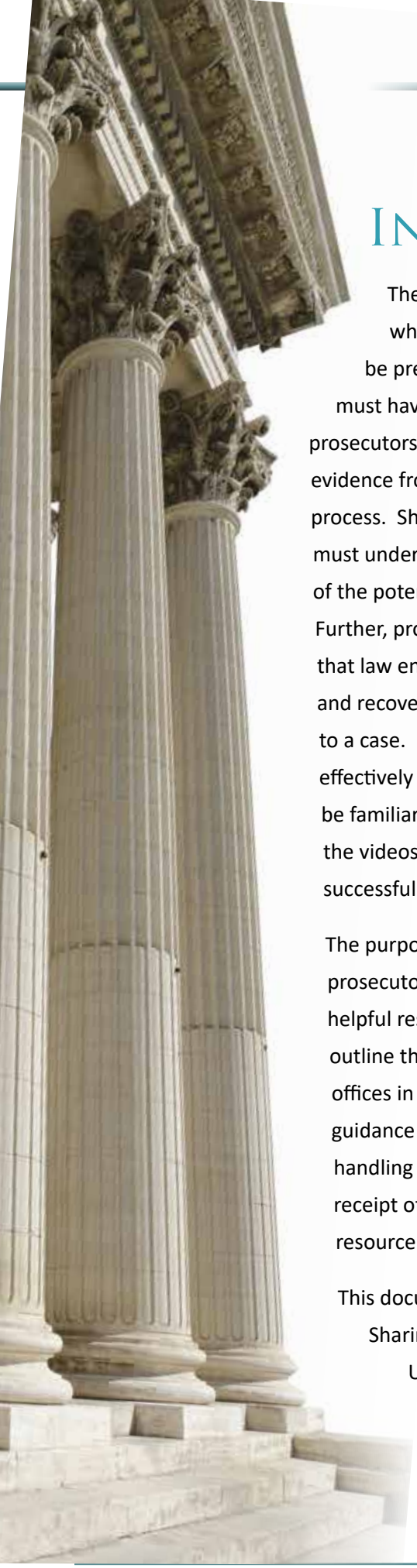
Bureau of Justice Assistance
U.S. Department of Justice

Global Justice Information Sharing Initiative

Video Evidence

A Primer for Prosecutors

Even ten years ago, it was rare for a court case to feature video evidence, besides a defendant's statement. Today, with the increasing use of security cameras by businesses and homeowners, patrol-car dashboard and body-worn cameras by law enforcement, and smartphones and tablet cameras by the general public, it is becoming unusual to see a court case that does not include video evidence. In fact, some estimate that video evidence is involved in about 80 percent of crimes.[1] Not surprisingly, this staggering abundance of video brings with it both opportunities and challenges. Two such challenges are dealing with the wide variety of video formats, each with its own proprietary characteristics and requirements, and handling the large file sizes of video evidence. Given these obstacles, the transfer, storage, redaction, disclosure, and preparation of video evidence for evidentiary purposes can stretch the personnel and equipment resources of even the best-funded prosecutor's office. This primer provides guidance for managing video evidence in the office and suggests steps to take to ensure that this evidence is admissible in court.



Introduction

The opportunities inherent in video evidence cannot be overlooked. It is prosecutors who are charged with presenting evidence to a jury. Today, juries expect video to be presented to them in every case, whether it exists or not.[2] As a result, prosecutors must have the resources and technological skill to seamlessly present it in court. Ideally, prosecutors' offices could form specially trained litigation support units, which manage all video evidence from the beginning of the criminal process through trial preparation and the appellate process. Short of that, individual trial attorneys must understand the opportunities and be aware of the potential pitfalls inherent in video evidence. Further, prosecutors must be diligent to ensure that law enforcement investigators have identified and recovered all existing video evidence relevant to a case. In any event, to use video evidence effectively in the courtroom, prosecutors must be familiar with evidentiary foundations to admit the videos and the technological requirements to successfully display those videos to the jury.

To use video evidence effectively in the courtroom, prosecutors must be familiar with evidentiary foundations to admit the videos and the technological requirements to successfully display those videos to the jury.

The purpose of this resource is to provide prosecutors educational material, introduce helpful resources regarding video evidence, outline the benefits of its use in court, and acknowledge the challenges faced by prosecutors' offices in handling video evidence. A sample process flow is also provided as step-by-step guidance on the general procedures and processes prosecutors may follow when preparing and handling video evidence. It has been designed to correspond to the typical flow of a case from receipt of evidence through the trial process. Finally, a glossary of terms used throughout this resource is included, as well as a list of recommended resources for further reading.

