is only exacerbated by the transition to electronic records. As courts continue to migrate to a fully electronic environment, consideration of a comprehensive electronic records retention and destruction plan will be critical. Following the suggestions of this resource bulletin should provide courts with a roadmap toward developing a plan that will ensure appropriate access to court records is maintained well into the future.

Reference

Emerging Models

In 2002 the Research Libraries Group (RLG) defined the concept of a trusted digital repository as an institution created to ensure long-term access to digital resources.²² As the most basic level a repository must maintain digital resources

²² RLG/OCLC Working Group on Digital Archive Attributes. *Trusted Digital Repositories: Attributes and Responsibilities*. Rep. Research Libraries Group, May 2002. Web. 7 Nov. 2014.

over the long term in a consistent manner, meet or exceed standards for access, management and security, and be audited for performance and quality management. The concept has continued to evolve with the development of various models and related standards.²³ These models are described further in the following sections.

Open Archival Information System Reference Model

The Open Archival Information System (OAIS) reference model has become the de facto standard for evaluating digital repositories. In addition to the reference model, other tools have been recently developed as guides for assessing the readiness of an organization to preserve digital materials. The following schematic gives a high-level view of the OAIS model and its components:²⁴



Figure 5: OAIS Model

Ingest: The steps required to transfer items from their current location into the archive in a managed manner.

Archival Storage: The storage of the bulk data (usually files) based on standard storage management tools.

Data Management: Tools to manage archival storage, including metadata.

Administration: Tools for system administration and access.

Access: Tools to search, browse and download content.

²³ Brown, Adrian, Shadrack Katuu, Peter Sebina, Anthea Seles, and International Records Management Trust. "Training in Electronic Records Management, Module 4: Preserving Electronic Records." 2009. Web. 7 Nov. 2014.

²⁴ Tilbury, Jonathan. *The Active Preservation of Digital Information* (July 2013). Web. 8 Nov. 2014.

Preservation Planning: Overall management to ensure long term access.

In addition to these fundamental characteristics, an OAIS-compliant repository should employ best practices in all areas, including:

- Standards for metadata encoding, management and records description
- Proper environmental controls for storage
- Timely and appropriate backups
- Emergency recovery, business continuity and contingency planning, and risk mitigation activities
- Adequate security features, including hierarchical password access, audit trails, firewalls, virus protection and encryption

The OAIS Reference Model has been adopted by the International Organization for Standardization as ISO 14721. Additional standards have been developed, such as ISO 16363, specify auditing criteria for certifying a trustworthy repository.

Digital Preservation Capability Preservation Model

Building on the trustworthy repository concept, authors Lori Ashley and Charles Dollar developed the Digital Preservation Capability Maturity Model.²⁵ This model is designed to provide a high level analysis of organizational capability for long-term digital preservation. Based on the Capability Maturity Model developed by the Software Engineering Institute of Carnegie Mellon University, the DPCMM defines seven components that are critical to a sustained effort to preserve electronic records:

- Digital preservation policy
- Digital preservation strategy
- Governance
- Collaboration
- Technical expertise
- Open standard/technology neutral formats
- Designated community

The model further defines eight components that are required to sustain an electronic record repository. The model includes five levels of capability or maturity as a metric to assess current program capability, identify gaps, and

²⁵ Dollar, Charles M., and Lori J. Ashley. "[Assessing Digital Preservation Capability Using a Maturity Model Process Improvement Approach](#)." Feb. 2013. Web. 7 Nov. 2014.

create a roadmap to achieve a higher level of organizational competency. The maturity model was updated in April 2014.

Levels of Digital Preservation Framework

The National Digital Stewardship Alliance (NDSA) has also developed a set of recommendations to guide organizations in the development of digital preservation systems and activities. NDSA is described as a group of “over 140 organizations whose mission is to establish, maintain, and advance the capacity to preserve our nation’s digital resources for the benefit of present and future generations.”²⁶

The Levels of Digital Preservation framework defines five functional areas required for effective digital preservation:

1. Storage and geographic location
2. File fixity and data integrity
3. Information security
4. Metadata
5. File formats

Similar to the DPCMM, the Levels of Digital Preservation framework includes four tiers or levels of compliance in each of these areas, with the goal of providing a tool to evaluate capacity to mitigate risk of information loss and identify technical steps that can be taken to improve preservation.

Applicable Standards

The following are examples of records management standards that have application to records preservation. This list is by no means exhaustive and it should be noted that standards are being continually updated with the emergence of new technologies and best practices.²⁷

Digital Document Management

ISO 19005-1:2005 *Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)* – specifies how to

²⁶ Phillips, Meg, Jefferson Bailey, Andrea Goethals, and Trevor Owens. *The NDSA Levels of Digital Preservation: An Explanation and Uses*. Working paper. Library of Congress, NSDA Infrastructure Working Group, n.d. Web. 05 Nov. 2014.

²⁷ Jones, Virginia, “Standards for Establishing Records and Information Management Programs,” *Information Management*, July – August 2012, p.38.

use the portable document format (PDF) 1.4 for long-term preservation of electronic documents.

NIST SP 500-252 *Care and Handling of CDs and DVDs – A Guide for Librarians and Archivists* – provides guidance on how to maximize the lifetime and usefulness of optical discs, specifically CD and DVD media, by minimizing chances of information loss caused by environmental influences or physical handling.²⁸

ISO 13008:2012 *Information and documentation – Digital records conversion and migration process* –provides guidance in understanding recordkeeping requirements, the organizational and business framework for conducting the conversion and migration process, technology planning issues, and monitoring/controls for the process. [Supersedes ANSI/ARMA 16-2007 *The Digital Records Conversion Process*.]

ISO/TR 13028:2010 *Information and documentation – Implementation guidelines for digitization of records* –establishes guidelines for creating and maintaining records in digital format only and establishes best practice guidelines for digitization to ensure the trustworthiness and reliability of records.

ISO/TR 15801:2009 *Document management – Information stored electronically – Recommendations for trustworthiness and reliability* – describes the implementation and operation of document management systems that can be considered to store electronic information in a trustworthy and reliable manner.

Indexing and Metadata

Controlled Language in Records and Information Management (ARMA International) – describes what controlled language is and how it benefits organizations by reducing search time and increasing the reliability of search results, improving organizational communication, avoiding duplication, and reducing corporate risk exposure in legal and other discovery processes.

ISO 23081-1:2006 *Information and documentation – Records management processes – Metadata for records – Part 1: Principles* – covers the principles that underpin and govern records management metadata.

²⁸ Byers, Fred R., and Chris Keithley. *Care and Handling of CDs and DVDs — A Guide for Librarians and Archivists*. Washington, CD: US Dept. of Commerce, 2003. NIST Information Technology Laboratory. National Institute of Standards and Technology and Council on Library and Information Resources, Oct. 2003. Web. 17 Nov. 2014. NIST Special Publication 500-252

ISO 23081-2:2009 *Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues* – establishes a framework for defining metadata elements consistent with the principles and implementation considerations outlined in ISO 23081-1:2006.

Facilities and Storage

ARMA TR01-2011 *Records Center Operations, 3rd Ed.* – assists organizations with selecting an appropriate records center site and designing, equipping, staffing, operating, and managing a records center. Additional sections discuss vaults, security, records center software, and commercial records storage facilities.

Guideline for Evaluating Offsite Records Storage Facilities (ARMA International) – assists organizations with evaluating storage needs, determining whether business practices make outsourcing the best decision, and assessing the ability of vendors to meet storage requirements.

Guideline for Outsourcing Electronic Records Storage and Disposition (ARMA International) – provides information to assist organizations in making decisions about outsourcing electronic records storage, retrieval, disposition to third-party providers and evaluating and selecting a service provider.

Guideline for Outsourcing Electronic Records Storage to the Cloud (ARMA International) – addresses information management issues related to cloud-based records storage, including benefits and risks of using cloud-based records storage, how to mitigate legal risks, issues related to retention, disposition, privacy, and security, standards and best practices, and vendor selection.

Vital Records and Risk Mitigation

ANSI/ARMA 5-2010 *Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records* – sets the requirements for establishing a vital records program including requirements for: identifying and protecting vital records, assessing and analyzing their vulnerability, and determining the impact of their loss on the organization.

Guideline for Evaluating and Mitigating Records and Information Risks (ARMA International) – provides a framework for establishing systems to evaluate information risks and describes a process for framing a risk management system using a risk quadrant of administrative risks, records control risks, legal/regulatory risks, and technology risks.

ISO/IEC 27002: 2005 *Information Technology – Security techniques – Code of Practice for Information Security* – establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. It outlines objectives that provide general guidance on the commonly accepted goals of information security management. *[Formerly ISO 17799:2005.]*

Assessing Digital Preservation Capability Using a Maturity Model Process Improvement Approach

Charles M. Dollar and Lori J. Ashley

April 2014

Abstract

The public and private sector have recognized over the last decade that the systematic management of their digital assets requires implementing a program that ensures on-going access to authentic, usable digital records that have long-term¹ operational, regulatory, legal, or cultural memory value. The Open Archival Information System (OAIS) Reference Model (ISO 14721) identifies high level services and requirements that a trustworthy repository should provide to support long-term access. Additional standards (i.e., ISO 16363) specify auditing criteria for the certification of trustworthy repositories. Both standards are notable contributions to the emerging field of digital preservation but they have several implementation limitations.

In this paper we introduce a Capability Maturity Model (CMM) that organizes the digital preservation requirements of the ISO Standards into fifteen components with metrics to assess maturity. The model is a tool for charting the evolution from disorganized and undisciplined management of electronic records, or the lack of a systematic digital continuity approach, into increasingly mature stages of digital preservation capability.

The goal of our Digital Preservation Capability Maturity Model (DPCMM)© is twofold:

1. To help practitioners identify at a high level the capabilities of their organization relative to optimal digital preservation capabilities; report gaps, capability levels, and preservation performance metrics to resource allocators and other stakeholders; establish priorities for achieving enhanced capabilities to preserve and ensure access to long-term electronic records; and
2. To focus attention on digital continuity as a discipline for proactively addressing digital preservation issues at or near the time of the capture or creation of electronic records of long-term value.

What Is A Capability Maturity Model?

