JTC Resource Bulletin

Managing Digital Evidence in Courts

Version 1.0
Adopted February 17, 2016

Abstract

Technologies including smart phones and body-worn cameras are capturing an ever-increasing volume of evidence. The exponential increase in the quantity of digital evidence is challenging the court's ability to receive, evaluate, protect, and present digital evidence. This report identifies potential challenges and recommends steps courts should consider.

Document History and Version Control

Version	Date Approved	Approved by	Brief Description
1.0	2/17/2016	JTC	Release document

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

Digital Evidence Focus Group:

Tracy BeMent
Georgia District Court Administrator

Ken Bosier
CIO, Iowa AOC

James Emerson
International Association of Chiefs of Police

Jeff Marecic
CIO, North Carolina AOC

Snorri Ogata
CIO, Superior Court of California, Los Angeles

Duane Pearson
Denver Police Crime Lab Specialist

Michael S. Rainken
Director, Colorado Bureau of Investigation

Steve Steadman
Colorado Court Security Specialist

David Slayton
Texas State Court Administrator

NCSC Staff

Tom Clarke
Vice President, Research and Technology

Paul Embley
Manager, Technology and CIO

Keith Fisher
Principal Court Management Consultant, Court Services

Greg Hurley
Senior Analyst, Knowledge and Information Services

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

Robin Sweet
Nevada Administrative Office of the Courts

NACM Appointments

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

Paul DeLosh
Supreme Court of Virginia

Danielle Fox
Circuit Court for Montgomery County, Maryland

Kelly C. Steele
Florida Ninth Judicial Circuit Court

Jeffrey Tsunekawa
Seattle Municipal Court

NCSC Appointments

The Honorable O. John Kuenhold
State of Colorado

The Honorable Michael Trickey
Washington Court of Appeals, Division 1

CITOC Appointments

Jorge Basto
Judicial Council of Georgia

Casey Kennedy
Texas Office of Court Administration

Ex-officio Appointments

Joseph D.K. Wheeler
IJIS Courts Advisory Committee

NCSC Staff

Paul Embley

Jim Harris

Contents

Executive Summary

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. Key considerations:

Storage
This is one of the most significant issues. Courts must estimate the storage that will be required, evaluate whether to invest in storage hardware or cloud storage, and consider business continuity and disaster recovery requirements.

Preservation and Disposition
Because appellate proceedings may continue for a lengthy period of time and digital evidence may take large amounts of storage, courts will need to consider how long and how to retain digital evidence. Courts should consider "active archive" solutions that allow the court to maintain the evidence in a less available state that is still retained. Discuss preservation and disposition policies with law enforcement and prosecutors.

Centralization vs Decentralization
Regardless of the state's unique court structure, states should consider whether to build a statewide repository of digital evidence or to have localized repositories.

Formats and Conversion
Courts may approach the complicated issue of file format by choosing to accept only a limited range of formats. However, there are significant issues with converting digital evidence or requiring that digital evidence be submitted with the native format player. Courts may face technical difficulties displaying evidence correctly; computer speeds and display resolutions can distort digital evidence.

Infrastructure
Cost and performance issues will dictate the best solution in the tradeoff between local storage and the use of networks to transfer digital evidence. However, some technical strategies may not be options because of policies that specify who can store the original files and whether streaming live in a courtroom from a remote location is permissible.

Chain of Custody
The chain of custody protocol may be different in an electronic digital evidence environment. Courts must secure electronically stored digital evidence to ensure there is no possibility of tampering.

Readiness
The state of the technical infrastructure, the process for receiving digital video evidence, and how such evidence is played, stored, retained, and accessed are aspects of readiness that each court must evaluate.

Access
Courts must decide whether digital evidence introduced into the court record will be treated as a court filing or an exhibit, determine whether the evidence becomes subject to open records statutes and/or rules, and provide a mechanism for the public to access information guaranteed under public access policies or open records provisions.