This document was a collaborative effort executed through the Global Justice Information Sharing Initiative (Global), which is supported by BJA, Office of Justice Programs, U.S. Department of Justice. Global acknowledges that this document does not address all subject areas of this complex topic but rather provides a high-level understanding of video-evidence processes to help guide prosecutors.

Benefits & Challenges

Video evidence can come from numerous sources, with both benefits and challenges.




Examples
of Video-Evidence Sources

The following are examples of sources of video evidence from which video may be recorded or recovered.

- Security cameras/digital video recorders (DVRs) at government buildings, businesses, or private homes
- Traffic and toll-booth cameras
- Red-light cameras
- License plate readers
- Video/audio recording technology triggered by gunshots
- Patrol-car cameras
- Body-worn cameras (BWCs)[3]
- Law enforcement interviews of witnesses and suspects at police stations
- Social media providers (pursuant to search warrants) and/or screen captures made by law enforcement
- Forensic searches from digital devices (e.g., computer, phone, tablet), pursuant to search warrants

Benefits
of Using Video Evidence

It is important to note that while video evidence may be only one piece of evidence in a case, it can be extremely powerful. The following are examples of the power of using video evidence in presenting a case to the jury.

- Incorporate into opening and closing arguments (e.g., showing the jury critical parts of the defendant's recorded confession)
- Incorporate clips into a slideshow presentation or trial presentation software
- Capture and print stills for use as supplemental exhibits
- Potential for the in-court identification of the defendant as the perpetrator
- Captures the identified defendant in the act of committing the crime
- May corroborate eyewitness testimony
- May be used to impeach defense witness testimony

Challenges
for Prosecutors Using Video Evidence

The resource challenges documented below do not come close to the degree of impact that the volume of video from body-worn cameras will have on prosecutor office resources, once BWCs are widely adopted across the United States.[4] Aside from these impending challenges, video evidence is subject to a host of other procedures and challenges that differ from other types of evidence. These include the following:

- Having the proper video players and codecs installed on the prosecutor's computer
- Having enough time and resources to review video, often within severe court-imposed charging time constraints (e.g., 24 to 48 hours) for in-custody suspects
- Obtaining and affording adequate storage for the video in the prosecutor's office
- Developing processes and protocols for the storage of video in the prosecutor's office
- Redacting video for privacy and legal challenges
- Allocating sufficient time for discovery, a time-sensitive and time-consuming process involving redaction, rendering, and creating copies of all discoverable video evidence
- The cost of equipment and software to review, process, prepare, and share video evidence
- Ensuring that personnel have the technical and legal training to comply with constitutional disclosure requirements, the National District Attorneys Association (NDAA) Rules of Conduct, National Prosecution Standards,[5] and all other relevant law

- If a video is edited, it must go through a rendering process. The current state-of-the-art, high-end video rendering equipment and software can cost in excess of $100,000. Video rendering can be accomplished with desktop computers, but at a much slower rate.

  Example: A prosecutor may have an eight-hour homicide video interview that the court has ordered to be redacted to eliminate polygraph references. This can be accomplished by using video-evidence software or screen-capture software. Both processes require rendering. Using a standard desktop, an eight-hour video may take eight hours or longer to render.

- Responding to novel legal challenges related to the use of video evidence
- Preserving video evidence for appeal

As discussed in this section, video evidence can come from a host of sources. It can be both beneficial to a case as well as challenging for prosecutors. The following section will help prosecutors address these challenges and will provide guidance on the video-evidence process.

Crime Scene to Courtroom

Video-Evidence Process

This section provides specific guidance on the procedures prosecutors follow and the processes they employ for the receipt, handling, and use of video evidence, whether that evidence is recovered by law enforcement, by prosecutors' offices directly, or by private citizens who then turn it over to the prosecutor. Regardless of how the evidence is received by prosecutors, the following information should be helpful.