The Software Engineering Institute of Carnegie Mellon University released the Capability Maturity Model for Software (CMM or SW-CMM) in 1990. The CMM was developed to enable organizations to assess the maturity of their software development processes and identify key practices necessary to improve the capability of those processes.² The CMM defines five progressive stages of process maturity³ based on an organization's support for certain key software development areas that are described generally as Initial, Repeatable, Defined, Managed, and Optimized. Each stage includes a series of associated activities and baseline metrics used to measure performance. These maturity stages are cumulative: an organization achieving a higher stage of maturity must implement and sustain all of the requirements for that stage in addition to requirements for all of the lower stages. This capability maturity model has been adapted for human resources,⁴ system engineering,⁵ software acquisition,⁶ technology investment,⁷ enterprise architecture,⁸ and records management,⁹ among others disciplines.¹⁰

Why A Digital Preservation Capability Maturity Model?

The Open Archival Information System (OAIS) Reference Model (ISO 14721) identifies high level services and requirements that an archive should provide to support long-term access. An additional standard (i.e., ISO 16363) specifies auditing criteria for the certification of trustworthy repositories. Both standards are notable contributions to the emerging field of digital preservation but they have several implementation limitations. The objective of ISO 14721 is to serve as a reference model. The OAIS defines digital preservation services and associated activities at a very high level. OAIS services and activities must be deconstructed into terms that are readily understood and can be applied in operational archival environments. In contrast, the audit criteria certification checklist of ISO 16363 includes more than one hundred requirements, and conducting an audit presumes an external audit team is on site and authorized to certify the repository. An audit typically involves months of preparation to acquire and organize documentation. More importantly, neither standard identifies explicit performance metrics to assess the current digital preservation capabilities of repositories (digital archives) or information systems that may act as surrogate trustworthy repositories. Both standards imply a "one size fits all" approach to ensuring long-term access to authentic electronic records. Finally, neither standard explicitly supports an incremental digital preservation capability improvement plan.

The Digital Preservation Capability Maturity Model (DPCMM)¹¹ presented in this paper draws upon the overall framework of the CMM development model but is not intended to be a rigorous model with precisely defined parameters. The DPCMM is a systematic tool to chart the evolution from a disorganized and undisciplined electronic records management program, or one that does not exist, into increasingly mature stages of digital preservation capability. The DPCMM is designed to help identify, protect and provide access to long-term and permanent digital assets. The goal of the DPCMM is to support the management of a digital preservation program that:

- Identifies and monitors at a high level where the program is in relation to an optimal digital preservation program;
- Establishes priorities and an improvement roadmap to achieve enhanced digital preservation capabilities over time;
- Reports digital preservation capability gaps and achievements to resource allocators and stakeholders.

Stages of Digital Preservation Capability Maturity

The Digital Preservation Capability Maturity Model displayed in Figure 1 has five stages that track closely with the five stages of the CMM discussed earlier, albeit with a specific digital preservation emphasis.

Stage 1: (Nominal) a systematic digital preservation program has not been undertaken and **most, if not all, electronic records that merit long-term retention are at risk.**

Stage 2: (Minimal) digital preservation capabilities are rudimentary and do not rise to the level of ISO 14721/ISO 16363 specifications. **Consequently, most electronic records that merit long-term retention are at risk.**

Stage 3: (Intermediate) the organization supports ad hoc initiatives and projects that approach but do not conform fully to ISO 14721/ISO 16363 specifications. There is an established basis for proactive and sustainable digital preservation improvement actions over time. **Nevertheless, it is likely that some electronic records that merit long term retention remain at risk.**

Stage 4: (Advanced) the organization has a robust infrastructure and the preservation of electronic records is undertaken with a governance and operational framework that conforms to most of the ISO 14721 specifications and the criteria of ISO 16363. **Few electronic records that merit long-term preservation are at risk.**

Stage 5: (Optimal) represents the highest level of sustainable conforming ISO 14721/ISO 16363 digital preservation capability and repository “trustworthiness” that an organization can achieve. **No records that merit long-term retention are at risk.**

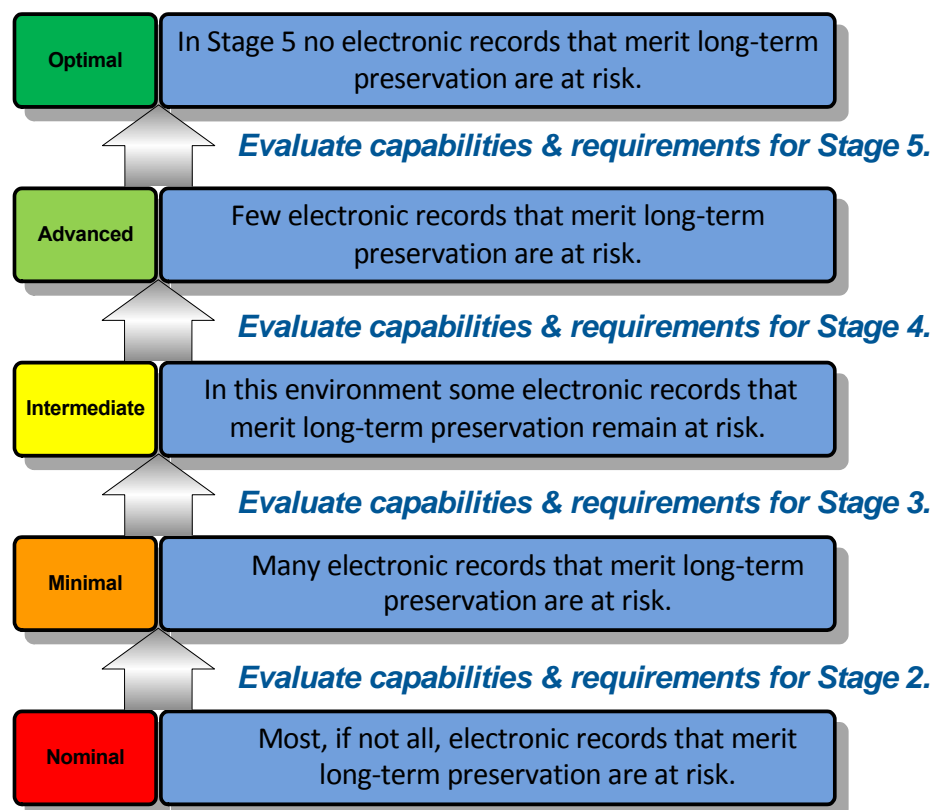


Figure 1. Stages of Digital Preservation Capability Maturity

Digital Preservation Capability Maturity Model Components

The Digital Preservation Capability Maturity Model (DPCMM) consists of three interdependent domains: infrastructure, one or more digital preservation repositories, and services. Figure 2 displays the fifteen components of the DPCMM and their relationship to the top level domains.

These components of the DPCMM are an amalgamation of key specifications, requirements, and activities abstracted from ISO 14721 and 16363 standards and digital preservation “best practices”.¹² Two major stakeholder groups – records producers (or donors) and users who seek access to the contents of the digital repository - also appear in the model.

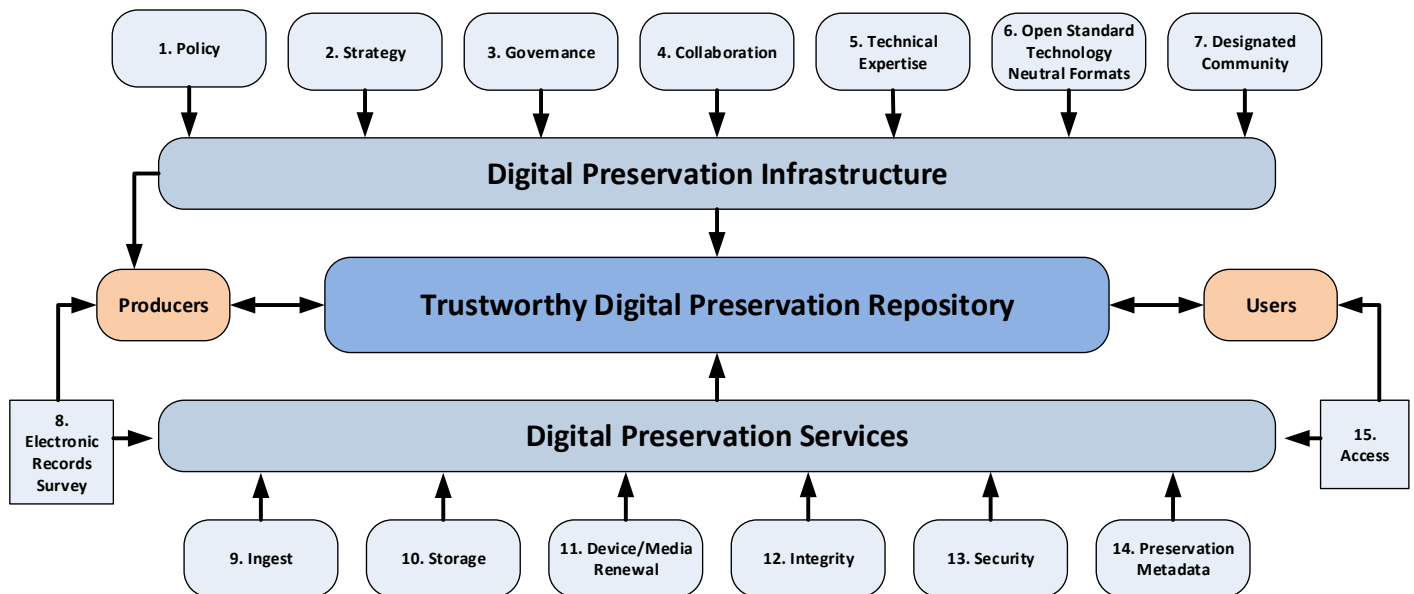


Figure 2. Digital Preservation Capability Maturity Model©

Digital Preservation Infrastructure features seven (7) components that are essential to ensuring sustained organizational commitment including, human, technical and financial resources, to the long-term preservation of electronic records that are created, received or acquired by the organization. The Digital Preservation Infrastructure components are:

- Digital Preservation Policy
- Digital Preservation Strategy
- Governance
- Collaboration
- Technical Expertise
- Open Standard Technology Neutral (“OS/TN”) Formats
- Designated Community

Digital Preservation Services include eight (8) components that are required for continuous monitoring of external and internal environments to plan and take necessary preservation actions that sustain the integrity, security, usability and accessibility of electronic records stored in repositories. The Digital Preservation Services are:

- Electronic Records Survey
- Ingest
- Archival Storage
- Media/Device Renewal
- Integrity
- Security
- Preservation Metadata
- Access

The DPCMM describes the scope and focus of each of the fifteen components. The Electronic Records Survey component (*below*) is a critical interface between Records Producers, the repository, and the Digital Services domain. An Electronic Records Survey addresses the need for an informed estimate of the volume, file formats, and types (e.g., images, text, and databases) of digital content that will be transferred to the digital repository or safeguarded by record producers in their own technology environments. The Electronic Records Survey component is also dedicated to mitigating technological obsolescence at the time of records transfer to the repository. Practitioners are encouraged to engage records producers to capture preservation-ready electronic records at or near the time of their creation or receipt. Below is the DPCMM description of the Electronic Records Survey component.