Privacy
Digital video regularly records individuals and their property that are not a party to the case at hand. Prior to a video being entered into evidence, the faces and license plates of bystanders can be redacted or blurred out. Local practices will determine if a court needs to establish a court rule or policy, bearing in mind that redaction is very time-intensive.

Vendor Management
Ensure vendor contracts take into account security, auditing provisions, ownership of evidence, access, and other court-specific issues.

Expectations Management
Courts must manage the expectations of both the public and the judges and other courtroom stakeholders. A “CSI” effect may create very unrealistic expectations about what courts can reasonably do.

Introduction

Digital evidence includes “information on computers, audio files, video recordings, and digital images.”[1] This type of evidence is not new to courts, but the explosion of digital video evidence due to law enforcement body-worn cameras, as well as the public’s prolific capturing of digital video evidence, are now causing courts to evaluate their approach to handling digital evidence. Digital video is ubiquitous: it is inevitable that evidence in cases will increasingly include it. Court officials and the public have come to expect that digital evidence be readily accessible and integrated into the normal flow of court proceedings.

The submission and use of digital evidence of all kinds in state and local courts has surged over the last few years. What started as compilations of word processing documents on CDs in large court cases a decade ago has now become a rapidly growing stream of many media types. As electronic filing and electronic courtrooms become more common, courts are both better positioned to handle digital evidence and more exposed to its use.

The Joint Technology Committee (JTC) of the Conference of State Court Administrators (COSCA), National Association for Court Management (NACM) and National Center for State Courts (NCSC) recognized a need to advise courts on how best to deal with digital evidence, especially digital video. With facilitation by the NCSC, JTC held a focus group on court digital evidence in Denver on October 5-6, 2015. This report summarizes the information gathered in that focus group, provides information on the potential challenges courts may face with digital evidence, and makes recommendations for state court consideration.

General Challenges to Court Digital Evidence

Adapting to the surge in digital evidence includes both technical and practical challenges. Courts must rapidly adapt to changes in digital evidence technologies as well as legal precedent, managing the dramatic increase in requirements with no proportional increase in funding.

[1] "Digital Evidence." *Law Enforcement Standards Office*. National Institute of Standards and Technology, US Department of Commerce, 16 July 2012. Web. 09 Feb. 2016.

Common Law

The common law on the use of digital video evidence is very limited, and existing common law references evidence in general.[2] It is likely that the changes in digital evidence will result in issues that generate court cases and produce new common law. Thus, courts may need to plan to respond to changes in the law as those cases produce new common law precedents in the area of digital evidence.

Electronic Filing, Case and Document Management System Capabilities

Most court electronic filing, case management and document management systems are designed primarily for electronic documents and not multimedia formats, although some systems can partially accommodate digital video evidence. Transitioning to electronic delivery and storage of digital evidence may require courts and the industry to develop new capabilities in these systems.

Funding Limitations

There is little likelihood that most courts will be able to obtain any significant new funding needed to acquire new systems, hardware, vendor services or other capabilities to handle digital video evidence. Courts must consider how to manage digital evidence with current capabilities and begin planning to transition to more sophisticated methods of handling and storing digital evidence in the future.

Given these challenges, the need for best practices around the use of digital video evidence is even more salient and timely.

Key Considerations and Recommendations

Courts can take a variety of paths in handling digital evidence. Regardless of the path each court selects, there are issues to consider. The JTC Digital Evidence Focus Group identified the following key issues and formulated recommendations to help guide courts as they navigate the process of incorporating digital evidence. This paper identifies decision points for each of the areas.

Because decisions will impact every aspect of the justice process, courts should involve a broad spectrum of stakeholders including law enforcement, evidence technicians, prosecutors, defense attorneys, clerks, judges, and court reporters in addition to court information technology leaders. All will likely have key insights to assist the court in its planning.

---

[2] For examples of existing law used in Body-Worn Camera cases, see Hurley, Greg. *Body-Worn Cameras and the Courts*. Publication. Williamsburg, VA: National Center for State Courts, 2016. Web. 9 Feb. 2016.