Video-Evidence Receipt

There are two main methods of transfer of video evidence from law enforcement to the prosecutor's office:

- **Cloud Transfer—**One method for video transfer is utilizing a government-approved secure cloud provider. To the extent that law enforcement agencies turn to cloud storage for retaining video evidence, they should avail themselves of the cloud's ability to efficiently transfer video-evidence files to a prosecutor. Some cloud solutions also provide remote viewing for prosecutors that does not require physically moving the video-evidence files. In addition, cloud functionality can allow for online redaction, audit trails, and digital transfer of discovery to the defense attorney. For more information on cloud technology, refer to the Global *Public Safety Primer on Cloud Technology*[6]—a high-level primer for law enforcement and public safety communities regarding video evidence and the cloud. Developed as a frequently-asked-question (FAQ) guide, the primer answers straightforward questions about cloud technology and includes guidance for agencies considering cloud vendor contracts. More important, this resource provides critical information on privacy, security, and data ownership, as well as a glossary of cloud terminology and a list of recommended resources.

  Agencies may also be interested to learn about the Federal Risk and Authorization Management Program (FedRamp)[7]—a government-wide program that streamlines federal agencies' ability to make use of cloud vendor platforms and offerings and introduces an innovative policy approach to developing trusted relationships between federal agencies and cloud vendors. While FedRamp requirements are mandatory for federal agencies using the cloud, the standards and list of FedRamp-compliant cloud vendors may be of interest to public safety agencies. FedRamp requires that cloud vendors who want to secure federal data in the cloud undergo security assessments to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA)[8] and with the National Institute of Standards and Technology's (NIST's) Security and Privacy Controls for Federal Information Systems and Organizations (NIST 800-53).[9] For more information on FedRamp, refer to www.fedramp.gov. To view FedRamp-compliant vendors, refer to www.fedramp.gov/marketplace/compliant-systems/.

- **Physical Transfer—**Another method for law enforcement agencies to turn over video files to a prosecutor is physical transfer via discs, flash drives, SD cards, portable hard drives, etc., or by providing a link to files or including in an e-mail attachment.

It should be noted that in most cases, video evidence is collected from some type of DVR; however, there are exceptions, such as video evidence collected from smartphones and social media. This resource, however, addresses how a prosecutor receives video evidence that law enforcement collects, regardless of its source, format, or quality.

Law enforcement agencies should provide prosecutors with two complete copies of the video evidence. The first copy should contain the video in its original format as recovered (with the proprietary video-player software included). The second copy should contain the video in a playable nonproprietary format (e.g., MP4, WMV, AVI, MPEG).

Note: Some DVRs/devices can export video files to an MP4 format[10] with the metadata all in one file. These files can play in the proprietary media player with the metadata displayed, as well as in a standard media player with just the video and sound. This is a recommended format.

Privacy Redaction

Prosecutors' offices will need to develop their own individual policy regarding the privacy redaction of video when it is shared for discovery and/or Freedom of Information Act (FOIA) purposes. In some jurisdictions, police departments make the initial privacy redaction on the discovery copy of the video and then it is reviewed by the prosecutor's office prior to release by the defense. In other jurisdictions, the prosecutor's office prepares and redacts all video prior to release for discovery to the defense. In some cases, videos cannot be redacted prior to release for discovery, and protective orders may be necessary.

Video-Evidence Preparation

Whatever process a prosecutor uses to prepare and render video for trial, the process should be transparent to the court and, when requested, to the defense. The following is an example of a video-evidence preparation process from a prosecutor's perspective—from receipt of the video to post-trial. It represents a scenario in which evidence is first received by the prosecutor's office on disc, flash drive, or portable hard drive. This sample process flow is provided as step-by-step guidance on the general procedures and processes prosecutors may follow when preparing and handling video evidence.

Pre-Trial

- Store and back up video files (e.g., video discs), including images of any physical writing or labeling on the outside of the discs,[11] consistent with the prosecutor's case management process, policies, and available resources.
- Review received files to determine whether additional privacy redactions and/or witness safety concern redactions are needed.
- Provide a copy of the redacted video files to defense counsel, pursuant to local discovery rules and practices.
- As needed for presentation in court, prosecutors should be able to obtain from law enforcement a copy of the unredacted original video file in a nonproprietary format (e.g., MP4, WMV, AVI, MPEG). It is recommended that prosecutors and law enforcement consult on what video format(s) work best for use in court. If a prosecutor chooses to accept only the proprietary format from law enforcement, he or she may have to use the provided proprietary software, when available, or download the player from the manufacturer to export the video to a nonproprietary format. Prosecutors also could use screen-capture software to render a copy of the video in a nonproprietary format, assuming the prosecutor is able to fully authenticate the video.
- The nonproprietary video can then be redacted, as needed, for considerations of relevance, prejudice,[12] and trial strategy.
- Before trial, create a CD or a DVD of the video to be marked and admitted as an exhibit to be authenticated by the witness(es).
    a. Tip: Computers often freeze when playing videos from disc drives. It is recommended that video files be copied from the exhibit disc onto the hard drive of the computer that will be used in the courtroom for playback to allow for seamless playback during court.