DPCMM COMPONENT 8: Electronic Records Survey

Each organization is responsible for records created, received or acquired that are evidence of its business activities, regardless of the format or media used. The records' authenticity, integrity, usability and reliability must be ensured for as long as they are required. Records with long-term retention requirements or archival (permanent) value are often transferred to the custody of a centralized Records Management and/or Archives function for preservation.

Due to the fragility of electronic records, organizations are advised to proactively address digital preservation as close to the time of electronic records creation or capture as practicable. This can only be accomplished if the organization has a comprehensive inventory of electronic records as well as collaborative working relationships and agreements between stakeholders that include Records Producers, Legal/Compliance, Archives, Records Management, Information Technology/Services as well as third party application, solution and service providers.

A key feature of a conforming ISO 14721 open archival information system is the reliance on open standard interoperable technology neutral formats. During Ingest electronic records in proprietary formats must be transformed into formats that the organization and/or repository have adopted. Over time and with increasing volumes of electronic records, format transformation during the Ingest process may become burdensome. This obligation can be mitigated in part if "preservation-ready" records, that is, records that are in open standard interoperable technology neutral formats, are made at or near the time Records Producers create or capture the records.

The objective of an Electronic Records Survey is to identify three broad categories of records in order to support planning and preservation activities.

- **"Preservation-Ready"** electronic records;
- **"Near Preservation-Ready"** records, that is electronic records in formats for which tools are available that can export native format documents to open standard interoperable technology neutral formats.
- **"Legacy"** records, that is, electronic records in a proprietary native format for which no export or viewer technology tools exist. Transformation of proprietary native formats into open standard, interoperable, and technology neutral formats is likely to require writing code to support this transformation, which in turn is likely to be costly.

The collection and analysis of data for an Electronic Records Survey can be accomplished by a variety of means including: web enabled surveys of Record Producing units and service providers, interviews with selected business units or third parties that routinely create, receive or acquire electronic records, review of the organization's records retention and disposition schedules, analysis of the organization's information technology portfolio and strategic plan, as well as the use of "crawler" functionality to identify specific file formats currently used in the capture and storage of electronic records on network drives.

Digital Preservation Surrogates and Thresholds

ISO 14721 and ISO 16363 are the "gold standard" for digital preservation. While many organizations will strive to implement and sustain a conforming ISO 14721/16363 digital preservation environment, the reality is that some organizations cannot or choose not to implement a traditional standalone repository. Reliance on routine operational environments for long-term storage is the usual alternative to a standalone repository. Other organizations lack a sufficiently mature information infrastructure and architecture, and/or have such limited technical and financial resources, that in the short run they cannot aspire to implementing a conforming ISO 14721/ISO 16363 digital preservation repository.

In the meantime some organizations have accessioned "born digital" or scanned digital images through manual or semi-automated workflows. Others are addressing some digital preservation requirements with tools and services such as Contentdm®, Archivelt, BagIt, LOCKSS, and DSpace. In the public sector, grant-based projects and state-level collaboration in federally funded database and email archiving projects has been underway for years. These tools, services and projects are noteworthy despite not being in full conformance with ISO 14721 specifications. They are substantive and represent important emerging capabilities and market recognition of digital preservation requirements and standards. A handful of organizations is currently building or are testing digital repository technologies that are likely to conform to the ISO 14721/ISO 16363 specifications.

The DPCMM takes into account this spectrum of digital preservation surrogates by distinguishing between ISO 14721 conforming and partially-conforming capabilities and services by incorporating two concepts: 1) surrogate digital repositories, and 2) digital preservation thresholds. A surrogate digital repository as defined by the DPCMM refers to a range of services, tools, projects and initiatives currently used to address digital preservation requirements that are substantive and represent evolving/emerging capabilities.

A surrogate digital repository may not fully or even explicitly comply with ISO 14721/16363 specifications. The DPCMM maps threshold statements to Stage 1 and Stage 2 performance metrics for each of the fifteen components to assist practitioners and other stakeholders to understand and apply these concepts.

Digital Preservation Performance Metrics

The five incremental maturity levels described previously comprise performance metrics for each component of the Digital Preservation Capability Maturity Model. The performance metrics of each Digital Preservation component constitute a checklist that is used to conduct a self-assessment of an organization's current digital preservation capability vis-a-vis that of an optimal capability. They also serve to raise awareness and educate stakeholders about current and evolving operational digital preservation practices, technology solutions, and standards.

Performance metrics for the Electronic Records Survey Component are provided below.

Level	Capability Description
0	The organization has little or no capability or resources to collect and analyze information about the volume, location, media, format types, and life cycle management requirements for electronic records.
1	The organization relies on existing retention schedules to identify electronic records of permanent historical, fiscal, and legal value in the custody of Records Producing units. It may also conduct ad hoc, one-time interviews and surveys to identify other electronic records of permanent historical, fiscal, and legal value.
2	The organization uses systematic interviews, surveys, and retrospective analysis of existing retention schedules to identify electronic records of permanent historical, fiscal, and legal value in the custody of selected records producing units. This may be enhanced by focusing on identifying “at risk” electronic records in the custody of selected Records Producing units.
3	The organization supplements analysis of “at risk” electronic records through collection of information about the volume and location (e.g., shared drives, databases, applications), media and format types of electronic records of long-term and permanent historical, fiscal and legal value in the custody of Records Producing units. The organization has identified preservation-ready and non preservation-ready electronic records in the custody of most records producing units.
4	The organization has identified preservation-ready and non preservation-ready permanent electronic records in the custody of all Records Producing units. It uses this information along with other information collected from Records Producing units to systematically manage the transfer and ingest of electronic records.

Figure 3. Electronic Records Survey Component – Performance Metrics

Digital Preservation Capability Assessment

Each of the 75 capability statements in the Digital Preservation Capability Maturity Model has an integer value ranging from 0 to 4. Using the previously described Electronic Records Survey component as an example, an organization that relies solely on its record retention schedules to identify long-term and permanent records to be transferred to their digital preservation repository would yield a score of “1.” This score becomes the **index value** for the organization’s current Electronic Records Survey capability. Performing this assessment for all of the 15 components of the DPCMM produces an Aggregated Digital Preservation Capability Index Score that is mapped to the appropriate level of digital preservation capability.

<i>Capability Level</i>	<i>Index Score</i>
Nominal	0
Minimal	Between 1 and 15
Intermediate	Between 16 and 30
Advanced	Between 31 and 45
Optimum	Between 46 and 60

Table 1. Digital Preservation Capability Level Assessment

Both the Digital Preservation Index score for each component as well as the Aggregated Digital Preservation Capability Index Score function as a high level assessment. An organization can use the assessment results to measure its status against peer organizations as well as to develop a roadmap for incremental capability improvement. The improvement roadmap should take into account available resources and on-going initiatives and may help mitigate near-term risk exposure on some, but not all, of the components. This is an important consideration in designing an incremental digital preservation plan that is suited to the mission and designated communities of stakeholders. It is likely that constrained resources will require the prioritization of some components where significant improvement may be achieved while other components by default may undergo little improvement for the foreseeable future.

Interestingly, use of the DPCMM gap analysis checklist/performance metrics methodology thus far by the authors has raised individual and organizational awareness of the importance of digital preservation, identified interdependencies between and among various stakeholders, and sparked debate and dialogue. The assessment raises issues about the desired future state of an organization’s digital preservation capabilities and the level of risk its leadership is willing to take on.

In many instances, this is likely to come down to the question of what constitutes digital preservation that is “good enough” to fulfill the organization’s mission and meet the expectations of its stakeholders within its constrained resources. This is a critical issue that the digital preservation community and those who depend on access to long-term electronic records and cultural resources need to confront.

Case Study: Council of State Archivists

In July 2011, the Council of State Archivists¹³ (“CoSA”) launched an initiative focused on improving efforts to manage, preserve, and provide access to U.S. state government electronic records nationwide. The goal of Phase 1 of the State Electronic Records Initiative (SERI) was to create a profile of electronic records programs in order to develop an action plan that addresses the needs of state archives and records management programs and identifies next steps.

CoSA compiled information on electronic records management and digital preservation programs as part of the SERI Phase 1 initiative. Responses to questions and transcripts from phone interviews with the directors and electronic records staff were collected from 55 state and territorial archives. CoSA invited Charles Dollar and Lori Ashley, the developers of the DPCMM, to analyze the survey results and map the findings to the fifteen (15) components of the model. In addition to providing a composite “score” on the readiness of each state and territory archives to preserve long-term and permanent electronic records, the analysis highlighted current good practices as well as enormous gaps. The consultant report stated that “Almost one-half (21) of the responding states/territories (48) registered an absolute Nominal digital preservation capability index score on each of the fifteen key process areas.”¹⁴ In November 2011, Julia Marks Young, the President of CoSA, included excerpts from this analysis at a meeting of the National Historical Publications and Records Commission.

Subsequently in 2012, the Institute of Museums and Library Services (IMLS) awarded CoSA a three-year \$500,000 grant to identify training needs and priorities for state archives, organize and conduct training programs, and to benchmark the effectiveness of the program. The program called for each state archives to take a self-assessment survey and establish a base-line digital preservation capability score. At the end of the grant program each state archives will take the self-assessment survey again and thereby document its improved digital preservation capabilities.