Courts should consider their structure, opportunities, and limitations, then determine the best roadmap for their jurisdiction.

Storage

One of the largest issues facing courts is how to store digital evidence. In most courts, storage of digital evidence is still handled in a physical form, primarily in the form of CDs and DVDs. While this method may continue to be feasible in the near future, courts need to consider how to handle an increase in volume, as well as the technology changes that will make CDs and DVDs obsolete. A better long-term solution will be to store digital evidence electronically on networked devices, but that transition is not without challenges.

The magnitude of the storage issue will depend on three factors:

1. The volume of digital evidence the court elects to keep, with space increasing linearly with volume.
2. The timeliness of retrieval needed by the court, with the cost of storage being significantly more expensive for instant availability versus less instant availability.
3. The willingness of the court to accept cloud storage as an option, with cloud storage providing greater control over cost by paying for only the space needed rather than having to anticipate capacity and buy space that will be unused for a time.

To date there is very little experience in the court technology arena upon which to base a realistic estimate of expected volume.[3] This lack of knowledge about storage requirements is troubling since significant increases in volume will certainly cause problems for many courts.

Presumably, this is an even bigger issue for law enforcement, prosecution, and defense. As with other criminal justice volume issues, the amount looks like a metaphorical funnel as it passes through the justice system from law enforcement to prosecution to the courts. Each successive step considers and passes on only a subset of what was originally created. By the time digital video evidence gets to a court, there are reasonable expectations it will be only a small subset of the original video. In addition, courts will most likely only have digital video entered into evidence in cases

[3] The North Carolina Administrative Office of the Courts has estimated that prosecutors are likely to have an average of 10 GB of digital evidence provided to them for each felony case, with some cases reaching over 100 GB.

that proceed to trial, a small subset of the overall criminal filing volume.[4] Appellate courts should expect to see an even smaller amount of digital evidence.

Much of the digital evidence flooding the courts today comes from a proliferation of body-worn cameras. The following table outlines the recording specifications for most cameras, including smart phone and body-worn, sold today:[5]

Recording Format	Recording Speed (Frames per second)	Max Video Resolution	Bit rate (Kilobits per second)
MPEG-4	30 fps	640x480 to 1920x1080	1,500-7,000 Kbps
MOV	30 fps, 60 fps	1920x1080	1,500-7,000 Kbps
H.264	30 fps, 60 fps	1920x1080	1,500-7,000 Kbps

Table 1 - Typical recording specifications of body-worn cameras

Image resolution (quality), compression type, and frame rate[6] determine the amount of storage that will be required. The estimated storage space requirement for body-worn camera video can be calculated using the following formula[7]:

(Approximate bit rate / 8) * seconds per hour = KB per hour

KB per hour / 1000 = MB per hour

A rough estimated of the storage required for one hour of body-worn camera video using an average bit rate would be calculated as follows:

(4,250 / 8) * 3600 = 1,912,500 KB / 1000 = 1,912 MB

To estimate annual storage requirements:

MB per hour * # of hours * annual caseload

Using the estimated storage requirement example above, a court with 2,000 hours of body-worn camera video evidence per year would need to be prepared to store, protect, and manage 3.824 additional terabytes[8] of data annually.

---

[4] Digital evidence may also be exchanged among the parties as part of pre-trial discovery that will create a dispute that the court must consider.

[5] United States Department of Justice, Office of Justice Programs, National Institute of Justice. *A Primer on Body-Worn Cameras for Law Enforcement.* September 2012. Web. January 28, 2016.

[6] The amount of motion and light in the video also influence the amount of storage required.

[7] Red Leaf Security. *Bandwidth and Storage Space Calculations*. (Undated). Web. January 28, 2016.

[8] To calculated terabytes (TB), divide the number of megabytes (MB) by 1,000,000.

Use known factors (predicted case loads) and best guesses at unknown factors (quantity of video evidence and how much will be retained) to project storage requirements. Scenario estimates may yield projections that range from moderately manageable to very unmanageable.

