

Evidentiary issues relevant to in-car camera system video

As a leading manufacturer of digital in-car camera systems, Integrian is very confident in our products and their on-going use by the law enforcement community; this includes the frequent use of Digital Patroller video as evidence in court. It is imprudent however to offer any guarantee regarding the proceedings of a criminal court even to dispel negative rumors around this subject. We can assure you that as the technical guidelines of in-car camera systems evolve, we are committed to updating and complying with all aspects of in-car camera systems that affect evidentiary value of the video content.

Summary

To the best of our knowledge there is no precedent setting case law which prohibits the submission of in-car camera video as evidence in a court of law. That said, “admissibility or exclusion of video evidence is at the discretion of the trial court”. Therefore, while no guarantee can be made as to the admissibility of video evidence, knowledge of the factors effecting admissibility and the establishment and adherence to policies insures the greatest likelihood that video evidence can be used.

Rules of Evidence

Admissibility of video evidence is judged by the same criteria applied to photographic evidence generally. The presentation of video evidence in a criminal proceeding is based on a number of factors:

- Is the video evidence a “fair and accurate” portrayal of the events?
- What is the foundation for admissibility – can a witness confirm the observed portrayal?
- Is the evidence an illustrative or substantive exhibit?
- Is the video evidence from a so-called “silent witness” [automatic surveillance]?
- Is there testimony available as to the equipment, its correct operation, and the handling of the media (Chain of Custody)?

Your Municipal, State or Federal District Attorney’s office is the best resource to consult regarding the relevant Federal or State Rules of Evidence.

Additionally, a good reference is “Modern Visual Evidence” by Gregory P. Joeseeph, Law Journal Press, 2005. Please see Chapter 5 – Use of Videotape Evidence in Criminal Cases”.

Standards Activity

The International Association of Chiefs of Police (IACP) sponsored by the U.S. Department of Justice, completed an 18-month study in late 2004 on the use and efficacy of in-car camera systems by state and local law enforcement. A copy of the study entitled – “The Impact of Video Evidence on Modern Policing - Research and Best Practices of In-Car Camera Systems” is available at:

<http://www.theiacp.org/documents/pdfs/WhatsNew/IACP%20In%20Car%20Camera%20Report%202004%2Epdf>

This report includes an overview of the evidentiary issues, but does not proffer a definitive conclusion.

Subsequent to the study, the IACP, again with the sponsorship of the DOJ and now with the additional support of the National Institute of Science and Technology (NIST), has undertaken a collaborative law enforcement and industry effort to establish minimum guidelines for in-car camera systems. The effort is broken down into five working groups including – Officer Safety, Video Quality, Data Security. Integrian is represented on all the working groups.

The preliminary report of the minimum guidelines was released by the IACP for public comment this summer [2006] and is expected to be ratified at the annual IACP conference this fall. Integrian fully supports these guidelines and commits its future products to full compliance.

The IACP In-Car Video Camera System Performance Specification program is being lead by Grady Baker.

Contact Info:

Wm. Grady Baker
Program Manager
In-Car Camera Technical Assistance
International Association of Chiefs of Police
515 North Washington Street
Alexandria, VA 22314
(703) 836-6767, ext. 240
(703) 684-5728 (fax)
Email: baker@theiacp.org

The DVS specification is available at:

<http://www.theiacp.org/research/CuttingEdge/DVSSpecificationsFrameworkVersion10-06-13-06.pdf>

On a preliminary basis, the law enforcement community and collaborative industry representatives have not been able to establish or identify an individual technology or product feature which can “guarantee” the evidentiary value of video content from in-car camera systems; however, portions of the IACP guidelines specifically address authentication and the handling / transfer of video files to help insure their viability as evidence.

Anti-Tamper Mechanisms

Much of the concern about the admissibility of video evidence from in-car camera systems can be attributed to the continued improvement and accessibility of digital still cameras and digital video cameras in conjunction with computer based video editing tools for professional and consumers.

It would be ideal if a single technology could be identified and adopted within the industry that could guarantee authenticity such as some form of encryption or watermarking. Unfortunately, the community – law enforcement (including the FBI) and the industry – do not have, nor are they promoting a single open standard for content authentication. Furthermore, no single method for video content authentication has been utilized and subsequently scientifically endorsed by the court through a Frye or Daubert hearing.

Each manufacturer offers some proprietary method to “authenticate” content within their system, but no single manufacturers system or method has been so “blessed” by a court of law. The net result of this is that the law enforcement agency, and associated prosecuting office must rely on the established standards for evidence admissibility as discussed earlier.

However, every law enforcement agency can improve the likelihood of evidentiary value of its in-car camera system by establishing and adhering to its internal guidelines governing the use of such systems.

Guidelines and Policies

First, we have assumed that every law enforcement agency has already established a policy for the handling of evidence in a criminal case and a “chain of custody”. Further, they are assumed to have an IT policy on the access to law enforcement information systems and User IDs and passwords. The use and operation of in-car camera systems will be an extension of these basic policies.

The IACP report mentioned earlier includes a draft policy for in-car camera use and best practices. In addition to the IACP guidelines, The Commission on Accreditation for Law Enforcement Agencies, Inc. (CALEA), has a model policy and recommendation that can be used.

The most important aspect factors are:

- The equipment is consistently installed, operated and maintained.
- The officers using the equipment are trained (periodically).
- Video evidence can be tracked from the vehicle to a back-office storage/management system where access control is maintained with an audit trail.
- A designated evidence technician follows an established guideline for generating video copies (on a read-only medium) as required by the prosecuting and defense attorneys.
- A witness is available to the court that can outline the procedures and document the adherence to said standards.
- A guidelines for the use and operation of the in-car camera is established – ie. what type of activity is recorded, when is it recorded, when is the recording stopped.

DigitalPatroller Data Security Features

In summary the current security features of DigitalPatroller1 which help insure reliable authentic video files are:

- Physically secure device and storage medium in the vehicle (key lock)
- A proprietary device application with no method to erase or overwrite files
- Windows userid and password protection for electronic device access
- File Transfer Protocol with userid and password protection for wired transfer and WPA2 encryption for wired transfer
- Device and server application features which prevent unauthorized transfer between devices and servers not configured within the same system
- A proprietary server application
- Windows userid and password protection for the server within a Windows domain controller
- Windows Server based access control for storage resources
- A proprietary file format and file extension for DP files
- Embedded metadata file tags
- Date and time accuracy corrected by GPS reference
- Redundant in-car file storage with RAID 1 hard disk drives
- Optional in-car UPS