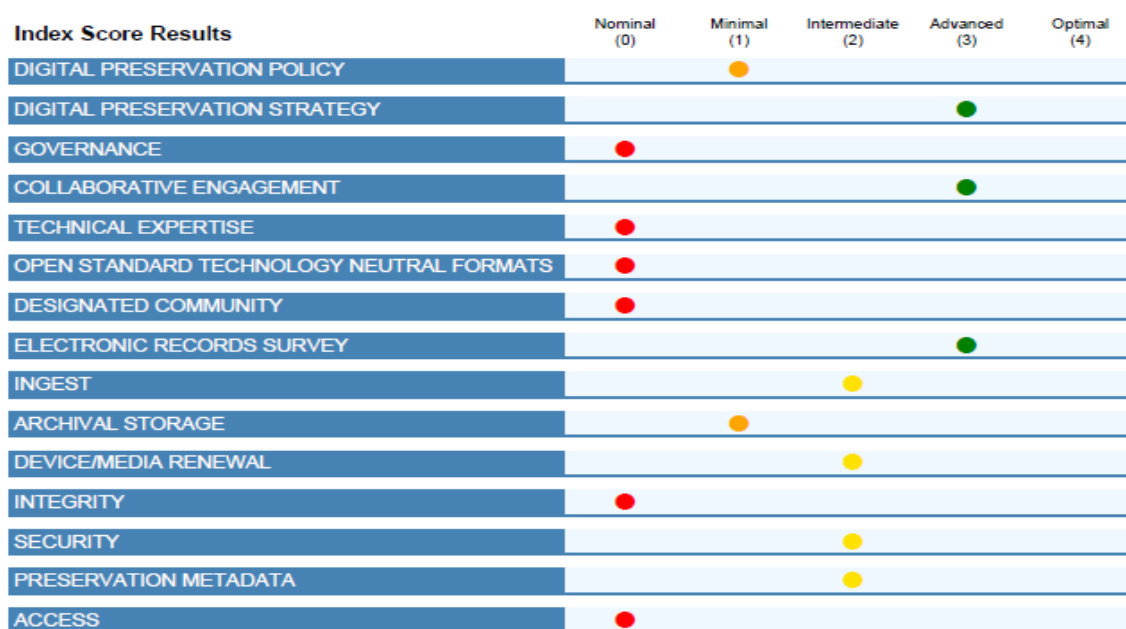


Figure 4. Aggregated Digital Preservation Index Score for a U.S. State Archives

Figure 4 is the baseline digital preservation capability scorecard of one of the state institutions that participated in the June 2012 CoSA Digital Preservation Capability self-assessment survey. The Aggregated Digital Preservation Index Score of 19 places this State Archives in the lower range of Minimal Digital Preservation Capability, which means that most of the electronic records that merit long term retention are at risk.

Conclusions and Outlook

The key strengths of the Digital Preservation Capability Maturity Model (DPCMM)© - mapping of the specifications and requirements of ISO 14721 and ISO 16363 to fifteen components and the identification of incremental levels of digital preservation capability with explicit performance criteria - appear to be gaining traction within sectors of the digital preservation community. The authors of this white paper applied DPCMM to develop a five year digital preservation strategy and improvement road map for the City of Toronto (2010 – 2011). DPCMM was also used to identify the components of a digital preservation policy framework for the Kansas State Historical Society (2011–12) and to develop a digital preservation policy and a five year capability improvement roadmap for the Wyoming State Archives (2012-13). Currently they are engaged in content expert support for a mobile application, Mobile Archives Standardization Tool (MAST), which is being developed by the Section of International Organizations (SIO) of the International Council on Archives (ICA). MAST adapts DPCMM performance metrics to the needs and requirements of this international community and the capabilities of mobile technology.

DPCMM is a part of savingthedigitalworld.com, a website dedicated to fostering communication and collaboration among practitioners who are working to address long-term digital continuity and preservation challenges. Additional background information about the DPCMM, updated metrics, and additional case studies will be published on this site and on www.securelyrooted.com in summer 2014.

Founding members¹⁵ of savingthedigitalworld.com hope that it will become a resource for individuals and organizations interested in understanding digital preservation issues and learning from the experience of others. In addition, the founders hope that the site will become a forum for on-going dialogue about the opportunities for and impediments to ensuring long-term access to digital content that has legal, regulatory, business, and cultural memory value.

Acknowledgements

The genesis of this Digital Preservation Capability Maturity Model Methodology is rooted in a presentation given to the Arizona Digital Records Management Task Force in 2002. Introduction to the potential use of a digital records management capability maturity model by Timothy Sprehe led to significant enhancements. The Digital Preservation Capability Maturity Model performance metrics presented in this paper were inspired in part by material developed by the International Records Management Trust to support an assessment of an organization's readiness to undertake a digital records management program. The first use of DPCMM was in a 2007 project at the State of Delaware Public Archives. The DPCMM Methodology has undergone significant enrichment since its first formal use, the most notable being the decision of the Council of State Archivists (CoSA) to support adaptation

of the model to a web-based digital preservation capability survey for fifty-six state and territorial archives.

Gary Miller (Wind Lake Solutions), Richard Pearce-Moses (Clayton State University), Milovan Mistic (World Intellectual Property Organization) and Ton Bezemer (Anth.P.Bezemer LLM, The Netherlands) provided valuable commentary on the DPCMM and during development of the CoSA Digital Preservation Capability Self-Assessment. We are grateful to Milovan Mistic, President of the ICA Section of International Organizations, for his interest and skill in adapting the DPCMM framework to mobile technology.

Notes

¹ Long-term is a period of time long enough for there to be concern about the impacts of changing technologies on information held in a digital repository. This can be as short as five to seven years and extends indefinitely. In this document long-term is assumed to be 10 years or more (10+ years).

² In 2002 the Software Engineering Institute replaced CMM with a new product, Capability Maturity Model Integrated (CMMI), and discontinued support of CMM. CMMI is a robust but generic business process improvement model.

³ A good source for a description of the CMM is Mark C. Paulk, et al, "The Capability Maturity Model: A Summary," which can be accessed through the Carnegie Mello Research Showcase at <http://repository.cmu.edu>

⁴ <http://www.sei.cmu.edu/reports/01mm001.pdf>

⁵ <http://www.sei.cmu.edu/reports/96hb004.pdf>

⁶ <http://www.sei.cmu.edu/library/abstracts/reports/02tr010.cfm>

⁷ U.S. General Accounting Office, Information Technology Investment Management: A Framework for Assess and Improving Processing Maturity, GAO-04-394Gm 2004). Available at <http://www.gao.gov/new.items/d04394g.pdf>.

⁸ U.S. General Accounting Office, Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management, Ver. 1.1, GAO-03-584G (2003).

⁹ See Timothy Sprehe and Charles McClure, "Study of Exemplary Practices in Electronic Records Management" (General Accounting Office, May 2003) and Karen Strong, "What's Your ECRM Number?" (Managing Electronic Records Conference, Chicago, May 21, 2007). Also see Christopher Becker, et al, "Assessing Digital Preservation Capabilities Using a Checklist Assessment Method," iPRES 2012, October 1 - 5, Toronto, Canada. Available at <https://ipres.ischool.utoronto.ca>

¹⁰ Tessella published a brief Digital Archiving Maturity Model White Paper. Available at <http://www.digital-preservation.com/wp-content/uploads/Maturity-Model-Web.pdf>.

¹¹ The genesis of this Digital Preservation Capability Maturity Model is rooted in a presentation given to the Arizona Electronic Records Management Task Force in 2002. The actual Digital Preservation Readiness Capability Maturity Model presented here was inspired in part by material developed by the International Records Management Trust to support assessment of the readiness of an organization to undertake an electronic records management program.

¹² Based on a 2010 review by the authors of the digital preservation practices of fifteen national, state and provincial-level programs.

¹³ The Council of State Archivists (www.statearchivists.com) is a national organization comprising the individuals who serve as directors of the principal archival agencies in each state and territorial government. Under regulations of the National Historical Publications and Records Commission, these individuals also serve as the State Historical Records Coordinators who chair their respective State Historical Records Advisory Boards (SHRABs).

¹⁴ CoSA SERI Phase 1, Mapping of Survey Results to the Digital Preservation Capability Maturity Model – Findings and Recommendations, Charles M. Dollar and Lori J. Ashley, September 2011, page 4.

¹⁵ The founding members of www.savingthedigitalworld are Lori Ashley, Charles Dollar, Michael Peterson, Bob Rogers, and the late Don Post.

The Governance of Long-Term Digital Information

IGI 2016 BENCHMARK





TABLE OF CONTENTS

Benchmark Quick Takes: Five Key Insights	3		
Introduction	5		
About the Governance of Long-Term Digital Information: An IGI 2016 Benchmark	7		
IG Snapshot	9		
Preserving State History and Ensuring Citizen Access to Digital Government Records Using the Cloud	9		
Why Do We Need Long-Term Protection and Access?	11		
IG Snapshot	13		
A Practical Approach to Governing 170 Years of Critical Corporate Records	13		
What Technologies Are Organizations Using?	14		
The Awareness and Action Gap	15		
IG Snapshot	17		
		Future-Proofing Critical Digital Data in an Increasingly Complex Global Regulatory Environment	17
		Governing Long-Term Digital Information: Taking Action	19
		1. Triage	20
		2. Assess	20
		3. Address the Past, but Protect the Future	20
		4. Catalog Consequences	20
		5. Build Your Rules	20
		6. Assess the IT Environment	20
		Endnotes	21
		About this Publication	22
		About the Information Governance Initiative	22
		About Preservica	22

BENCHMARK QUICK TAKES: FIVE KEY INSIGHTS



“The critical role of digital . . . archives in ensuring the future accessibility of information with enduring value has taken a back seat to enhancing access to current and actively used materials. As a consequence, digital preservation remains largely experimental and replete with the risks . . . representing a time bomb that threatens the long-term viability of [digital archives].”