It may or may not be in the best interest of the court to invest in servers and infrastructure to meet projected storage requirements.[9] If courts find that they are unable to deal with the volume of digital video evidence using local storage hardware an alternative is to use a cloud storage vendor. A number of law enforcement agencies are already employing this option. Large law firms routinely do so as well.

Courts have been more conservative adopters of cloud services, using them primarily for back office email and word processing. Many courts immediately reject cloud storage as an option because of the risks associated with losing control of the data, including its legal validity, reliability, integrity, and confidentiality. For more information about the challenges and benefits of cloud storage, see the JTC resource bulletin *Cloud Computing*,[10] which discusses the challenges and implementation considerations. Courts may wish to review that bulletin as part of their decision process.

Recommendations:

- Estimate the increase in storage that will be required to retain digital evidence, including the likely increase in volume due to body-worn camera and other video evidence. Those estimates should drive immediate and future budgets.
- Evaluate whether to invest in storage hardware or cloud storage.
- Consider business continuity and disaster recovery requirements. As courts make the transition to more online digital evidence, they will also need a means to recover in the event of equipment failure, natural disaster and other business interruptions. Taking these factors into account, storage needs can double or even triple in order to provide continued access to digital evidence.

Preservation and Disposition

COSCA and JTC recently published white papers on records management, including archiving.[11] [12] Those two papers provide general guidance in overall records preservation and disposition, as well as specific guidance on how to develop a plan for

[9] Estimates for storage servers with a capacity of one TB range from $5,000-$8,000 per unit.

[10] Joint Technology Committee. *JTC Resource Bulletin: Cloud Computing*. (December 2014). Web. January 28, 2016.

[11] Linhares, Gregory J. and Nial Raaen, "To Protect and Preserve: Standards for Maintaining and Managing 21st Century Court Records." *NCSC.org*. Conference of State Court Administrators (2013). Web. 11 February 2016.

[12] Resource Bulletin: Developing an Electronic Records Preservation and Disposition Plan. *NCSC.org*. Joint Technology Committee, 2014. Web. 11 February 2016.

electronic records. These papers can help courts considering digital evidence preservation and disposition. However, there are additional considerations for digital evidence preservation and disposition policies. First, courts will need to consider how long to retain digital evidence in light of the fact that appellate proceedings may continue for a lengthy period of time. Due to the large amount of storage likely needed for digital evidence, courts may want to consider "active archive" solutions, which allow the court to maintain the evidence in a less available state that is still retained. This minimizes active storage space requirements, lessening overall storage capacity requirements.

Courts should also consider discussing preservation and disposition policies with law enforcement and prosecutors. If a court proceeding only includes a portion of the full amount of digital evidence (i.e. 30 seconds of a three-hour video), law enforcement and prosecutors may need to retain the full version for future proceedings, including forensic analysis. While the court is unlikely to be the one to retain the lengthier version of the digital evidence, it is vital that the court discuss these issues with other stakeholders who may not consider the ramifications of their policies to the court process.

Recommendations

- Create and implement a plan for digital evidence preservation and disposition.
- Discuss digital evidence preservation and disposition plans with law enforcement and prosecutor agencies to ensure appropriate preservation of evidence.

Centralization vs Decentralization

Court structures within states vary along several pertinent dimensions. These include large versus small, well-funded versus underfunded, centralized versus decentralized, and independently elected clerks versus court-appointed clerks. Each structural dimension raises unique issues.

Large and/or well-funded courts may be much better positioned to deal with digital evidence. They may have better funding, more IT personnel capacity and skill sets, courtrooms that are already equipped to handle new technology, and faster bandwidth. In less well-funded courts, clerks may have to convert some evidence to paper or static pictures. In other situations, lawyers may have to bring all necessary equipment to the courtroom.