Advanced Video Use Tips

Prosecutors may consider using slideshow or trial presentation software to present video evidence in court. It allows for case organization, seamless presentation, and flexibility on direct examination and cross-examination.

1. Depending on the needs or strategy of the case, a prosecutor may want to have the audio portions of any video transcribed for use as exhibits in court. Current litigation software allows video files to be synchronized to transcripts for simultaneous viewing in court. It is important to note that this process can be time-consuming and expensive.
2. Prosecutors may wish to identify clips for use in opening, direct, cross, and closing statements with slideshow software and/or trial presentation software. If necessary, individual clips can be created with nonproprietary video software or with screen-capture software. These clips are made from video files that have already been provided to the defense counsel. Prosecutors may consider creating a disc of clips to admit as a separate exhibit with defense stipulation; however, this is not required, since in most cases the original disc was already admitted for the record.

Trial Tip

An eyewitness to the material on the video may answer questions about events shown in the video as it is played for the jury or shortly after it is played, depending on the jurisdiction. In addition, a witness who has some specialized knowledge about the video or the events depicted therein that is helpful to the jury in understanding the video may testify about that knowledge. For example, a person familiar with a subject in the video may identify that person, or an officer who has viewed the video multiple times or in slow motion may point out items in the video that might not be apparent on full-speed initial view. However, neither the prosecutor nor any witness can give an opinion about what the video shows that does not rest on special knowledge that the jury does not have. Doing this invades the province of the jury and is improper.

b. Tip: Avoid using adhesive labels on discs (e.g., evidence stickers) to prevent adverse effects on playback and damage to the data contained on the disc. The label should be placed, instead, on the envelope or CD case. However, it is advisable to write the case number or other identifier in permanent marker on the top of the CD as the data is on the bottom and is unaffected by the writing on top. This will be helpful if the CD becomes separated from the CD sleeve/case.

- In some cases, one may wish to capture individual frames (i.e., still images) from the video that can be marked as separate exhibits and used in court. Be sure to provide copies of these to the defense. Whatever process is used to create the still images should be disclosed and placed on the record.
- If any enhancement[13] of the video and/or still images is required, this should be completed only by a qualified expert witness, not the prosecutor.
- Test video playback of all files on the actual device that will be used to play them in court before introducing them into evidence.

Trial

- For video files to be introduced into evidence, they must be authenticated. This can occur when an eyewitness with knowledge testifies that the video file is a fair and accurate representation[14] of what transpired, or when no eyewitness is available to testify, the "silent witness theory" can apply.[15] If introducing video evidence under this theory and absent a stipulation, it is a good practice for a prosecutor to prepare to call, if necessary, a witness who can testify to the operation of the device that recorded the video, the witness who recovered the video and placed it on evidence, any witness with knowledge, and/or any other relevant chain-of-custody witnesses.[16]
- It is critical for prosecutors' offices to maintain technologically current equipment for the display of video evidence in court.
- At trial, if a prosecutor chooses to play clips of a video, those clips must be from a video file that is already admitted as evidence (see Advanced Video Use Tips).
- During a trial, if less than the full video is played, the record must reflect what portion of the video (time sequence or transcript reference) is being played for the jury.
- It is important to ensure that all of the jury can see and hear the video while it is being played.
- Jury deliberation: Requests by the jury for playbacks of video evidence are common. One common practice is to bring the jury back to the courtroom for any requested playbacks during deliberations. If the court orders that the jury have access to the video in the jury room, a prosecutor should ensure that any laptop or playback device (1) has no other files on it other than the software required to run the video, (2) cannot be connected to the Internet, and (3) has been inspected by defense counsel, who has confirmed this inspection on the record.

Post-Trial

- It is a good practice for the prosecutor's office to maintain a copy of all digital exhibits shown to the jury. Responsibility for maintaining trial exhibits will vary by jurisdiction.