DIGITAL PRESERVATION: A TIME BOMB FOR DIGITAL LIBRARIES¹

- 1. We have a problem.** Virtually every organization surveyed (98 percent) has digital records and information it must keep (or wants to keep) for longer than ten years. Digital information asset protection and access over the long term is a universal problem for public and private organizations—both large and small—across a wide swath of verticals.
- 2. It is a technology problem.** Shared network drives are the most common repository for the storage of information ***we know must be protected and accessed for at least ten years*** (68 percent identified it as a storage location—the top response). Every day at the IGI, we are exposed to the maladies that afflict IG programs, but this result surprised even us. Shared network drives are the nicotine of IT infrastructure: easy to access, highly addictive, and incredibly dangerous over the long term. We should know better. There are many better alternatives that replicate the convenience of shared drives but radically improve governance. This addiction to shared drives must end, particularly for digital information we want or need to keep for longer than the next tech update cycle.
- 3. It is a business problem.** We see a tendency among business leaders to view the problem of long-term protection and access as an academic one or one owned by museums and national archives. This is demonstrably untrue. In fact, 86 percent of our survey respondents said they have responsibility for ensuring the protection and access for ***business records for longer than ten years***, not just archival or historical information. Further, the line between these categories is blurring, as you will see in our Snapshot on the Associated Press below.
- 4. It is a legal problem.** Legal requirements are by far the number one reason that organizations are keeping digital information for ten years or longer (89 percent said it was a driver, and it was the top category in our results). These statutory, regulatory, and other legal obligations are not theoretical nor are they going away. In fact, the trend is moving in exactly the opposite direction, toward greater regulation of information, broader retention, and more prescriptive and, in some cases, even longer retention periods. It is not unusual for a single multinational corporation to maintain a records retention schedule that incorporates over 8,000 individual legal recordkeeping requirements. One provider of legal information services maintains over 10,000 citations from over 30 countries globally. Moreover, these requirements are proliferating, with one provider estimating that its legal citation database grows by 6 percent or more annually.
- 5. We know what we must do, but are we doing it?** 97 percent of our survey respondents told us that they are *“aware that technology (hardware and software) obsolescence could mean that long-term digital records and information are at risk of not being readable or useable in the future.”* This is great news—awareness is very high. The bad news? The number one solution to this problem currently being undertaken by our industry: *“we are currently considering our approach.”* (44 percent) The second most common approach? *“We have no comprehensive strategy.”* (31 percent). Only 16% are actually transferring this critical long-term information to a standards-based digital preservation system. The contrast between awareness and action is disappointing, but not unexpected. We have identified some of the perceptual factors at work, but another factor has been that, until relatively recently, there has not been a practical and systemic way to tackle this problem.



THE GOVERNANCE OF LONG-TERM DIGITAL INFORMATION

IGI 2016 BENCHMARK

“We are moving into an era where much of what we know today, much of what is coded and written electronically, will be lost forever. We are, to my mind, living in the midst of digital Dark Ages . . .”

TERRY KUNY, “DIGITAL DARK AGES?”²

Introduction

Twenty years ago, a nonprofit representing hundreds of universities, national archives, museums, and other cultural institutions across the globe produced a landmark examination of the threat that digital transformation represented to our ability to capture, preserve, and provide access to our most important information. The report called for a global effort to design and develop “national information infrastructure to ensure that longevity of information is an explicit goal.”³

Today, no such global infrastructure exists. And, although significant progress has been made to address the challenge by industry bodies, individual institutions, and providers of digital preservation technology, the existential and commercial threat represented by our accelerating and deepening reliance on digital information has only grown exponentially in the intervening 20 years.

Archivists, historians, and librarians—among many others—have been sounding the alarm about an impending “digital dark age” and taking action to protect their digital information for decades.⁴ However, for most corporations and organizations not explicitly engaged in historical preservation, this threat largely seems to have been relegated to the domain of academic specialists perceived as isolated from the prosaic demands of everyday commerce. Compounding the problem is the obvious human inclination to simply ignore problems for which there seems to be no easy or immediate solution.

However, this concern is neither academic nor theoretical. In fact, it is a problem shared equally by historians, by anyone taking a digital photograph, and by all organizations, large and small, who have replaced paper with digital in their businesses. In short, it is a problem we all share.

In the specialized world of archives, this problem is known as “long-term digital preservation.” The word “preservation” is used here to denote a set of activities that go beyond simply storing a piece of information, but rather ensuring that the information remains accessible, trustworthy, secure, and authentic through its entire existence—even if that existence is forever.

A core part of our mission at the Information Governance Initiative (IGI) is to drive awareness and adoption of information governance (IG) as deeply as we can into the practices of public and private institutions around the globe. In fulfilling that mission, we are constantly seeking ways to “de-jargonize” information governance and its domains. In our experience, the term “preservation” is one of several that causes managers and executives to reflexively gaze down at their mobile devices and zone out until that part of the discussion is over. Further, it is our hope that this Benchmark will serve as an accessible introduction to the problem of long-term digital preservation for all audiences, not just those who already recognize it as a problem begging for a solution.

For this reason, throughout this Benchmark, we have adopted the phrase, “long-term protection and access.” This phrase not only fairly captures the primary concerns of this domain, but also puts the focus on activities that are most relatable and top-of-mind for the managers and executives, i.e., those people who ultimately have the greatest influence on our ability to solve this problem simply because they control the money. “Protection” resonates because there is clearly a heightened and growing awareness of the need to

invest in information security to confront the baseline threat that now exists in the digital world. “Access” is personally relatable to any executive who has been on the job for more than a few years and who has inevitably experienced the frustration (and fear) of not being able to locate and use an aging document vital to their job.

But, how long is “long-term?” At the IGI, we have yet to see a records retention schedule from a large organization that does not have several “PERMANENT” categories, even if those are just foundational corporate legal and financial documents. But even outside of this permanent category, most organizations have vast amounts of data that must be kept for periods longer than ten years (98 percent of them, in fact, as you will soon see).

This begs the question: in the digital world is there a material distinction between the need to keep something permanently and the need to keep something for at least ten years? We believe the answer is no. The inherent challenges of digital information (i.e., its ephemeral nature; proprietary data formats; proprietary software; software and hardware obsolescence; short-term thinking on IT architecture and infrastructure; storage media longevity; threats arising from complexity and volume; and so on) are essentially the same once you move out even a few years. For this reason, we have somewhat arbitrarily (but logically) chosen ten years as the practical equivalent to “very long” or even “permanent.” Further, our ability to imagine keeping information for eternity is roughly equivalent to our ability to imagine infinity, i.e., very poor and difficult to act upon.

The IGI and its Supporters like Preservica are dedicated to advancing our understanding of this problem and its solutions. We share a vision with Preservica that this is a solvable problem. And, as you will see throughout this Benchmark, in addition to sharing our quantitative research, this Benchmark also includes snapshot stories of organizations and their visionary IG leaders who have done just that. This combination of data and anecdote provides a powerful message that we hope will play even a small role in helping organizations fulfill their responsibility to protect and provide access to their most critical digital information over the long term. Today, there is no difference between the digital world and the “real world.” The time for short-term thinking is over. Let’s take action.



Barclay T. Blair
Executive Director and Founder
Information Governance Initiative

ABOUT THE GOVERNANCE OF LONG-TERM DIGITAL INFORMATION: AN IGI 2016 BENCHMARK



“We are nonchalantly throwing all of our data into what could become an information black hole without realizing it . . . documents or presentations that we’ve created may not be readable by the latest version of the software. So even if we accumulate vast archives of digital content, we may not actually know what it is.”

VINT CERF, INTERNET PIONEER: CHIEF INTERNET EVANGELIST AT GOOGLE: DISTINGUISHED VISITING SCIENTIST, NASA JET PROPULSION LABORATORY⁵

The Governance of Long-Term Digital Information:
An IGI 2016 Benchmark is based on quantitative, survey-based research conducted by the IGI in Spring 2016 that was distributed to our community of IG professionals. Nearly 400 professionals completed the survey in whole or in part. Respondents were a mix of both IG providers (i.e., people who work for organizations that provide IG products and/or services) and IG practitioners (people charged with doing IG at and for the organization where they work).

Because we believe this data to be the most insightful and revelatory of current industry perceptions, throughout this Benchmark we have chosen to primarily report on data drawn exclusively from IG practitioners who completed the entire survey, a population of 196.

About two-thirds of respondents in that population were from the USA, with the remainder split nearly evenly between Canada, the UK, and a group of other nations. By vertical, survey respondents were diverse, with about a quarter from Government and Military, 15% from Financial Services, and the majority of the rest from Legal, Healthcare, Utilities, Education, Manufacturing, and Pharma (ranked in descending order).

Organizations, both large and small, were also well represented, with about a third from large organizations (i.e., 5,001 or more), a third from mid-sized organizations (i.e., 501-5,000), and a third from small organizations (i.e., from 1-500 employees).



The majority of respondents identified their primary IG role as records and information management, which is in line with our expectations given the focus of the Benchmark. There was also strong representation from respondents focused on electronic discovery, data governance, legal, compliance, risk management, IT management, privacy, information security, and business management (in descending order).

In summary, we were very pleased with the survey response rates and diversity. We believe this data provides a very strong and deep insight into current attitudes and activities from practitioners who are well qualified to represent their organizations’ attitudes and activities regarding long-term protection and access.

Preserving State History and Ensuring Citizen Access to Digital Government Records Using the Cloud

“Most records today are born digital. As the official archive of state government we need to retain many of these records permanently. To meet this challenge we invested in expanding and enhancing our digital preservation capabilities, which was a significant undertaking. I’m confident that our approach will ensure that these essential government records remain accessible long into the future.”

JELAIN CHUBB, TEXAS STATE ARCHIVIST

The Texas State Library and Archives Commission (TSLAC) is taking action to ensure that critical digital records are properly governed and preserved in fulfillment of its mission to “safeguard government and historically significant records and to provide information services to support research, education, and individual achievement.”⁶

TSLAC, with over 160 employees, was established in 1909. It supports a state government that has an annual budget of over \$200 billion and employs more than 200,000 people.⁷ Texas, if it were a country, would have the world’s 12th largest economy.⁸ TSLAC faces a massive ongoing deluge of digital information that must be governed and preserved in accordance with its legal obligations and agency mission.

One recent challenge for TSLAC was taking ownership of over 7 terabytes of digital records created by an outgoing gubernatorial administration which consisted of policy documents, press releases, and correspondence in a number of different file types (including digitized audio, still images, and video). On top of this, TSLAC had already created 26 terabytes of digital surrogates that required management and long-term preservation. In addition to preserving this information, TSLAC’s mandate includes ensuring that both government users and the public at large have ready and secure access to records in its custody (as required by law). TSLAC also faces budgetary constraints and the pressure “to do more with less,” just like many other organizations in both the public and private sectors.

To address its governance, access, and cost requirements, TSLAC developed a set of clear system requirements that it used to evaluate and select the tools and systems it needed.