Courts should consider whether to build a statewide repository of digital evidence or to have localized repositories. There are advantages and disadvantages to each approach:

Repository Method	Advantages	Disadvantages
Centralized	Uniformity in solution Uniform method of upload, download Enhanced disaster tolerance Better management and control of data	Requires very robust networks to provide acceptable response time throughout the pre-trial and trial processes Inconsistent or slower download and playback, especially to geographically isolated courts or those without high-speed connections Less customization to meet local needs Larger storage needs
Decentralized	Consistent or faster download, playback Customization to meet local needs Less storage required	Fragmented capabilities and procedures Need for a more robust disaster recovery plan More difficult to manage in multi-location districts Greater one-time hardware costs Greater personnel costs

Table 2 – Comparison of Repository Methods

Resources are scarce and there are many valuable programs contending for those resources, so courts must be measured in their approach to managing digital evidence. When evaluating options, courts must balance equal treatment and justice across a state or jurisdiction against the ability of smaller courts or courts with very limited budgets to support certain capabilities. Using multiple or hybrid approaches may better meet a court's unique requirements. Carefully consider a valid business case and common sense before expending resources on new capabilities.

Recommendations

- Carefully consider minimum necessary capabilities for handling digital evidence.
- Evaluate centralized, decentralized, and hybrid approaches for a digital evidence repository and select the design appropriate for your jurisdiction.

Formats and Conversion

A growing number of courts have established policies for what digital video formats may be used when presenting evidence to their courts. In general, those courts have opted to limit accepted formats to a small number chosen by the court without regard for which formats are used most often by vendors, law enforcement, prosecutors, or the general

public. Those limitations are typically driven by a desire to minimize the cost and complexity of dealing with video evidence.

Forensic labs and others have established national best practices for the conversion of digital video evidence. Those practices have been driven in part by scientific research about the impact of conversions on the quality of the video evidence,[13] including distortions that might be legally meaningful. The general conclusion is that it is dangerous to convert formats at all. Rather, it is better to submit the video in its original format with the native player for that format.

While law enforcement may consider this a best practice, submitting video in its original format raises a number of significant issues for courts. Courts cannot afford to acquire the large number of proprietary players required to access the many different video formats. Thus, law enforcement and prosecution will need to provide the players to the court with the evidence. Native players would need to be retained with the digital video evidence even as updated players are released, since the version used when the video was captured might be required to properly play the video evidence. Even with the appropriate player, the court may face technical difficulties displaying the evidence correctly, as computer speeds and display resolutions can distort digital evidence.[14]

The national court e-filing technical standard[15] does not support the inclusion of video players in filings. If the e-filing standard allowed the transmission of a video player, most courts would be reluctant to allow executable program files submitted from an outside source to be downloaded to a court network due to security concerns.

It is likely that case law will eventually resolve the conversion issue in a definitive way, but that guidance is not yet available.

Recommendations

- Avoid creating arbitrary limitations on acceptable formats for digital evidence.
- Work with law enforcement, prosecutors, and local labs to consider the tradeoffs between converting and not converting digital video evidence.

---

[13] For an explanation of the impact of file format, conversion, and compression, see Hoffman, Chris. "What Lossless File Formats are and Why You Shouldn't Convert Lossy to Lossless." *How-to Geek*. November 6, 2015. Web. 11 February 2016.

[14] Carner, Doug. *Detect and Prevent File Tampering in Multimedia Files*. (Unknown Date.). Web. January 28, 2016.

[15] *Electronic Court Filing Version 4.01*. OAISIS - Advancing Open Standards for the Information Society, 23 May 2013. Web. 11 Feb. 2016.

Infrastructure

Technology infrastructure includes hardware, systems software, network, and facilities.[16] Technology infrastructure requirements will vary according to the anticipated volume of digital evidence and the decisions the court makes about how to handle that evidence. Courts will be better positioned to manage digital evidence to the extent that they have high-speed networks, sufficient bandwidth, sophisticated electronic filing and case management systems, extensive storage capacity, and a willingness to work with external vendors if cloud solutions are required. In-house IT expertise handling multimedia formats will also be helpful to the court in planning and managing digital evidence.