Litigation Technology Units and Training

Given the increasing volume of video evidence prosecutors are faced with on a daily basis, prosecutors' offices should consider establishing litigation technology units (LTUs) to support the prosecutor's preparation and use of video evidence at trial. A typical LTU should be supervised by a technically savvy attorney with trial experience. Qualified retired law enforcement investigators, legal interns, and clerical staff are examples of personnel who could make up the technicians in such a unit.

Prosecutors' offices should pursue training on trial presentation software, slideshow software, video/audio editing software, trial advocacy, and courtroom technology.

Conclusion

The growing amount of video now available from security cameras, patrol-car dashboard and body-worn cameras, and smart devices is creating a significant strain on budgets and resources across the justice domain. While the availability of video evidence can present opportunities for prosecutors who are charged with presenting evidence to a jury, the complex process of transferring, storing, redacting, disclosing, and preparing video evidence for evidentiary purposes is having a considerable impact on prosecutors' offices. With video evidence estimated to be involved in approximately 80 percent of crimes, prosecutors must have the resources and technological skill to seamlessly and effectively present video evidence in court. To do this, they must have a clear understanding of both the benefits and challenges of video evidence and, more important, the solutions and techniques to address them. This primer provides general guidance on the procedures and processes prosecutors may follow, from pre- to post-trial, when preparing and handling video evidence.

Terms

Original file—A file that is continuous and free from unexplained alterations (e.g., additions, deletions, edits, or artifacts) and is consistent with the stated operation of the recording device used to make it. However, Federal Rules of Evidence (FRE) 1001(d) defines an original of a writing or recording as "the writing or recording itself or any counterpart intended to have the same effect by the person who executed or issued it. For electronically stored information, 'original' means any printout—or other output readable by sight—if it accurately reflects the information."[17] Further, "if data [is] stored [on] a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" *Lorraine v. Markel Am Ins Co*, 241 FRD 534, 577 (D Md 2007). FRE 1001(e) states that a duplicate is "a counterpart produced by a mechanical, photographic, chemical, electronic, or other equivalent process or technique that accurately reproduces the original."

Proprietary video—A video file format that is unique to a specific manufacturer or product that contains data that is ordered and stored according to a particular encoding scheme, designed by the company or organization to be secret, such that the decoding and interpretation of this stored data is easily accomplished *only* with particular software or hardware that the company itself has developed. A *proprietary format* also can be a file format whose encoding is in fact published but is restricted (through licenses) such that only the company itself or licensees may use it. It is important to note that not all proprietary software exports the proprietary players with the video files. If a law enforcement agency chooses to use a proprietary format, it is a best practice for prosecutor offices to encourage the law enforcement agency to use only proprietary software players that have the ability to export video into a nonproprietary format.

Nonproprietary video—A video format that is not encumbered by any copyrights, patents, trademarks, or other restrictions so that anyone may use it at no monetary cost for any desired purpose.

Screen-capture software—Software that can capture screenshots of images and videos and save them as graphic files or record a computer screen and save the recordings as video files.

Rendering—The process by which video software and hardware convert video from one format to another.

Codec—A computer algorithm that controls the compression/decompression and/or encoding/decoding of audio and video files. A codec encodes a data stream or signal for transmission, storage, or encryption or decodes it for playback or editing. It is possible for multiple file formats to utilize multiple codecs. If a video file will not play, many times the problem has to do with not having the correct codecs—a computer program that both shrinks large movie files and makes them playable on computers. In some cases, computers try to automatically download a codec from the Web, but this may be blocked based on connectivity or security settings (for example, some viruses are concealed in codecs). Prior to playing a video, seek the help of IT personnel to get the proper codec installed.

Recommended Resources

This list of resources provides a starting point for prosecutors wanting to learn more about video-evidence processes.