Critical evaluative criteria for TSLAC included:

- **Cloud delivery.** TSLAC had concluded that cloud delivery was the best fit for the organization given the potential for lower acquisition, operational costs, and maintenance costs.
- **Support for standards.** Support for relevant standards such as the Open Archival Information System (OAIS) reference model (ISO 14721).
- **Migration.** Automated migration of records into new file types for long-term preservation to fulfill its mandate to ensure access for the entire life of the record (and in some cases, forever).
- **Integration.** Ability to function alongside and integrate with existing content and records systems.
- **Sector-specific expertise.** TSLAC concluded that it was important to select a provider with demonstrable understanding of unique governmental requirements.
- **Secure and reliable cloud infrastructure.** In particular, TSLAC was drawn to the AWS GovCloud, which was designed to support governmental use cases and requirements including, for example, encryption of records both in transit and at rest.

To meet these requirements, TSLAC selected and deployed a cloud-based solution from IGI Supporter Preservica. Preservica’s service now also powers the recently launched Texas Digital Archive, which provides access to the publicly available electronic records collections of the TSLAC.

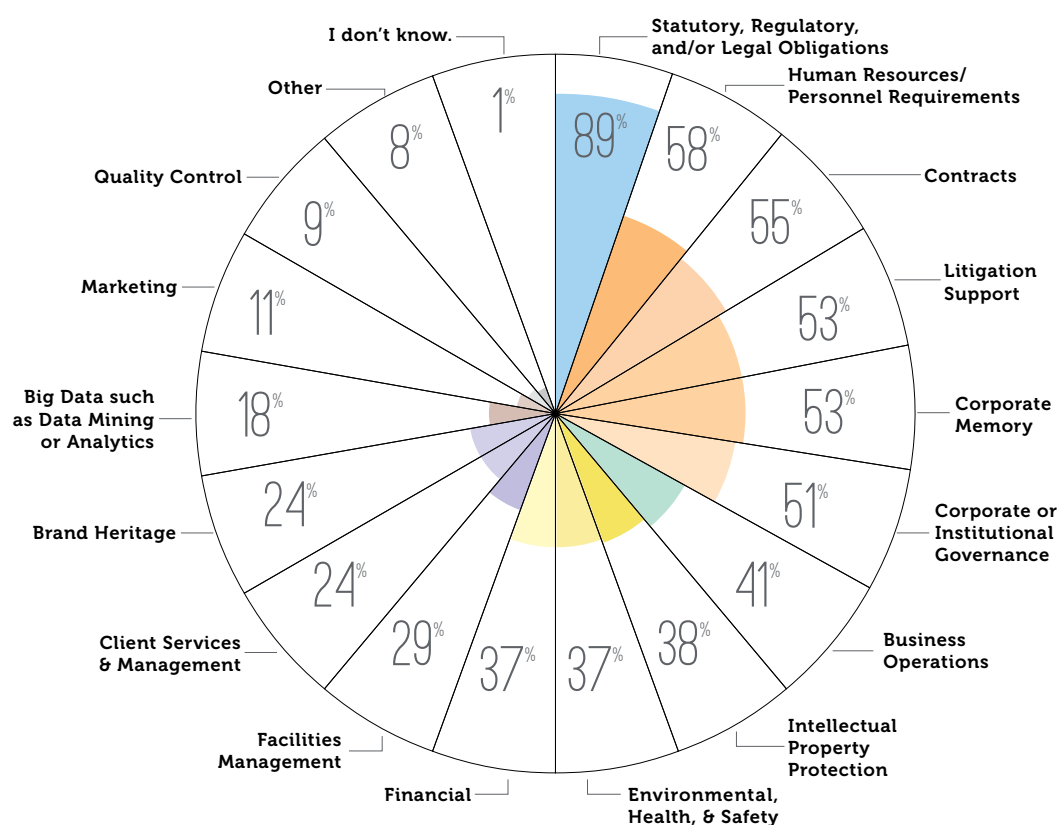


DEEPER ANALYSIS

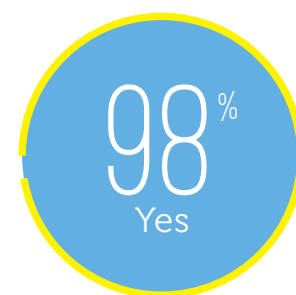
WHY DO WE NEED LONG-TERM PROTECTION AND ACCESS?

MOST ORGANIZATIONS HAVE DIGITAL RECORDS AND INFORMATION THEY KEEP LONG TERM BECAUSE OF THEIR IMPORTANCE

Organizations Report a Variety of Reasons Why They Keep Digital Information



The vast majority of practitioners (98%) report that their organizations have digital records and information they keep or need to keep for more than 10 years.





We asked practitioners whether or not their organizations had digital records and information they *keep or need to keep* in excess of 10 years. As the infographic shows, an overwhelming majority of respondents (98 percent) reported that they do.

These results are not surprising and are consistent with our anecdotal experience of organizational behavior—many organizations do keep records long term. The results are also consistent with preliminary research IGI conducted as part of our **2015-16 Annual Survey**. In that research, a majority of practitioners (91 percent) reported that their organization's records retention policies and schedules included permanent records, and 89 percent said they had *digital records* that they must retain in excess of 10 years.

What are the digital records and information that organizations keep? We asked practitioners to tell us the reasons why they are keeping digital records and information for more than 10 years and to select all that applied. As the infographic shows, most organizations are keeping them for a range of important reasons (e.g., six of the responses were selected by over half of respondents).

"Statutory, Regulatory, and/or Legal Obligations" led

the way as the most common response (89 percent). This is consistent with other research by the IGI that shows reducing or responding to outside risks are common drivers of organizations' IG policies. Indeed, these may be drivers behind a number of the options practitioners selected, here, for why their organizations keep digital records and information long term.

But a number of the reasons organizations say they are keeping digital records and information long term may have another side to them—regardless of whether organizations *have* to keep them, those digital information assets are likely to be important to the day-to-day functioning of the organization, too. "Human Resources/Personnel Requirements," "Contracts," "Corporate or Institutional Governance" were each selected by more than half of respondents and "Business Operations" by more than 40 percent, for example.

Regardless of the reason, digital assets should be considered business-critical, warranting formal steps to ensure that they are findable, readable, usable, and trustworthy long into the future. To do that requires a commitment to providing long-term protection and access as an inherent and critical part of an overall IG program.

A Practical Approach to Governing 170 Years of Critical Corporate Records

“With digital-only records, a number of things can go wrong. We have to deal with playback media that degrades and file formats and software becoming obsolete, among other long-term access challenges. It was vital to protect our unique digital assets from these risks by using digital preservation techniques much more sophisticated than simply storing the ‘bits and bytes.’”

VALERIE KOMOR, DIRECTOR, ASSOCIATED PRESS CORPORATE ARCHIVES

As one of the only truly global news reporting organizations, Associated Press (AP) has been bringing us the news for 170 years. With journalists in over 100 countries, AP has been at the center of history for nearly two centuries. In the process AP has become the custodian of a vast treasure-trove of irreplaceable and historically significant information in a dizzying array of formats.

The task of ensuring that vital digital information is protected, preserved, and accessible for the next 170 years falls to Valerie Komor and her team in AP's Corporate Archives group. In 2003, the Corporate Archives was established with the mission to acquire, organize, preserve, and make available the historically valuable records of the institution, which include corporate, news and administrative records as well as photograph, audio and video collections. Today, the Archives holds 4,000 linear feet of records and over 30 TB of digital files. As nearly every document is today born digital, Valerie's challenge has been growing not only by volume, but also by complexity—with no end in sight.

Valerie and her team took on this challenge by focusing on ways they could practically govern their information while minimizing the burden on the organization. Here are the steps they took:

1. **Pragmatic & risk/value focused.** Valerie and her team are responsible for a massive amount of information requiring governance. It cannot all be tackled at the

same time, nor does all of it require the same level of governance. So, the team conducted a prioritization process and started with corporate records and information essential to documenting AP's business history in the event of a system failure or other disruptive event.

2. **Phase and iterate.** In addition to prioritizing IG activities based on a clear assessment of information risk and value, AP adopted a phased approach. This means they divided their information into chunks based on content, anticipated use, and physical condition. This was the only practical way to approach their project because the volume of records is too great to allow any other approach. Valerie started with full sets of annual reports and charters and bylaws and intends to bring in other collections as they are reviewed. These include vast amounts of original wire copy, the ephemeral sheets of news copy, which flowed off teletype machines from 1920 until 1986 and survive within bureau records and other files.

To support this strategy, AP selected Preservica's standards-based digital preservation system, an approach that will also enable them to automate the operational and technical aspects of the project while meeting AP's needs for IG and long-term accessibility of its one-of-a-kind corporate history.

WHAT TECHNOLOGIES ARE ORGANIZATIONS USING?

CURRENTLY USED STORAGE SOLUTIONS ARE PUTTING LONG-TERM DIGITAL RECORDS AND INFORMATION AT RISK

WHERE ARE DIGITAL RECORDS AND INFORMATION BEING STORED?	
Shared Network Drive	68%
Line of Business Applications (e.g. CRM, ERP, Manufacturing, HR Systems, etc.)	52%
Enterprise Content Management System (ECM)	47%
Disk or Tape Backup Systems	44%
Records Management System (e.g. EDRMS)	43%
Application-specific Archiving (e.g. email)	33%
Removable Media (e.g. CD or USB)	22%
Enterprise Information Archiving System (EIA)	14%
Purpose-built, Long-term Digital Preservation System	11%
Other	9%
Commodity Cloud Storage (e.g. Amazon)	8%
I don't know.	1%

Most organizations are not storing their long-term digital assets in a manner sufficient to ensure their long-term protection and accessibility. In fact, the top method is shared network drives. This option, like a number of the others listed (including ECM and EDRMS), even with additional backup or archiving, provides no inherent capability to address the unique requirements of this class of information. This exposes the organization to the risk of not being able to read and use these digital information assets in the future, for example, if your organization no longer supports or licenses a particular

application or the file format becomes obsolete. In addition, shared network drives are notoriously insecure and nearly impossible to govern well, further exposing these assets to accidental or malicious tampering and deletion.

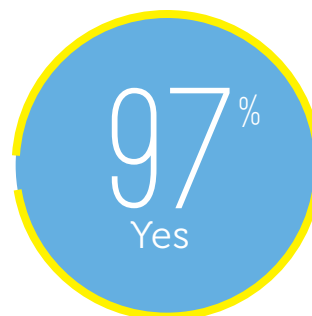
Organizations should seek out technological solutions that are purpose-built for the unique requirements of long-term protection and access. Unfortunately today, only a small percentage of organizations (11 percent) are employing these systems, putting vast swaths of critical information across the globe at risk.