Cost and performance issues will dictate the best solution in the tradeoff between local storage and the use of networks to transfer digital evidence. Small courts with low volumes may be able to deal with digital evidence using traditional strategies. A single DVD can store up to nine hours of video, depending on the format, compression, and quality of the video.

Bandwidth constraints may cause states or large court systems to store more digital video evidence locally rather than offsite. Fiber networks with "quality of service" (guaranteed bandwidth for certain media types, applications, or organizations) may be able to handle file transfer requirements for large video files. Newer real-time streaming formats use network bandwidth much more efficiently but may be costly. Finally, some courts may be able to transmit large files during off hours and make local copies on CDs or DVDs for actual display in a courtroom during a hearing.

Some technical strategies may not be options because of policies that specify who can store the original files and whether streaming live in a courtroom from a remote location is permissible.

Courts should also consider how digital evidence will be transmitted from trial courts to appellate courts. Courts might consider allowing access to streaming media, where available, or instead choose to upload the files to appellate court servers.

No matter the method chosen, courts will need to have an effective business continuity plan in the event of a disaster that impacts the stored digital evidence.[17]

---

[16] *Court Technology Framework*. Joint Technology Committee. Web. January 28, 2016.

[17] Seven criminal cases, including a homicide case, were impacted by a failure of a video recording system in Milwaukee in 2015 that caused the department to lose critical video footage relevant to the cases. See Sanchick, "Milwaukee Police Department: Seven criminal cases impacted by failure of video recording system." *Fox6Now.com*. May 13, 2015. Web. January 28, 2016.

Recommendations

- Evaluate current infrastructure to determine if it is sufficient to handle the demands of an electronic digital evidence environment, including cloud storage.
- Determine how digital evidence will be transmitted to appellate courts.
- Assess the possibility of accommodating streaming presentation technologies in courtrooms.
- Develop a short-term and medium-term approach to the use of streaming technologies.
- Review external resources for best practices; train relevant court personnel to competently manage multimedia formats, external cloud storage, and streaming vendors.
- Ensure that disaster recovery plans include digital evidence retained by the court.
- Consider using vendors and solutions that can scale in real time to meet demand.

Chain of Custody

While some may raise chain of custody issues in the law enforcement and prosecution areas, the issue is likely less of a problem for digital evidence introduced to the court. Once digital evidence is admitted to the court, the common chain of custody protocols apply. (For example, a court reporter or clerk would typically store evidence.) This chain of custody protocol may be different in an electronic digital evidence environment. Courts must ensure that there is no possibility of tampering. This will likely involve limiting physical access to digital evidence and implementing a system that provides an audit trail of when digital evidence is accessed and by whom. If storage is out-sourced, courts should ensure proper controls are in place to prevent tampering during storage or transmission.

Any system for transferring and storing digital evidence must effectively address all the potential phases of delivering digital evidence to the court:

1. Attorneys for each side may have digital evidence to present.
2. Attorneys may introduce digital evidence to the court that is not yet admitted.
3. Digital evidence may be introduced and admitted into evidence.
4. Digital evidence must be retained in case of an appeal.

Any system should ensure that access to digital evidence is restricted at each stage of the process even if evidence is preloaded into the system for expediency during the trial.

Recommendations

- Establish protocols that ensure that digital evidence is not tampered with, including providing security and an audit trail.
- Ensure that any out-sourced storage or transmission of digital evidence is controlled to limit tampering with the evidence.
- Design systems to accommodate digital evidence at each phase of the process and to ensure expediency in the delivery of evidence to the court.

Readiness

Readiness is a multi-dimensional concept that includes the state of the technical infrastructure, the process for receiving digital video evidence, and how such evidence is played, stored, retained, and accessed. It is likely that each court has a different level of readiness to handle digital evidence.