- Video Players, CNET offers links to many of the video players/codecs needed to play video, such as VideoLAN Client (VLC), Gretech Online Movie (GOM) players, and more, http://download.cnet.com/s/video-players/.
- Comparison of Video Player Software, Wikipedia, https://en.wikipedia.org/wiki/Comparison_of_video_player_software.
- Producing Camtasia Videos for Local Playback, https://www.youtube.com/embed/IM8XxDsOjks?vq=hd1080. This video contains useful tips on export settings to use for rendering in general.
- "5 Tips for Using Mobile Video Evidence in Your Agency," PoliceOne.com, April 10, 2014, Panasonic System Communications Company of North America, www.policeone.com/police-products/police-technology/mobile-data/articles/7067437-5-tips-for-using-mobile-video-evidence-in-your-agency/.
- "A Simplified Guide to Forensic Audio and Video Analysis," National Forensic Science Technology Center, Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice (DOJ), www.forensicsciencesimplified.org/av/AudioVideo.pdf.
- "A Simplified Guide to Forensic Evidence Admissibility and Expert Witnesses," National Forensic Science Technology Center, Bureau of Justice Assistance (BJA), Office of Justice Programs, DOJ, http://www.forensicsciencesimplified.org/legal/index.htm.
- "Admissibility of Electronic Evidence: A New Evidentiary Frontier," the Honorable Alan Pendleton, *Bench & Bar of Minnesota*, Minnesota State Bar Association, October 14, 2013, http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/. — While not a video-evidence-focused article, the "Analytical Framework" for the admissibility of electronic evidence may be useful.
- "Addressing Video Evidence at Trial," Doug Wyllie, Senior Editor, PoliceOne.com, June 24, 2008, www.policeone.com/police-products/investigation/tips/1706936-Addressing-video-evidence-at-trial/.
- "Best Practices for Image Authentication, Forensic Science Communications," April 2008, Volume 10, Number 2, FBI's Scientific Working Group on Imaging Technologies (SWGIT), www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2008/index.htm/standards/2008_04_standards02.htm.
- "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors," National Institute of Justice (NIJ), DOJ, January 2007, www.ncjrs.gov/pdffiles1/nij/211314.pdf. This guide focuses primarily on digital computer evidence but is useful in guiding prosecutors through the process of acquisition, integrity, discovery, courtroom preparation and evidence rules, and the presentation of digital computer evidence.
- "Forensic Imaging and Multi-Media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), and Forensic Video (FV)," Version 7.0, Last Updated July 15, 2006, Law Enforcement and Emergency Services Video Association (LEVA), www.leva.org/pdfs/GlossaryV7.pdf.
- "Guidelines for Facial Comparison Methods," Facial Identification Scientific Working Group (FISWG), February 2, 2012, www.fiswg.org/document/viewDocument?id=25.
- "How to Play a DPD Confession Video," Prosecutor Kym L. Worthy, Wayne County Prosecutors Office, Michigan. This is an example of a guide made to assist defense attorneys with playing proprietary police video files received during discovery. https://www.linkedin.com/pulse/sample-how-instructions-playing-proprietary-video-file-patrick-muscat?published=t.
- Law Enforcement and Emergency Services Video Association (LEVA), www.leva.org.
- Statewide/Centralized Evidence Laboratories, National Clearinghouse for Science, Technology and the Law, http://www.ncstl.org/resources/laboratories.
- *Using and Presenting Digital Evidence in the Courtroom: Training Material* (CD-ROM), NIJ, DOJ, 2008, www.nij.gov/publications/pages/publication-detail.aspx?ncjnumber=215094. —This CD-ROM is an interactive training program on using and presenting digital evidence in a courtroom setting.

Endnotes

1 Dale Garrison, "Advanced Video Forensics," *Evidence Technology Magazine*, July–August 2014 Issue, www.evidencemagazine.com/index.php?option=com_content&task=view&id=1688&Itemid=49.

2 Ibid.

3 "Body-Worn Camera Toolkit," Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, https://www.bja.gov/bwc/.

4 Kay Chopard Cohen, "The Impact of Body-Worn Cameras on a Prosecutor," National District Attorneys Association, http://ndaajustice.org/pdf/BWC_Blog_Post_Draft_09%2002%202015_FINAL.pdf.

5 *National Prosecution Standards*, Third Edition, Rules of Conduct, Section 1–1.4, National District Attorneys Association, http://www.ndaajustice.org/pdf/NDAA%20NPS%203rd%20Ed.%20w%20Revised%20Commentary.pdf.

6 *Public Safety Primer on Cloud Technology*, Global Justice Information Sharing Initiative, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, May 2016.

7 The Federal Risk and Authorization Management Program (FedRamp) is a government-wide program that streamlines federal agencies' ability to make use of cloud services and introduces an innovative policy approach to developing trusted relationships between federal agencies and cloud vendors. FedRamp provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services that secure federal data, www.fedramp.gov.

8 The Federal Information Security Management Act of 2002 requires each federal agency to develop, document, and implement an agencywide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

9 *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, Special Publication 800-53A, Revision 4, National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

10 MP4 in PowerPoint, FAASOFT, June 12, 2014, www.faasoft.com/articles/mp4-in-powerpoint.html.

11 In some jurisdictions, it is required to provide the defense with a copy of any writing or labeling on the outside of the disc.