THE AWARENESS AND ACTION GAP

PRACTITIONERS KNOW DIGITAL RECORDS AND INFORMATION ARE AT RISK,
BUT PRESERVATION STRATEGIES HAVE NOT CAUGHT UP

HOW ARE ORGANIZATIONS ADDRESSING THE CHALLENGE?	
We are currently considering our approach.	44%
Convert official records to formats like PDF, TXT, CSV, etc.	33%
We have no comprehensive strategy.	31%
Postpone action until required (such as on-demand conversion or migration)	16%
Transfer to a standards based digital preservation system	16%
Other	12%
Convert to analog format (paper or film)	10%
I don't know.	6%

Most practitioners (97%) are aware that technology obsolescence could put long-term digital records and information at risk of not being readable or useable in the future.



Why aren't organizations doing more to protect their digital information assets? Awareness of the problem is very high—97 percent. Yet, many are failing to take definitive action to ensure that their critical information assets are protected and accessible over the long term.

We asked practitioners what their organizations were doing to address the unique challenge of safeguarding their long-term digital records and information and to select all that applied. While it is good news to see that 44 percent are currently considering what to do (as the infographic shows), only 16 percent report that they are transferring data to a standards-based digital preservation system. Further, nearly a third of our respondents (31 percent), report that their organizations do not have a comprehensive approach.

Sixteen percent report postponing action until it is required—a risky strategy. As discussed previously, if you delay the steps necessary to safeguard your information from the start, degradation, corruption, and obsolescence can happen in the meantime. You

may find when you need digital records and information they are not fully intact or that the costs (time, money, and technical resources) necessary to access and read them are prohibitively high.

Finally, a third of respondents report that they are converting official records to a common file type (e.g. PDF, TXT, or CSV). While this approach might seem to work, for now, for certain types of documents, there is also the risk that the chosen file format itself might become obsolete. If you adopt a strategy of converting once (especially if you do not also retain the original format), you also risk losing your vital information should such obsolescence occur. To be effective, digital preservation needs to be an active process. In addition, these simplified formats do not really work for certain content. You can't preserve multimedia files (images, video, and audio, for example) this way. Further, other content, like websites, emails, spreadsheets, slide presentations, and maps, for example, lose their interactivity, context, and inherent value when saved this way.



Future-Proofing Critical Digital Data in an Increasingly Complex Global Regulatory Environment

“We have a very large repository of physical and digital records that require long-term preservation and access. Critical digital information is also being created every day, at high volume. We needed a system that could help us govern information over the long-term and also integrate with our existing systems so we could achieve a single, cohesive view of our most important information assets.”

TINA STAPLES, HSBC GLOBAL HEAD OF ARCHIVES

HSBC, one of the largest financial services organizations in the world, was founded 150 years ago in Hong Kong with a mandate to finance trade between Europe and Asia. With a fascinating corporate history that is woven into the fabric of world history, itself, HSBC today serves nearly 50 million customers in 72 countries.

Along the way, the bank has accumulated a vast and fascinating archive that includes photos, letters, and bank notes as well as critical evidence of strategic decision-making at the bank. This information plays a vital role in enhancing brand value, supporting a wide variety of HSBC projects and events, and informing researchers, historians, and the general public. However, the challenge does not end at preserving and presenting history.

Tina Staples is global head of HSBC’s Archives team, a group of twenty specialists located in London, Hong Kong, Paris, and New York. As the group’s name suggests, Tina’s team governs HSBC’s historical information, but her mandate has expanded to governing the digital information that the bank creates every day—information of enduring historical value, that will provide essential evidence of the bank’s activities and decision-making.

It was critical that the bank’s approach to IG addressed both the **past** and the **future**. In order to future-proof and safeguard digital information the HSBC team realized they needed an approach that would not only provide

long-term preservation of existing information, but one that would integrate with the HSBC cataloguing system to provide a unified view of the archive. This was a practical need that Tina’s team knew was essential for both adoption and usability. However, this needed to be done in a way that addressed the compliance complexity inherent to an organization in a heavily-regulated sector, operating globally, and subject to the (sometimes contradictory) laws and regulations of numerous jurisdictions.

HSBC’s legal and regulatory environment is incredibly complex, meaning that its information assets are subject to multiple overlapping privacy and security requirements. To achieve compliance, HSBC adopted a foundational IG approach focused on identifying and addressing interests, concerns, and requirements of critical stakeholders including HSBC’s chief legal officer as well as senior representatives from RIM, IT, Legal, Compliance, and Risk. Making sure all relevant stakeholders were consulted during such efforts was a key to successful implementation and project success.

To address these needs as part of its overall IG program, HSBC opted for on-premise software from Preservica. The bank has already ingested many born-digital records from HSBC’s more recent business activities and continues to develop and evolve its capabilities to ensure long-term preservation and access for its critical digital assets.



GOVERNING LONG-TERM DIGITAL INFORMATION: TAKING ACTION



What can you do, today, to help make sure that your organization's long-term digital records and information are protected? Here are our recommendations to help you get started.

1. Triage

You might have digital information in your organization right now that is in serious danger of being lost, damaged, or rendered inaccessible. This is not the time for careful deliberation or assessment. It is time for action. Perhaps, some repositories or information types immediately come to mind? The 10,000 backup tapes for the merger that seems like just yesterday but in fact will be ten years in June? The obsolete email archive filled with records you know you need to keep, but the system is moldering away in a forgotten data center somewhere? Talk to people responsible for IT storage infrastructure and also line-of-business owners about their most immediate concern, and start there.

2. Assess

Once the most critical at-risk repositories and information types have been stabilized and addressed, it is time to conduct a formal assessment so that you can benefit from strategic planning and economies of scale. Do you have digital information that you need to keep longer than ten years? If so, where is it, what is it, and who had control of it? Is there a plan in place for its protection and access? Does your records retention schedule say that you are supposed to be keeping some records for ten years or longer? (Hint: This is likely the case). A critical first step is simply an assessment of the current state and visibility into your information environment.

An additional tip: if you are not already involved in electronic discovery (i.e., the process by which information is found, collected, and produced by your organization in the context of lawsuits and other formal proceedings), talk to the people who are as they often have a very comprehensive view of the information environment, and especially ancient data repositories that they have been required to produce data from. Another lesson to learn from these colleagues is pragmatism. These practitioners are often forced to accomplish complex information collection, categorization, processing, and management tasks under intense pressure and ridiculously short timeframes in incredibly high-stakes situations. In this environment, perfection is simply not possible, nor is it the goal. Rather, the standard is reasonable efforts and most importantly, progress and completion. All IG practitioners can and should learn from this as they approach long-term protection and access: focus on progress, pragmatism, and incremental improvement.

3. Address the Past, Protect the Future

Our massive stores of legacy information clearly must be brought under governance. However, legacy information may not be the right place for your organization to start (after you have triaged immediate risks as described above, that is). While you focus on the past, the present is conspiring to magnify and compound your IG problem. Every day your organization is creating new information—some of which likely requires protection and access over the long-term (as our research shows). Every day you fail to govern this new information is a day that only makes your future IG problem more difficult and expensive.

4. Catalog Consequences

Do you clearly understand the consequences of not being able to access, use, and rely upon your own records and information? Does your management? The consequences can be disastrous, and you need to assess, catalog, and rank these potential negative outcomes. What are the digital records and information your organization is keeping long term? Are they important or business critical? Knowing why they are of value to your organization can help you make the case for investing adequately in their preservation (e.g. fines for non-compliance, cost of legal challenge, reputational damage, failure to meet mandate, inability to leverage and re-use company knowledge, etc.).

5. Build Your Rules

Protection and accessibility of digital information over the long term must be a standardized part of your IG program. This means creating and enforcing rules. Do your existing IG policies and procedures address this need? If not, get to work. If you want to be sure your digital information assets will be available when you need them in the future, your policies, procedures, and systems must ensure that you can find, read, and use them.

6. Assess the IT Environment

Do you have the systems and infrastructure in place to protect and ensure access to your digital information assets over the long term? Despite widespread reliance revealed here by our research, shared drives and other general-purpose storage repositories are generally insufficient to address these unique requirements, without specialized customizations or add-ons that can address preservation beyond simple bit-level protection. In this regard, adherence to open industry standards is critical as a means to avoid the risk of inaccessibility due to the obsolescence of a proprietary technology. Standards are also critical for ensuring that these systems for long-term protection and access can talk to and exchange data with line of business applications, electronic content management (ECM) systems, and other repositories where these assets are created or temporarily stored.



ENDNOTES

We have used the following numeric convention for survey data throughout this document: results that included a half percentage point or more were rounded up, and results below half a percentage point were rounded down. As such, in some cases aggregated results for particular questions do not add up to 100 percent.

This work should be cited as: Information Governance Initiative, "The Governance of Long-Term Digital Information: An IGI 2016 Benchmark" (Information Governance Initiative LLC, May 2016).

- 1 Margaret Hedstrom, "Digital Preservation: A Time Bomb for Digital Libraries," *Computers and the Humanities* 31: 189-202, 1998. 1998 Kluwer Academic Publishers.
- 2 Terry Kuny, "A Digital Dark Ages? Challenges in the Preservation of Electronic Information," delivered at the 63rd annual International Federation of Library Associations and Institutions Conference, September 4, 1997.
- 3 "Preserving Digital Information," Report of the Task Force on Archiving of Digital Information. Commissioned by The Commission on Preservation and Access and The Research Libraries Group, May 1, 1996.
- 4 See, e.g., the seminal paper referenced above: "Digital Dark Ages? Challenges in the Preservation of Electronic Information," delivered by Terry Kuny at the 63rd annual International Federation of Library Associations and Institutions conference on September 4, 1997.
- 5 Ian Sample, "Google boss warns of 'forgotten century' with email and photos at risk," *The Guardian*, February 13, 2015.
- 6 State of Texas Legislative Budget Board, "Fiscal Size-Up 2014-2014 Biennium," February 2014.
- 7 State of Texas Legislative Budget Board, "Fiscal Size-Up 2014-2014 Biennium," February 2014.
- 8 If Texas were a country, its economic output of \$1.65 trillion would make it the world's 12th largest economy. Mark J. Perry, "If New York is Spain and California is Brazil, What is Texas?" *Newsweek*, June 22, 2015. Online at: <http://www.newsweek.com/if-new-york-spain-and-california-brazil-what-texas-344702>



ABOUT THIS PUBLICATION

This publication was created by the IGI as part of our ongoing work exploring issues, strategies, and techniques related to information governance. As part of our commitment to excellence and to maintain objectivity, the IGI does not recommend, evaluate, or endorse specific products, services, or providers. However, the IGI's work is made possible through the generous contributions of our supporters for which we are grateful. This publication was made possible by Preservica's support of the IGI.