Some differences in approach to the handling of digital video evidence reflects choices about business models rather than the general readiness of the court. For example, courts might decide between on-site and cloud storage models. The ability to handle streaming video may be both a business and maturity dimension.

Courts at a very basic level of readiness might receive digital evidence on physical media and handle it in the same way as physical evidence. Courts with a more advanced state of readiness might have some digital evidence infrastructure and capability. A very advanced court might be capable of supporting streaming video, storing digital evidence in the cloud, and managing comprehensive enterprise policies for handling digital evidence.

Recommendations

- Assess readiness to migrate to an electronic digital evidence environment and proceed in the areas where improvements can be successfully implemented.
- Consider seeking an objective assessment by another group familiar with needs and requirements for managing digital evidence.

Access

While the issue of access to paper court records is long-ago settled, courts are now struggling with the issue of providing access to electronic information.[18] This issue is only heightened by the introduction of digital evidence that may invoke significant public

[18] Conference of State Court Administrators. *Concept Paper on Access to Court Records*. (August 2000); CCJ/COSCA Resolution 33: Endorsing and Supporting Public Access to Court Records – Guidelines for Policy Development by State Courts. Web. January 28, 2016.

interest to the digital record. By definition, courts will only have digital evidence for actual court cases. Further, virtually all current court policies on access to court records do not explicitly consider multimedia formats.

If digital evidence is treated like traditional exhibits, it may be permissible to handle it according to existing policies for management of exhibits in general. Some current court records access policies do not explicitly mention exhibits at all.

Courts may also need to consider whether digital evidence introduced into the court record becomes subject to open records statutes and/or rules. Law enforcement and prosecutors often have protections from open records provisions if the case is still in the investigative or pre-filing phase. However, most court records are deemed open to the public as part of the open courts doctrine. If the digital evidence introduced into the court record is determined to be subject to open records or open courts provisions, courts should evaluate the impact on releasing that information to the public, and how that is to happen. No matter where video is stored, if there is significant public interest, the servers storing the video may be overwhelmed by requests, potentially slowing and disrupting business processes and cases.

Recommendations

- Evaluate how to categorize digital evidence introduced to the court record as either a court filing or an exhibit.
- Determine if current public access policies or open records provisions for records and exhibits require modification in light of digital evidence.
- Consider how the public will access digital evidence. (See Infrastructure.)

Privacy

While courts have long struggled with the issue of expectations of privacy in other areas, digital video evidence raises new concerns. Digital video regularly captures video of individuals and their property that are not a party to the case at hand. Consider a drug transaction captured on video outside of a convenience store that also contains footage of a family with children in a van outside of the store. Modern facial recognition technology makes it relatively easy to identify such people who in the past might remain anonymous.

While individuals in a public place will not necessarily have an expectation of privacy, many may feel being included as a bystander in video evidence violates cultural expectations of reasonable anonymity. This issue is heightened based on the availability of digital video evidence to the public.

Law enforcement groups have worked with relevant interest and pressure groups to formulate model policies around this issue.[19] In most cases, the solution to privacy concerns takes the form of redacting or blurring out the faces of bystanders and license plates prior to the video being entered into evidence (while maintaining the original video for analysis purposes). If this is a law enforcement routine before digital video evidence gets to the court, then it may not be an issue for the court at all. However, digital video evidence may be introduced by bystanders that may not include this type of redaction. Local practices will determine if a court needs to establish a court rule or policy to deal with it. A state statute would accomplish the same goal of policy clarity for a larger group of courts.

It should be noted that a strict redaction policy can lead to an exponentially increasing workload. While there are numerous tools available to perform redaction, the time and effort it takes to properly review and redact video may be time and cost prohibitive.

Recommendations

- Determine if law enforcement and/or prosecutors have policies concerning redaction in digital video evidence, and if not, explore whether rule, policy or statutory changes are necessary to protect privacy interests.
- Consider how to handle digital video evidence introduced by non-law enforcement bystanders that may not be redacted upon submission to the court.