12 *People v. Musser*, 835 N.W.2d 337 (Michigan Supreme Court, 2013).

13 *Forensic Imaging and Multi-Media Glossary Covering Computer Evidence Recovery (CER), Forensic Audio (FA), Forensic Photography (FP), and Forensic Video (FV)*, Version 7.0, Last Updated July 15, 2006, LEVA, www.leva.org/pdfs/GlossaryV7.pdf.

14 Authenticating or Identifying Evidence, Federal Rules of Evidence (FRE), Rule 901, http://federalevidence.com/rules-of-evidence#Rule901.

15 The silent witness theory is a theory in the law of evidence whereby photographic evidence (as photographs or videotapes) produced by a process whose reliability is established may be admitted as substantive evidence of what it depicts without the need for an eyewitness to verify the accuracy of its depiction. In *People of Illinois v. Taylor*, 956 N.E.2d 431, 353 ILL. Dec. 569 (2011), surveillance video of the defendant committing the crime was captured on a digital medium and transferred to a VHS tape for trial. The defense continually objected on foundational grounds, arguing that it had not been shown that the camera worked properly. The Illinois Court of Appeals, after discussing the silent witness theory, found that the tape was inadmissible based on issues demonstrating chain of custody, confirming the camera worked properly, ensuring the original digital recording was preserved, and concerns regarding the method used to transfer the video from digital to VHS format. While the Illinois Supreme Court agreed with the issues the Court of Appeals examined, it disagreed with its analysis and found adequate support for each foundational factor within the trial record and under Illinois law. The tape was ultimately admitted and the defendant's conviction affirmed. Chain-of-custody issues in establishing foundation generally go to weight, not admissibility.

16 Chain-of-custody issues in establishing foundation generally go to weight, not admissibility.

17 Federal Rules of Evidence 1001(d), https://www.law.cornell.edu/rules/fre/rule_1001.

About Global

The Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) serves as a Federal Advisory Committee to the U.S. Attorney General. Through recommendations to the Bureau of Justice Assistance (BJA), the GAC supports standards-based electronic information exchanges that provide justice and public safety communities with timely, accurate, complete, and accessible information, appropriately shared in a secure and trusted environment.

GAC recommendations support the mission of the U.S. Department of Justice, initiatives sponsored by BJA, and related activities sponsored by BJA's Global. BJA engages GAC-member organizations and the constituents they serve through collaborative efforts to help address critical justice information sharing issues for the benefit of practitioners in the field.

IT.OJP.GOV/Global

Acknowledgements

A special thank-you to Global's prosecutor drafting team for their valuable contributions in authoring and guiding the development of this resource.

Kay Chopard Cohen
National District Attorneys Association

David McCreedy
Appellate Section
Wayne County Prosecutor's Office, Michigan

John Wolfstaetter
Courtroom Technology
New York County District Attorney's Office, New York

Patrick Muscat
Violent Crime Unit
Wayne County Prosecutor's Office, Michigan

Mark Shlifka
Continuing Legal Education and Trial Technology
Cook County State's Attorney's Office, Illinois

Appreciation is also shared for the following individuals and organizations who contributed to the development and vetting of this resource.

Kevin Bowling
20th Circuit Court, Ottawa, Michigan
Representing the National Association for Court Management

Kristine Hamann
Bureau of Justice Assistance
U.S. Department of Justice

The Honorable William J. Ihlenfeld, II
United States Attorney's Office, Northern District of West Virginia
Representing the Executive Office for United States Attorneys

David Labahn
Association of Prosecuting Attorneys

Fred Lederer
Center for Legal and Court Technology
William and Mary Law School
Representing the National Center for State Courts

The Honorable Barbara Mack
National Council of Juvenile and Family Court Judges

Mark Perbix
SEARCH, The National Consortium of Justice Information and Statistics

Raj Prasad
Wayne County Prosecutor's Office, Michigan

Sean Smith
New York Prosecutors Training Institute

Christopher A. Toth
National Association for Attorneys General

Members of the Criminal Intelligence Coordinating Council and the National Association for Court Management's Joint Technology Committee who participated in the vetting of this resource.

This project was supported by Grant No. 2014-DB-BX-K004 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, in collaboration with the Global Justice Information Sharing Initiative. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Department of Justice.

Issued 10/2016