About the Information Governance Initiative

The Information Governance Initiative (IGI) is a think tank and community dedicated to advancing the adoption of Information Governance (IG) practices and technologies through research, events, advocacy, and peer-to-peer networking. We are dedicated to the professionalization of IG and have called for the creation of a new kind of information leader called the Chief Information Governance Officer. Our Annual Report has become an industry standard reference guide for

organizations benchmarking and building their IG programs. The IGI Community is where thousands of practitioners from cybersecurity, IT, analytics, privacy, legal, records management and the other facets of IG come together and learn from each other. We produce hands-on educational workshops and executive roundtables each year. The IGI was founded by recognized leaders in the field of IG, and is supported by leading providers of IG products and services. You can find us online at iginitiative.com. Join us.

About Preservica

Preservica is a world leader in digital preservation software, consulting and research with active preservation solutions used by businesses, archives, libraries, museums, and government organizations globally to safeguard and share valuable digital content, collections and electronic records, for decades to come. Customers include the European Commission, Texas State Archives, Wellcome Library, the Associated Press, and HSBC, to name a few. More information about Preservica can be found online at: www.preservica.com

©2016 Information Governance Initiative LLC ("the author"). All rights reserved unless otherwise noted. This publication may not be reproduced or distributed without the author's prior permission. The information contained in this publication has been obtained from sources the author believes to be reliable. The author disclaims all warranties as to the completeness, adequacy, or accuracy of such information and shall have no liability for errors, omissions, or inadequacies herein. The opinions expressed herein are subject to change without notice. Although the author may include a discussion of legal issues, the author does not provide legal advice or services, and its research should not be used or construed as such.

Trusted Digital Repository Standards and Other Useful Resources

All standards and resources listed below are subject to revision so please check for the most recent edition.

International Organization for Standardization. ISO 14721:2012, *Space data and information transfer systems—Open Archival Information System—Reference model*. Geneva, Switzerland: International Organization for Standardization, 2012. Available for purchase at www.iso.org.

Consultative Committee for Space Data Systems. *Reference Model for an Open Archival Information System (OAIS)*. Washington, D.C.: National Aeronautics and Space Administration, June 2012. Available at: <http://public.ccsds.org/publications/archive/650x0m2.pdf>.

Consultative Committee for Space Data Systems. *Audit and Certification for Trustworthy Digital Repositories. Recommended Practice*. Washington, D.C.: National Aeronautics and Space Administration, September 2011. Available at: <http://public.ccsds.org/publications/archive/652x0m1.pdf>

International Organization for Standardization. ISO 20652: 2015, Space data and information transfer system – Producer-archives interface-Methodology abstract standard. Available from <http://public.ccsds.org/publications/archive/651x1b1.pdf>

International Organization for Standardization. ISO 31000: 2009, Risk Management – Principles and Guidelines. Available for purchase at www.iso.org.

International Organization for Standardization. ISO 15489-1:2001, *Information and documentation—Records management—Part 1: General*. Geneva, Switzerland: International Organization for Standardization, 2001. Available for purchase at www.iso.org [Currently under revision]

50 Most Prevalent Formats in KB e-Depot (March 2014) is available at: <https://gist.github.com/bitsgalore/21028de28b7f05066585#file-extensionskbdm-md>

ISO 16363 Primary Trustworthy Digital Repository Authorisation Body (IS)-PTAB can be reached at: <http://www.iso16363.org/> A sample self-assessment for an ISO 16363 audit is available at: <http://www.iso16363.org/preparing-for-an-audit/>

Pearce-Moses, R. *A Glossary of Archival and Records Terminology*. Chicago: The Society of American Archivists, 2005. Available at: <http://www.archivists.org/glossary/index.asp>

British Library Digital Preservation Strategy 2013-2016. Available at: <http://www.bl.uk/aboutus/stratpolprog/collectioncare/digitalpreservation/strategy/dpstrategy.html>

University of Southern California (USC) Digital Repository provides an overview of their cloud storage, digital preservation and archiving services at <http://repository.usc.edu/>. A planning worksheet is available for download at: http://repository.usc.edu/wp-content/uploads/2012/11/USCDR_Worksheet.pdf

Trusted Digital Repository Resources continued

DRAMBORA - Digital Repository Audit Method Based on Risk Assessment

<http://www.repositoryaudit.eu/>

Ten Core Requirements for Digital Archives

1. Mandate & Commitment to Digital Object Maintenance
2. Organizational Fitness
3. Legal & Regulatory Legitimacy
4. Efficient & Effective Policies
5. Adequate Technical Infrastructure
6. Acquisition & Ingest
7. Preservation of Digital Object Integrity, Authenticity & Usability
8. Metadata Management & Audit Trails
9. Dissemination
10. Preservation Planning & Action

Minnesota Archives Trustworthy Information Systems Criteria

<http://www.mnhs.org/preserve/records/tis/tis.html>

1A. SYSTEM DOCUMENTATION SHOULD INCLUDE, BUT IS NOT LIMITED TO:

1. Hardware (procurement, installation, modifications, and maintenance)
2. Software (procurement, installation, modifications, and maintenance)
3. Communication Networks (procurement, installation, modifications, and maintenance)
4. Interconnected Systems
 - a) list of interconnected systems (including the Internet)
 - b) names of systems and unique identifiers
 - c) owners
 - d) names and titles of authorizing personnel
 - e) dates of authorization
 - f) types of interconnection
 - g) indication of system of record
 - h) sensitivity levels
 - i) security mechanisms, security concerns, and personnel rules of behavior

Trusted Digital Repository Resources continued

University of Minnesota Libraries. (2015). Electronic Records Task Force Final Report. Retrieved from the University of Minnesota Digital Conservancy, <http://hdl.handle.net/11299/174097>.

Truman, Gail. 2016. Web Archiving Environmental Scan. Harvard Library Report.
<https://dash.harvard.edu/handle/1/25658314>

This report details the results of an environmental scan of the current issues and trends in web archiving nationally and internationally conducted by the Harvard Library. The purpose of the environmental scan was to explore and document current web archiving programs to identify common concerns, needs, and expectations in the collection and provision of web archives to users; the provision and maintenance of web archiving infrastructure and services; and the use of web archives by researchers.

Digital Preservation Capability Maturity Model© (DPCMM)

BACKGROUND AND PERFORMANCE METRICS

Version 2.7 - Released July 6, 2015 www.securelyrooted.com/dpcmm

This document provides an overview of the Digital Preservation Capability Maturity Model© (DPCMM) including its origins and foundations, performance metrics, and suggested use. The purpose of DPCMM is to provide practitioners with an integrated process model and business case planning tool to aid in benchmarking and improving digital preservation capabilities.

Digital Preservation Capability Self-Assessment Survey

The Digital Preservation Capability self-assessment application is based on the DPCMM. The tool, which generates a score card and provides the full set of self-assessment statements upon completion of the survey, is free and open to any organization and practitioner. Register at www.DigitalOK.org.

We ask that you begin the self-assessment within 72 hours of registering or your registration will lapse. You can re-register at a more convenient time. It is not necessary to complete the survey in a single session—save it and return to finish it at a later date.

Download your assessment (pdf) to share with digital preservation stakeholders and communities of interest. Use the component descriptions and performance metrics to inform your digital preservation planning and implementation efforts.



Digital Preservation Capability Self-Assessment

Name:

Title:

Organization:

Location(s):

Repository:

Index Score Results	Nominal (0)	Minimal (1)	Intermediate (2)	Advanced (3)	Optimal (4)
DIGITAL PRESERVATION POLICY					
DIGITAL PRESERVATION STRATEGY					
GOVERNANCE					
COLLABORATION					
TECHNICAL EXPERTISE					
OPEN STANDARD TECHNOLOGY NEUTRAL FORMATS					
DESIGNATED COMMUNITY					
ELECTRONIC RECORDS SURVEY					
INGEST					
ARCHIVAL STORAGE					
DEVICE/MEDIA RENEWAL					
INTEGRITY					
SECURITY					
PRESERVATION METADATA					
ACCESS					

Index Score: /60

Based upon your responses, the digital preservation capabilities and services of your organization and designated repository fall into the__Stage ().

This scorecard indicates the current capabilities of the organization/repository for each component in the Digital Preservation Capability Maturity Model. The filled in circles (red, orange, yellow, light green, dark green) denote where all of the respective requirements have been met.

Level	Digital Preservation Capability
0	Based on your responses, the digital preservation capabilities and services of your organization and repository fall into the Nominal level. A systematic digital preservation program has not been undertaken and practically all electronic records that merit long-term retention are at risk.
1	Based on your responses, the digital preservation capabilities and services of your organization and repository fall into the Minimal level. Digital preservation capabilities are rudimentary and most electronic records that merit long-term retention are at risk.
2	Based on your responses, the digital preservation capabilities and services of your organization and repository fall into the Intermediate level. The organization supports initiatives and projects that approach but do not fully comply with the ISO 14721/ISO 16363 specifications. There is an established basis for proactive and sustainable digital preservation improvement actions over time. Nevertheless, it is likely that many electronic records that merit long term retention remain at risk.
	ISO 14721 Conformance
3	Based on your responses, the digital preservation capabilities and services of your organization and repository fall into the Advanced level. The organization has robust infrastructure and the preservation of electronic records is undertaken with a framework that is partially compliant with the specifications of ISO 14721/ISO 16363. Some electronic records that merit long-term preservation may be at risk.
4	Based on your responses, the digital preservation capabilities and services of your organization and the repository are at the Optimal level. Your organization maintains a strategic focus on digital preservation outcomes by continuously improving the manner in which electronic records lifecycle management is executed. Few if any electronic records that merit long-term preservation remain at risk.

Register for the Digital Preservation Capability Self-Assessment at www.DigitalOK.org. The self-assessment survey is based on the Digital Preservation Capability Maturity Model (DPCMM) which is available at www.securelyrooted.com/dpcmm.