Vendor Management

The vendor community supporting digital evidence is already robust. Many vendors already work with law enforcement to manage digital video evidence. Courts may be particularly interested in companies that offer cloud storage and streaming services. These types of services are rapidly evolving and courts have an opportunity to influence that evolution.

Ensure vendor contracts take into account security, auditing provisions, ownership of evidence, access, and other issues.[20] Because courts have little experience contracting with video editing and production companies, there is a need to establish model policies and contracts to guide courts during procurements. Law enforcement associations are

[19] Miller, L., Toliver, J., and Police Executive Research Forum. 2014. *Implementing a Body-Worn Camera Program: Recommendations and Lessons Learned*. Washington, DC: Office of Community Oriented Policing Services.

[20] For a discussion of some of the issue, see Sallee, Vern. "Outsourcing the Evidence Room: Moving Digital Evidence to the Cloud." *The Police Chief - The Professional Voice of Law Enforcement*. International Association of Chiefs of Police, Feb. 2016. Web. 11 Feb. 2016.

somewhat ahead of the courts in this area due to the proliferation of video from body-worn cameras. Courts may usefully start with resources developed for law enforcement.

Recommendations

- Carefully consider and craft contracts with outside industry to ensure that digital evidence is protected.
- Retain legal services familiar with technology licensing and contracts. Because courts don't often handle such contracts, vendors have a great advantage.

Expectations Management

Most courts have fairly significant financial limitations and may not be in a position to immediately invest in new technology or technical capabilities. Courts must assess the return on investment (ROI) before making major investments in new capabilities for handling digital evidence. The results of these assessments must be communicated to stakeholders and the public in a compelling way that explain the rationale for the direction the court is pursuing. Including stakeholders in the decision-making process will help ensure buy-in for those decisions and help set appropriate expectations for the use of digital evidence.

ROI estimates should be based primarily on objective considerations but need not be restricted to hard cost savings. Courts must also consider more subjective issues including public perceptions of court competence for implementing and managing technology. A "CSI" effect may particularly influence what the public expects. Effectively communicating technology options and budget limitations can help manage public expectations about what courts can reasonably do.

Courts may also struggle to manage the expectations of judges and other courtroom stakeholders. Given sufficient funding, courts can likely build a system that will meet high expectations from judges and other stakeholders. However, a high-cost/high-feature solution may conflict with the ROI analysis, which may point to a lower but acceptable standard. For instance, courts may choose to limit bandwidth for cost reasons, resulting in slower uploads or downloads of digital evidence. Ensure that judges and other stakeholders understand and support ROI-based decisions.

Consider whether new technology capabilities improve or change the legal process for cases in any substantive way. In well-equipped courtrooms with projectors, juror/witness presentation screens, and other media presentation devices, the use of digital video evidence may work well and meet expectations for the presentation of fair and objective evidence. In less well-equipped courtrooms, attempts to do so may result in disruption and badly presented evidence.

Another practical consideration is the variety of digital evidence that may be introduced. Allowing the introduction of video from personal dash-cams, cell phones, and other sources for a routine traffic stop may slow court efficiencies and proceedings if not properly managed.

Recommendations

- Assess ROI using accepted cost/benefit methodologies before making major investments in new capabilities for handling digital evidence.
- Work with judges and other courtroom stakeholders to communicate decisions that may impact performance in an effort to manage expectations.
- Consider and implement reasonable digital evidence guidance and/or rules.

Conclusions and Recommended Actions

Digital evidence is a rapidly growing phenomenon and courts have little experience or capacity for dealing with it. Further, it is unclear to what extent digital evidence, especially digital video evidence, will pose operational problems since estimates of volume are only speculative.

Given this state of uncertainty, courts should focus their digital evidence planning efforts on three key initiatives:

1. Beginning relevant multi-stakeholder policy discussions.
2. Developing pilot projects at courts of various sizes and with a variety of infrastructures to gather critical information about the issue.
3. Creating a roadmap of policies and procedures for handling digital evidence in the court's unique electronic environment.